CYBERPATRIOT

AFA's National Youth Cyber Education Program

Program Overview

CyberPatriot is the Air Force Association's National Youth Cyber Education Program, created to motivate students toward careers in cybersecurity and other science, technology, engineering, and mathematics (STEM) disciplines. The program features the National Youth Cyber Defense Competition for high school and middle school students, AFA CyberCamps, an Elementary School Cyber Education Initiative, the Cyber Education Literature Series, and CyberGenerations – the Senior Citizen's Guide to Cyber Safety.

The National Youth Cyber Defense Competition

The national youth cyber defense competition is an online, tournament-structured event in which teams of 2-6 students are scored how well they identify and secure known vulnerabilities on a virtual network. Through a partnership with Cisco, they are also tested on a networking curriculum and are required to build secure, virtual networks.

Students compete in three divisions:

- **Open Division**: Open to all high schools, scouting units, boys and girls clubs, home school programs, and other approved youth organizations
- **All Service High School Division**: JROTC programs / Civil Air Patrol / Naval Sea Cadet Corps
- **Middle School Division:** Open to teams of middle school students

After a series of online qualification rounds, the top teams advance to the National Finals Competition, an in-person event held in Baltimore, Md., each spring. Winners are awarded scholarships, and all registered competitors are eligible to apply for internship opportunities. Not only is the competition fun and exciting, it also creates a career path for today's students, fostering continued education from middle school through college and into the beginning of their careers.

Registration for CyberPatriot XI (2018-2019 school year) is open until October 3, 2018.

AFA CyberCamps

Held during the summer months, AFA CyberCamps emphasize fun, hands-on learning of cybersecurity principles that are relevant and applicable to everyday life. Through this 20-hour, 5-day camp, students will learn the importance of cyber safety and how to protect their personal devices and information from outside threats. Camps are designed for high school or middle school students (at the discretion of the hosting organization).

For more information on AFA CyberCamps, visit the "Special Initiatives" section of www.uscyberpatriot.org.

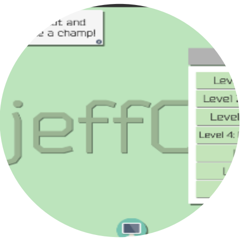
CYBERPATRIOT

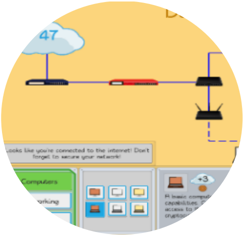
AFA's National Youth Cyber Education Program

Elementary School Cyber Education Initiative

Using game-like computer training software, the Elementary School Cyber Education Initiative is designed to:

- Excite students about education in cybersecurity and other STEM disciplines.
- Help students understand the widespread importance of cybersecurity in their everyday lives and equip them with skills to better protect themselves on the Internet
- Encourage students to apply cyber ethics principles in their online interactions
- FREE downloads available online





Cyber Education Literature Series

The Cyber Education Literature Series introduces cybersecurity principles to our youngest audience in storybook format. The first book in the series *Sarah the Cyber* Hero was published in December of 2017 and is available for purchase through BookBaby.com, Amazon, and Barnes & Noble.

Sarah the Cyber Hero features a female protagonist living in a town full of superheroes. She must earn her superhero cape using the cyber skills she has learned in her school's cyber education program to protect the town from a virus downloaded to a computer.

CyberGenerations

CyberGenerations -- the Senior Citizen's Guide to Cyber Safety -- is designed to encourage and equip more seniors to practice cyber safety. The program covers topics such as password hygiene, malware and ransomware, marketing and fraud scams, and social media awareness. The program also provides resources for individuals who may have been a victim of a cybercrime.

Presented by:

NORTHROP GRUMMAN Foundation

NATIONAL YOUTH CYBER DEFENSE COMPETITION

CyberPatriot – AFA's National Youth Cyber Education Program

Who is on a team?

Coach: The team coach is typically a teacher or adult leader of a team-sponsoring school or youth organization. Coaches need no special technical background. Any individual with the desire to help students learn something new and relevant can be a great CyberPatriot coach!

Competitors: The team roster must have between two and six competitors (five active, one substitute who are registered with the CyberPatriot Program Office and enrolled with the school or organization they are competing with. All cyber teaching materials are provided and no prior cybersecurity knowledge is required for a competitor to be successful.

Technical Mentor (Optional): In cases where a team desires help with the provided online training or with specific topics, the coach may request assistance from the CyberPatriot Program Office in finding qualified technical mentors from our program. Technical mentors are registered volunteers who possess appropriate IT knowledge and skills. Background checks are performed on all technical mentors in our network.

Teams compete in three divisions:

- **Open Division:** High schools, scouting units, boys and girls clubs, home school programs, and other youth organizations upon approval from CyberPatriot Program Office
- **All Service Division:** High school JROTC / Civil Air Patrol / Naval Sea Cadet Corps
- **Middle School Division:** Open to teams of middle school students (typically grades 6-8)

Team registration for CyberPatriot XI (2018-2019) ends on October 3, 2018

What are the technical requirements?

Two to three computers and an Internet connection are required for occasional weekend use during the online portions of the competition. A full list of hardware and software requirements is available on www.uscyberpatriot.org. For teams needing alternate Internet connection, CyberPatriot provides a limited number of AT&T 3G Air Cards on needs/first come-first serve basis.

What does it cost to participate?

There is a $205 registration fee for each high school team and a $165 fee for each middle school team registered for the competition, with the exception of the following fee waiver opportunities:

- **All-Girl teams:** In an effort to attract more girls to STEM, all-female teams may request a fee waiver
- **Title I Schools:** Teams from Title I schools and other schools with inadequate funding may request fee waivers
- **All Service Division:** JROTC/CAP/NSCC team fees are automatically waived (agreement with service HQs)

The fee covers access to the Microsoft Imagine store as well as to Cisco's Networking Academy. These programs allows the team to download a number of operating systems and productivity tools that can be used to prepare for the competition. Additionally, participants are sent a CyberPatriot t-shirt during the season.

NATIONAL YOUTH CYBER DEFENSE COMPETITION

CyberPatriot – AFA's National Youth Cyber Education Program

What training materials are needed?

Although coaches are welcome to supplement the provided teaching materials as they wish, all materials necessary for a successful competition are provided on the CyberPatriot website. Teachers (and other coaches) are encouraged to use the provided materials not solely for use in preparing their team for competition, but also to educate all students in their school or organization about good cybersecurity practices and safe computer and Internet use.

How does the competition work?

The early rounds of the competition are done online during weekends from teams' home locations (schools, homes, libraries, etc.).

Prior to the rounds, teams download "virtual image" representations of operating systems with known cybersecurity "vulnerabilities." At the beginning of the round, a password to unlock the virtual image is sent out. Teams then choose any 6-hour period during the designated round to compete, finding and fixing the cybersecurity vulnerabilities while keeping critical computer functions working. Additionally, students are tested and scored on networking knowledge and building virtual, secure networks. Team progress is recorded by a central CyberPatriot scoring system.

For the Open and All Service divisions, the scores from two online qualification rounds are added together to determine team placement into one of three tiers for the State Round: Platinum, Gold, or Silver. These tiers have cybersecurity challenges of different degrees of complexity, with the Platinum Tier having the highest degree of difficulty and being the only tier where teams have the opportunity to advance to the National Finals competition.

The top 12 Open Division teams and the top two teams from each All Service Division category (Air Force/Army/Marine Corps/Navy JROTC, CAP, NSCC, and one wildcard team) advance, all-expenses paid, to the in-person National Finals Competition held in Baltimore, Md. There, the Finalists compete face-to-face against other teams in their division to defend virtual networks from a professional aggressor team. Winners are awarded scholarship grants.

The competition is slightly different at the middle school level. There are no skill tiers in the Middle School Division, and all teams compete against each other for the full duration of the season. After three qualifying rounds, the top 50% of teams advance to the Semifinals. From there, the top three teams advance to the National Finals Competition.

Presented by:

NORTHROP GRUMMAN Foundation

AFA CYBERCAMPS

CyberPatriot – AFA's National Youth Cyber Education Program

The AFA CyberCamp curriculum is designed to instruct students, both novice and advanced, about cyber ethics, online safety, and the fundamental principles of cybersecurity.

How does an AFA CyberCamp work?

Through the AFA CyberCamp program, schools and educational organizations can purchase a curriculum kit consisting of five, four-hour instruction modules, as well as accompanying instructor guide, student workbooks, demonstration software, and competition software that will teach students important skills in cybersecurity. Local organizations and volunteer instructors can execute the 20-hour curriculum as a week-long summer program supplemented by guest speakers and additional group activities.

The camp's 20-hour curriculum is designed for completion over five days (must be Monday-Friday), with the final day serving as a "miniature cyber competition day."

Topics covered during a camp include:

Standard Camp:

- **Introduction:** Cybersecurity career opportunities, cyber ethics, online safety, how computers work, cyber threats, cybersecurity principles, virtual machines
- **Windows 10:** Basic security policies and tools, account management, file protections, auditing and monitoring **Linux/Ubuntu 16:** Introduction to Linux, Ubuntu 16 terminology and concepts, basic graphical user interface security, basic command line security, intermediate Ubuntu security.

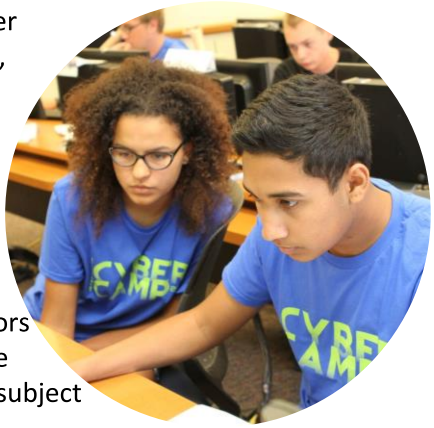
Advanced Camp:

- **Windows 10 Module**: Graphical utilities, command line, optional sysinternals suite
- **Ubuntu 16 Module:** Init systems, advanced command line, processes and scheduled tasks, optional security policies and PAM, optional networking
- **Cisco**: NetAcad Networking

Who can host a camp?

Public/private middle schools and high schools, home schools, universities and other higher education or career technical education institutes, Civil Air Patrol squadrons, Naval Sea Cadet units, scouting units, boys and girls clubs, and other non-profit organizations. AFA CyberCamps cannot be conducted as a for-profit activity. All applying entities are subject to approval by the CyberPatriot National Commissioner.

Host organizations are responsible for providing instructors. Standard camp instructors should have experience working with computers, basic knowledge of cybersecurity, and some familiarity with virtual machines. Advanced camp instructors should be advanced subject matter experts. It is highly desired that instructors have advanced knowledge of networking and intermediate Windows 10 and Ubuntu 16 subject matter. We recommend two or more instructors for advanced camps.



AFA CYBERCAMPS

CyberPatriot – AFA's National Youth Cyber Education Program

What technical resources are required?

The AFA CyberCamp curriculum and activities are largely computer based. To maximize student engagement, the hosting school or organization should provide one computer for every 1-3 participating students. The camp instructor(s) will need a projector and presentation computer with Microsoft PowerPoint.

The campers' computers, as well as the presentation computer, must have internet access and must be capable of running VMWare Player, WinMD5, and 7-Zip, all of which are free software programs. Full technical specifications are available on the CyberPatriot website.

What is the cost of an AFA CyberCamp?

Standard Camp: $1,150 – Includes access to two demonstration images, two competition images, and digital copies of the Instructor Guide and Student Workbook

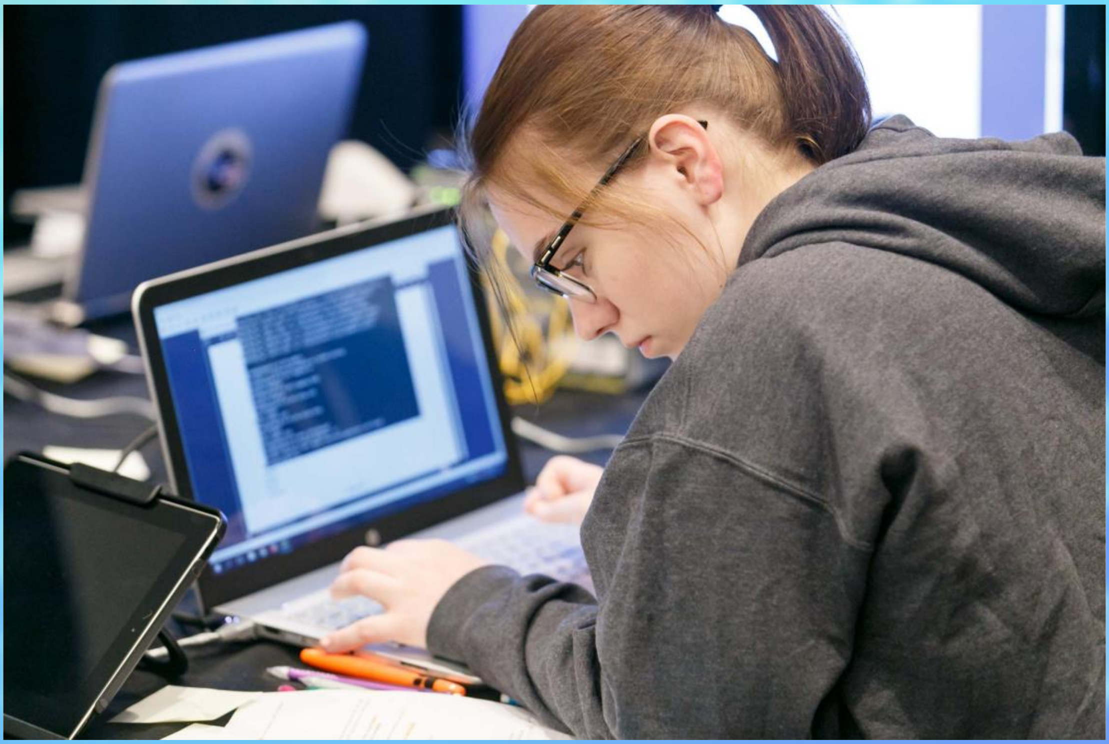
Advanced Camp: $1,450 – Includes access to two demonstration images, two advanced competition images, Cisco Network Academy curriculum, and digital copies of the Instructor Guide and Student Workbook.

For an additional cost, host organizations can request hard-copy workbooks and instructor guides, as well as t-shirts and sunglasses.

Presented by:

NORTHROP GRUMMAN Foundation

2018
AFA Advanced CyberCamp



Instructor's Guide

Authored and edited by Emily Rauer and the Center of Infrastructure Assurance and Security (CIAS)

Advanced CyberCamp Administrative Items

Icon Key

☆ **Note to instructor:** Text that follows is a note to the instructor and should not be read aloud.

👆 **Animation:** Indicates that a mouse click is required to activate a text or picture animation on the slide.

🕒 **Timing Note:** Indicates the estimated duration of a set of instruction slides or an activity.

- **Suggested script or question for the students:** Identifies suggested comments and questions for instructor to say. To keep students engaged, we recommend asking questions frequently.

- **Example:** Identifies examples supporting the content in the proceeding bulleted script or question item.

Setup and Materials

☆ **Before your Camp:** Make sure all of the student computers and the presentation computer have access to the Internet. Install VMWare 6, 7-zip, and WinMD5 to all of the student computers*, as well as to the presentation computer. Next, download the supplied demonstration images and competition images to student computers and the presentation computer.

*When resources allow, one computer should be provided for each team of 2-3 students.

☆ **Demo Image log-in info for Quick Reference:**

- Windows 10: User Name cyberpatriot Password: CyberPatriot!

- Ubuntu 16: User Name cyberpatriot Password: CyberPatriot!

☆ **Module Materials:**

- **3.5 hours Monday: Cyber Ethics & Windows 10**
  - **Student Workbook**
  - **Demonstration Image**
- **4.5 hours Tuesday: Ubuntu**
  - **Student Workbook**
  - **Demonstration Image**
- **4.5 hours Wednesday: Cisco (Module 1/Begin Module 2)**
  - **Student Workbook**
  - **Demonstration Image**
- **4.5 hours Thursday: Cisco (Finish Module 2/Module 3)**
  - **Student Workbook**
  - **Demonstration Image**
- **4.5 hours Friday: Final Activity Packet Tracer, Windows 10, Ubuntu 16 - Competition Day!**
  - **Competition Images**

☆ **In the Camp Space:** Check the sound system to ensure students can hear audio from clips and music you will be playing. Have students sit together in the same teams of 2-3 for the duration of the CyberCamp.

Instructor Pre-Survey

Dear Camp Coordinator & Instructors,

Thank you for hosting an AFA CyberCamp for summer 2018!

Before or on Day 1 of your camp, please take a moment to fill out our Camp Coordinator/Instructor Pre-survey. Your feedback helps us improve our CyberCamp experience for you and your students. On Day 5 we will have another reminder in this Instructor Guide letting you know about a post-survey opportunity (page iii). Each survey takes about 5-10 minutes.

We have also included in the Student Workbook a student focused Pre-survey for students to fill out on Day 1 (Monday) of their camp session as well as a Post-survey to be filled out on Day 5 (Friday) after their Competition. Each survey takes about 5-10 minutes.

Thank you again for taking the time to give us your valuable feedback for our AFA CyberCamp program. The CyberPatriot Program Office wishes you a wonderful summer of cyber!

2018 Instructor Pre-Survey

https://www.surveymonkey.com/r/MBT7BQJ

Advanced CyberCamp Instructor’s Guide Table of Contents

Cyber Ethics

Student Workbook Activities

Slide 0

AFA Advanced CyberCamp

Cyber Ethics

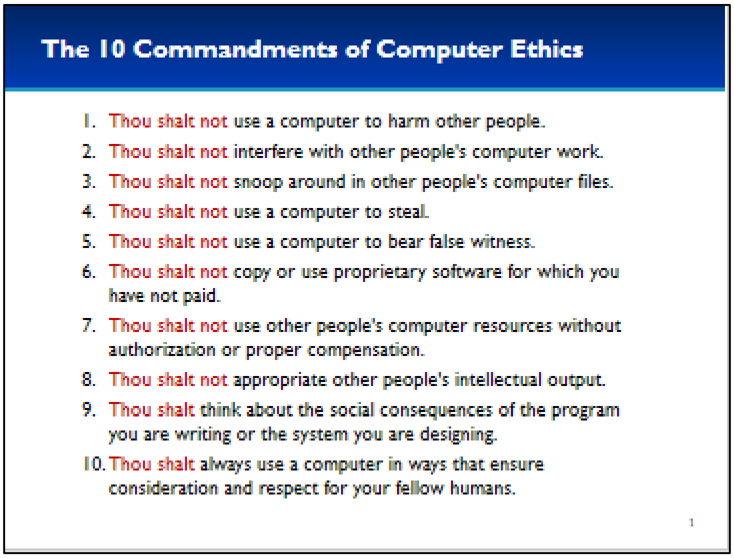
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM
AFA
AFA

- This module will cover Cyber Ethics topics: Commandments of Cyber Ethics, Cyberbullying and the CyberPatriot Code of Conduct.

☆Slides 1-4 should take 25-30 minutes, to include two-minute video on slide 3.

☆Slide 4 students will sign their individual Code of Conduct page in their student workbook (page i).

Slide 1



The 10 Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

1

- Overall, computers have improved our lives dramatically, but they can also cause serious harm. Cyber ethics means acting responsibly and ethically when using computers.

- In 1992, when computers and the Internet were first becoming popular, the Computer Ethics Institute in D.C. created a list of the 10 Commandments of Computer Ethics.

Click to reveal each of the 10 commandments.

☆Read through the list asking students to describe or give examples of to what kind of behavior the commandment is referring.

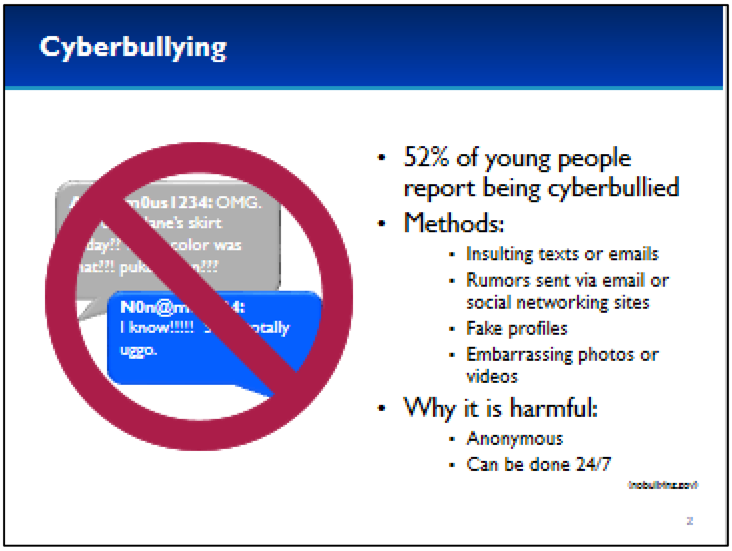
- e.g. "Thou shalt not use a computer to bear false witness:" You should not use a computer to spread rumors, impersonate someone, or launch a smear campaign.

- Who knows what etiquette means? What do you think the term "netiquette" means?

- Netiquette refers to the commonly accepted rules of how to behave online. It's a term commonly used to refer to the general concepts outlined by these 10 Commandments of Computer Ethics.

Source: http://computerethicsinstitute.org/

Slide 2



...m0us1234: OMG. ...ane's skirt ...day!! ...color was ...at!!! puk... ...n!!!
N0n@m...4: I know!!!!! ... ...otally uggo.

Cyberbullying

- 52% of young people report being cyberbullied
- Methods:
  - Insulting texts or emails
  - Rumors sent via email or social networking sites
  - Fake profiles
  - Embarrassing photos or videos
- Why it is harmful:
  - Anonymous
  - Can be done 24/7

(nobullying.com)

2

- Bad netiquette often translates or escalates into cyberbullying.

Click to reveal sample chat.

- Maybe this doesn’t seem too mean, but we don’t know the context. What if “Jane” gets bullied all the time for the way she dresses? What if this chat gets spread around school?

Click to reveal the first bullet.

- According to the latest government statistics, nearly one in two students is a victim of cyberbullying each year, and that number is growing.

- Besides through instant messaging, like in the example here, what other means do cyberbullies use?

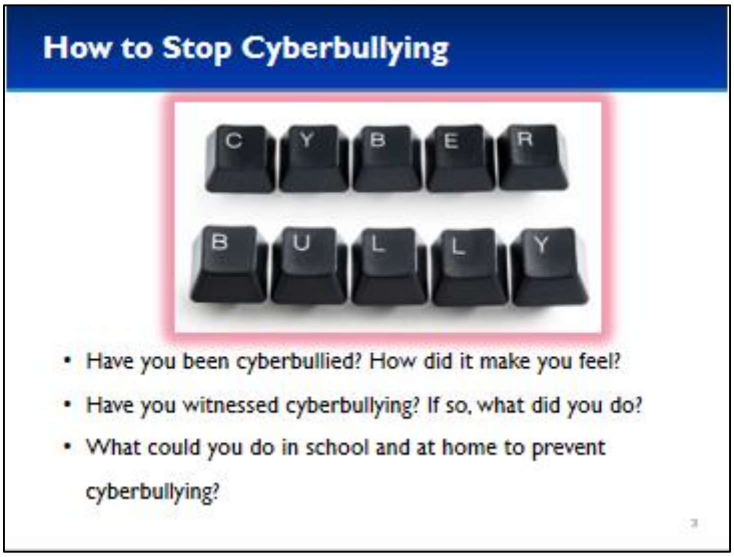
Click to reveal list of methods.

- Why do you think cyberbullying is so harmful?

Click to reveal answer.

Click to reveal a red cross-out symbol over the chat text.

Slide 3



How to Stop Cyberbullying

- Have you been cyberbullied? How did it make you feel?
- Have you witnessed cyberbullying? If so, what did you do?
- What could you do in school and at home to prevent cyberbullying?

3

☝ Click on the photo to see video about How to Stop Cyber-bullying. If an advertisement starts, click the "Skip Ad > " button in bottom-right corner of video. (2:32 minutes)

☆Return to the slide. The next three clicks will be for group discussion or you can have students share amongst themselves in small groups.

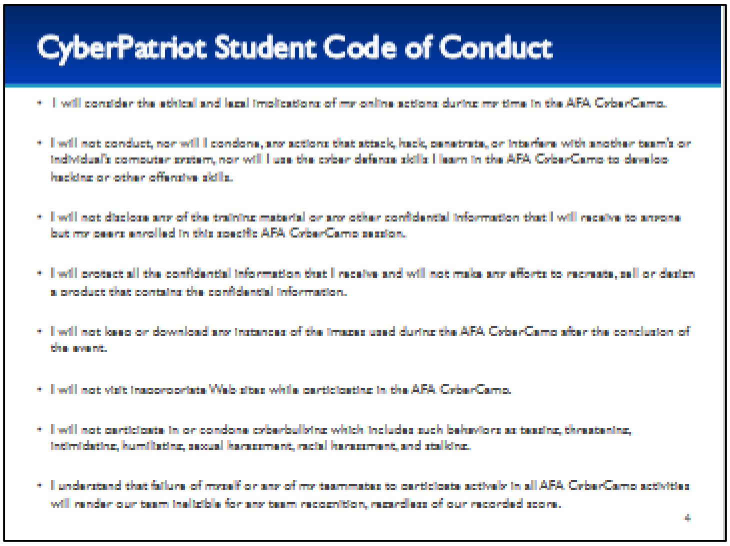
☝Click 1: Have you been cyberbullied? How did it make you feel?

☝Click 2: Have you witnessed cyberbullying, if so what did you do?

☝Click 3: What could you do in school and at home to prevent cyberbullying?

Sources: https://www.youtube.com/watch?v=WegCMoQ-UNs

Slide 4



CyberPatriot Student Code of Conduct

- I will consider the ethical and legal implications of my online actions during my time in the AFA CyberCamp.
- I will not conduct, nor will I condone, any actions that attack, hack, penetrate, or interfere with another team's or individual's computer system, nor will I use the cyber defense skills I learn in the AFA CyberCamp to develop hacking or other offensive skills.
- I will not disclose any of the training material or any other confidential information that I will receive to anyone but my peers enrolled in this specific AFA CyberCamp session.
- I will protect all the confidential information that I receive and will not make any efforts to recreate, sell or design a product that contains the confidential information.
- I will not keep or download any instances of the images used during the AFA CyberCamp after the conclusion of the event.
- I will not visit inappropriate Web sites while participating in the AFA CyberCamp.
- I will not participate in or condone cyberbullying which includes such behaviors as teasing, threatening, intimidating, humiliating, sexual harassment, racial harassment, and stalking.
- I understand that failure of myself or any of my teammates to participate actively in all AFA CyberCamp activities will render our team ineligible for any team recognition, regardless of our recorded score.

4

- All participants of the CyberPatriot National Youth Defense Competition are expected to abide by the CP Student Code of Conduct.
- In preparation to learn and compete this week, all students will sign the Code of Conduct pledging to behave responsibly and ethically throughout the duration of the AFA CyberCamp.

☝Click the eight bullets individually, reading them out loud or choosing a student to read the bullet.

☆Once all bullets have been reviewed, have students turn to page i in their student workbooks and sign their individual Code of Conduct.

☆Students will keep this page inside their Student Workbook for the entirety of the CyberCamp.

Instructor’s Guide Table of Contents

Windows 10

Student Workbook Activities

Slide 0

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM
AFA
AFA

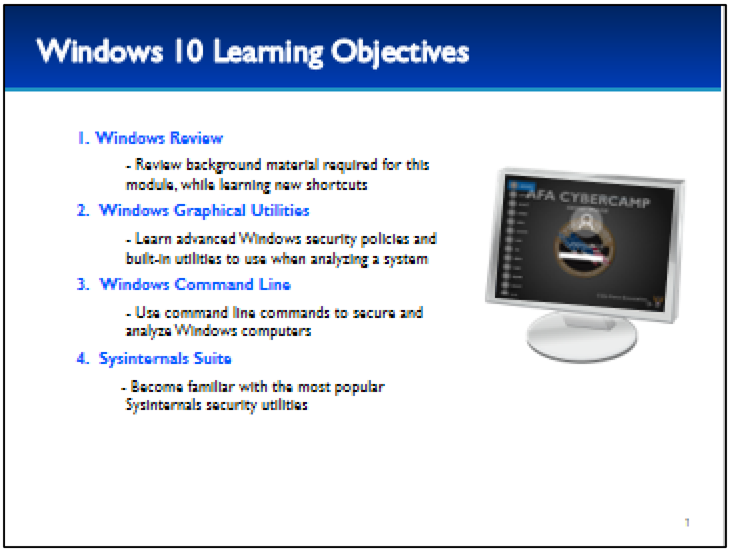
AFA Advanced CyberCamp
Windows 10

- This module will cover advanced topics on Windows 10.

☆Section 1 Windows Review is intended for the Instructor to go through the Demo with students, instead of having the students using the Demo in order to save time.

☆Students should follow along on their Advanced CyberCamp Demo Windows 10 image for Sections 2 Windows Graphical Utilities and 3 Windows Command Line (Section 4 Sysinternals Suite is optional if time permits).

Slide 1



Windows 10 Learning Objectives

1. Windows Review
   - Review background material required for this module, while learning new shortcuts
2. Windows Graphical Utilities
   - Learn advanced Windows security policies and built-in utilities to use when analyzing a system
3. Windows Command Line
   - Use command line commands to secure and analyze Windows computers
4. Sysinternals Suite
   - Become familiar with the most popular Sysinternals security utilities

1

- First, we will briefly cover material from the basic CyberCamp, while learning some new shortcuts to help navigate Windows faster. We are going to cover this material quickly, so do not follow along on your demo images in order to help save time.

- Next, we are going to cover some additional built-in graphical Windows utilities to help analyze and improve your security posture.

- After that, we are going to cover some useful command line utilities that are built into Windows.

- Lastly, we are going to cover some of the security utilities in the Sysinternals Suite to help you detect and analyze malware.

- For sections 2 and 3 (and 4 if time allows), students should follow along on their Windows Demo image.

- At the end of sections 2, 3, and 4 there will be a lab that will ask you to perform tasks and answer questions related to the Windows Demo image.

Slide 2

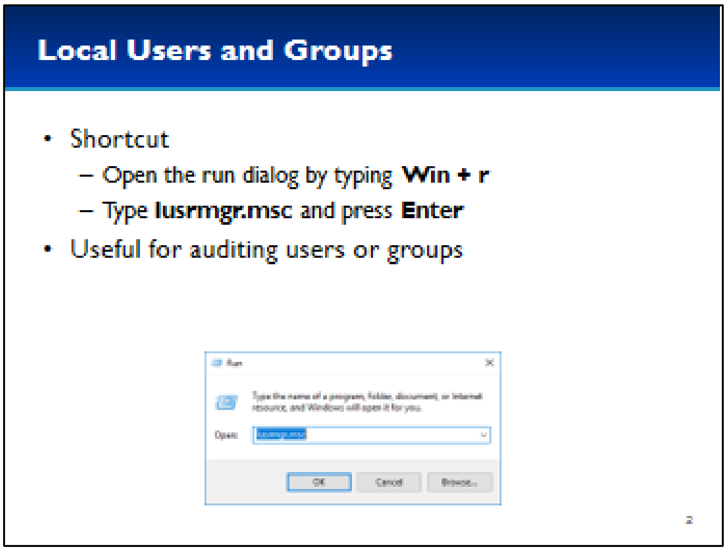
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

Windows Review

🕒 Devote about 20 minutes for slides 3-18. There is no activity after this section.

☆Section 1 Windows Review is intended to be done without students following along on their Demo to save time.

Slide 3



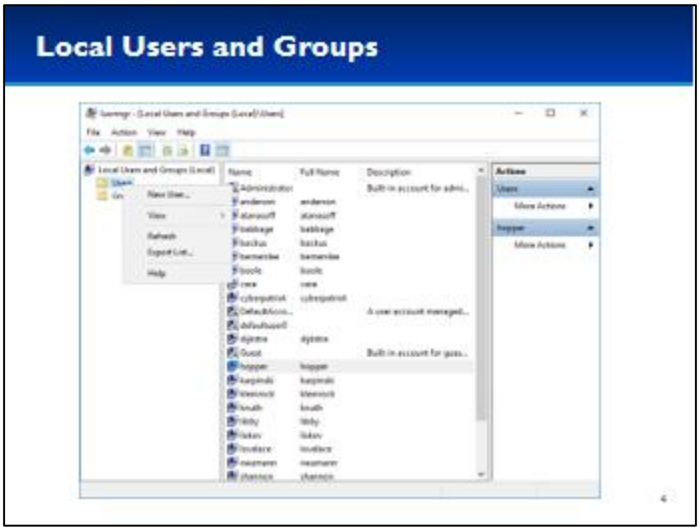
Local Users and Groups

- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **lusrmgr.msc** and press **Enter**
- Useful for auditing users or groups

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
lusrmgr.msc
OK
Cancel
Browse...
2

- The Local Users and Groups Microsoft Management Console snap-in is useful for auditing users and groups on the system, and can display hidden users in the Control Panel Users tool.
- Using MMC to add snap-ins can be tedious, but you can start them easily if you know the run command.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r** (lowercase).
- Next to **Open**, type **lusrmgr.msc** (you can remember this as an abbreviation for Local User Manager).
- MMC plugins end with the .msc extension.
- Press **Enter** or click **OK**.

Slide 4

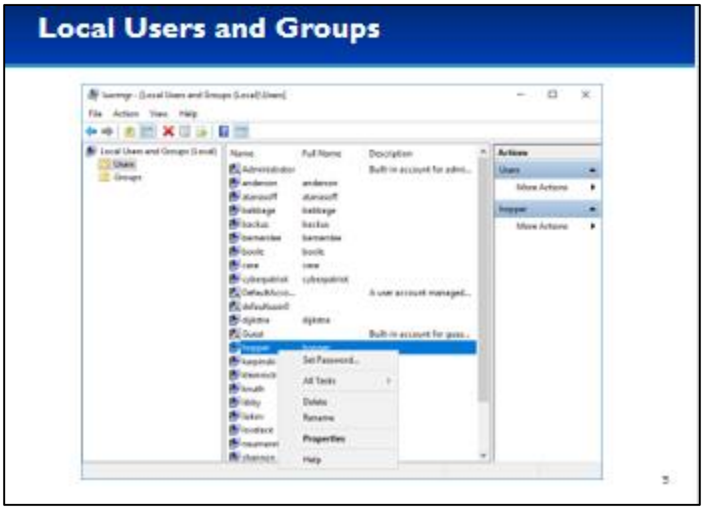


Local Users and Groups

Name	Full Name	Description
Administrator		Built-in account for admi...
anderson	anderson	
atanasoff	atanasoff	
babbage	babbage	
backus	backus	
bernerslee	bernerslee	
boole	boole	
cwe	cwe	
cyberpatriot	cyberpatriot	
DefaultAcco...		A user account managed...
defaultuser0		
dijkstra	dijkstra	
Guest		Built-in account for gues...
hopper	hopper	
karpinski	karpinski	
kleinrock	kleinrock	
knuth	knuth	
libby	libby	
liskov	liskov	
lovelace	lovelace	
neumann	neumann	
shannon	shannon	

- In Local Users and Groups, you can easily add new users or groups by right-clicking on the corresponding folders.

Slide 5



Local Users and Groups

Name	Full Name	Description
Administrator		Built-in account for admi...
anderson	anderson	
atanasoff	atanasoff	
babbage	babbage	
backus	backus	
bernerslee	bernerslee	
boole	boole	
cerf	cerf	
cyberpatriot	cyberpatriot	
DefaultAcco...		A user account managed...
defaultuser0		
dijkstra	dijkstra	
Guest		Built-in account for gues...
hopper	hopper	
[illegible]		
[illegible]		
knuth		
[illegible]		
[illegible]		
lovelace		
neumann		
[illegible]		

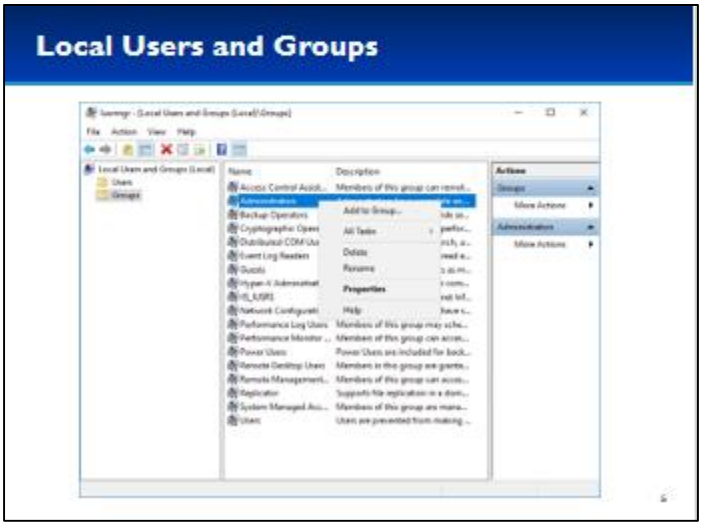
- You can delete, rename, or change the password of a user by right-clicking that user.

- You can also delete a user by selecting that user and pressing the delete key.

- In the user Properties, you can perform additional tasks such as setting the user’s password to never expire, disable the account, unlock the account, and manage group memberships.

- You can also open the user Properties by double-clicking on that user.

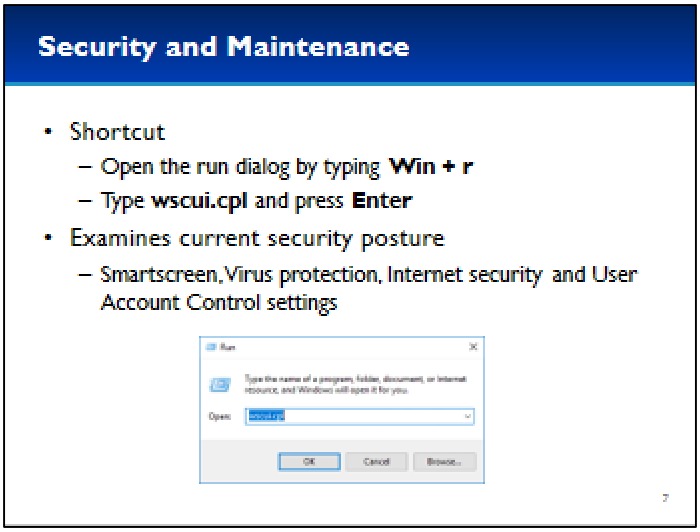
Slide 6



Local Users and Groups

- By right-clicking on a group you can easily delete or rename it.
- You can also delete a group by selecting it and pressing the delete key.
- In the group Properties, or by clicking Add to Group, you can view all members of a group and easily add or remove users from it.
- You can also open the Properties for a group by double-clicking on it.

Slide 7



Security and Maintenance

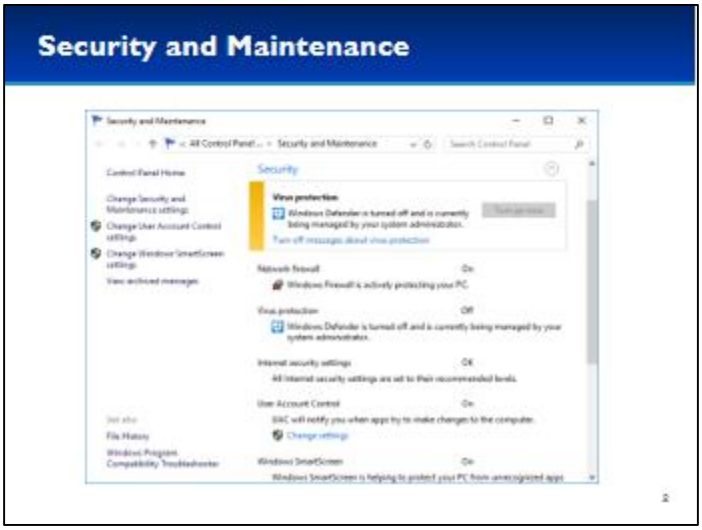
- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **wscui.cpl** and press **Enter**
- Examines current security posture
  - Smartscreen, Virus protection, Internet security and User Account Control settings

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wscui.cpl

- Security and Maintenance monitors your computer's security status.
- Security and Maintenance can be found in the Control Panel in Windows 10. It was previously named Action Center, and Security Center before that.
- The Security Center is a great place to start when determining your computer's security status.
- To save time, you can navigate to it directly without having to go through the Control Panel.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- Next to **Open**, type **wscui.cpl** (you can remember this as an abbreviation for Windows Security Center User Interface).
- Control Panel Windows end with the .cpl extension.
- Press **Enter** or click **OK**.

Slide 8



Security and Maintenance

Security and Maintenance
All Control Panel... › Security and Maintenance
Search Control Panel
Control Panel Home
Change Security and Maintenance settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
See also
File History
Windows Program Compatibility Troubleshooter
Security
Turn on now
Turn off messages about virus protection
Change settings

Virus protection
Windows Defender is turned off and is currently being managed by your system administrator.

Network firewall — On
Windows Firewall is actively protecting your PC.

Virus protection — Off
Windows Defender is turned off and is currently being managed by your system administrator.

Internet security settings — OK
All Internet security settings are set to their recommended levels.

User Account Control — On
UAC will notify you when apps try to make changes to the computer.

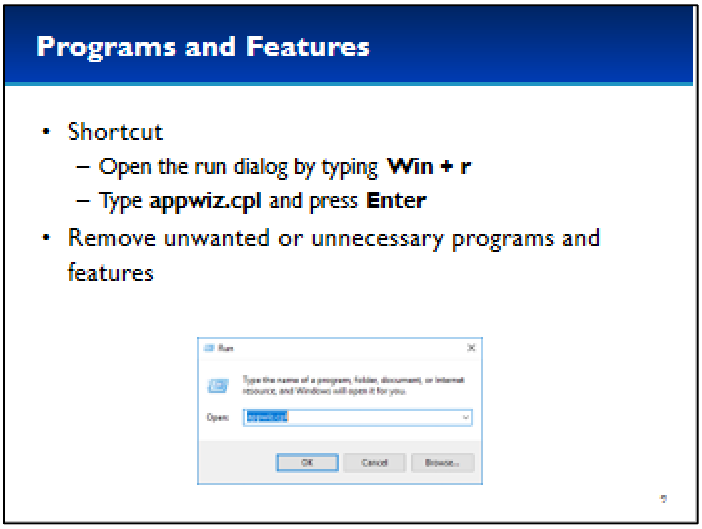
Windows SmartScreen — On
Windows SmartScreen is helping to protect your PC from unrecognized apps

2

- Click the arrow across from Security to see the Firewall and other settings. Security and Maintenance monitors several aspects of a computer security, including Virus protection, Network firewall, Internet security settings, User Account Control, and Window SmartScreen.

- Below this there is an additional Maintenance section that can handle regular maintenance of your computer, including performing tasks such as backups. Remember, making sure you have backups of your data is critical to computer security.

Slide 9



Programs and Features

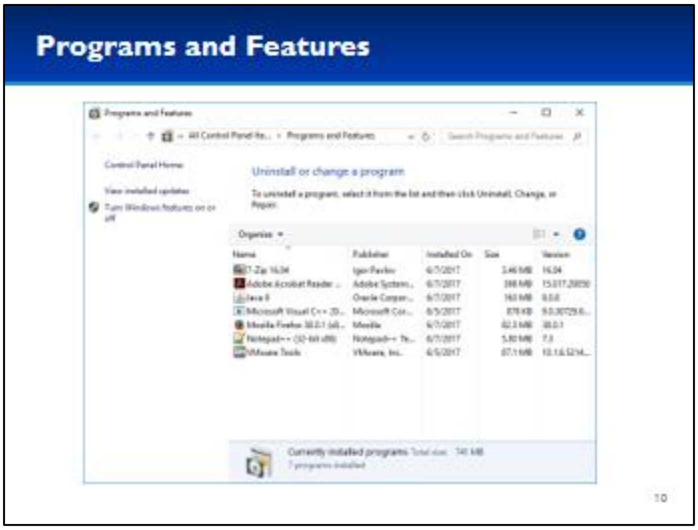
- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **appwiz.cpl** and press **Enter**
- Remove unwanted or unnecessary programs and features

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: appwiz.cpl

- You can easily add and remove many programs using **Programs and Features** under the **Control Panel**.
- To save time, you can navigate to it directly without having to go through the Control Panel.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- Next to **Open**, type **appwiz.cpl** (you can remember this as an abbreviation for Application Wizard).
- Press **Enter** or click **OK**.

Slide 10



Programs and Features

Programs and Features

All Control Panel Ite... › Programs and Features

Search Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize ▾

Name	Publisher	Installed On	Size	Version
7-Zip 16.04	Igor Pavlov	6/7/2017	3.46 MB	16.04
Adobe Acrobat Reader ...	Adobe Systems...	6/7/2017	398 MB	15.017.20050
Java 8	Oracle Corpor...	6/7/2017	160 MB	8.0.0
Microsoft Visual C++ 20...	Microsoft Cor...	6/5/2017	878 KB	9.0.30729.6...
Mozilla Firefox 38.0.1 (x8...	Mozilla	6/7/2017	82.3 MB	38.0.1
Notepad++ (32-bit x86)	Notepad++ Te...	6/7/2017	5.80 MB	7.3
VMware Tools	VMware, Inc.	6/5/2017	87.1 MB	10.1.6.5214...

Currently installed programs Total size: 741 MB
7 programs installed

10

- Here you can view the applications currently installed on your computer.

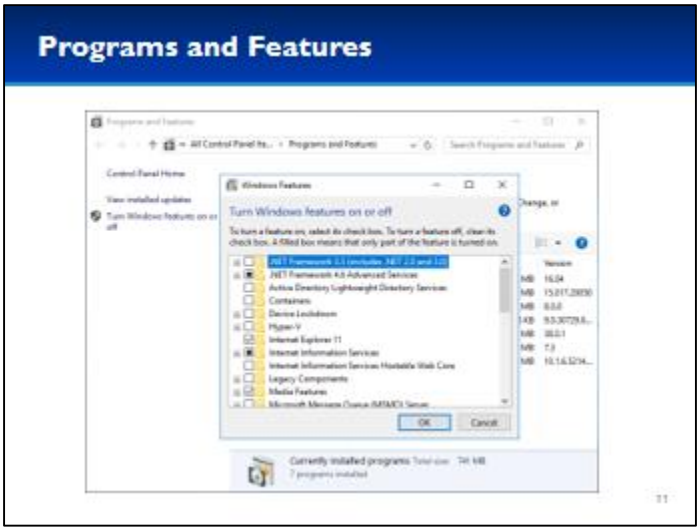
- Often, additional information is available which can be very helpful.

  - Looking at the version of the application installed can help you determine if it needs to be updated.

  - Looking at when a program was installed can help you track down old or unwanted programs.

  - Looking at the size of an installed application can help you when trying to free up disk space.

Slide 11



Programs and Features

Programs and Features

All Control Panel Ite... › Programs and Features

Search Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.6 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Device Lockdown
- □ Hyper-V
- ☑ Internet Explorer 11
- ■ Internet Information Services
- □ Internet Information Services Hostable Web Core
- □ Legacy Components
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server

Currently installed programs Total size: 74 MB
7 programs installed

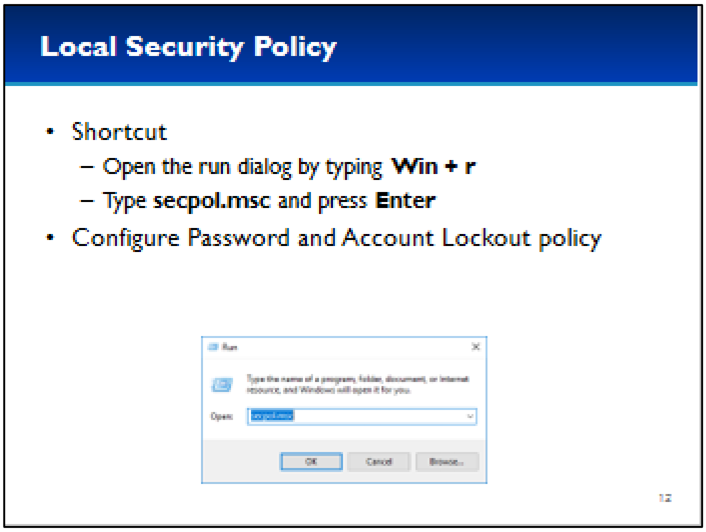
11

- Under Programs and Features, you can click on **Turn Windows features on or off.** Windows generally comes with a good set of enabled features, but sometimes you may want to modify this.

- For example, you may need to install .NET framework 3.5 in order to run applications that require it.

- Notice that a portion of Internet Information Services (IIS) is installed. This generally means the computer is running an FTP or HTTP server. If this isn’t a service that is supposed to be running on your computer, it’s probably a good idea to remove it.

Slide 12



Local Security Policy

- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **secpol.msc** and press **Enter**
- Configure Password and Account Lockout policy

Run

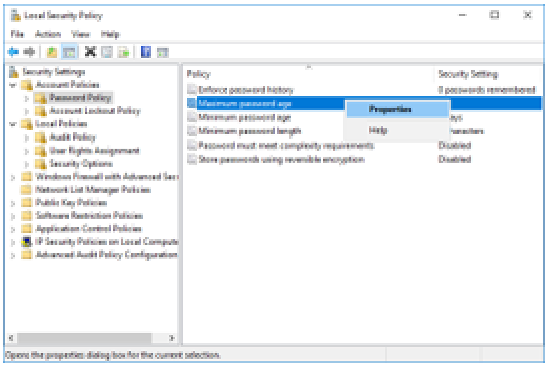
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: secpol.msc

- The Local Security Policy is very important, and allows you to set secure system policies for passwords, account lockout, and auditing.
- Using MMC to add snap-ins can be tedious, but you can start them easily if you know the run command.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- Next to **Open**, type **secpol.msc** (you can remember this as an abbreviation for Security Policy).
- Press **Enter** or click **OK**.

Slide 13

Local Security Policy



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	
Minimum password age	ays
Minimum password length	haracters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Opens the properties dialog box for the current selection.

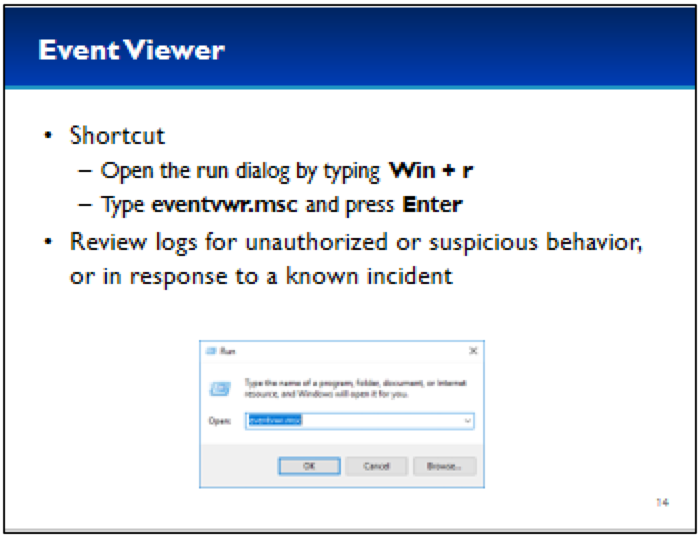
12

- Password Policy and Account Lockout Policy are under Account Policies.

- In order to change a setting, just double-click on it, or right-click and select Properties.

- We’re going to be using the Local Security Policy in the next section to modify User Rights Assignments and Security Options.

Slide 14



Event Viewer

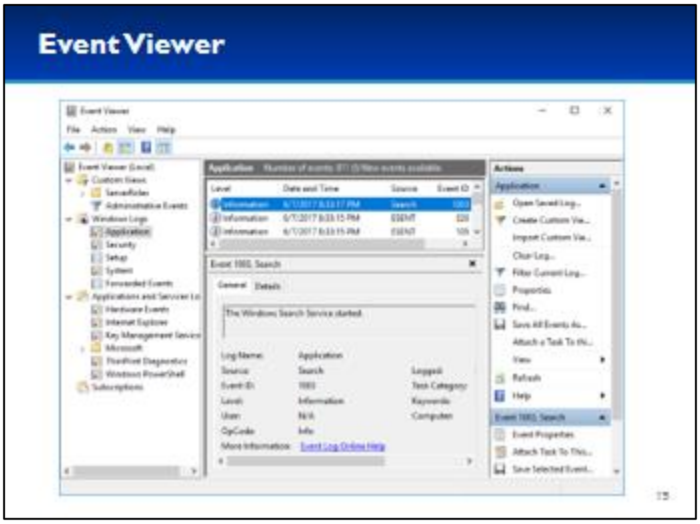
- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **eventvwr.msc** and press **Enter**
- Review logs for unauthorized or suspicious behavior, or in response to a known incident

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: eventvwr.msc

- Logs are a critical part of computer security, development, and general maintenance.
- Event Viewer is another MMC plugin.
- Using MMC to add snap-ins can be tedious, but you can start them easily if you know the run command.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- Next to **Open**, type **eventvwr.msc** (you can remember this as an abbreviation for Event Viewer).
- Press **Enter** or click **OK**.

Slide 15



Event Viewer

Application Number of events: 871 (!) New events available

Level	Date and Time	Source	Event ID
Information	6/7/2017 8:33:17 PM	Search	1003
Information	6/7/2017 8:33:15 PM	ESENT	326
Information	6/7/2017 8:33:15 PM	ESENT	105

Event 1003, Search

The Windows Search Service started.

Log Name: Application
Source: Search
Event ID: 1003
Level: Information
User: N/A
OpCode: Info
More Information: Event Log Online Help

Logged:
Task Category:
Keywords:
Computer:

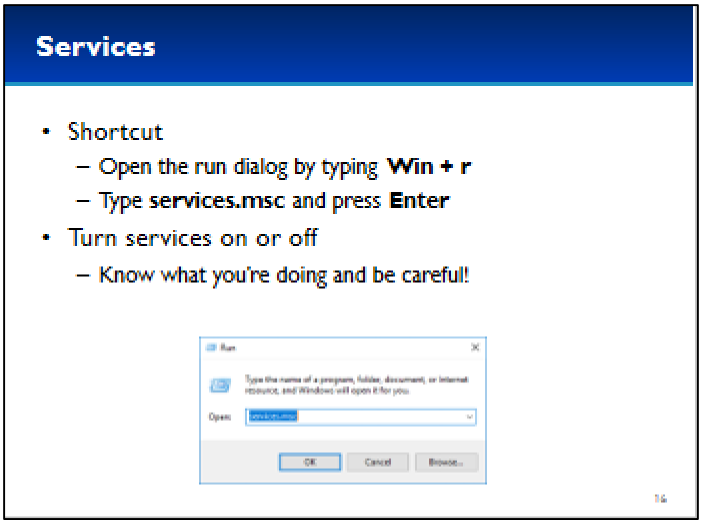
- Event Viewer contains a vast amount of information including application logs, security logs, and system logs.

- Application logs include data from many Microsoft applications, Windows services, and third-party applications.

- Security logs include auditing events. If auditing is enabled in Local Security Policy, this is where those events would be logged.

- System logs include logs for drivers, or functionality built into the Windows OS, such as DHCP, DNS, file system drivers, time service, power management, and modifications to Windows Service configurations.

Slide 16



Services

- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **services.msc** and press **Enter**
- Turn services on or off
  - Know what you're doing and be careful!

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

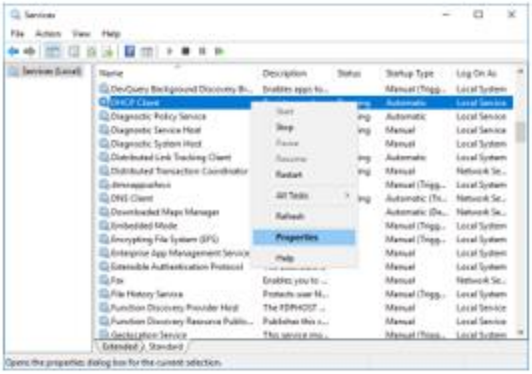
Open: services.msc

16

- Viewing and making changes to Windows Services can be done through the Services MMC plugin.
- In some versions of Windows there is a Services.exe executable which is exactly the same.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- Next to **Open**, type **services.msc**.
- Press **Enter** or click **OK**.

Slide 17

Services



Name	Description	Status	Startup Type	Log On As
DevQuery Background Discovery Br...	Enables apps to...		Manual (Trigg...	Local System
DHCP Client	[illegible]	[illegible]	Automatic	Local Service
Diagnostic Policy Service		ing	Automatic	Local Service
Diagnostic Service Host		ing	Manual	Local Service
Diagnostic System Host			Manual	Local System
Distributed Link Tracking Client		ing	Automatic	Local System
Distributed Transaction Coordinator		ing	Manual	Network Se...
dmwappushsvc			Manual (Trigg...	Local System
DNS Client		ing	Automatic (Tri...	Network Se...
Downloaded Maps Manager			Automatic (De...	Network Se...
Embedded Mode			Manual (Trigg...	Local System
Encrypting File System (EFS)			Manual (Trigg...	Local System
Enterprise App Management Service			Manual	Local System
Extensible Authentication Protocol			Manual	Local System
Fax	Enables you to ...		Manual	Network Se...
File History Service	Protects user fil...		Manual (Trigg...	Local System
Function Discovery Provider Host	The FDPHOST ...		Manual	Local Service
Function Discovery Resource Public...	Publishes this c...		Manual	Local Service
Geolocation Service	This service mo...		Manual (Trigg...	Local System

Opens the properties dialog box for the current selection.

17

- Services display all the services available, their current Status, and their Startup Type.

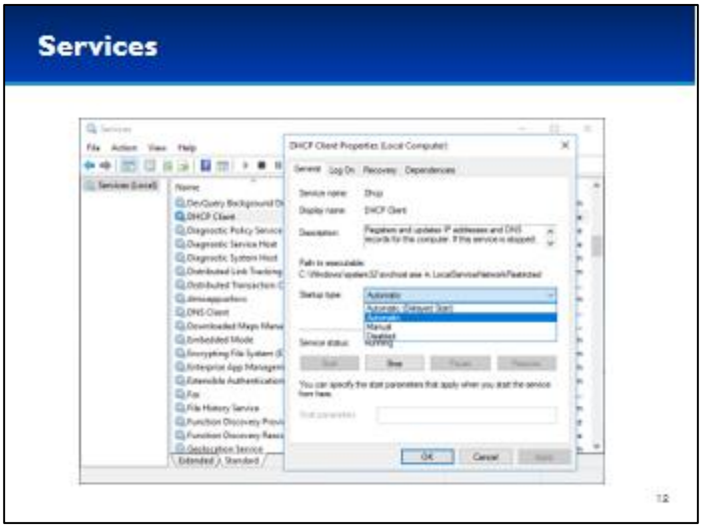
- Remember you can sort by columns by clicking on the column header. This can make auditing your services configuration much easier.

- You can easily start or stop a service by right-clicking on the service and selecting **Start** or **Stop**.

- Starting and stopping services is a good first step when testing and troubleshooting, but it's important to also configure the Startup Type.

- In order to change the Startup Type, double-click the service, or right-click the service and select Properties.

Slide 18



Services

DHCP Client Properties (Local Computer)

Service name: Dhcp

Display name: DHCP Client

Description: Registers and updates IP addresses and DNS records for this computer. If this service is stopped

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

- Inside the service Properties you can configure the service to start Automatically, Manually, or Disabled.

- If a service is set to start Automatically, it will always start when the system boots up. Manually means that it can be started by a user, or if needed by another service or application. If a service is set to Disabled, it will never start.

- Be very, very careful when changing services, many of these services are important to the correct functionality of your computer. If you Stop or Disable the wrong services, your computer will be unusable.

- Make sure and do your research first before making changes to services.

- The Windows defaults are a good place to start, with several resources available online from Microsoft or other websites.

Slide 19

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

Windows Graphical Utilities

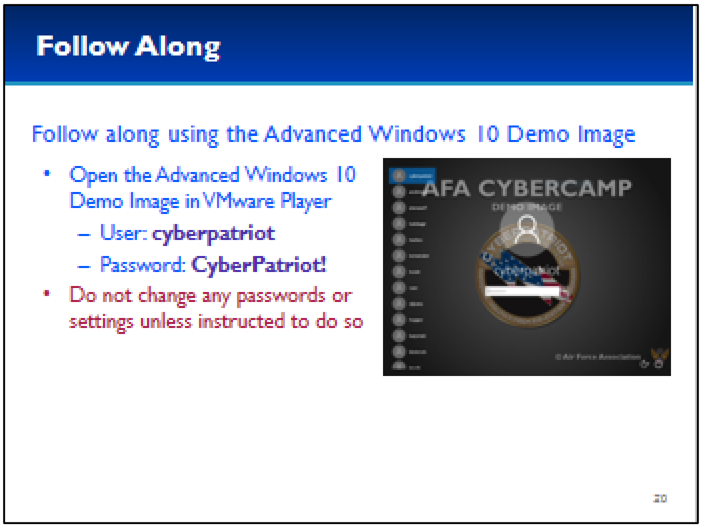
🕒 Devote 30 minutes to slides 20-48. Allow the students 20 minutes to complete the activity on slide 49.

☆ Throughout this section, students should follow along in the **Advanced Windows 10 Demo Image**.

☆ Actions the students are supposed to take are highlighted in blue and purple.

☆ Purple indicates the exact text they are supposed to type or GUI elements they should interact with.

Slide 20



Follow Along

Follow along using the Advanced Windows 10 Demo Image

- Open the Advanced Windows 10 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Do not change any passwords or settings unless instructed to do so

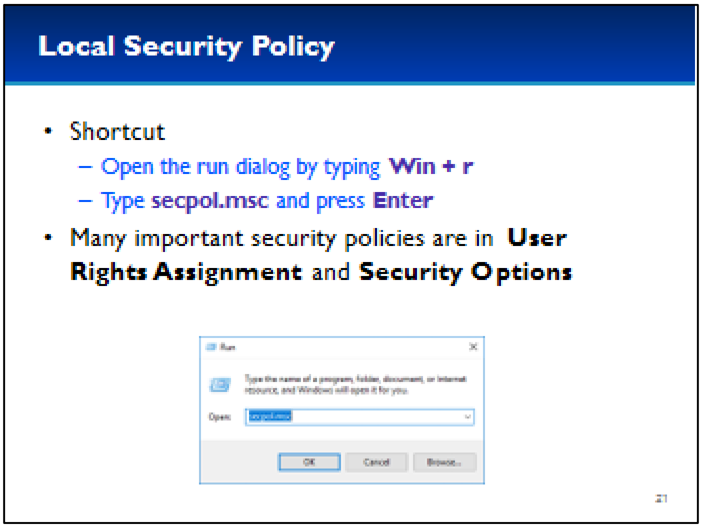
20

☆Have the students follow along as time permits.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so.

☆Users are NOT automatically logged in, they should log in as the user cyberpatriot with the password CyberPatriot!

Slide 21



Local Security Policy

- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **secpol.msc** and press **Enter**
- Many important security policies are in **User Rights Assignment** and **Security Options**

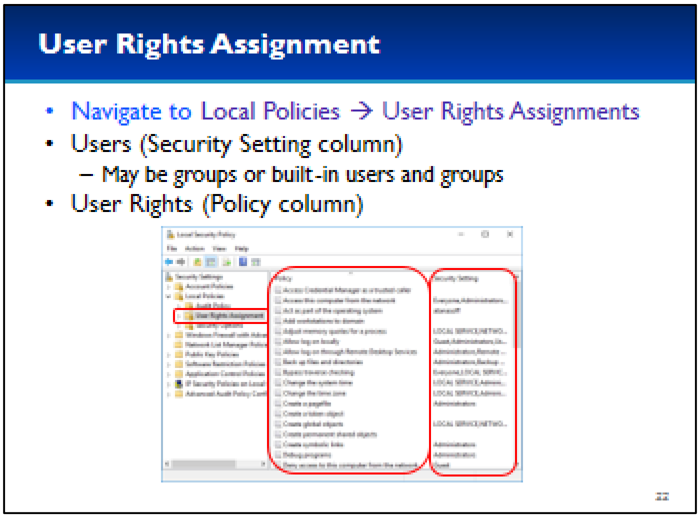
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: secpol.msc

- In addition to **Password Policy**, **Account Lockout Policy**, and **Auditing**, there are many more important security policies in the **Local Security Policy** such as **User Rights Assignments** and **Security Options**.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- Next to **Open**, type **secpol.msc**.
- Press **Enter** or click **OK**.

Slide 22



User Rights Assignment

- Navigate to Local Policies → User Rights Assignments
- Users (Security Setting column)
  - May be groups or built-in users and groups
- User Rights (Policy column)

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advan
Network List Manager Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Confi

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,...
Act as part of the operating system	[illegible]
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Guest,Administrators,Us...
Allow log on through Remote Desktop Services	Administrators,Remote ...
Back up files and directories	Administrators,Backup ...
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guest

22

- Navigate to Local Policies → User Rights Assignments.

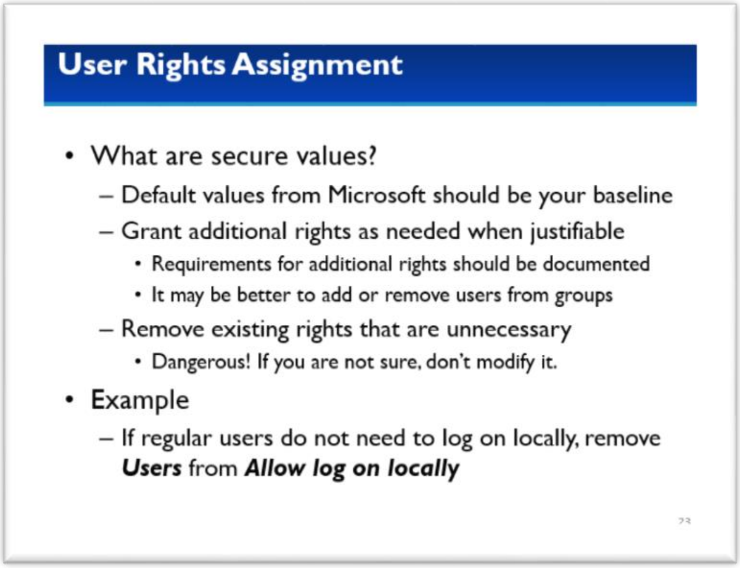
- To expand items on the left you can double-click the item, or click the arrow on the left side of the item.

- The Policy column contains the User Rights.

- The Security Setting column contains the users or groups that have been granted that right.

  - Some of the users and groups are built-in and are not visible in the Local User and Groups Manager.

Slide 23



User Rights Assignment

- What are secure values?
  - Default values from Microsoft should be your baseline
  - Grant additional rights as needed when justifiable
    - Requirements for additional rights should be documented
    - It may be better to add or remove users from groups
  - Remove existing rights that are unnecessary
    - Dangerous! If you are not sure, don't modify it.
- Example
  - If regular users do not need to log on locally, remove ***Users*** from ***Allow log on locally***

23

- How do you know what secure settings are?

  - The default values from Microsoft are a good starting point.

  - You may need to grant additional rights to users depending on your business needs, but there should be a justifiable and documented reason for this.

  - Normally, it is more appropriate to add and remove users from groups that have already been granted rights, such as Backup Operators.

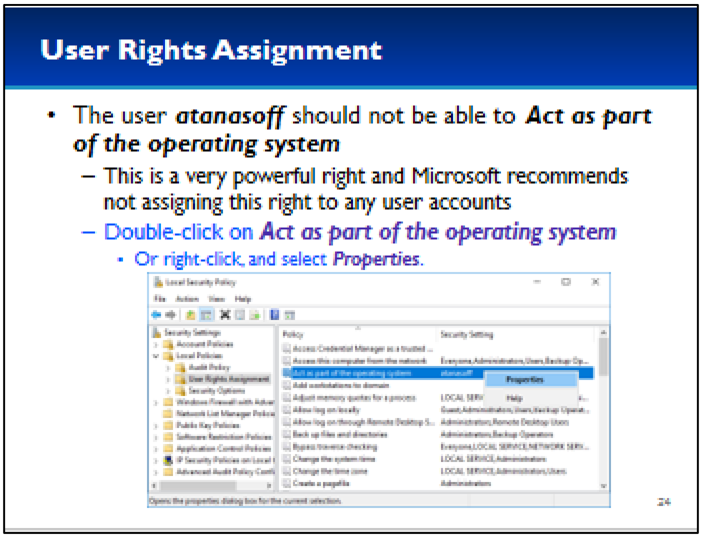
  - Remove existing rights that are unnecessary; typically these are rights that have been granted above and beyond the default.

  - Modifying rights can be dangerous so make sure you've done your research before making any changes.

- For example, server systems in an access restricted area are typically meant to be only accessible locally by administrators.

  - In this case it would be a good idea to remove users from the Allow log on locally, while ensuring that Administrators are still granted that right.

Slide 24



User Rights Assignment

- The user ***atanasoff*** should not be able to ***Act as part of the operating system***
  - This is a very powerful right and Microsoft recommends not assigning this right to any user accounts
  - Double-click on ***Act as part of the operating system***
    - Or right-click, and select *Properties.*

Policy	Security Setting
Access Credential Manager as a trusted ...	
Access this computer from the network	Everyone,Administrators,Users,Backup Op...
Act as part of the operating system	atanasoff
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERV...
Allow log on locally	Guest,Administrators,Users,Backup Operat...
Allow log on through Remote Desktop S...	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERV...
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,Users
Create a pagefile	Administrators

Opens the properties dialog box for the current selection.

24

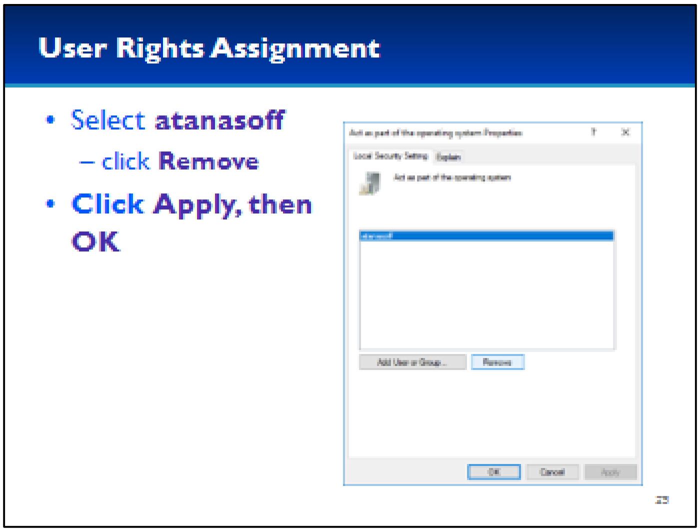
- On your demo image, the user atanasoff should not have privileges that allow him to Act as part of the operating system.

  - This is a very powerful right that Microsoft strongly recommends not assigning to any users or groups.

- Double-click on the Policy Act as part of the operating system.

  - Alternatively, you could right-click on the Policy and select Properties.

Slide 25



User Rights Assignment

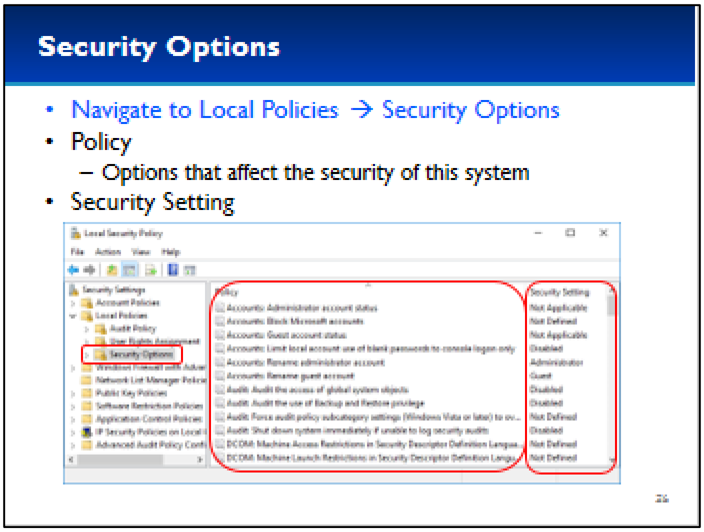
- Select **atanasoff**
  - click **Remove**
- **Click Apply, then OK**

Act as part of the operating system Properties
?
X
Local Security Setting
Explain
Act as part of the operating system
atanasoff
Add User or Group...
Remove
OK
Cancel
Apply
25

- To remove atanasoff, select the user and click Remove.

- Click Apply**,** then OK to apply the changes and close the Properties window.

Slide 26



Security Options

- Navigate to Local Policies → Security Options
- Policy
  - – Options that affect the security of this system
- Security Setting

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advan
Network List Manager Polici
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Confi

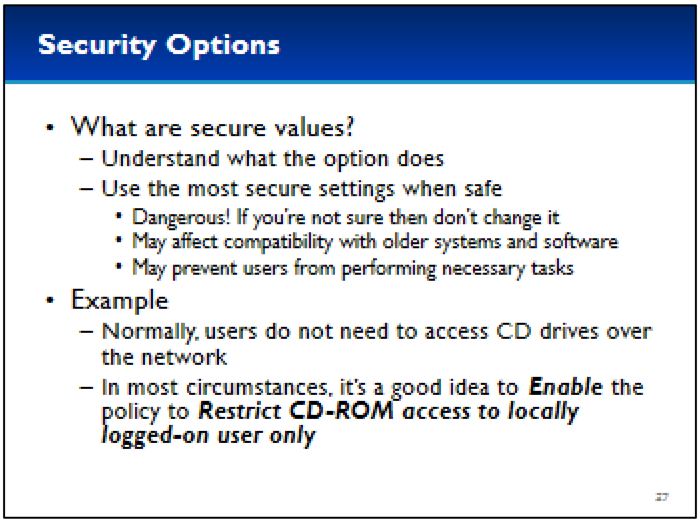
Policy	Security Setting
Accounts: Administrator account status	Not Applicable
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Applicable
Accounts: Limit local account use of blank passwords to console logon only	Disabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to ov...	Not Defined
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Langua...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Langu...	Not Defined

26

- Navigate to Local Policies → Security Options.
- In the Policy column, there are settings that affect the security of the system.
- In the Security Settings column is the current value of the corresponding setting.

  - Typically values may be Not Defined, Enabled, or Disabled, but many options have settings that are specific to the corresponding setting.

Slide 27



Security Options

- What are secure values?
  - Understand what the option does
  - Use the most secure settings when safe
    - Dangerous! If you're not sure then don't change it
    - May affect compatibility with older systems and software
    - May prevent users from performing necessary tasks
- Example
  - Normally, users do not need to access CD drives over the network
  - In most circumstances, it's a good idea to ***Enable*** the policy to ***Restrict CD-ROM access to locally logged-on user only***

27

- How do you know what secure values are?

  - Before you try to determine the correct setting, understand what the option does.

  - Again, the default values provided by Microsoft are a good starting point.

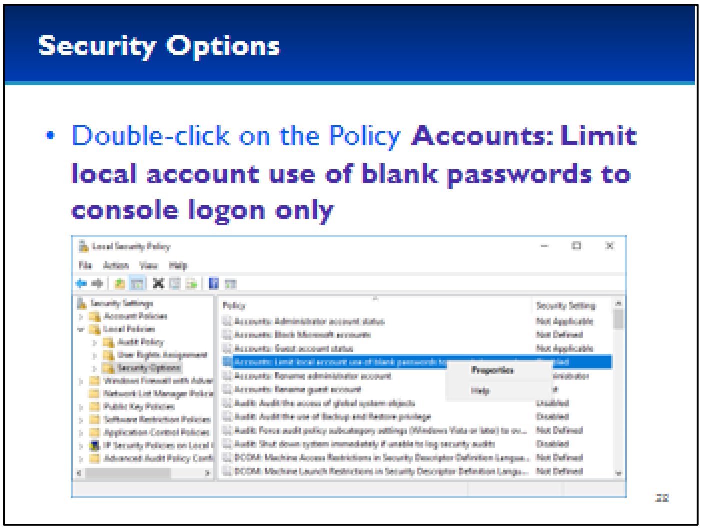
  - Modifying these values can be dangerous, and if you don't know what you are doing you could accidentally make your system less secure, unusable, or affect compatibility with applications or network services.

- For example, there may be justified documented reasons to allow users to log in remotely on some computers.

  - However, remote users typically do not need to access CD-ROM drives remotely.

  - If there is no reason for users to do this in your environment, you should Enable the policy to Devices: Restrict CD-ROM access to locally logged-on user only.

Slide 28



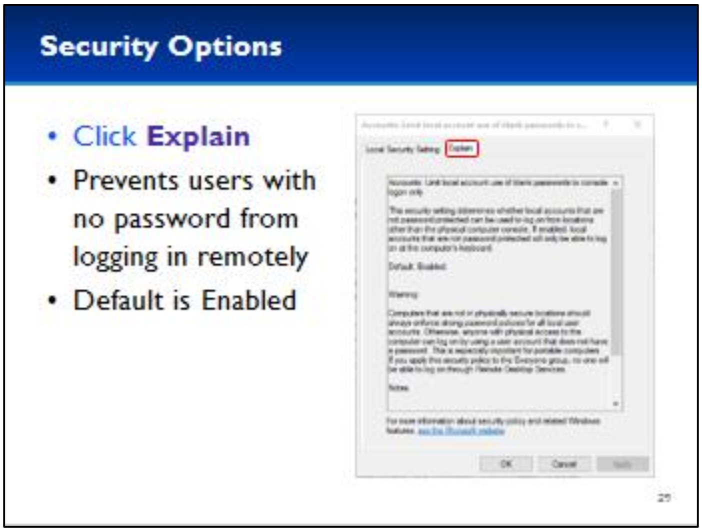
Security Options

- Double-click on the Policy **Accounts: Limit local account use of blank passwords to console logon only**

Policy	Security Setting
Accounts: Administrator account status	Not Applicable
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Applicable
Accounts: Limit local account use of blank passwords to	...bled
Accounts: Rename administrator account	...inistrator
Accounts: Rename guest account	...t
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to ov...	Not Defined
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Langua...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Langu...	Not Defined

- Double-click on the Policy Accounts: Limit local account use of blank passwords to console logon only.
- Alternatively you can right-click on the Policy and select Properties.

Slide 29



Security Options

- Click **Explain**
- Prevents users with no password from logging in remotely
- Default is Enabled

Accounts: Limit local account use of blank passwords to c...
Local Security Setting
Explain
OK
Cancel
Apply
29

Accounts: Limit local account use of blank passwords to console logon only

This security setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If enabled, local accounts that are not password protected will only be able to log on at the computer's keyboard.

Default: Enabled.

Warning:

Computers that are not in physically secure locations should always enforce strong password policies for all local user accounts. Otherwise, anyone with physical access to the computer can log on by using a user account that does not have a password. This is especially important for portable computers. If you apply this security policy to the Everyone group, no one will be able to log on through Remote Desktop Services.

Notes

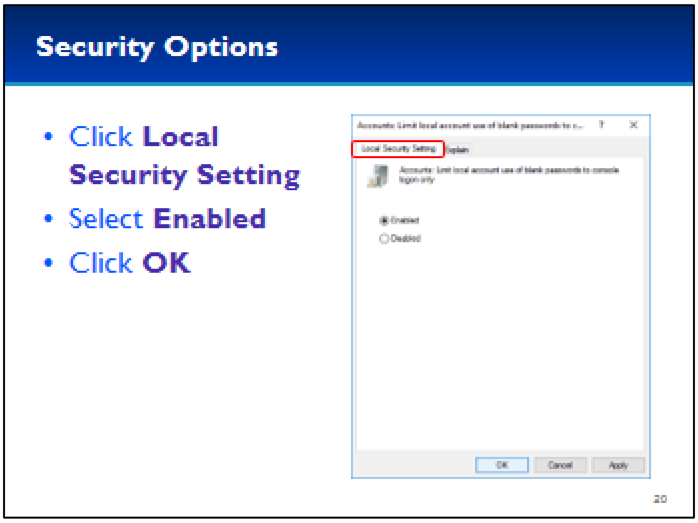
For more information about security policy and related Windows features, see the Microsoft website.

- In the Properties window, click the tab Explain.
- Reading the description, you can see this Security Setting prevents users without a password from logging in remotely. The Default value is Enabled. However, in the Demo the value is set to Disabled.
- This seems like a very good security policy to enable, which we will do in the next slide.
- There is also a warning advising you of common pitfalls.

  - You still should have a secure password policy even with this enabled.

  - You could affect the ability of all users to log in remotely if you computer is misconfigured.

Slide 30



Security Options

- Click **Local Security Setting**
- Select **Enabled**
- Click **OK**

Accounts: Limit local account use of blank passwords to c...

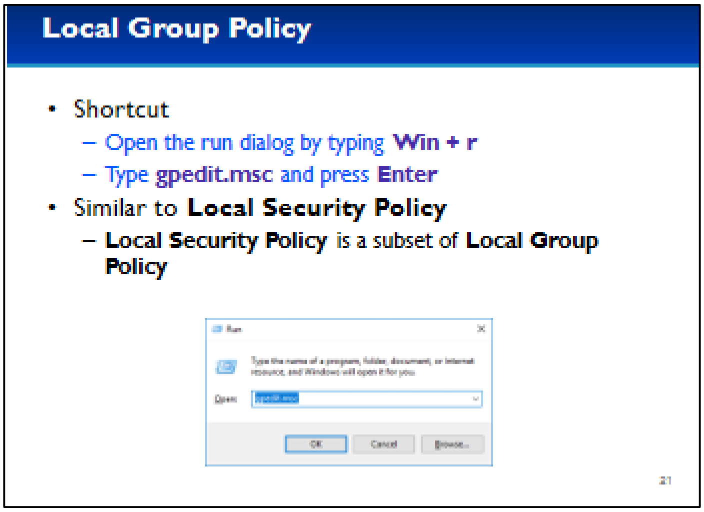
Accounts: Limit local account use of blank passwords to console logon only

● Enabled

○ Disabled

- Based on this information we should enable this security option.
- Click the Local Security Setting tab.
- Select Enabled.
- Click OK to apply the changes and close the Properties window.

Slide 31



Local Group Policy

- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **gpedit.msc** and press **Enter**
- Similar to **Local Security Policy**
  - **Local Security Policy** is a subset of **Local Group Policy**

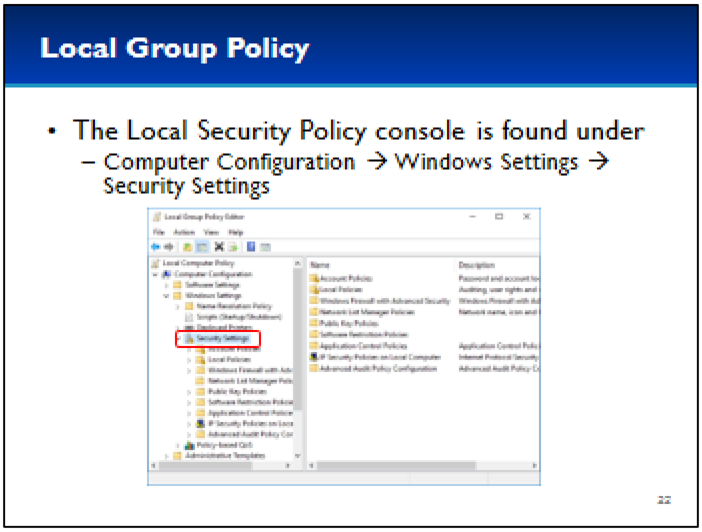
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

- The Local Group Policy is similar to the Local Security Policy.
- In fact, the Local Security Policy is contained within the Local Group Policy.
- Open the run dialog box by holding down the Windows key and pressing the letter **r** (lower case).
- Next to Open, type gpedit.msc.
- Press Enter or click OK.

Slide 32



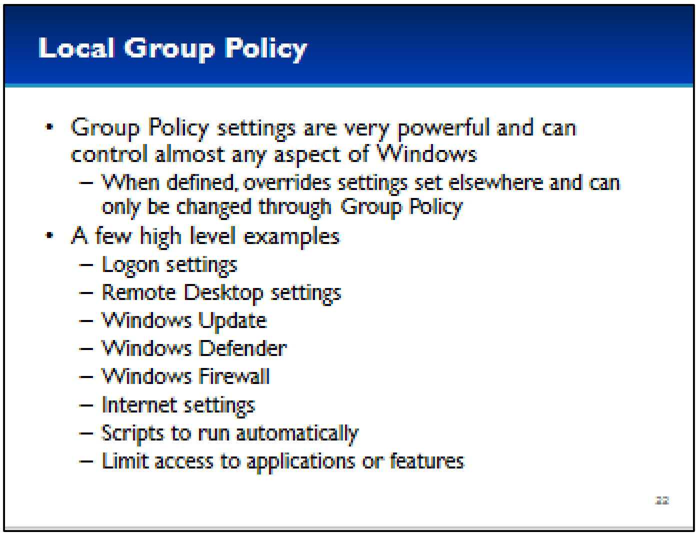
Local Group Policy

- The Local Security Policy console is found under
  - Computer Configuration → Windows Settings → Security Settings

Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Firewall with Adv
Network List Manager Polic
Public Key Policies
Software Restriction Polici
Application Control Policie
IP Security Policies on Loca
Advanced Audit Policy Cor
Policy-based QoS
Administrative Templates
Name
Description
Account Policies
Password and account lo
Local Policies
Auditing, user rights and
Windows Firewall with Advanced Security
Windows Firewall with Ad
Network List Manager Policies
Network name, icon and
Public Key Policies
Software Restriction Policies
Application Control Policies
Application Control Polic
IP Security Policies on Local Computer
Internet Protocol Security
Advanced Audit Policy Configuration
Advanced Audit Policy Co
32

- In the Local Group Policy Editor, you can find the Local Security Policy settings under Computer Configuration → Windows Settings → Security Settings.

Slide 33



Local Group Policy

- Group Policy settings are very powerful and can control almost any aspect of Windows
  - When defined, overrides settings set elsewhere and can only be changed through Group Policy
- A few high level examples
  - Logon settings
  - Remote Desktop settings
  - Windows Update
  - Windows Defender
  - Windows Firewall
  - Internet settings
  - Scripts to run automatically
  - Limit access to applications or features

22

- Group Policy settings are very powerful and can control almost any aspect of Windows, Windows services, and even some applications.

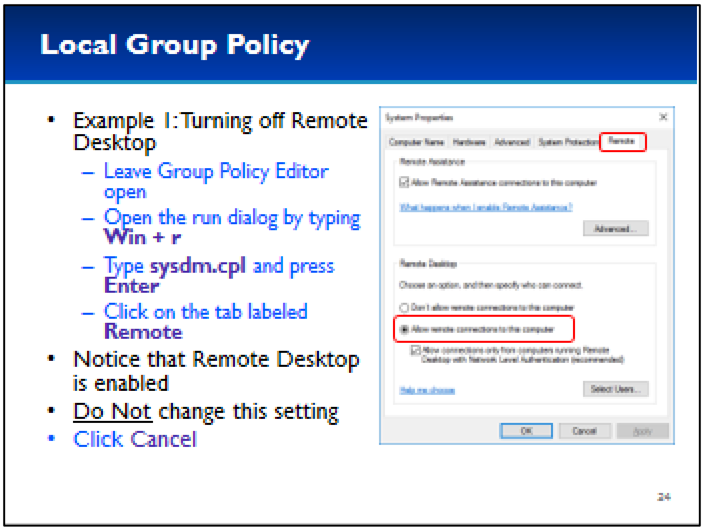
  - By default many Group Policy settings are not defined. If you define them, they will override other settings in Windows, and prevent you from changing them in other locations.

- Group Policy contains far too many settings to list, but a few high level examples include Logon settings, Remote Desktop settings, Windows Update, Windows Defender, Windows Firewall, Internet settings, and scripts that run automatically.

- Group Policy settings are also used to lock down a computer by limiting access to applications and features, or installing unapproved software.

  - This is typically done when setting kiosks or other specific purposes when the users may not be entirely trustworthy.

Slide 34



Local Group Policy

- Example 1: Turning off Remote Desktop
  - Leave Group Policy Editor open
  - Open the run dialog by typing **Win + r**
  - Type **sysdm.cpl** and press **Enter**
  - Click on the tab labeled **Remote**
- Notice that Remote Desktop is enabled
- Do Not change this setting
- Click Cancel

System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

OK | Cancel | Apply

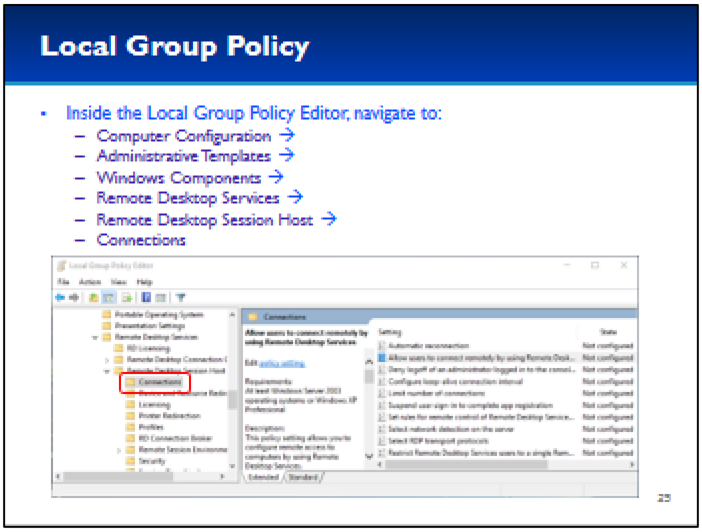
- Let’s demonstrate this by turning off Remote Desktop via the Local Group Policy.

- But first, we will verify that remote desktop is on from the System Properties window.

- Leave the Local Group Policy Editor open since we will go back to it on the next slide.

- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- To open, type **sysdm.cpl**.
- Press **Enter** or click OK.
- Notice that Remote desktop is enabled.
- Don’t make any changes here, and click Cancel to close the System Properties window.

Slide 35



Local Group Policy

- Inside the Local Group Policy Editor, navigate to:
  - Computer Configuration →
  - Administrative Templates →
  - Windows Components →
  - Remote Desktop Services →
  - Remote Desktop Session Host →
  - Connections

Allow users to connect remotely by using Remote Desktop Services

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
This policy setting allows you to configure remote access to computers by using Remote Desktop Services.

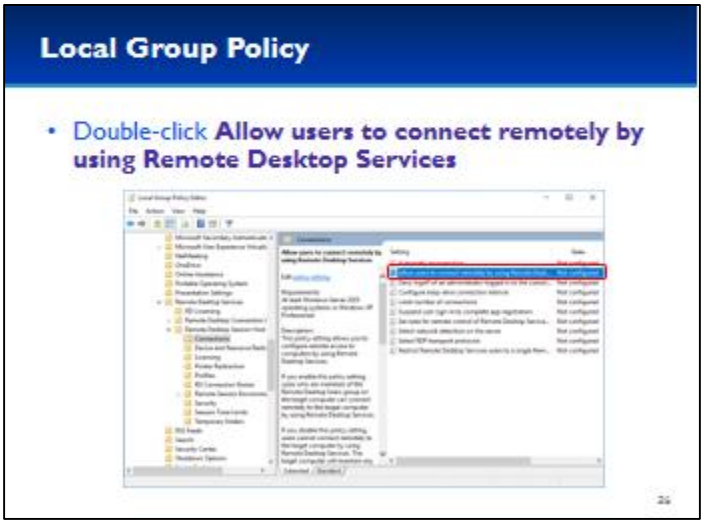
Setting	State
Automatic reconnection	Not configured
Allow users to connect remotely by using Remote Desk...	Not configured
Deny logoff of an administrator logged in to the consol...	Not configured
Configure keep-alive connection interval	Not configured
Limit number of connections	Not configured
Suspend user sign-in to complete app registration	Not configured
Set rules for remote control of Remote Desktop Service...	Not configured
Select network detection on the server	Not configured
Select RDP transport protocols	Not configured
Restrict Remote Desktop Services users to a single Rem...	Not configured

25

- Navigate to **Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections**.

☆Give the students a few seconds to navigate to this location.

Slide 36



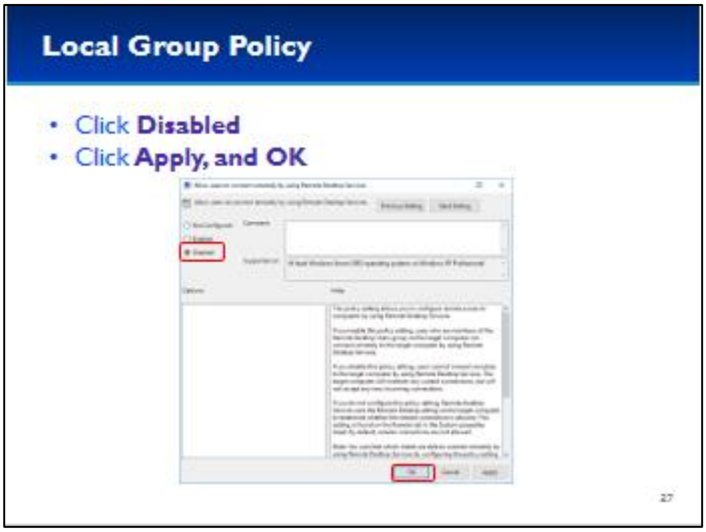
Local Group Policy

- Double-click **Allow users to connect remotely by using Remote Desktop Services**

36

- Double-click the Setting Allow users to connect remotely by using Remote Desktop Services.

Slide 37



Local Group Policy

- Click **Disabled**
- Click **Apply, and OK**

- Under Help there is a description of this policy:

  - Enabling this policy lets members of the Remote Desktop Users group log on remotely.

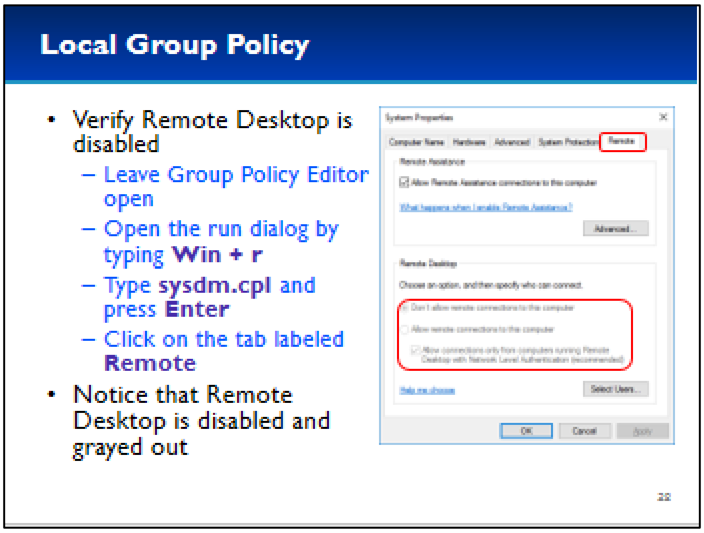
  - Disabling this policy prevents users from connecting remotely.

  - Not Configured allows this setting to be configured using the Remote tab in the System Properties window.

- Select Disabled.

- Click OK to apply the changes and close the Properties window.

Slide 38



Local Group Policy

- Verify Remote Desktop is disabled
  - Leave Group Policy Editor open
  - Open the run dialog by typing **Win + r**
  - Type **sysdm.cpl** and press **Enter**
  - Click on the tab labeled **Remote**
- Notice that Remote Desktop is disabled and grayed out

System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

● Don't allow remote connections to this computer

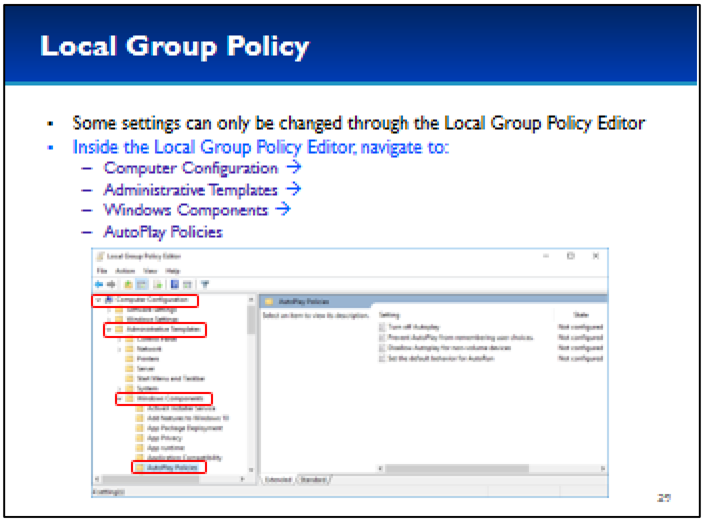
○ Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

- Leave the Group Policy Editor open and open the System Properties window.
- Make sure you open a new System Properties window, if you left the old window open, the changes may not be visible.
- Under the Remote tab, we can see that Remote Desktop is disabled. Additionally, the settings are greyed out and cannot be changed.

Slide 39



Local Group Policy

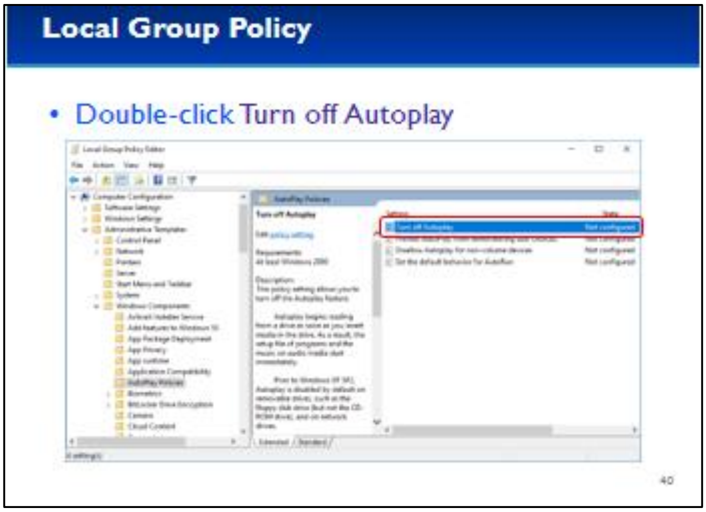
- Some settings can only be changed through the Local Group Policy Editor
- Inside the Local Group Policy Editor, navigate to:
  - Computer Configuration →
  - Administrative Templates →
  - Windows Components →
  - AutoPlay Policies

Setting	State
Turn off Autoplay	Not configured
Prevent AutoPlay from remembering user choices.	Not configured
Disallow Autoplay for non-volume devices	Not configured
Set the default behavior for AutoRun	Not configured

- Some settings can only be changed using the Local Group Policy Editor.

- For example, navigate to Computer Configuration → Administrative Templates → Windows Components → AutoPlay Policies.

Slide 40



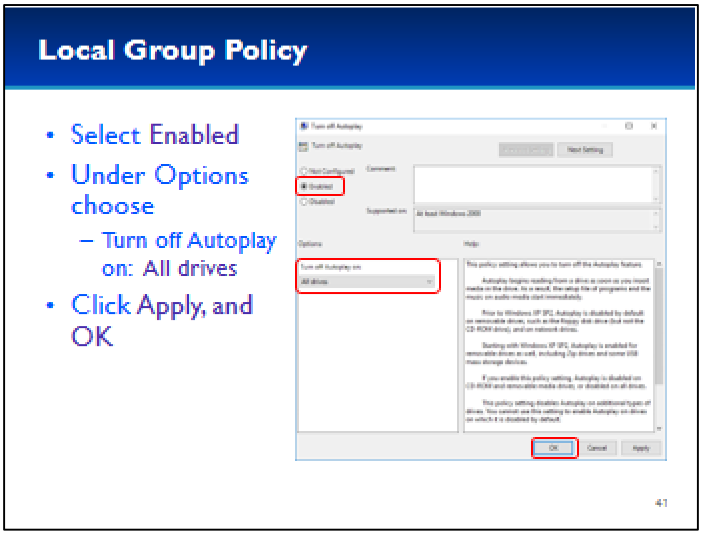
Local Group Policy

- Double-click Turn off Autoplay

- AutoPlay can be a security risk, and our company has no documented business need for it, so we should turn it off.

- Double-click the Setting Turn off Autoplay.

Slide 41



Local Group Policy

- Select Enabled
- Under Options choose
  - Turn off Autoplay on: All drives
- Click Apply, and OK

Turn off Autoplay

Turn off Autoplay

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Turn off Autoplay on:
All drives

Help:

This policy setting allows you to turn off the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.

Prior to Windows XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

Starting with Windows XP SP2, Autoplay is enabled for removable drives as well, including Zip drives and some USB mass storage devices.

If you enable this policy setting, Autoplay is disabled on CD-ROM and removable media drives, or disabled on all drives.

This policy setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default.

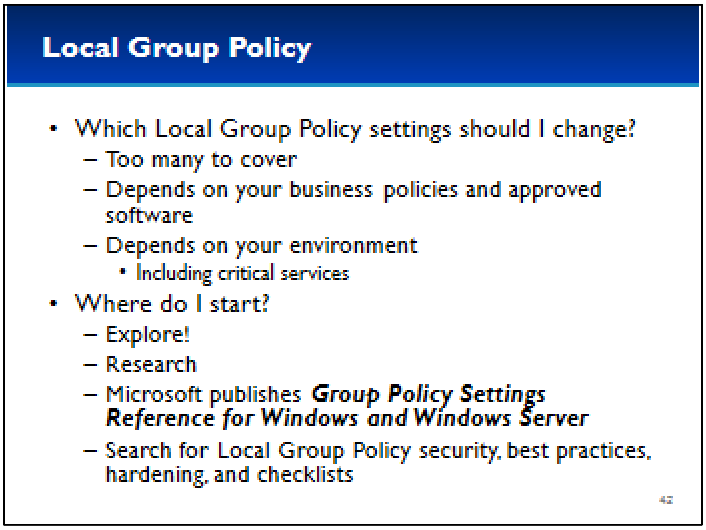
41

- Briefly read the Help section.

☆Give the students a few seconds:

- Select Enabled.
- Under Options ensure that Turn off Autoplay is set to All drives.
- Click Apply and OK to apply the settings and close the Properties window.

Slide 42



Local Group Policy

- Which Local Group Policy settings should I change?
  - Too many to cover
  - Depends on your business policies and approved software
  - Depends on your environment
    - Including critical services
- Where do I start?
  - Explore!
  - Research
  - Microsoft publishes ***Group Policy Settings Reference for Windows and Windows Server***
  - Search for Local Group Policy security, best practices, hardening, and checklists

42

- There are so many Group Policy settings, you may be wondering which ones you should change.

- The answer really depends on your business policies and your environment, including any critical services.

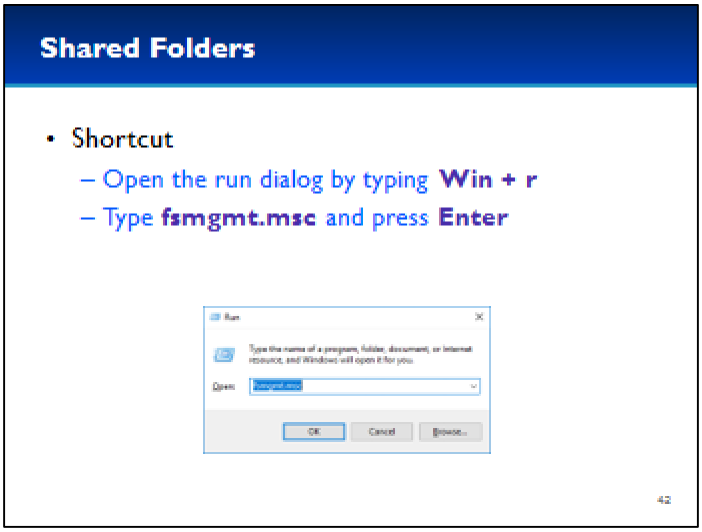
- There are too many settings to cover here, so it's up to you explore and research.

- Read the help sections for the different policies.

- Microsoft publishes a reference Excel spreadsheet online. You can search for "Group Policy Settings Reference for Windows and Windows Server."

- Research online and look for Group Policy best practices, hardening, and checklists.

Slide 43



Shared Folders

- Shortcut
  - Open the run dialog by typing **Win + r**
  - Type **fsmgmt.msc** and press **Enter**

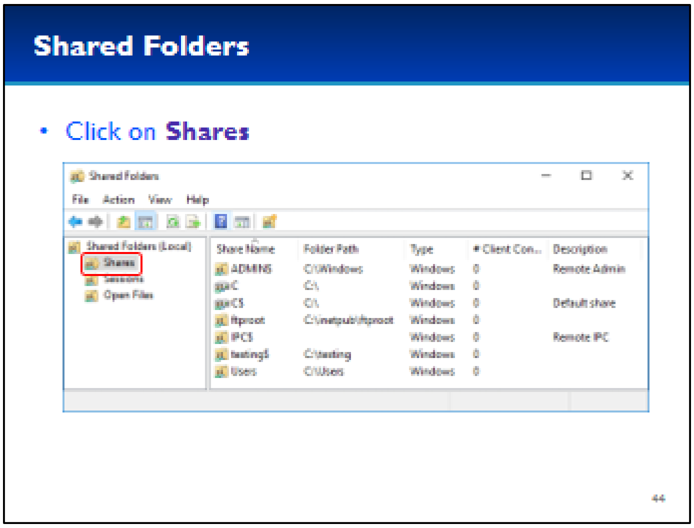
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: fsmgmt.msc

- Undocumented or unauthorized shares can be a security vulnerability.
- The Shared folders MMC plugin can help us analyze the current shares on the system.
- Open the run dialog box by holding down the **Windows key** and pressing the letter **r**.
- To open, type **fsmgmt.msc**.
- Press **Enter** or click OK.

Slide 44



Shared Folders

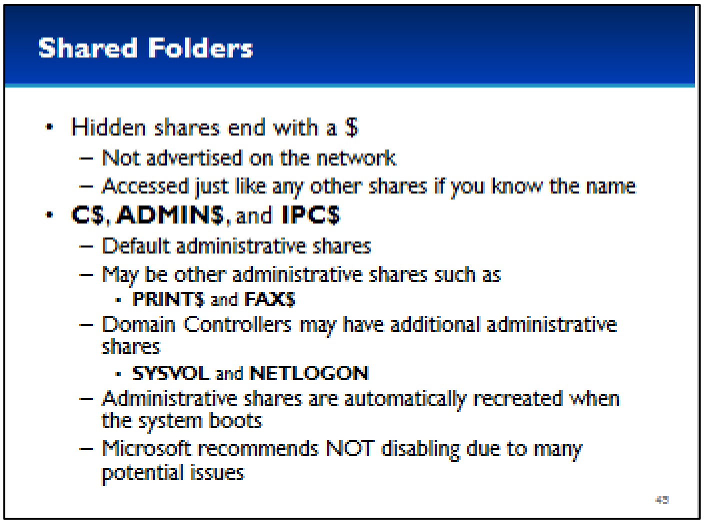
- Click on **Shares**

Share Name	Folder Path	Type	# Client Con...	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C	C:\	Windows	0	
C$	C:\	Windows	0	Default share
ftproot	C:\inetpub\ftproot	Windows	0	
IPC$		Windows	0	Remote IPC
testing$	C:\testing	Windows	0	
Users	C:\Users	Windows	0	

44

- Click on **Shares**.
- The Share Name is the name you would use when accessing the share over the network.
- The Folder Path is the path of the folder that is being shared.
- Additionally, Shared Folders displays the type of share, number of client connections, and an optional description of the share.

Slide 45



Shared Folders

- Hidden shares end with a $
  - Not advertised on the network
  - Accessed just like any other shares if you know the name
- **C$**, **ADMIN$**, and **IPC$**
  - Default administrative shares
  - May be other administrative shares such as
    - **PRINT$** and **FAX$**
  - Domain Controllers may have additional administrative shares
    - **SYSVOL** and **NETLOGON**
  - Administrative shares are automatically recreated when the system boots
  - Microsoft recommends NOT disabling due to many potential issues

45

- You are probably wondering what all these shares are.
- Hidden shares end with a $.

  - Hidden shares can be accessed just like a regular share, but they are not advertised on the network.

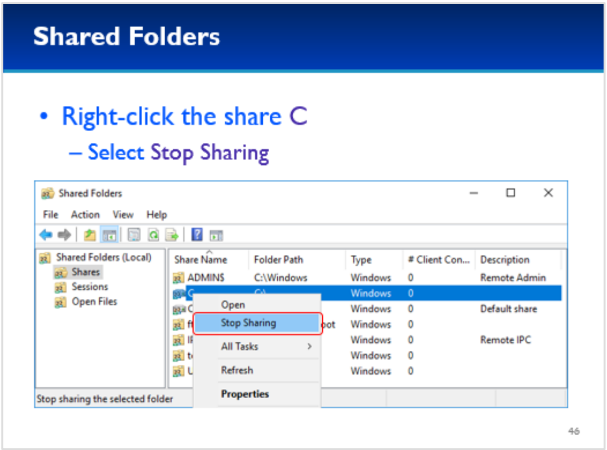
- The C$, ADMIN$, and IPC$ shares are default administrative shares created automatically by Windows.
- On some computers there may be additional default administrative shares such as PRINT$ or FAX$, and Domain Controllers may have even more default administrative shares such as SYSVOL and NETLOGON.

  - Notice that these default administrative shares do not end with $, and are not hidden.

- While it is possible to delete the default administrative shares, Windows automatically recreates the shares when the system boots.
- It is possible to prevent the creation of default administrative shares, but this is not covered here since Microsoft very strongly recommends against this.

  - https://support.microsoft.com/en-us/help/842715/overview-of-problems-that-may-occur-when-administrative-shares-are-missing

Slide 46



Shared Folders

- Right-click the share C
  - Select Stop Sharing

Share Name	Folder Path	Type	# Client Con...	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C	C:\	Windows	0	
C		Windows	0	Default share
f	oot	Windows	0	
I		Windows	0	Remote IPC
t		Windows	0	
U		Windows	0	

Stop sharing the selected folder

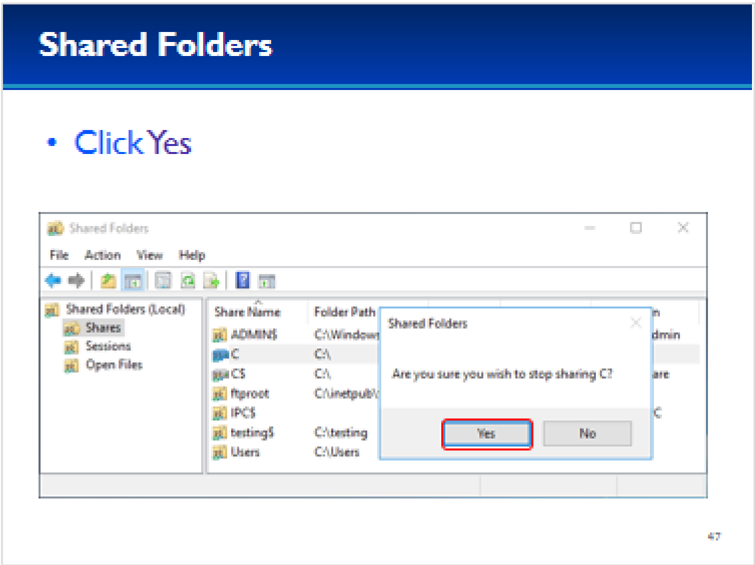
46

- Using Shared folders it is relatively simple to Stop Sharing the C drive.

- Right-click the C share and select Stop Sharing.

  - Make sure not to stop sharing the default administrative share C$.

Slide 47



Shared Folders

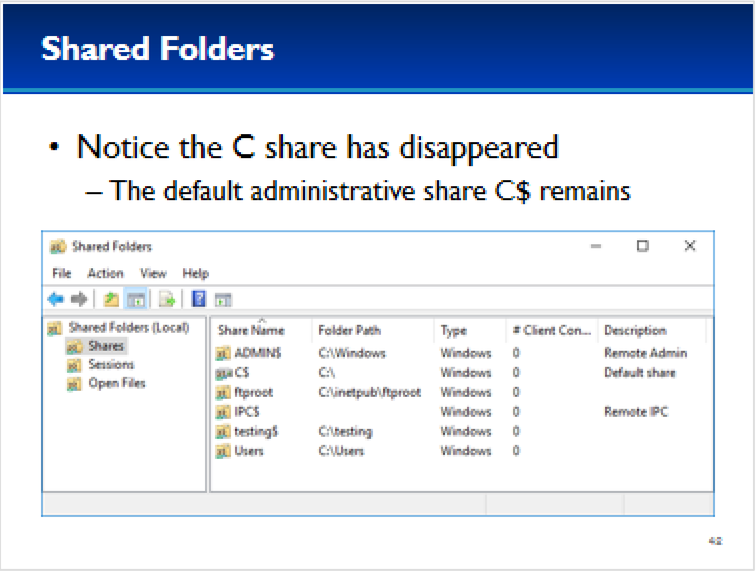
- Click Yes

Share Name	Folder Path	n
ADMIN$	C:\Window	dmin
C	C:\	
C$	C:\	are
ftproot	C:\inetpub\	
IPC$		C
testing$	C:\testing	
Users	C:\Users	

Are you sure you wish to stop sharing C?

- Windows will prompt you to confirm. Click Yes.

Slide 48



Shared Folders

- Notice the C share has disappeared
  - The default administrative share C$ remains

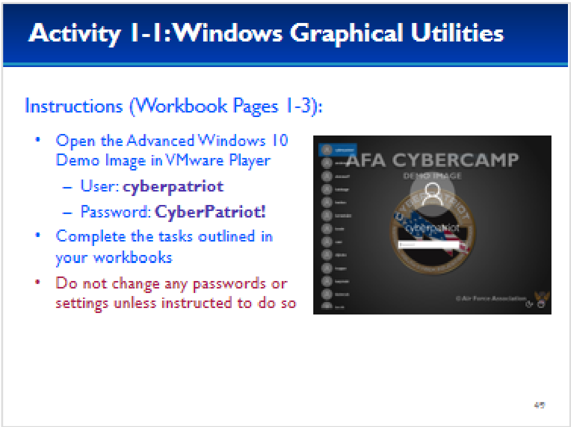
Share Name	Folder Path	Type	# Client Con...	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
ftproot	C:\inetpub\ftproot	Windows	0	
IPC$		Windows	0	Remote IPC
testing$	C:\testing	Windows	0	
Users	C:\Users	Windows	0	

42

- After confirming, The C share has been deleted.

  - Notice that the default administrative share C$ is still present.

Slide 49



Activity 1-1: Windows Graphical Utilities

Instructions (Workbook Pages 1-3):

- Open the Advanced Windows 10 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

49

◷ Give students about 20 minutes to complete the tasks listed on pages 1-3 of their Workbooks.

☆This lab will review the Local Security Policy, Local Group Policy Editor, and Shared Folders.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case they get locked out.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. Secpol.msc
2. Babbage
3. -
4. Administrators
5. -
6. Enabled
7. -
8. Gpedit.msc
9. Under Administrative Templates, System, Logon, Show first sign-in animation is Disabled. Under Adminstrative Templates, Windows Components, Windows Update, Configure Automatic Updates is Disabled
10. 1) Administrative Templates, System, Logon, Do not display network selection UI is Enabled;
    2) Administrative Templates, Windows Components, Delivery Optimization, Download Mode is Enabled;
    3) Administrative Templates, Control Panel, Personalization, Force a specific default lock screen and logon image is Enabled;
    4) Administrative Templates, Windows Components, OneDrive, Prevent the usage of OneDrive for file storage is Enabled;
    5) Administrative Templates, Windows Components, Windows Defender, Turn off Windows Defender is Enabled
11. fsmgmt.msc
12. ADMIN$, C$, IPC$
13. testing$
14. -

Slide 50

Windows Command Line

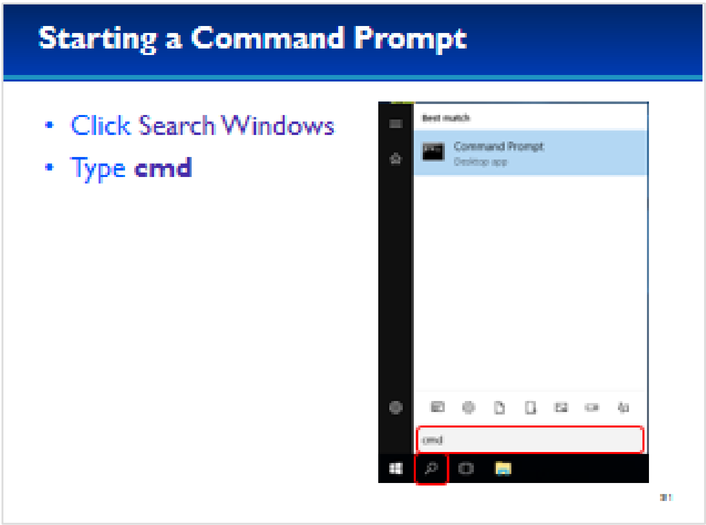
🕒 Devote 30 minutes to Slides 51-89. Allow the students 20 minutes to complete the activity on Slide 90.

☆Throughout this section, students should follow along in the **Advanced Windows 10 Demo Image**.

☆Actions the students are supposed to take are highlighted in blue and purple.

☆Purple indicates exact text they are supposed to type or GUI elements they should interact with.

Slide 51

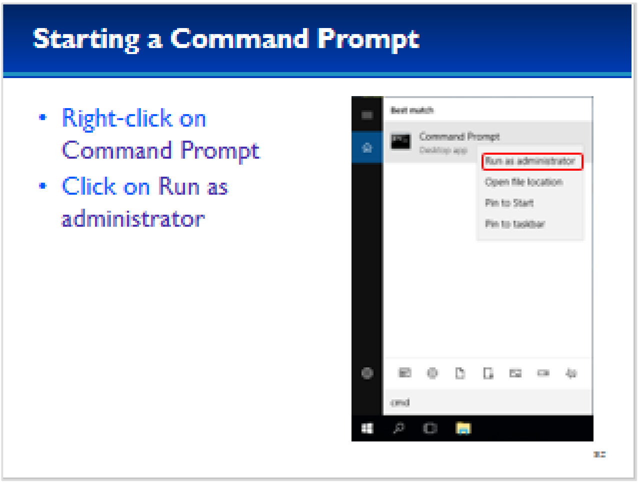


Starting a Command Prompt

- Click Search Windows
- Type **cmd**

- For this section we will need to open a command prompt as administrator in order to make full use of the commands we will be learning about.
- Click Search Windows (the magnifying glass next to the Start button).
- Type **cmd** but don’t press Enter.

Slide 52

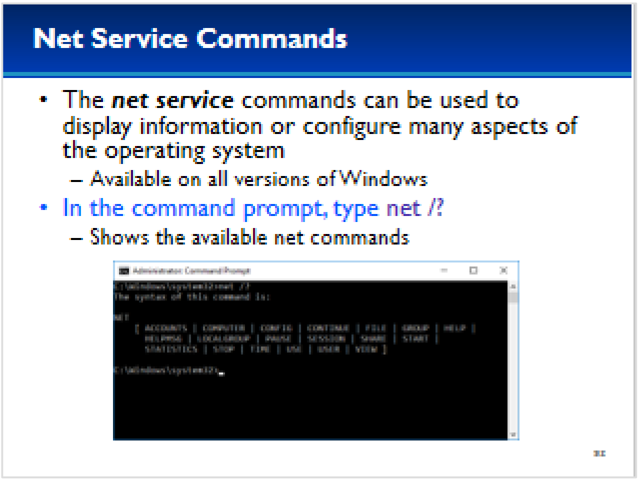


Starting a Command Prompt

- Right-click on Command Prompt
- Click on Run as administrator

- Right-click on Command Prompt and select Run as administrator.
- UAC will ask you if you want to allow this app to make changes to your device.
- Click Yes to continue.

Slide 53



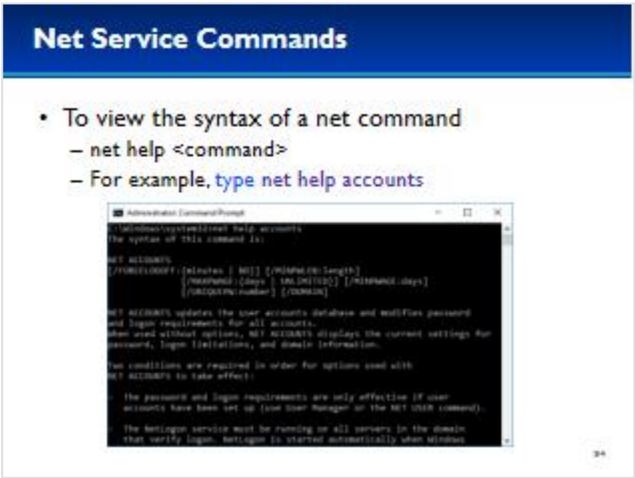
Net Service Commands

- The ***net service*** commands can be used to display information or configure many aspects of the operating system
  - Available on all versions of Windows
- In the command prompt, type net /?
  - Shows the available net commands

```
C:\Windows\system32>net /?
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Windows\system32>_
```

- The Net Service suite of commands can be used to configure or display information about the current configuration of the operating system.
- In the command prompt type: **net /?**
- As you can see, there are many different **net** commands available. We will only be covering a few of the most important ones today.
- Remember, in Windows, capitalization usually does not matter. The net commands can be typed as uppercase or lowercase, it makes no difference.

Slide 54



Net Service Commands

- To view the syntax of a net command
  - net help <command>
  - For example, type net help accounts

```
C:\Windows\system32>net help accounts
The syntax of this command is:

NET ACCOUNTS
[/FORCELOGOFF:{minutes | NO}] [/MINPWLEN:length]
              [/MAXPWAGE:{days | UNLIMITED}] [/MINPWAGE:days]
              [/UNIQUEPW:number] [/DOMAIN]

NET ACCOUNTS updates the user accounts database and modifies password
and logon requirements for all accounts.
When used without options, NET ACCOUNTS displays the current settings for
password, logon limitations, and domain information.

Two conditions are required in order for options used with
NET ACCOUNTS to take effect:

-  The password and logon requirements are only effective if user
   accounts have been set up (use User Manager or the NET USER command).

-  The Netlogon service must be running on all servers in the domain
   that verify logon. Netlogon is started automatically when Windows
```

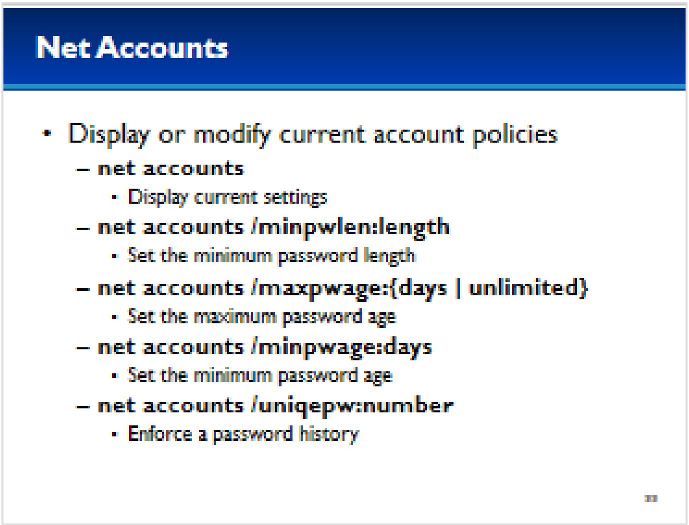
- The first command we are going to cover is **net accounts**.

- To display the syntax of the different **net** commands you can use the help command.

- Type **net help accounts** now to display the syntax for the accounts command.

- Take a minute to scroll up and down examining the output.

Slide 55



Net Accounts

- Display or modify current account policies
  - **net accounts**
    - Display current settings
  - **net accounts /minpwlen:length**
    - Set the minimum password length
  - **net accounts /maxpwage:{days | unlimited}**
    - Set the maximum password age
  - **net accounts /minpwage:days**
    - Set the minimum password age
  - **net accounts /uniqepw:number**
    - Enforce a password history

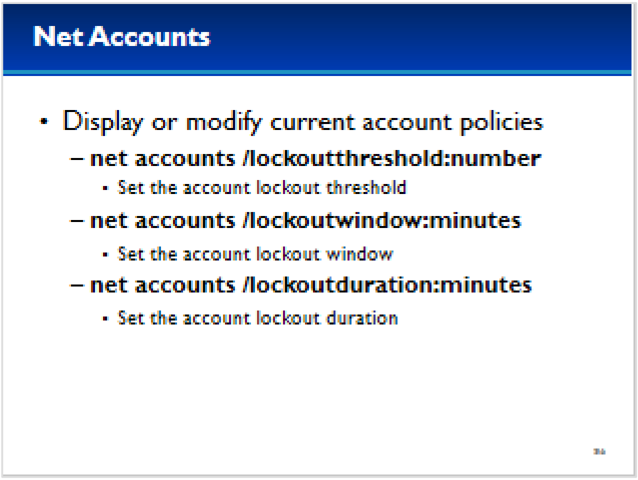
- We’re not going to cover everything the **net accounts** command can do, but here are is the syntax of some of the important operations.

- Running **net accounts** with no additional parameters will display the current settings.

- **Net accounts** can also be used to set the minimum password length, the maximum password age, and the minimum password age.

- Additionally, **net accounts** can be used to enforce a password history, preventing users from using the same password for a number of password changes.

Slide 56



Net Accounts

- Display or modify current account policies
  - net accounts /lockoutthreshold:number
    - Set the account lockout threshold
  - net accounts /lockoutwindow:minutes
    - Set the account lockout window
  - net accounts /lockoutduration:minutes
    - Set the account lockout duration

- Although it is not described in the help, **net accounts** can also set account lockout settings including the lockout threshold, lockout duration, and lockout window.

☆Stress that the students should not set the lockout threshold to a value less than five when participating in the competition on Friday to prevent locking themselves out while competing.

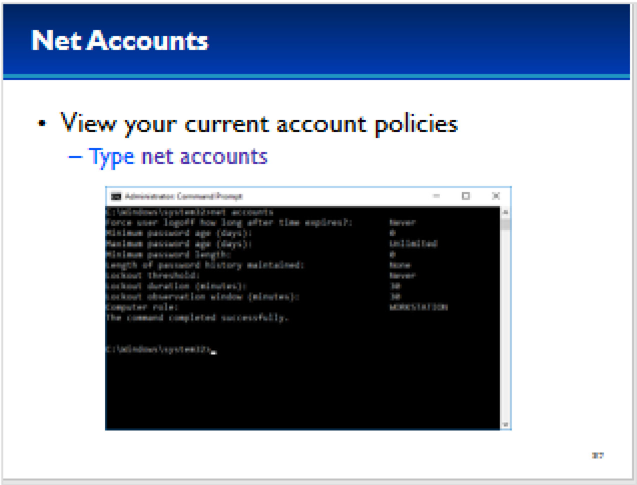
☆These settings were described in the basic class, but we will provide a brief description in case more elaboration is needed.

☆Lockout threshold is the number of invalid login attempts before the account is locked out; Microsoft recommends setting this to between 5-50 inclusive (https://technet.microsoft.com/en-us/library/hh994574(v=ws.11).aspx)

☆Lockout window is the amount of time after a failed login attempt before the lockout threshold counter is reset; Microsoft recommends setting this to approximately 30 (https://technet.microsoft.com/en-us/library/hh994568(v=ws.11).aspx)

☆Lockout duration is the amount of time that the account remains locked out; Microsoft recommends setting this to approximately 30 (https://technet.microsoft.com/enus/library/hh994569(v=ws.11).aspx)

Slide 57



Net Accounts

- View your current account policies
  - Type net accounts

```
C:\Windows\system32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          Unlimited
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.


C:\Windows\system32>
```

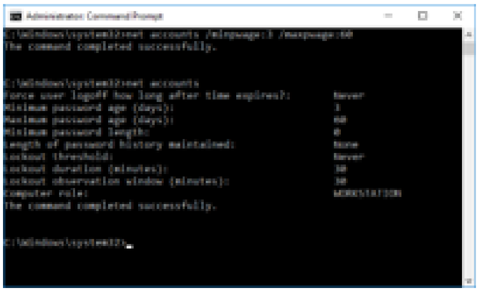
57

- Type **net accounts** to view the current settings.
- This computer currently has no password policy or account lockout policy.

Slide 58

Net Accounts

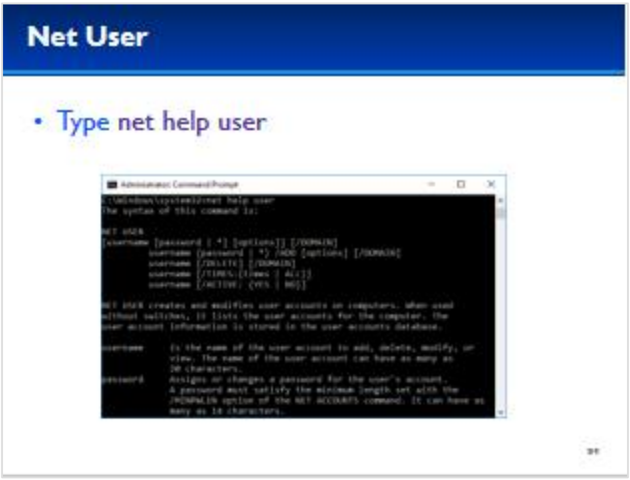
- Set a minimum and maximum password age
  - Type net accounts /minpwage:3 /maxpwage:60
  - To verify, type net accounts



```
C:\Windows\system32>net accounts /minpwage:3 /maxpwage:60
The command completed successfully.


C:\Windows\system32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          3
Maximum password age (days):                          60
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.


C:\Windows\system32>
```

- This computer needs a more secure password policy.
- Type **net accounts /minpwage:3 /maxpwage:60** and press **Enter**.
- This sets a minimum password age of three and a maximum password age of 60.
- Type **net accounts** again to verify the settings.

Slide 59



Net User

- Type net help user

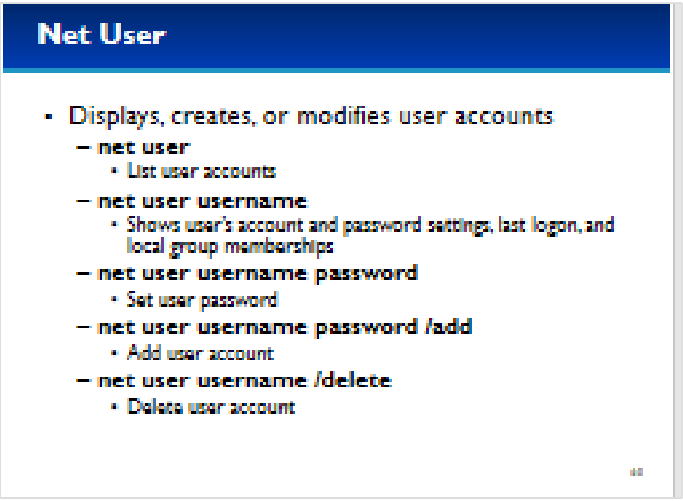
```
C:\Windows\system32>net help user
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]

NET USER creates and modifies user accounts on computers. When used
without switches, it lists the user accounts for the computer. The
user account information is stored in the user accounts database.

username     Is the name of the user account to add, delete, modify, or
             view. The name of the user account can have as many as
             20 characters.
password     Assigns or changes a password for the user's account.
             A password must satisfy the minimum length set with the
             /MINPWLEN option of the NET ACCOUNTS command. It can have as
             many as 14 characters.
```

59

- Now we are going to cover the **net user** command.

- Type **net help user** to display the help for the **net user** command.

Slide 60



Net User

- Displays, creates, or modifies user accounts
  - net user
    - List user accounts
  - net user username
    - Shows user’s account and password settings, last logon, and local group memberships
  - net user username password
    - Set user password
  - net user username password /add
    - Add user account
  - net user username /delete
    - Delete user account

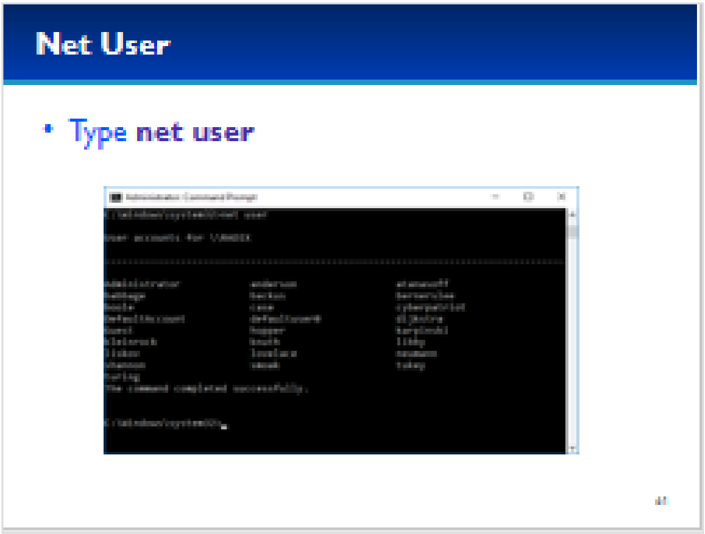
60

- **Net user** will list the current user accounts on the system, including accounts that may be hidden from Control Panel User Management.

  - These are the same users shown on the Local Users and Groups MMC plugin.

- **Net user** can be used to add or remove users, change user passwords, and see the last logon date and time as well as account and password settings.

Slide 61



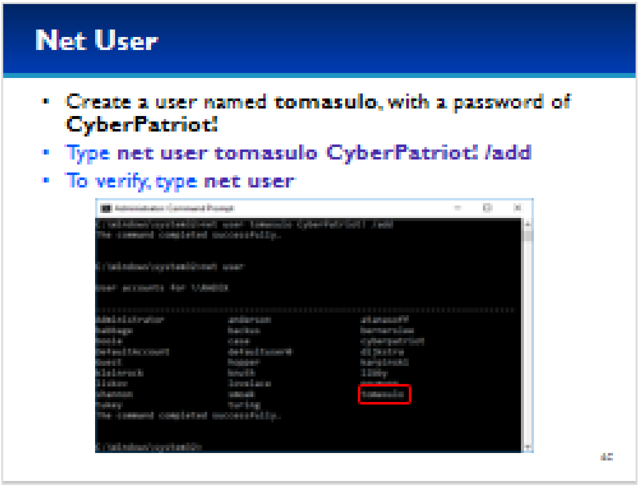
Net User

- Type **net user**

```
C:\Windows\system32>net user

User accounts for \\RADIX

-------------------------------------------------------------------------------
Administrator            anderson                 atanasoff
babbage                  backus                   bernerslee
boole                    case                     cyberpatriot
DefaultAccount           defaultuser0             dijkstra
Guest                    hopper                   karpinski
kleinrock                knuth                    libby
liskov                   lovelace                 neumann
shannon                  smook                    tokey
turing
The command completed successfully.


C:\Windows\system32>
```

- Type **net user** to display current user accounts.

Slide 62



Net User

- Create a user named tomasulo, with a password of CyberPatriot!
- Type net user tomasulo CyberPatriot! /add
- To verify, type net user

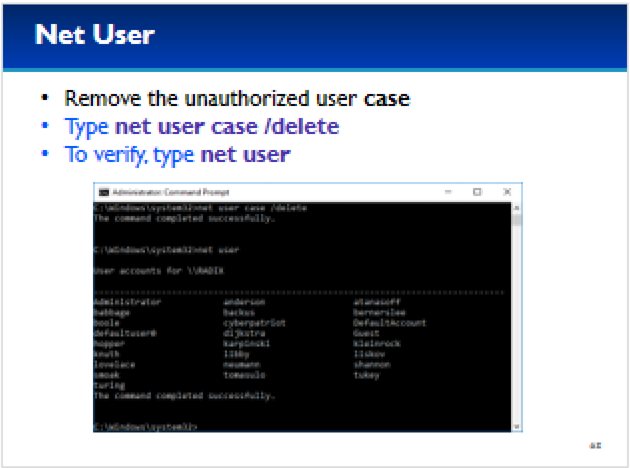
```
C:\Windows\system32>net user tomasulo CyberPatriot! /add
The command completed successfully.


C:\Windows\system32>net user

User accounts for \\[illegible]

-------------------------------------------------------------------------------
Administrator            anderson                 atanasoff
babbage                  backus                   bernerslee
boole                    case                     cyberpatriot
DefaultAccount           defaultuser0             dijkstra
Guest                    hopper                   karpinski
kleinrock                knuth                    lamport
liskov                   lovelace                 [illegible]
shannon                  [illegible]              tomasulo
tukey                    turing
The command completed successfully.


C:\Windows\system32>
```

46

- Let's create a new user named tomasulo with a password of CyberPatriot!
- Type: **net user tomasulo CyberPatriot! /add**
- Next, type **net user** in order to verify that we created the account.

☆Robert Tomasulo created a hardware algorithm allowing for dynamic out of order execution of computer commands, derivatives of this algorithm are present in most modern processers, this algorithm is commonly referred to as Tomasulo's algorithm.

Slide 63



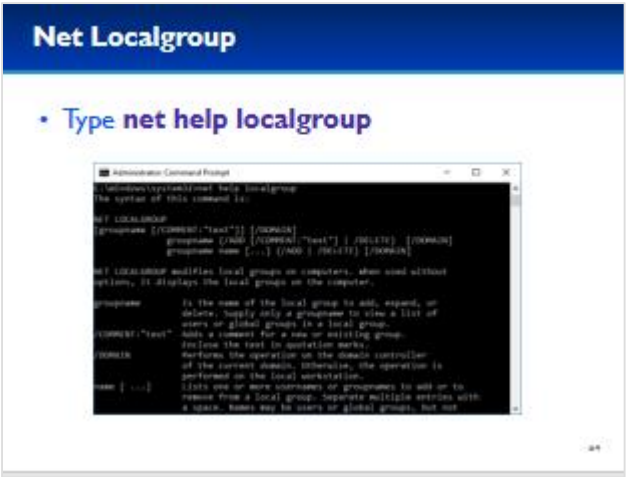
Net User

- Remove the unauthorized user case
- Type **net user case /delete**
- To verify, type **net user**

```
C:\Windows\system32>net user case /delete
The command completed successfully.


C:\Windows\system32>net user

User accounts for \\RADIX

-------------------------------------------------------------------------------
Administrator            anderson                 atanasoff
babbage                  backus                   bernerslee
boole                    cyberpatriot             DefaultAccount
defaultuser0             dijkstra                 Guest
hopper                   karpinski                kleinrock
knuth                    libby                    liskov
lovelace                 neumann                  shannon
smoak                    tomasulo                 tukey
turing
The command completed successfully.


C:\Windows\system32>
```

- The user case is unauthorized.
- Type: **net user case /delete**
- To verify the user was deleted, type: **net user**

Slide 64



Net Localgroup

- Type **net help localgroup**

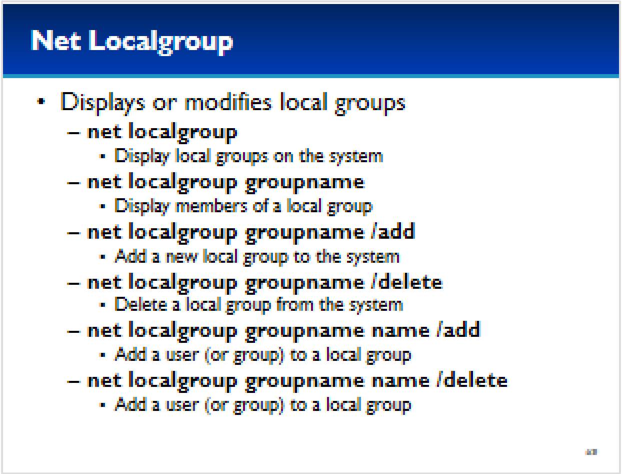
```
C:\Windows\system32>net help localgroup
The syntax of this command is:

NET LOCALGROUP
[groupname [/COMMENT:"text"]] [/DOMAIN]
              groupname {/ADD [/COMMENT:"text"] | /DELETE}  [/DOMAIN]
              groupname name [...] {/ADD | /DELETE} [/DOMAIN]

NET LOCALGROUP modifies local groups on computers. When used without
options, it displays the local groups on the computer.

groupname        Is the name of the local group to add, expand, or
                 delete. Supply only a groupname to view a list of
                 users or global groups in a local group.
/COMMENT:"text"  Adds a comment for a new or existing group.
                 Enclose the text in quotation marks.
/DOMAIN          Performs the operation on the domain controller
                 of the current domain. Otherwise, the operation is
                 performed on the local workstation.
name [ ...]      Lists one or more usernames or groupnames to add or to
                 remove from a local group. Separate multiple entries with
                 a space. Names may be users or global groups, but not
```

64

- The next command we are going to cover is the **net localgroup** command.

- Type **net help localgroup** to view the command syntax for the **net localgroup** command.

Slide 65



Net Localgroup

- Displays or modifies local groups
  - **net localgroup**
    - Display local groups on the system
  - **net localgroup groupname**
    - Display members of a local group
  - **net localgroup groupname /add**
    - Add a new local group to the system
  - **net localgroup groupname /delete**
    - Delete a local group from the system
  - **net localgroup groupname name /add**
    - Add a user (or group) to a local group
  - **net localgroup groupname name /delete**
    - Add a user (or group) to a local group

- Just like **net user**, **net localgroup** can display or modify local groups.

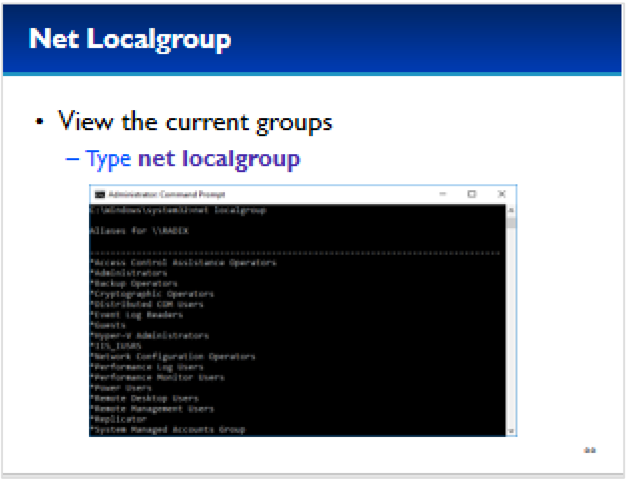
  - These are the same users shown on the Local Users and Groups MMC plugin.

- **Net localgroup** with no options will display the current local groups on the system.

- **Net localgroup** can add or delete groups.

- Additionally, **net localgroup** can add or remove users or groups from existing groups.

Slide 66



Net Localgroup

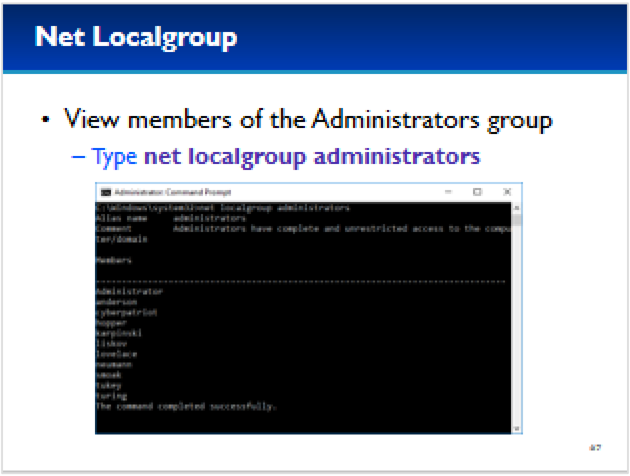
- View the current groups
  - Type **net localgroup**

Administrator: Command Prompt

```
C:\Windows\system32>net localgroup

Aliases for \\RADIX

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
```

- View the current groups on the system by typing: **net localgroup**

Slide 67



Net Localgroup

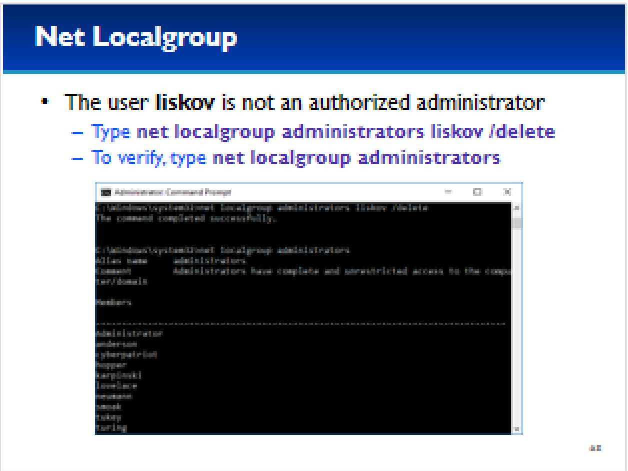
- View members of the Administrators group
  - Type **net localgroup administrators**

```
C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
anderson
cyberpatriot
hopper
karpinski
liskov
lovelace
neumann
smoak
tukey
turing
The command completed successfully.
```

67

- View the members of the Administrators group by typing: **net localgroup administrators**

Slide 68



Net Localgroup

- The user **liskov** is not an authorized administrator
  - Type **net localgroup administrators liskov /delete**
  - To verify, type **net localgroup administrators**

```
C:\Windows\system32>net localgroup administrators liskov /delete
The command completed successfully.


C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
anderson
cyberpatriot
hopper
karpinski
lovelace
neumann
smoak
tukey
turing
```

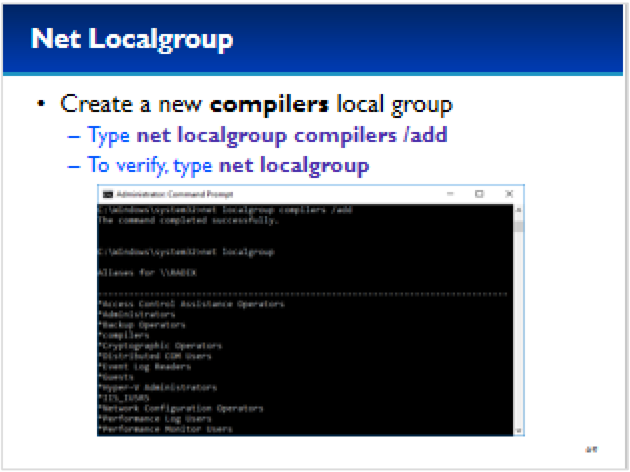
- The user liskov is not an authorized administrator and should be removed from the Administrators group.

- Type **net localgroup administrators liskov /delete** and press **Enter**.

- Next, type **net localgroup administrators** to verify that liskov is no longer in the Administrators group.

☆Barbara Liskov created the Argus programming language at MIT, a groundbreaking high-level programming language designed to support the development of distributed programs (She became one of the first women to receive a Ph.D. in computer science in 1968 from Stanford University).

Slide 69



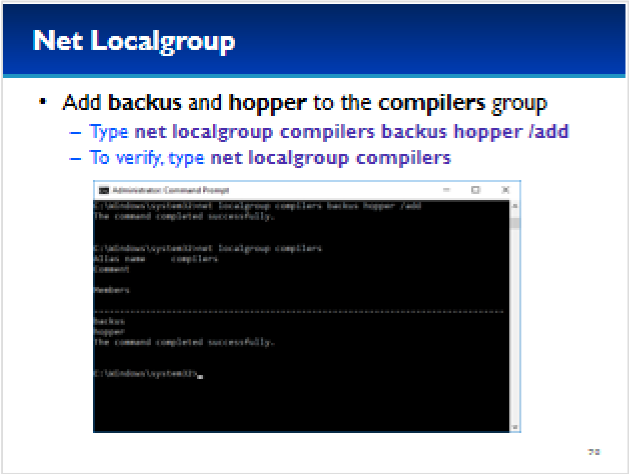
Net Localgroup

- Create a new **compilers** local group
  - Type **net localgroup compilers /add**
  - To verify, type **net localgroup**

```
C:\Windows\system32>net localgroup compilers /add
The command completed successfully.


C:\Windows\system32>net localgroup

Aliases for \\[illegible]

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*compilers
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
```

- Use **net localgroup** to create a new compilers group.
- Type: **net localgroup compilers /add**
- To verify the new group has been created, type: **net localgroup**

Slide 70



Net Localgroup

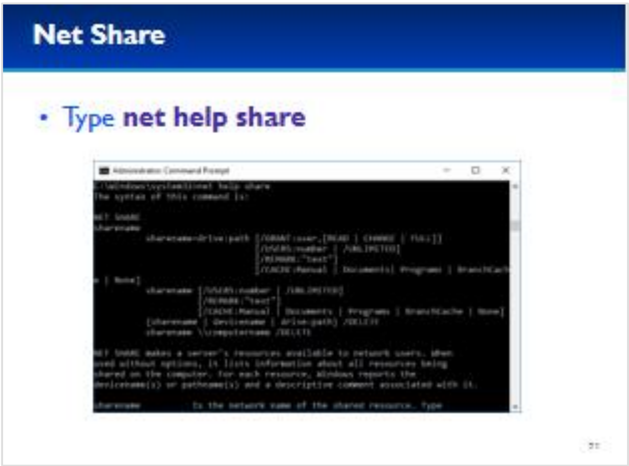
- Add **backus** and **hopper** to the **compilers** group
  - Type **net localgroup compilers backus hopper /add**
  - To verify, type **net localgroup compilers**

```
C:\Windows\system32>net localgroup compilers backus hopper /add
The command completed successfully.


C:\Windows\system32>net localgroup compilers
Alias name     compilers
Comment

Members

-------------------------------------------------------------------------------
backus
hopper
The command completed successfully.


C:\Windows\system32>
```

70

- Now that the compilers group has been created, add the users backus and hopper.
- Type: **net localgroup compilers backus hopper /add**
- To verify that backus and hopper are in the compilers group, type: **net localgroup compilers**

Slide 71



Net Share

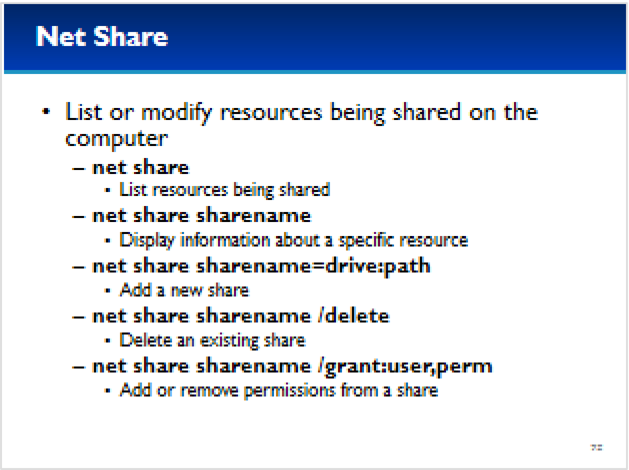
- Type **net help share**

```
C:\Windows\system32>net help share
The syntax of this command is:

NET SHARE
sharename
          sharename=drive:path [/GRANT:user,[READ | CHANGE | FULL]]
                               [/USERS:number | /UNLIMITED]
                               [/REMARK:"text"]
                               [/CACHE:Manual | Documents| Programs | BranchCach
e | None]
          sharename [/USERS:number | /UNLIMITED]
                    [/REMARK:"text"]
                    [/CACHE:Manual | Documents | Programs | BranchCache | None]
          {sharename | devicename | drive:path} /DELETE
          sharename \\computername /DELETE

NET SHARE makes a server's resources available to network users. When
used without options, it lists information about all resources being
shared on the computer. For each resource, Windows reports the
devicename(s) or pathname(s) and a descriptive comment associated with it.

sharename          Is the network name of the shared resource. Type
```

71

- The next command we are going to cover is the **net share** command.
- The **net share** command is similar to the Shared Folders MMC plugin covered in the last section.
- Type **net help share** to see the command syntax for **net share.**

Slide 72



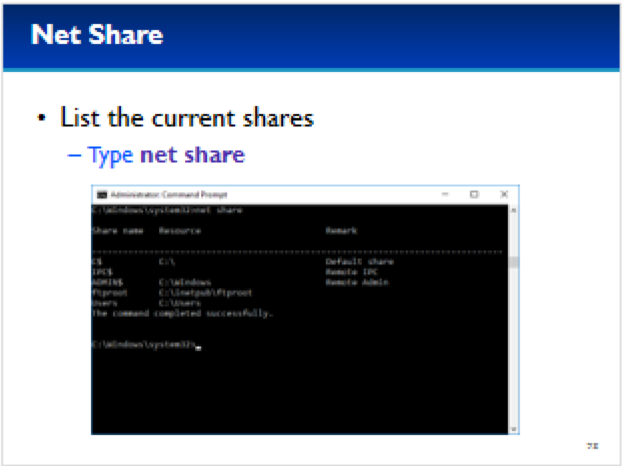
Net Share

- List or modify resources being shared on the computer
  - **net share**
    - List resources being shared
  - **net share sharename**
    - Display information about a specific resource
  - **net share sharename=drive:path**
    - Add a new share
  - **net share sharename /delete**
    - Delete an existing share
  - **net share sharename /grant:user,perm**
    - Add or remove permissions from a share

72

- **Net share** without any arguments lists the current resources being shared.
- **Net share** can also display information about a specific resource.
- It's also very simple to add or delete shares using **net share**.
- Share permissions can also be modified using the **grant** option.

Slide 73



Net Share

- List the current shares
  - Type **net share**

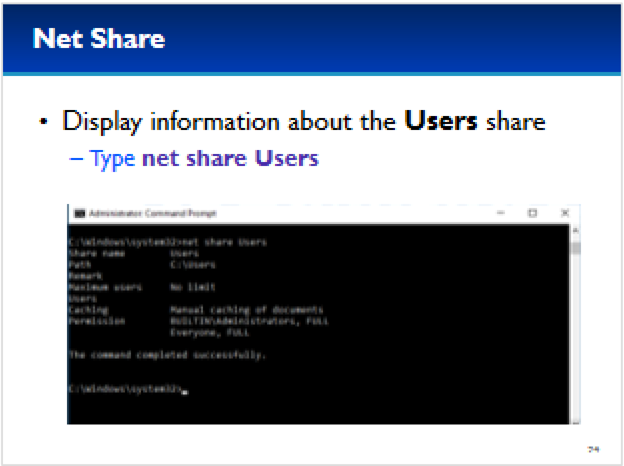
Administrator: Command Prompt

```
C:\Windows\system32>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
ftproot      C:\inetpub\ftproot
Users        C:\Users
The command completed successfully.


C:\Windows\system32>
```

73

- List the current shares by typing: **net share**
- Notice that this displays the same information as the Shared Folders MMC plugin.

Slide 74



Net Share

- Display information about the **Users** share
  - Type **net share Users**

```
C:\windows\system32>net share Users
Share name        Users
Path              C:\Users
Remark
Maximum users     No limit
Users
Caching           Manual caching of documents
Permission        BUILTIN\Administrators, FULL
                  Everyone, FULL

The command completed successfully.


C:\windows\system32>
```

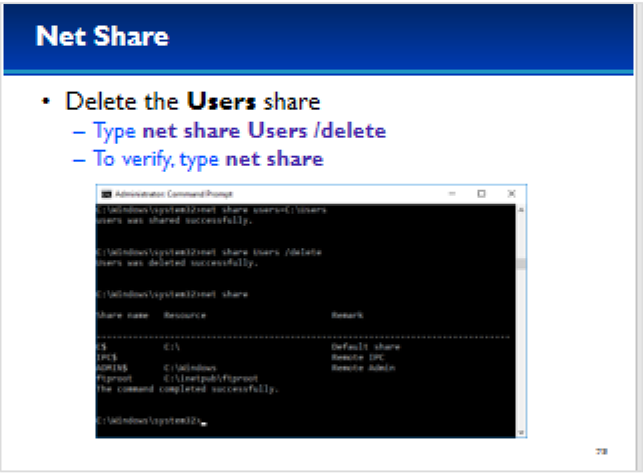
74

- Display information about the users share by typing: **net share Users**

  - Both Administrators and Everyone have full permission to access this share.

  - However, it is important to note that permissions are also dependent on the NTFS permissions of the C:\Users directory which are separate and not displayed by the **net share** command.

Slide 75



Net Share

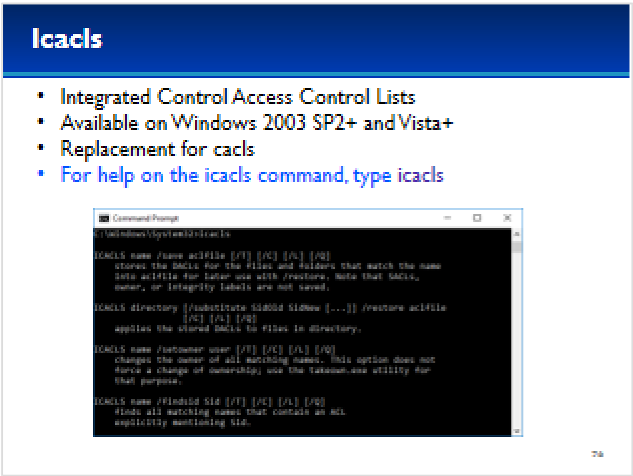
- Delete the **Users** share
  - Type **net share Users /delete**
  - To verify, type **net share**

```
C:\Windows\system32>net share users=C:\Users
users was shared successfully.


C:\Windows\system32>net share Users /delete
Users was deleted successfully.


C:\Windows\system32>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
ftproot      C:\inetpub\ftproot
The command completed successfully.


C:\Windows\system32>
```

78

- We don’t want to share the C:\Users directory on this computer.
- Delete the share by typing: **net share User /delete**
- Verify that the Users directory is no longer being shared by typing: **net share**

Slide 76



Icacls

- Integrated Control Access Control Lists
- Available on Windows 2003 SP2+ and Vista+
- Replacement for cacls
- For help on the icacls command, type icacls

Command Prompt

```
C:\Windows\System32>icacls

ICACLS name /save aclfile [/T] [/C] [/L] [/Q]
    stores the DACLs for the files and folders that match the name
    into aclfile for later use with /restore. Note that SACLs,
    owner, or integrity labels are not saved.

ICACLS directory [/substitute SidOld SidNew [...]] /restore aclfile
                 [/C] [/L] [/Q]
    applies the stored DACLs to files in directory.

ICACLS name /setowner user [/T] [/C] [/L] [/Q]
    changes the owner of all matching names. This option does not
    force a change of ownership; use the takeown.exe utility for
    that purpose.

ICACLS name /findsid Sid [/T] [/C] [/L] [/Q]
    finds all matching names that contain an ACL
    explicitly mentioning Sid.
```

76

- The **icacls** command stands for Integrated Control Access Control Lists and is available on Windows Server 2003 SP2 and later, and Windows Vista and later.

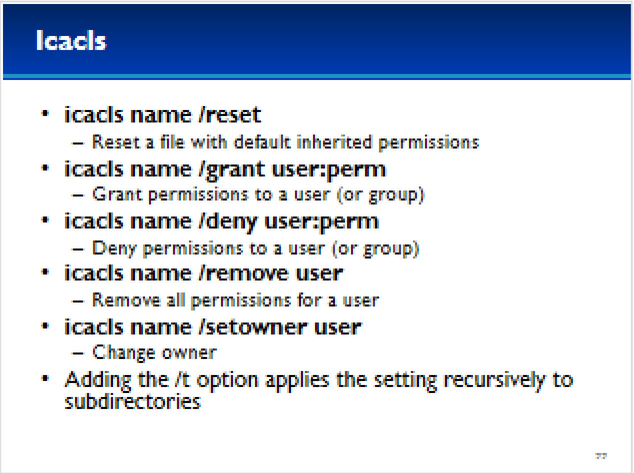
- This is a replacement for the **cacls** command, but still allows you to add, remove, grant, or deny permissions.

- Checking for and maintaining proper permissions is important for computer security.

- If you have trouble viewing, modifying, or deleting a file because of permissions issues, **icacls** can help resolve those issues.

- To view the command syntax for **icacls**, type **icacls** and press **Enter**.

Slide 77



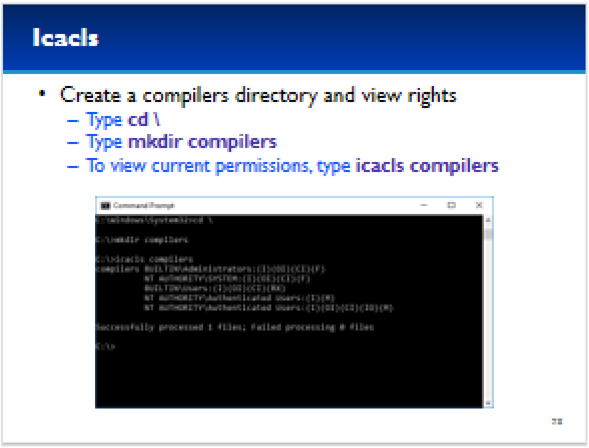
Icacls

- icacls name /reset
  - Reset a file with default inherited permissions
- icacls name /grant user:perm
  - Grant permissions to a user (or group)
- icacls name /deny user:perm
  - Deny permissions to a user (or group)
- icacls name /remove user
  - Remove all permissions for a user
- icacls name /setowner user
  - Change owner
- Adding the /t option applies the setting recursively to subdirectories

77

- **Icacls** can reset the permissions for a file to the default inherited permissions.
- **Icacls** can also grant or deny permissions to a specific user or group.
  - Remember, **deny** takes precedence over **grant**.
- **Icacls** can remove all references to a user or group
- The owner can also be changed using the **icacls** command.
- With the **/t** (forward-slash t) option, **icacls** will apply the operation recursively to all files and directories under the specified directory.

Slide 78



Icacls

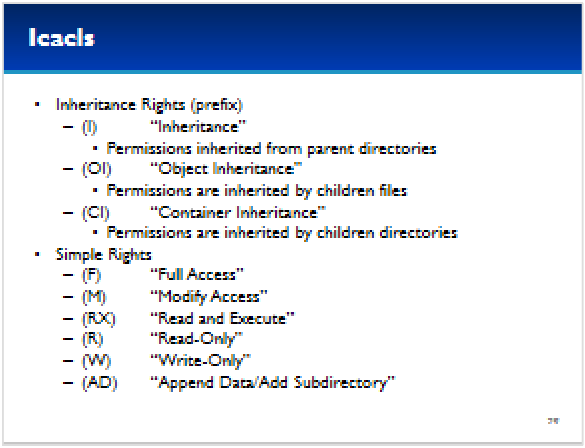
- Create a compilers directory and view rights
  - Type cd \
  - Type mkdir compilers
  - To view current permissions, type icacls compilers

```
C:\Windows\System32>cd \

C:\>mkdir compilers

C:\>icacls compilers
compilers BUILTIN\Administrators:(I)(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          BUILTIN\Users:(I)(OI)(CI)(RX)
          NT AUTHORITY\Authenticated Users:(I)(M)
          NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

78

- Change to the root directory by typing **cd \** (backslash).
- Create a new compilers directory by typing: **mkdir compilers**
- View the default permissions of the compilers directory by typing: **icacls compilers**

Slide 79



Icacls

- Inheritance Rights (prefix)
  - (I) “Inheritance”
    - Permissions inherited from parent directories
  - (OI) “Object Inheritance”
    - Permissions are inherited by children files
  - (CI) “Container Inheritance”
    - Permissions are inherited by children directories
- Simple Rights
  - (F) “Full Access”
  - (M) “Modify Access”
  - (RX) “Read and Execute”
  - (R) “Read-Only”
  - (W) “Write-Only”
  - (AD) “Append Data/Add Subdirectory”

- What does all this mean?

  - An **I** in parentheses indicates the permission is inherited from the parent directory, in this case: C:\

  - **OI** indicates files inside this directory will inherit these permissions.

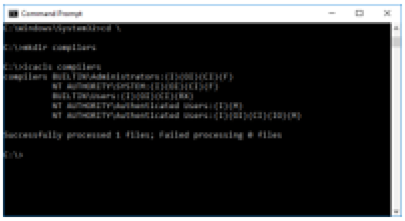
  - **CI** indicates directories inside this directory will inherit these permissions.

- These Simple Rights indicate what permissions are granted or denied.

- There are more rights that give you much more control over what permissions you can grant or deny.

Slide 80

Icacls



```
C:\Windows\System32>cd \

C:\>mkdir compilers

C:\>icacls compilers
compilers BUILTIN\Administrators:(I)(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          BUILTIN\Users:(I)(OI)(CI)(RX)
          NT AUTHORITY\Authenticated Users:(I)(M)
          NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

- All default rights are Inherited (I)
- Administrators and SYSTEM have Full Access (F)
- Users can Read and Execute (RX)
- Authenticated Users can Modify (M)

80

- Going back to our compilers directory, we can see the default permissions for the directory.

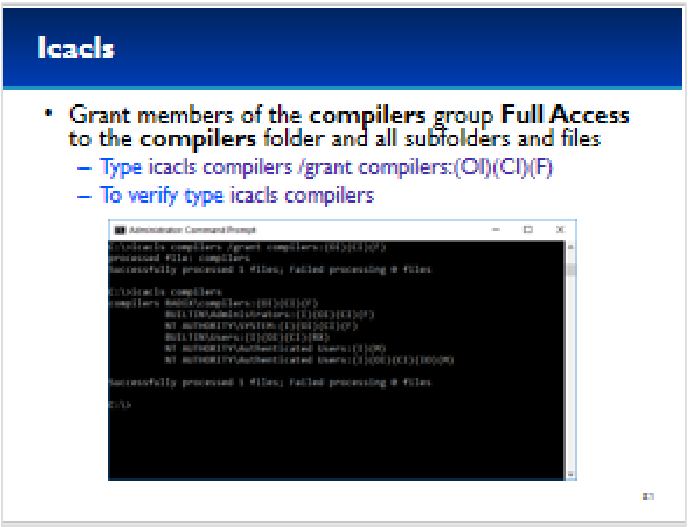
- All permissions have been inherited from the parent directory as indicated by the (I).

- Administrators and SYSTEM have Full Access indicated by the (F).

- Users have Read and Execute permissions.

- Authenticated users have been granted Modify rights. Modify allows users to read and write files and subfolders, as well as delete of the directory.

Slide 81



Icacls

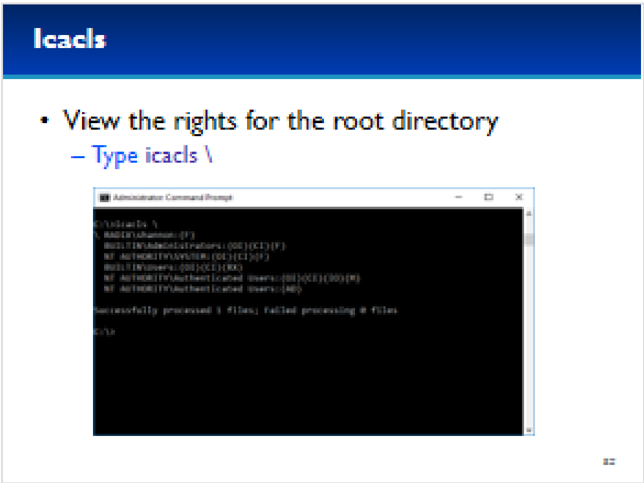
- Grant members of the **compilers** group **Full Access** to the **compilers** folder and all subfolders and files
  - Type icacls compilers /grant compilers:(OI)(CI)(F)
  - To verify type icacls compilers

```
C:\>icacls compilers /grant compilers:(OI)(CI)(F)
processed file: compilers
Successfully processed 1 files; Failed processing 0 files

C:\>icacls compilers
compilers [illegible]\compilers:(OI)(CI)(F)
          BUILTIN\Administrators:(I)(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          BUILTIN\Users:(I)(OI)(CI)(RX)
          NT AUTHORITY\Authenticated Users:(I)(M)
          NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

81

- Grant full access to the compilers folder using **icacls**.
- Type: **icacls compilers /grant compilers:(OI)(CI)(F)**
- This grants full access to the compilers group.
- **OI** and **CI** indicate that children files and directories will inherit these permissions.
- Verify that the rights were granted by typing: **icacls compilers**

Slide 82



Icacls

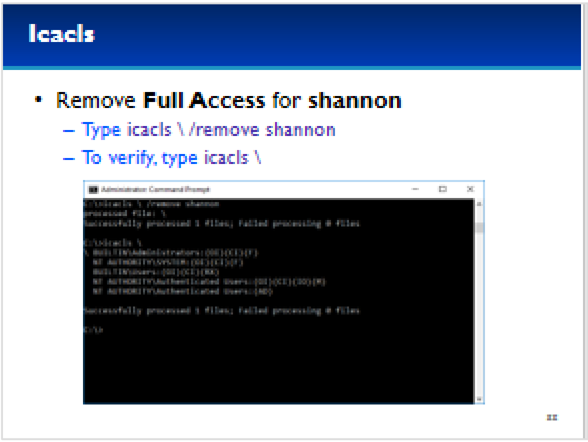
- View the rights for the root directory
  - Type icacls \

```
C:\>icacls \
\ RADIX\shannon:(F)
  BUILTIN\Administrators:(OI)(CI)(F)
  NT AUTHORITY\SYSTEM:(OI)(CI)(F)
  BUILTIN\Users:(OI)(CI)(RX)
  NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(M)
  NT AUTHORITY\Authenticated Users:(AD)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

82

- View the rights for the root directory by typing: **icacls \**
- It looks like the user Shannon has full control over the root directory.

Slide 83



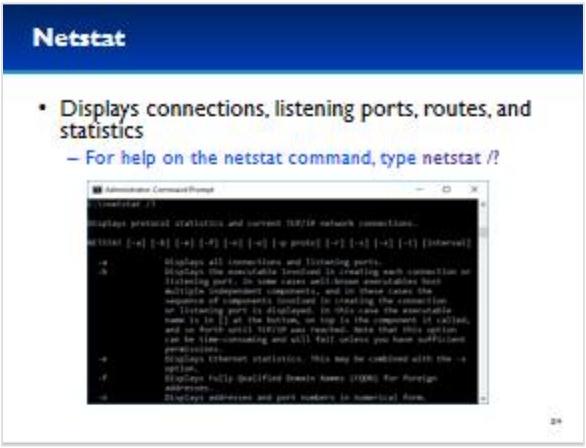
Icacls

- Remove **Full Access** for **shannon**
  - Type icacls \ /remove shannon
  - To verify, type icacls \

```
C:\>icacls \ /remove shannon
processed file: \
Successfully processed 1 files; Failed processing 0 files

C:\>icacls \
\ BUILTIN\Administrators:(OI)(CI)(F)
  NT AUTHORITY\SYSTEM:(OI)(CI)(F)
  BUILTIN\Users:(OI)(CI)(RX)
  NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(M)
  NT AUTHORITY\Authenticated Users:(AD)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

- Remove shannon from the root directory ACLs by typing **icacls \ /remove shannon** (there is a space between the \ and /).
- Verify that shannon has been removed by typing: **icacls **

Slide 84



Netstat

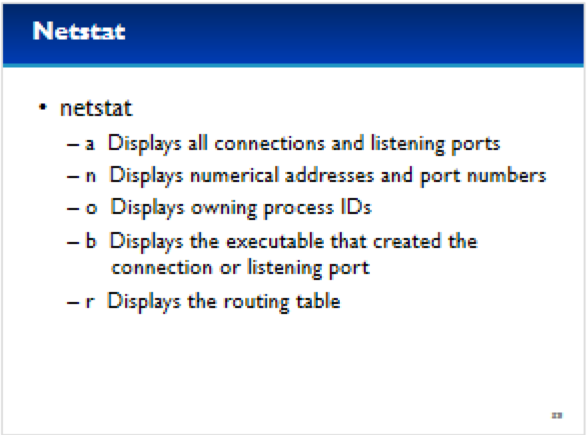
- Displays connections, listening ports, routes, and statistics
  - For help on the netstat command, type netstat /?

```
C:\>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
```

24

- The next command line command we are going to cover is **netstat**
- **Netstat** is a very useful tool for displaying information about current routes, connections, open ports, and statistics
- Type **netstat /?** To view the syntax for the **netstat** command.

Slide 85



Netstat

- netstat
  - – a Displays all connections and listening ports
  - – n Displays numerical addresses and port numbers
  - – o Displays owning process IDs
  - – b Displays the executable that created the connection or listening port
  - – r Displays the routing table

- Netstat options are often combined, here is what each switch does:

- The **a** option displays all connections and listening ports, instead of just established connections.

- The **n** option displays numerical addresses and port numbers. Without this option, netstat will try to resolve IP addresses to DNS names which can sometimes cause the program to take a long time to run.

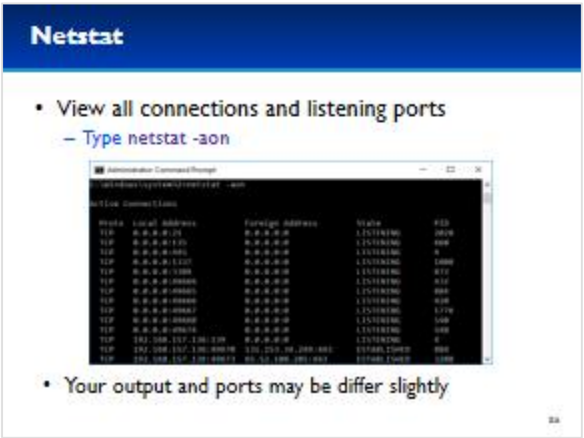
- The **o** option displays the owning process IDs.

- The **b** option displays the executable associated with the connection or listening port.

  - You may think the **b** option is more useful than the **o** option, however the output of the o option is much easier to read, so you may want to use **o** first and then switch to **b** if you really need it.

- The **r** option displays the current routing table and is very useful for troubleshooting network issues.

Slide 86



Netstat

- View all connections and listening ports
  - Type netstat -aon

```
C:\Windows\system32>netstat -aon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       [illegible]
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       [illegible]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]            0.0.0.0:0              LISTENING       [illegible]
  TCP    [illegible]:139        0.0.0.0:0              LISTENING       4
  TCP    [illegible]            [illegible]:443        ESTABLISHED     [illegible]
  TCP    [illegible]            [illegible]:443        ESTABLISHED     [illegible]
```

- Your output and ports may be differ slightly

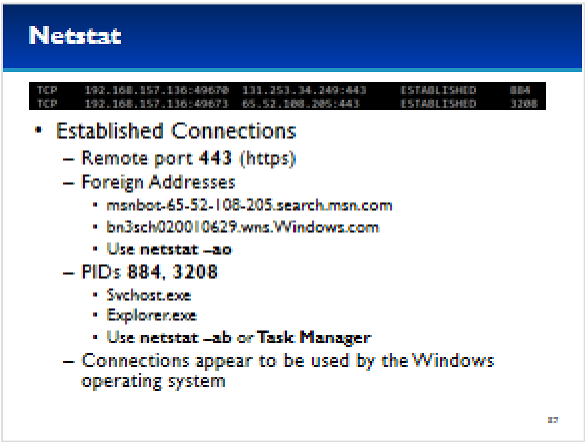
- View all connections and listening ports by typing: **netstat –aon**

  - This also displays numeric IPs and ports as well as printing out the PID.

- Scroll up to the top of the output from this command.

- Since some ports and connections change regularly, <u>parts of your output will differ from what is shown on these slides.</u>

Slide 87



Netstat

```
TCP    192.168.157.136:49670  131.253.34.249:443     ESTABLISHED     884
TCP    192.168.157.136:49673  65.52.108.205:443      ESTABLISHED     3208
```

- Established Connections
  - Remote port **443** (https)
  - Foreign Addresses
    - msnbot-65-52-108-205.search.msn.com
    - bn3sch020010629.wns.Windows.com
    - Use **netstat –ao**
  - PIDs **884, 3208**
    - Svchost.exe
    - Explorer.exe
    - Use **netstat –ab** or **Task Manager**
  - Connections appear to be used by the Windows operating system

87

- In this case there are two active connections from this computer to port 443 which is used by https (you may see only one active connection to port 443). Output may vary from the information of these slides.

- The two foreign IP addresses resolve to MSN and Windows names.

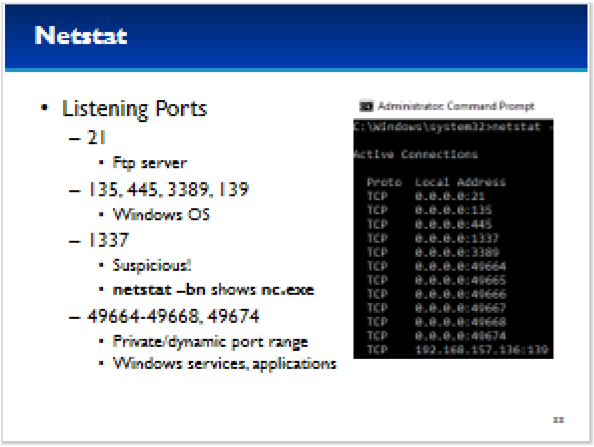
  - You can see this by running the same command without the **n** option.

- The two Process IDs (PIDs) associated with these connections belong to Svchost.exe and Explorer.exe.

  - You can see this information by using the **b** option instead of the **o** option, or with Task Manager.

- These connections appear to be used by the Windows operating system for sending and receiving information to and from different cloud-based services.

Slide 88



Netstat

- Listening Ports
  - 21
    - Ftp server
  - 135, 445, 3389, 139
    - Windows OS
  - 1337
    - Suspicious!
    - **netstat –bn shows nc.exe**
  - 49664-49668, 49674
    - Private/dynamic port range
    - Windows services, applications

Administrator: Command Prompt

```
C:\Windows\system32>netstat -

Active Connections

  Proto  Local Address
  TCP    0.0.0.0:21
  TCP    0.0.0.0:135
  TCP    0.0.0.0:445
  TCP    0.0.0.0:1337
  TCP    0.0.0.0:3389
  TCP    0.0.0.0:49664
  TCP    0.0.0.0:49665
  TCP    0.0.0.0:49666
  TCP    0.0.0.0:49667
  TCP    0.0.0.0:49668
  TCP    0.0.0.0:49674
  TCP    192.168.157.136:139
```

88

- There are several ports open and listening on this computer.

  - A Local Address of 0.0.0.0 means that the program is listening on all available interfaces and is accepting connections from the internet.

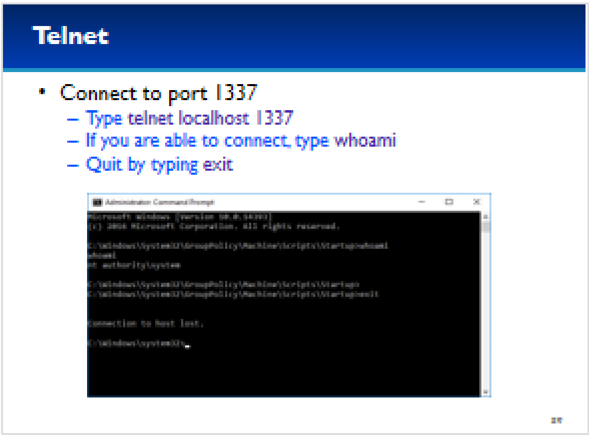
  - Port 21 is commonly used by the FTP service, so it seems likely that this computer is running a FTP server.

  - Ports 135, 445, 3389, and 139 are used by the Windows operating system for different network services such as Windows File Sharing and Remote Desktop Services.

  - Port 1337 looks really suspicious and we'll have to check that out next!

  - Ports 49152 through 65535 are dynamic/private port numbers and appear to be in use by Windows Services and components such as EventLog, Task Scheduler, the Local Security Authority Subsystem Service, and Spooler Subsystem App, which manages printing and fax services.

Slide 89



Telnet

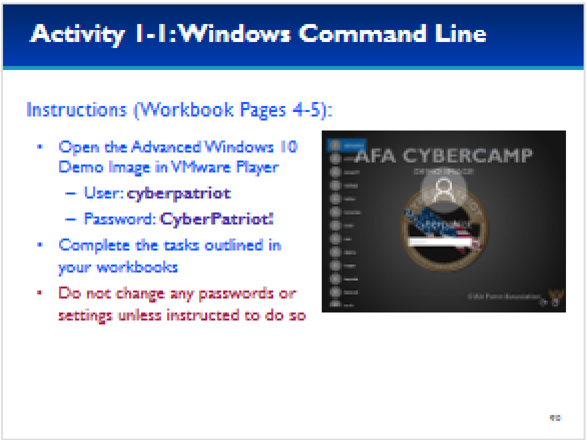
- Connect to port 1337
  - Type telnet localhost 1337
  - If you are able to connect, type whoami
  - Quit by typing exit

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup>whoami
whoami
nt authority\system

C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup>
C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup>exit


Connection to host lost.

C:\Windows\system32>_
```

89

- Let’s see what’s running on port 1337 using the telnet client (<u>you may not be able to make a connection to port 1337 if it is blocked by your firewall).</u>
- Type **telnet localhost 1337** to connect to port 1337 on your local computer.
- It looks like we got a new prompt in a different directory. This looks like a backdoor.
- Type **whoami** to see what user you are currently logged in as.
- It looks like you are logged in as the SYSTEM user which is even more powerful than administrator.
- Type **exit** to get out of the backdoor.
- Don’t remove the backdoor yet, we’re going to do more analysis on it in the next section.

Slide 90



Activity 1-1: Windows Command Line

Instructions (Workbook Pages 4-5):

- Open the Advanced Windows 10 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

90

🕒 Give students about 20 minutes to complete the tasks listed on Pages 4-5 of their Workbooks.

☆This lab will review the Windows Command Line including the net commands, netstat, and icacls.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. Never, 30, 30
2. net accounts /minpwlen:__
3. net user smoak /delete, net user anderson /delete
4. net user Johnson putinpassword /add
5. net user lovelace putinpassword
6. net user knuth Answer: 6/11/2017 5:21:57 AM
7. net localgroup administrators tukey /delete, net localgroup administrators karpinski /delete
8. net localgroup administrators Johnson /add
9. net localgroup “Backup Operators” Answer: boole, kleinrock
10. net localgroup Replicator Answer: Supports file replication in a domain
11. net share ftproot Answer: C:\inetpub\ftproot
12. net share ftproot Answer: Administrators, IIS_IUSRS
13. net share ftproot /delete
14. icacls c:\inetpub\ftproot Answer: Cyberpatriot, SYSTEM, Everyone, TrustedInstaller, Administrators
15. icacls c:\inetpub\ftproot /remove Everyone
16. netstat –ab Answer: RpcSs
17. netstat –ab Answer: 5353, UDP (although you may see a second one: 5355, UDP)

Slide 91

Sysinternals Suite

This section is an optional Advanced portion, if time permits.

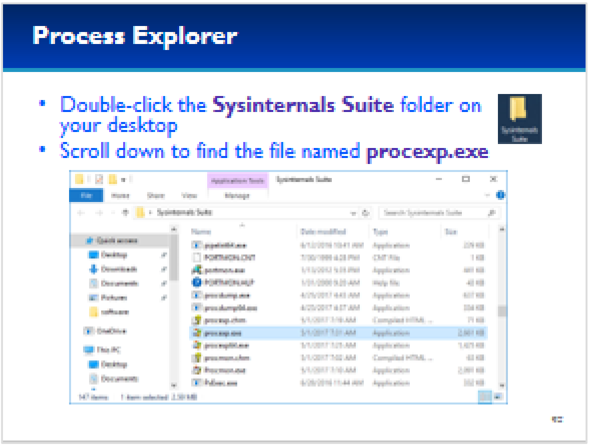
🕒 Devote 30 minutes to Slides 92-120. Allow the students 20 minutes to complete the activity on Slide 121.

☆ Throughout this section, students should follow along in the **Advanced Windows 10 Demo Image**.

☆ Actions the students are supposed to take are highlighted in blue and purple.

☆ Purple indicates exact text they are supposed to type or GUI elements they should interact with.

Slide 92



Process Explorer

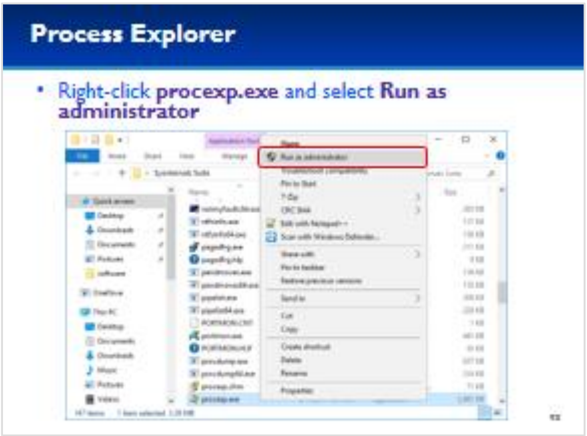
- Double-click the **Sysinternals Suite** folder on your desktop
- Scroll down to find the file named **procexp.exe**

Name	Date modified	Type	Size
pipelist64.exe	6/12/2016 10:41 AM	Application	229 KB
PORTMON.CNT	7/30/1999 4:28 PM	CNT File	1 KB
portmon.exe	1/13/2012 5:35 PM	Application	441 KB
PORTMON.HLP	1/31/2000 9:20 AM	Help file	43 KB
procdump.exe	4/25/2017 4:43 AM	Application	617 KB
procdump64.exe	4/25/2017 4:07 AM	Application	334 KB
procexp.chm	5/1/2017 7:18 AM	Compiled HTML ...	71 KB
procexp.exe	5/1/2017 7:01 AM	Application	2,661 KB
procexp64.exe	5/1/2017 7:25 AM	Application	1,425 KB
procmon.chm	5/1/2017 7:02 AM	Compiled HTML ...	63 KB
Procmon.exe	5/1/2017 7:18 AM	Application	2,091 KB
PsExec.exe	6/28/2016 11:44 AM	Application	332 KB

147 items   1 item selected 2.50 MB

- The Sysinternals Suite of utilities are available to download for free from technet.Microsoft.com.
- The suite has already been downloaded to your Demo image and extracted to the desktop.
- Double-click the Sysinternals Suite folder on your desktop and scroll down until you find the file named procexp.exe.

Slide 93

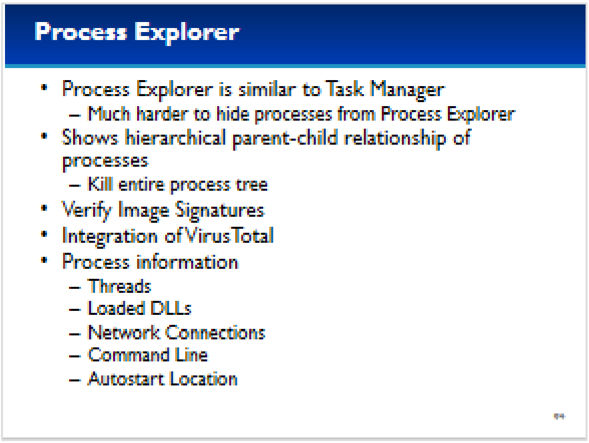


Process Explorer

- Right-click **procexp.exe** and select **Run as administrator**

- Right-click procexp.exe and Run as administrator, so that you can use its full capabilities.
- User Account Control may ask you if you want to allow this app to make changes to your device. We trust this application, so click Yes.

Slide 94



Process Explorer

- Process Explorer is similar to Task Manager
  - Much harder to hide processes from Process Explorer
- Shows hierarchical parent-child relationship of processes
  - Kill entire process tree
- Verify Image Signatures
- Integration of VirusTotal
- Process information
  - Threads
  - Loaded DLLs
  - Network Connections
  - Command Line
  - Autostart Location

- Process Explorer is similar to Task Manager, but because of the way Process Explorer gets its information, it is much harder to hide processes from Process Explorer.

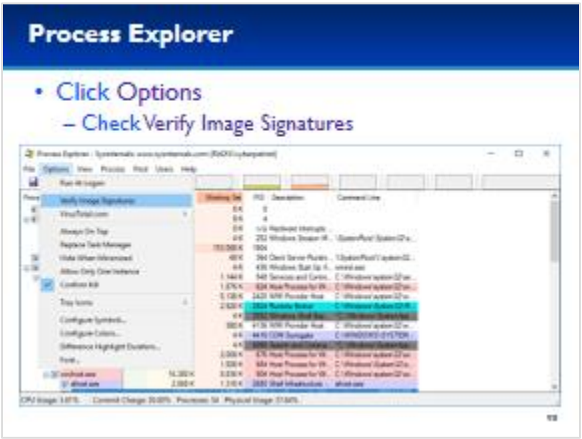
- The first thing you will notice about Process Explorer is that it shows the hierarchical parent-child relationship of processes.

  - When a process creates another process, the original process is referred to as the parent process, and the processes it creates is referred to as the child process.

- Process Explorer has some really helpful features such as being able to verify image signatures and integration of VirusTotal, a cloud based malware detection service.

- Lots of other useful information can be displayed by Process Explorer, including Threads, Loaded DLL's, Handles, Network Connections, The command line used to start the application, and the location responsible for automatically starting the application.

Slide 95

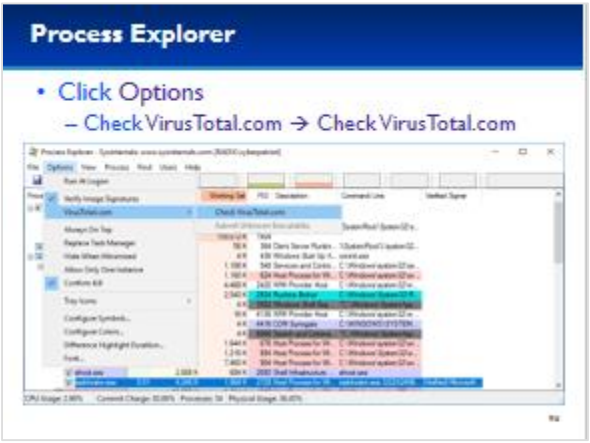


Process Explorer

- Click Options
  - Check Verify Image Signatures

- First, lets enable verification of image signatures.
- Click Options, and select Verify Image Signatures.
- You should see a new column on your screen, don't worry if it's blank for now.

Slide 96

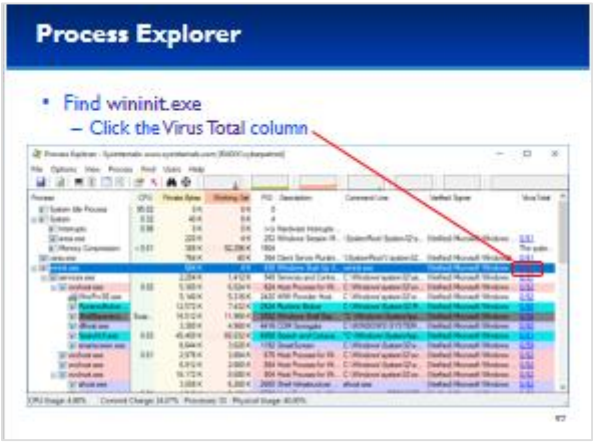


Process Explorer

- Click Options
  - Check VirusTotal.com → Check VirusTotal.com

- Next, let’s enable VirusTotal.com integration.
- Click Options, and Check VirusTotal.com→ Check VirusTotal.com.
- You should see a new VirusTotal column on the right.

Slide 97



Process Explorer

- Find wininit.exe
  - Click the Virus Total column

- Let's examine wininit.exe.

  - Wininit.exe is responsible for starting the services.exe process, therefore wininit.exe is the parent of services.exe.

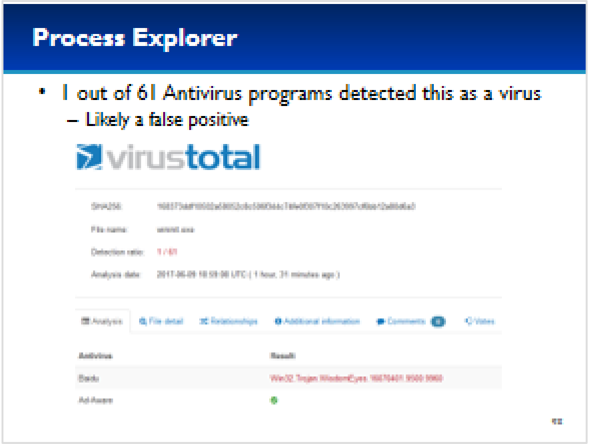
  - The services.exe process in turn is responsible for starting the services on your system, which is why the svchost.exe processes are children of services.exe.

- Back to the wininit.exe row, we can see that VirusTotal reports 1/61 in red.

  - Since VirusTotal.com is constantly changing your results might be different.

- Click the VirusTotal column for wininit.exe.

Slide 98



Process Explorer

- 1 out of 61 Antivirus programs detected this as a virus
  - Likely a false positive

SHA256: [illegible]

File name: wininit.exe

Detection ratio: 1 / 61

Analysis date: 2017-06-09 10:59:00 UTC (1 hour, 31 minutes ago)

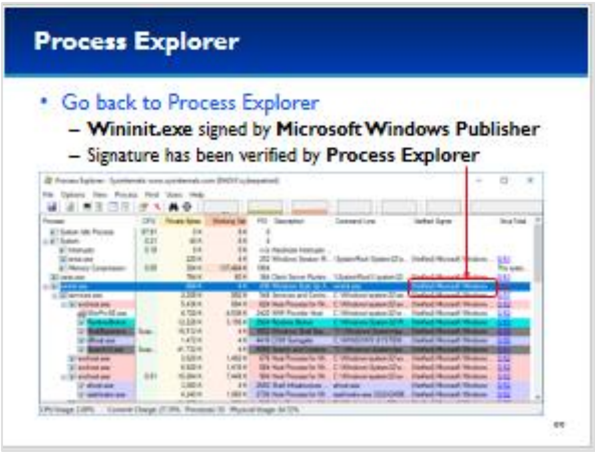
Antivirus	Result
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9960
Ad-Aware	●

- Clicking the VirusTotal column brings up a web page displaying information about the process (since VirusTotal is constantly changing, you may see a different number).

  - According to this web page, the file wininit.exe with this particular SHA256 was scanned by 61 different antivirus/antimalware products and one of them (Baidu) reported it as a Trojan.

  - I find the other antivirus products here much more trustworthy than Baidu, so this is likely a single false positive and nothing to worry about.

Slide 99



Process Explorer

- Go back to Process Explorer
  - **Wininit.exe** signed by **Microsoft Windows Publisher**
  - Signature has been verified by **Process Explorer**

99

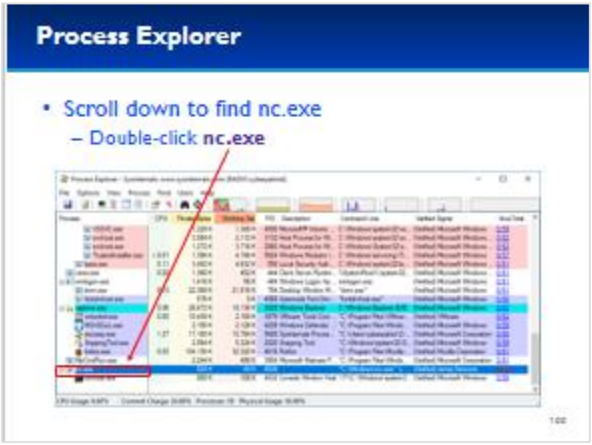
- Close out of the VirusTotal web page and look at the Verified Signer column for wininit.exe in Process Explorer.

- It looks like this executable has been verified as signed by Microsoft Windows Publisher.

  - Signatures use cryptographic constructs such as file hashes and public key encryption that allow us to verify that the person who “signed” this executable is actually that person and not someone trying to forge the signature.

  - Since this has been signed by Microsoft, this gives more validity to our assumption that the VirusTotal.com result was a false positive.

Slide 100



Process Explorer

- Scroll down to find nc.exe
  - Double-click **nc.exe**

100

- Next, let's examine the backdoor listening on our computer.

- Scroll down to find nc.exe.

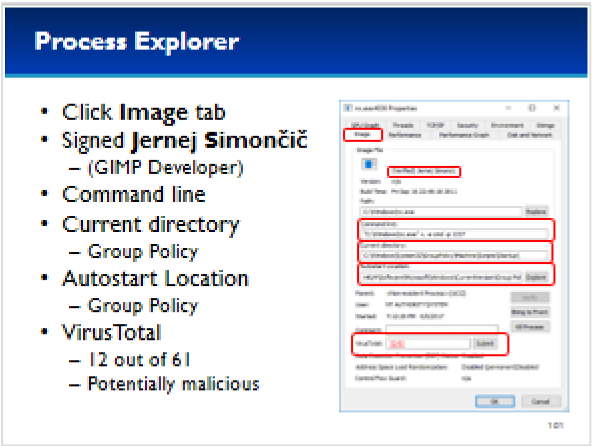
  - nc.exe has one child process, conhost.exe.

- The description for conhost.exe describes it as a Console Window Host.

  - This is part of Windows and it's the command shell that is being run by nc.exe.

- Double-click nc.exe to view more information.

Slide 101



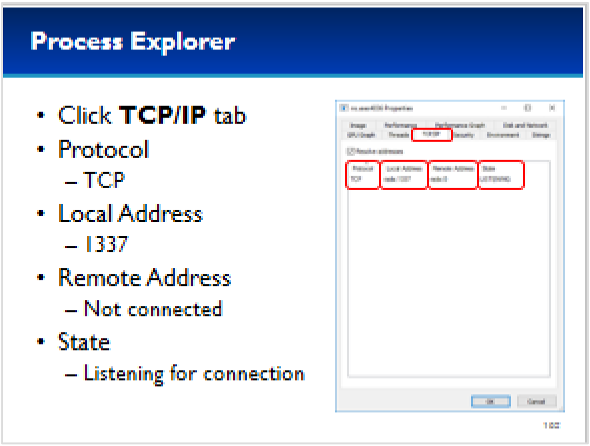
Process Explorer

- Click **Image** tab
- Signed **Jernej Simončič**
  - (GIMP Developer)
- Command line
- Current directory
  - Group Policy
- Autostart Location
  - Group Policy
- VirusTotal
  - 12 out of 61
  - Potentially malicious

101

- Click on the Image tab.
- This executable has been signed by Jernej Simončič.
  - Just because a file is signed, doesn’t mean it’s trusted.
  - I don’t trust Jernej nearly as much as I trust Microsoft.
- We can see the command line used to start the program, it appears that netcat is running a Command Prompt on port 1337.
- We can also see the Current Directory and Autostart Location, both of which point to this being a Group Policy setting that is responsible for starting this netcat backdoor.
- Also VirusTotal reports 12/61 Antivirus products report this as a virus (your VirusTotal result may be a little different).
  - Netcat is a useful program with many legitimate uses, but can also be used for nefarious purposes, which is probably why we see mixed results from VirusTotal.

Slide 102



Process Explorer

- Click **TCP/IP** tab
- Protocol
  - TCP
- Local Address
  - 1337
- Remote Address
  - Not connected
- State
  - Listening for connection

102

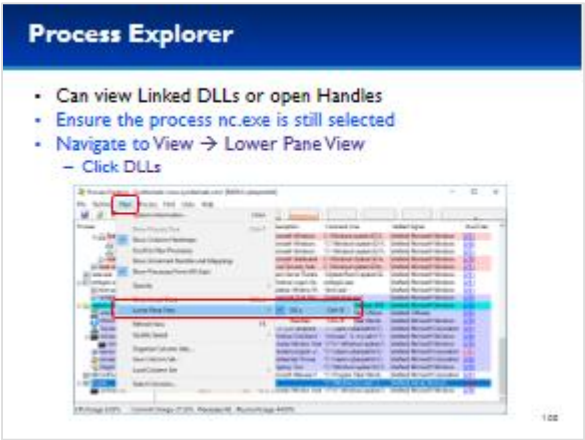
- Click on the TCP/IP tab of process explorer.

  - This process is listening on TCP port 1337.

  - It’s currently not connected which is why there is a remote address of 0 and a state of LISTENING.

  - Close by selecting Cancel.

Slide 103



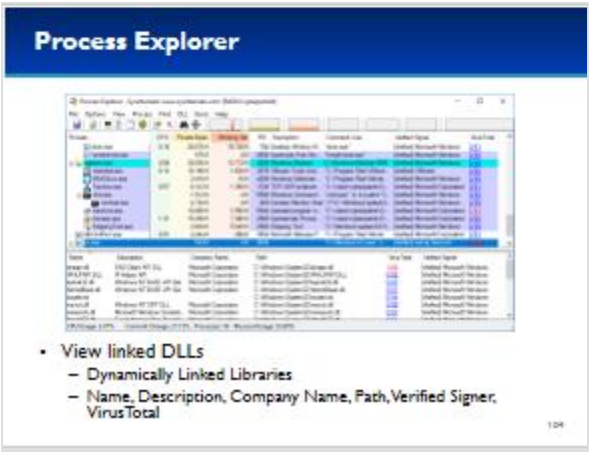
Process Explorer

- Can view Linked DLLs or open Handles
- Ensure the process nc.exe is still selected
- Navigate to View → Lower Pane View
  - Click DLLs

103

- Malware may exist in more than just executables however.
- Let's check out the DLLs linked to nc.exe.
- Click View and select Lower Pane View → DLLs.

Slide 104



Process Explorer

- View linked DLLs
  - Dynamically Linked Libraries
  - Name, Description, Company Name, Path, Verified Signer, VirusTotal

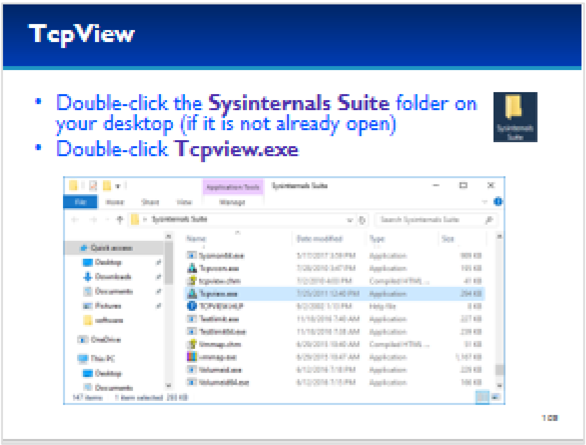
104

- It looks like there is nothing obviously bad here. All the DLLs loaded appear to be official, signed DLLs in the C:\Windows\System32 directory.

- The dnsapi.dll 1/60 result above appears to be another false positive (your result may vary slightly).

- Close out of Process Explorer.

Slide 105



TcpView

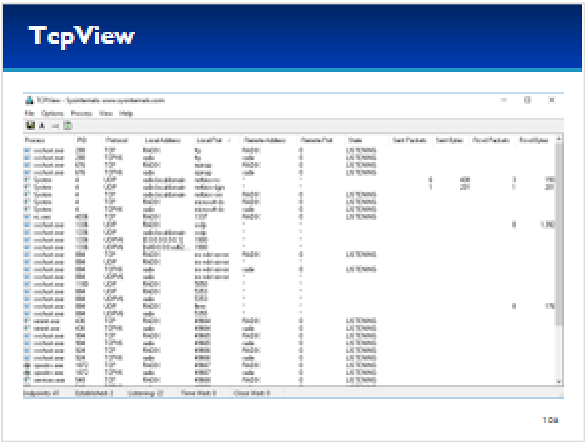
- Double-click the **Sysinternals Suite** folder on your desktop (if it is not already open)
- Double-click **Tcpview.exe**

- Next, let’s examine another extremely useful Sysinternals program called TcpView.
- Scroll down in the Sysinternals Suite directory to find Tcpview.exe.

  - Double-clicking Tcpview.exe will automatically start it as an administrator.

- User Account Control may ask you if you want to allow this app to make changes to your device. We trust this application, so click Yes.

Slide 106

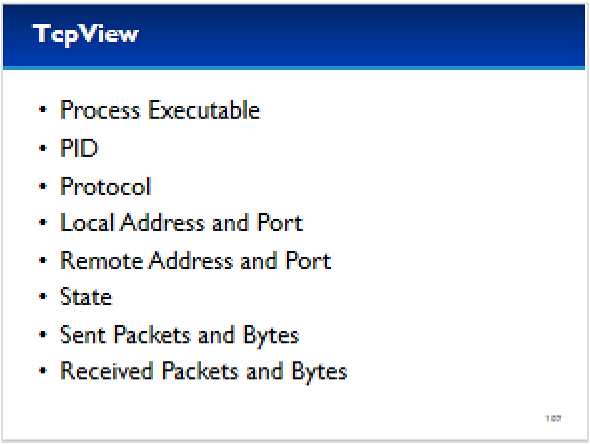


TcpView

106

- As you can see, TcpView shows a lot of the same information as **netstat**, but one big difference that is already visible is the ability to sort by columns.

Slide 107



TcpView

- Process Executable
- PID
- Protocol
- Local Address and Port
- Remote Address and Port
- State
- Sent Packets and Bytes
- Received Packets and Bytes

- TcpView has a row for each network connection or listening port.

- For each network connection, you can see:

  - The executable that created that connection.

  - The PID (Process ID).

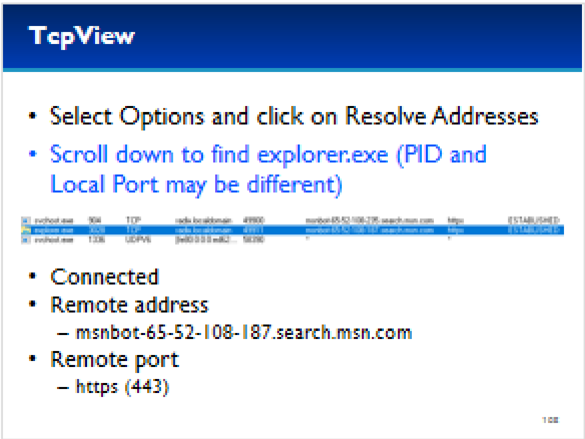
  - The local address and port.

  - The remote address and port (if a connection has been established).

  - The State of the connection, such as LISTENING or ESTABLISHED.

  - The number of packets and bytes sent and received.

Slide 108



TcpView

- Select Options and click on Resolve Addresses
- Scroll down to find explorer.exe (PID and Local Port may be different)

```
svchost.exe    904   TCP     radii.localdomain   49900   msnbot-65-52-108-235.search.msn.com   https   ESTABLISHED
explorer.exe   3028  TCP     radii.localdomain   49911   msnbot-65-52-108-187.search.msn.com   https   ESTABLISHED
svchost.exe    1336  UDPV6   [fe80:0:0:0:ed62...  58390   *                                     *
```

- Connected
- Remote address
  - msnbot-65-52-108-187.search.msn.com
- Remote port
  - https (443)

108

- Let’s examine one of the established connections on your computer.

  - These change regularly, <u>so what is on your computer will be slightly different</u>.

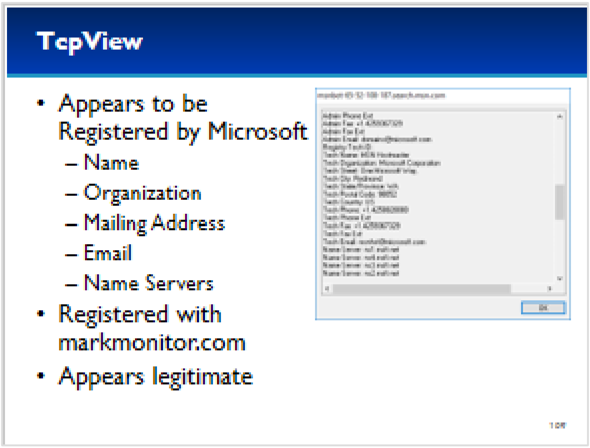
- Select Options and click on Resolve Addresses.

- It looks like Explorer.exe opened up a connection to a computer at search.msn.com on port 443 which is used by https.

- Right-click on Explorer.exe (if you have more than one Explorer.exe shown, click anyone that has an ESTABLISHED connection).

  - Process Explorer will let you manually end the process or kill the connection.

Slide 109



TcpView

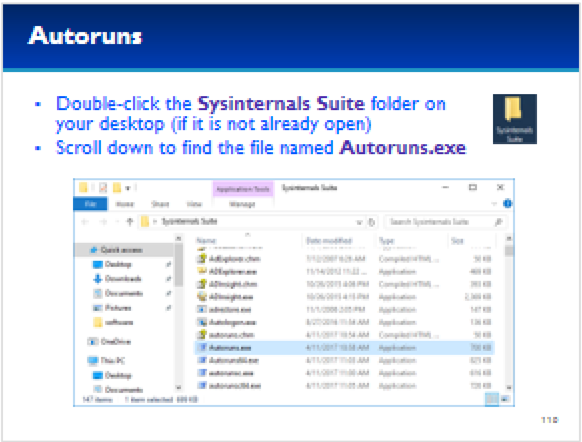
- Appears to be Registered by Microsoft
  - Name
  - Organization
  - Mailing Address
  - Email
  - Name Servers
- Registered with markmonitor.com
- Appears legitimate

```
msnbot-65-52-108-187.search.msn.com

Admin Phone Ext:
Admin Fax: +1.4258067329
Admin Fax Ext:
Admin Email: domains@microsoft.com
Registry Tech ID:
Tech Name: MSN Hostmaster
Tech Organization: Microsoft Corporation
Tech Street: One Microsoft Way
Tech City: Redmond
Tech State/Province: WA
Tech Postal Code: 98052
Tech Country: US
Tech Phone: +1.4258828080
Tech Phone Ext:
Tech Fax: +1.4258067329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns1.msft.net
Name Server: ns4.msft.net
Name Server: ns3.msft.net
Name Server: ns2.msft.net
```

108

- Right-click on Explorer.exe and select Whois, which is a protocol used for querying information about domain names.
  - Firewall may prevent you from using whois.
- Examining the dialog box that pops up, we can see that this domain is registered to Microsoft; we can make that assumption by looking at the Name, Organization, Mailing Address, Email, and Name Servers.
- This domain has been registered with markmonitor.com.
- We can’t be 100% certain, but the this appears to be legitimately owned by Microsoft.

Slide 110



Autoruns

- Double-click the **Sysinternals Suite** folder on your desktop (if it is not already open)
- Scroll down to find the file named **Autoruns.exe**

Name	Date modified	Type	Size
ADExplorer.chm	7/12/2007 6:26 AM	Compiled HTML ...	50 KB
ADExplorer.exe	11/14/2012 11:22 ...	Application	469 KB
ADInsight.chm	10/26/2015 4:08 PM	Compiled HTML ...	393 KB
ADInsight.exe	10/26/2015 4:15 PM	Application	2,369 KB
adrestore.exe	11/1/2006 2:05 PM	Application	147 KB
Autologon.exe	8/27/2016 11:54 AM	Application	136 KB
autoruns.chm	4/11/2017 10:54 AM	Compiled HTML ...	50 KB
Autoruns.exe	4/11/2017 10:58 AM	Application	700 KB
Autoruns64.exe	4/11/2017 11:03 AM	Application	825 KB
autorunsc.exe	4/11/2017 11:00 AM	Application	616 KB
autorunsc64.exe	4/11/2017 11:05 AM	Application	726 KB

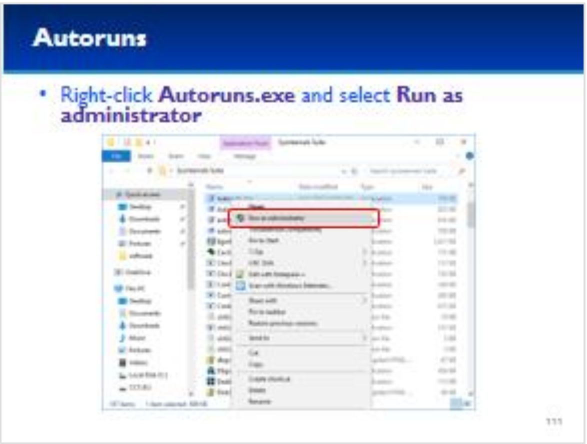
147 items 1 item selected 699 KB

110

- Close TcpView and go back to the Sysinternals Suite folder.

- Scroll up and find the executable Autoruns.exe.

Slide 111



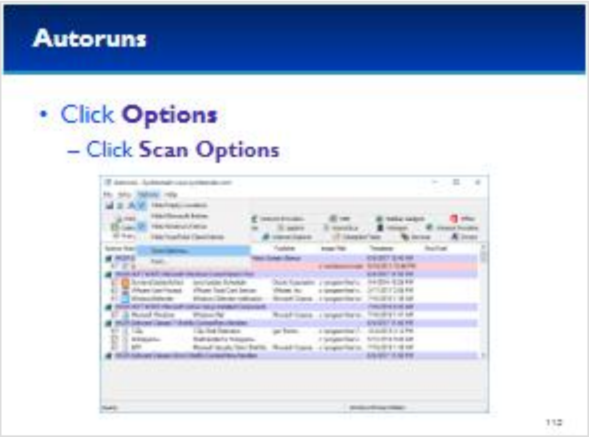
Autoruns

- Right-click **Autoruns.exe** and select **Run as administrator**

111

- Right-click on autoruns.exe and select Run as administrator.

Slide 112



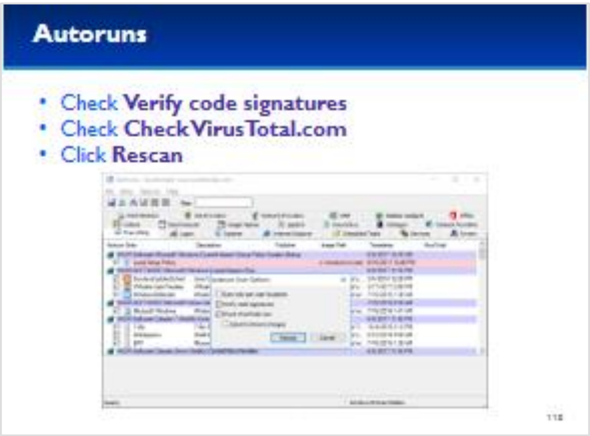
Autoruns

- Click **Options**
  - Click **Scan Options**

112

- First, let’s enable checking VirusTotal.com and signatures.
- Go to Options and select Scan Options.

Slide 113

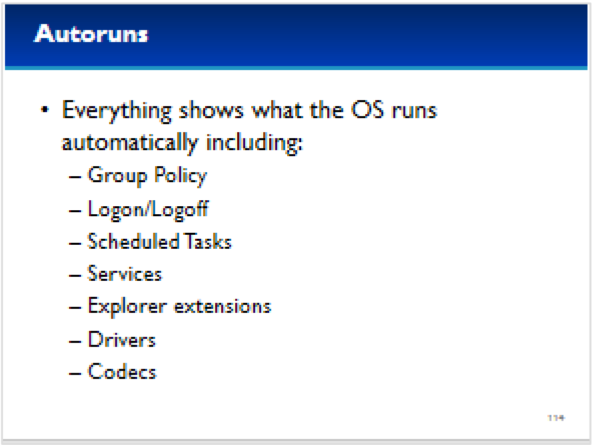


Autoruns

- Check **Verify code signatures**
- Check **Check VirusTotal.com**
- Click **Rescan**

- Check Verify code signatures and Check VirusTotal.com.
- Do not select Submit Unknown Images.
- Click Rescan.

Slide 114



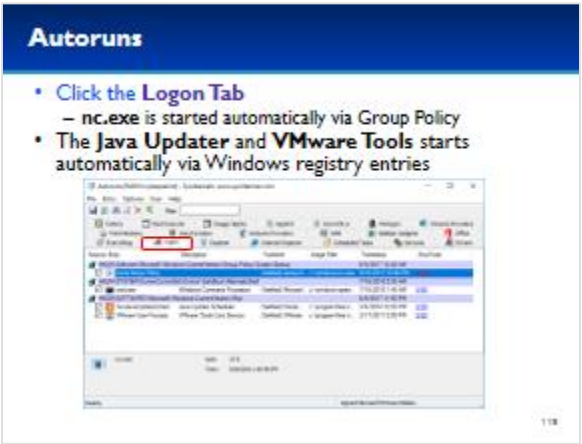
Autoruns

- Everything shows what the OS runs automatically including:
  - Group Policy
  - Logon/Logoff
  - Scheduled Tasks
  - Services
  - Explorer extensions
  - Drivers
  - Codecs

114

- The Everything tab shows what the OS runs automatically including:
  - Programs started by Group Policy settings.
  - Logon/Logoff and Startup scripts stored via registry entries.
  - Programs started by the Task Scheduler.
  - Services.
- Malware may also exist and be automatically loaded as Explorer extensions, drivers, or even media codecs.

Slide 115



Autoruns

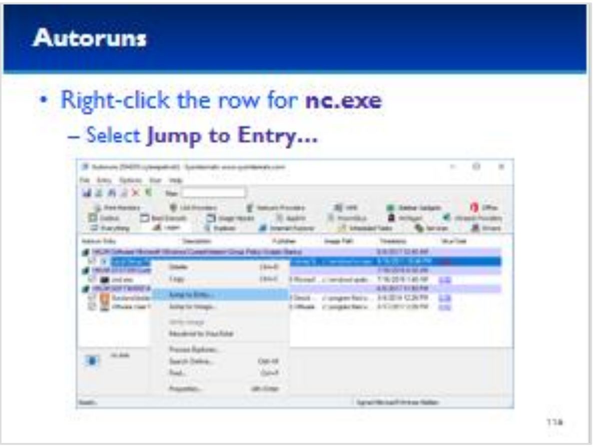
- Click the **Logon Tab**
  - **nc.exe** is started automatically via Group Policy
- The **Java Updater** and **VMware Tools** starts automatically via Windows registry entries

115

- To see the programs at logon/startup, click on the Logon Tab.

  - Here you can see the netcat backdoor is automatically started by the Local Group Policy.

Slide 116



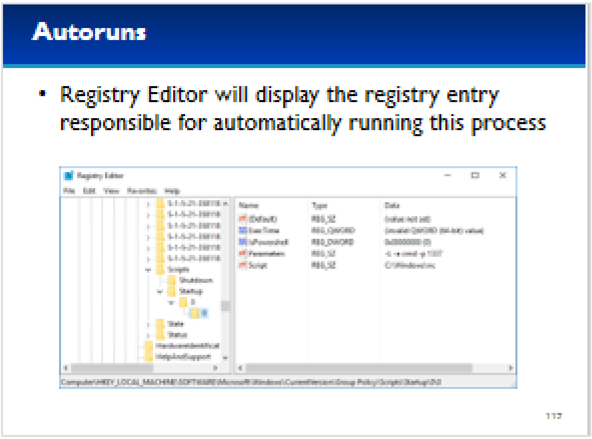
Autoruns

- Right-click the row for **nc.exe**
  - Select **Jump to Entry…**

116

- Right-click on the row for nc.exe and select Jump to Entry…

Slide 117



Autoruns

- Registry Editor will display the registry entry responsible for automatically running this process

Name	Type	Data
(Default)	REG_SZ	(value not set)
ExecTime	REG_QWORD	(invalid QWORD (64-bit) value)
IsPowershell	REG_DWORD	0x00000000 (0)
Parameters	REG_SZ	-l -e cmd -p 1337
Script	REG_SZ	C:\Windows\nc

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup\0\0

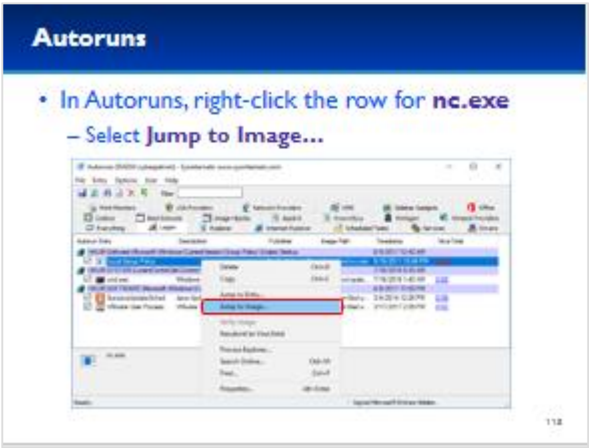
117

- This brings you directly to the Registry.

  - Here we can see the executable started at boot, and the parameters passed to it.

- Close the Registry Editor and go back to Autoruns.

Slide 118



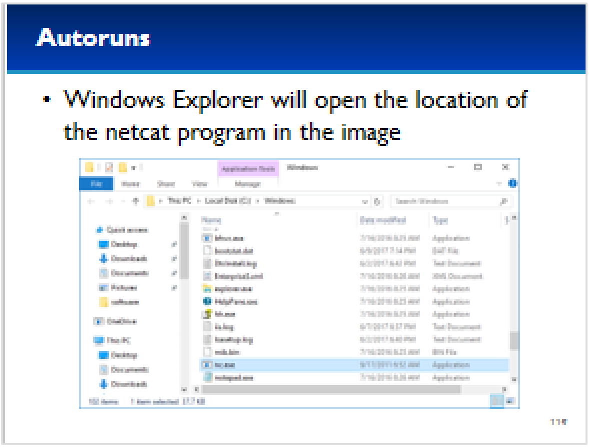
Autoruns

- In Autoruns, right-click the row for **nc.exe**
  - Select **Jump to Image…**

118

- Next, right-click the row for nc.exe again, but this time select Jump to Image…

Slide 119

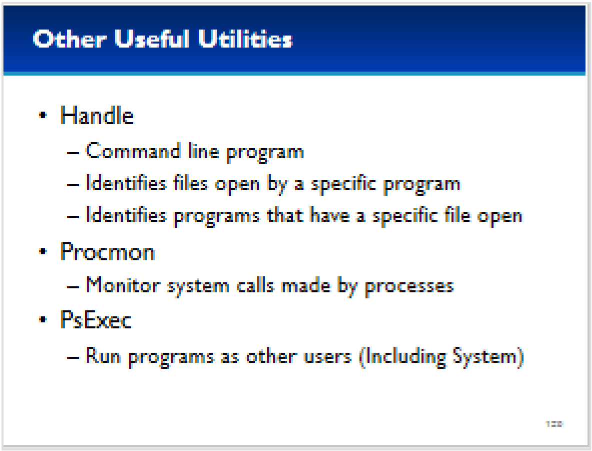


Autoruns

- Windows Explorer will open the location of the netcat program in the image

- A Windows Explorer window is automatically opened with the executable that is referenced already selected.
- Close out of Windows Explorer and Autoruns.

Slide 120



Other Useful Utilities

- Handle
  - Command line program
  - Identifies files open by a specific program
  - Identifies programs that have a specific file open
- Procmon
  - Monitor system calls made by processes
- PsExec
  - Run programs as other users (Including System)

120

- Other very useful programs in the Sysinternals suite are Handle, Procmon, and PsExec.

- Handle lets you find out what processes have a file open, or what files a process has open.

  - This can be very useful when trying to remove or analyze malware, (or even when Windows won't let you safely eject your USB drive).

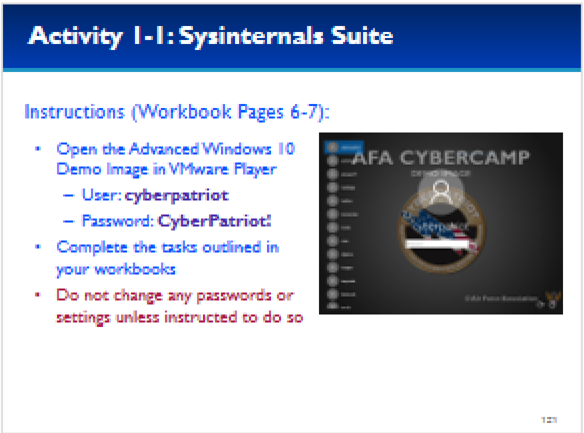
- Procmon (short for Process Monitor) can monitor the activity of all the processes on your system by monitoring various system calls.

  - For example, it can tell you what registry entries or files are accessed or modified by an executable.

- PsExec can be used to run programs as other users, including the System user.

  - This can also be useful to the bad guys, so it might be something you want to watch.

Slide 121



Activity 1-1: Sysinternals Suite

Instructions (Workbook Pages 6-7):

- Open the Advanced Windows 10 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

121

◷ Give students about 20 minutes to complete the tasks listed on Pages 6-7 of their Workbooks.

☆This lab will review the Sysinternals Suite.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. winlogon.exe
2. 4
3. Right-click on csrss.exe, select Properties, Image tab, look at the Command Line, and scroll all the way to the end. Answer: 16
4. Find the right svchost.exe, right-click, select Properties, select the Services tab. Answer: Base Filtering Engine, CoreMessaging, Diagnostic Policy Service, Windows Firewall
5. RiskWare.RemoteAdmin
6. 38db
7. 4
8. 21, 135, 137, 138, 139, 445
9. -
10. AdobeARM.exe
11. Yes
12. Adobe Systems (or Adobe Systems, Incorporated)
13. Igor Pavlov
14. C:\program files\7-zip\7-zip.dll
15. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Instructor's Guide Table of Contents

Ubuntu 16

Student Workbook Activities

Slide 0

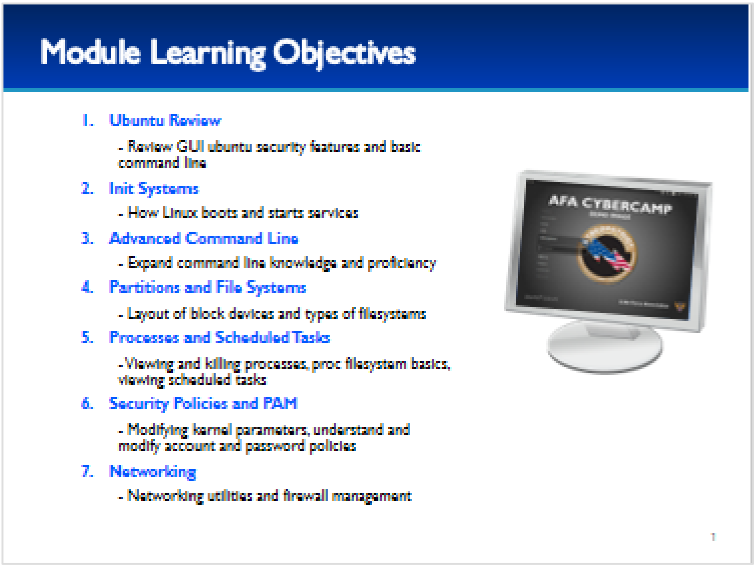
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM
AFA
AFA

AFA Advanced CyberCamp

Ubuntu 16

☆In this module, after the review, students should follow along on the **Advanced Ubuntu 16 Demo Image** you have downloaded to their machines.

Slide 1



Module Learning Objectives

1. Ubuntu Review
   - Review GUI ubuntu security features and basic command line
2. Init Systems
   - How Linux boots and starts services
3. Advanced Command Line
   - Expand command line knowledge and proficiency
4. Partitions and File Systems
   - Layout of block devices and types of filesystems
5. Processes and Scheduled Tasks
   - Viewing and killing processes, proc filesystem basics, viewing scheduled tasks
6. Security Policies and PAM
   - Modifying kernel parameters, understand and modify account and password policies
7. Networking
   - Networking utilities and firewall management

- Today, we are going to spend the majority of the time on the command line.

- We'll start off with an Ubuntu review and give you a quick refresh of some of the things you learned in the last CyberCamp.

- After the review, we will cover advanced init systems, going into detail about how Linux boots and starts services. You'll learn the many places to look to identify unwanted services and know how to disable them.

- Next, we'll cover advanced command line. After this section you should be comfortable on the command line, and know how to perform complex tasks such as finding files or redirecting input and output streams.

- Next, we'll cover the basis of block devices, partitions, and filesystems. Being able to manage a healthy filesystem is an important security task, and what you will learn forms the basis for advanced filesystem forensics.

- After that, you will learn multiple methods to determine what processes are being run on your system, how to kill unwanted processes, and methods for bypassing rootkits on a compromised machine.

- Then, we'll take a long look at a few of the many kernel parameters that can affect the security of your system, and the best way to modify them. In the second part of this section, we will break down PAM and explain how it works step-by-step so you know how to enable secure account and password policies.

- Finally, we'll wrap things up by looking at two different sets of networking utilities available on most modern Linux systems, and discuss how to easily enable the firewall and modify firewall rules from the command line.

Slide 2

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

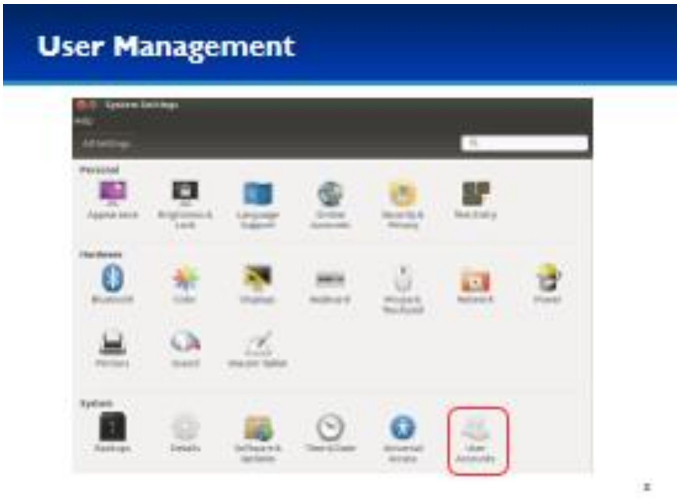
Ubuntu Review

🕒 Devote 20 minutes to slides 3-21. There is no activity at the end of this section.

☆To save time, this section was designed to be a quick review without having students follow along on their demo images, or going into too much detail.

☆We’ll start off with an Ubuntu review and give you a quick refresh of some of the things that are taught in the standard CyberCamp.

Slide 3

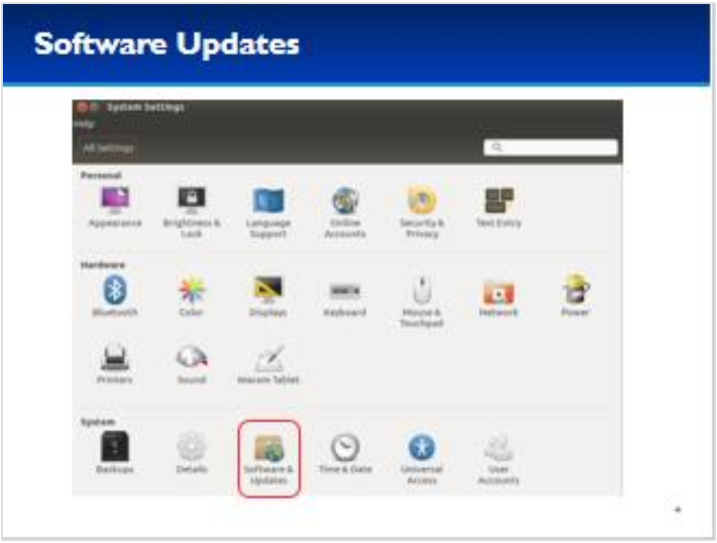


User Management

- User account management can be performed through the GUI using User Accounts under System Settings.

  - Here you can create or delete accounts, change account type, or change users passwords.

Slide 4

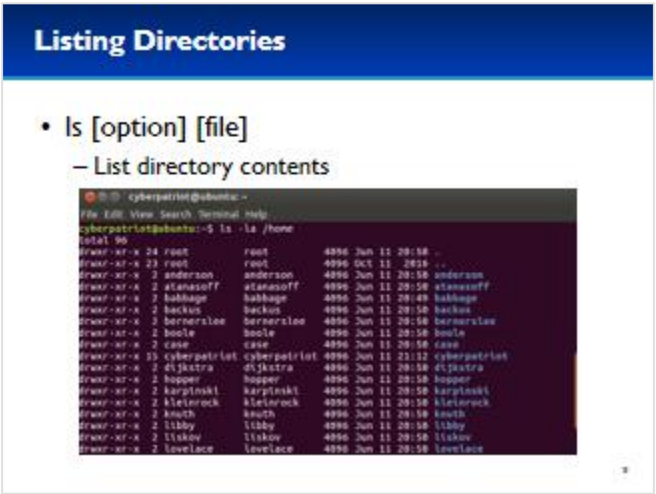


Software Updates

- Automatic updates can be configured through Software and Updates in System Settings.

  - Here you can configure software sources, as well as automatic update frequency.

Slide 5



Listing Directories

- ls [option] [file]
  - List directory contents

```
cyberpatriot@ubuntu: ~
File  Edit  View  Search  Terminal  Help
cyberpatriot@ubuntu:~$ ls -la /home
total 96
drwxr-xr-x 24 root         root         4096 Jun 11 20:58 .
drwxr-xr-x 23 root         root         4096 Oct 11  2016 ..
drwxr-xr-x  2 anderson     anderson     4096 Jun 11 20:58 anderson
drwxr-xr-x  2 atanasoff    atanasoff    4096 Jun 11 20:58 atanasoff
drwxr-xr-x  2 babbage      babbage      4096 Jun 11 20:49 babbage
drwxr-xr-x  2 backus       backus       4096 Jun 11 20:58 backus
drwxr-xr-x  3 bernerslee   bernerslee   4096 Jun 11 20:58 bernerslee
drwxr-xr-x  2 boole        boole        4096 Jun 11 20:58 boole
drwxr-xr-x  2 case         case         4096 Jun 11 20:58 case
drwxr-xr-x 15 cyberpatriot cyberpatriot 4096 Jun 11 21:12 cyberpatriot
drwxr-xr-x  2 dijkstra     dijkstra     4096 Jun 11 20:58 dijkstra
drwxr-xr-x  2 hopper       hopper       4096 Jun 11 20:58 hopper
drwxr-xr-x  2 karpinski    karpinski    4096 Jun 11 20:58 karpinski
drwxr-xr-x  2 kleinrock    kleinrock    4096 Jun 11 20:58 kleinrock
drwxr-xr-x  2 knuth        knuth        4096 Jun 11 20:58 knuth
drwxr-xr-x  2 libby        libby        4096 Jun 11 20:58 libby
drwxr-xr-x  2 liskov       liskov       4096 Jun 11 20:58 liskov
drwxr-xr-x  2 lovelace     lovelace     4096 Jun 11 20:58 lovelace
```

- Navigate to Applications → System Tools →Click on Terminal.

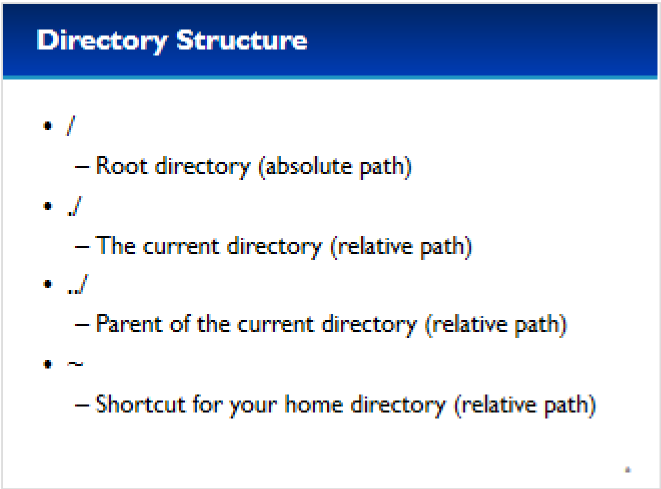
- **ls** lists information about a file or contents of a directory.

  - The **l** option outputs the "long" listing, which prints a lot of useful information such as file permissions, ownership, and modification time.

  - The **a** option outputs hidden files.

  - Hidden files in Linux begin with a dot.

Slide 6



Directory Structure

- /
  - Root directory (absolute path)
- ./
  - The current directory (relative path)
- ../
  - Parent of the current directory (relative path)
- ~
  - Shortcut for your home directory (relative path)

- Directory structures are like trees.

  - In Linux, everything is under the root directory which is represented as a single forward slash.

  - You can think of directories as branches of the tree, and files as the leaves.

- Paths can be either absolute or relative.

  - Absolute paths begin with the root directory.

  - Relative paths begin in the current working directory.

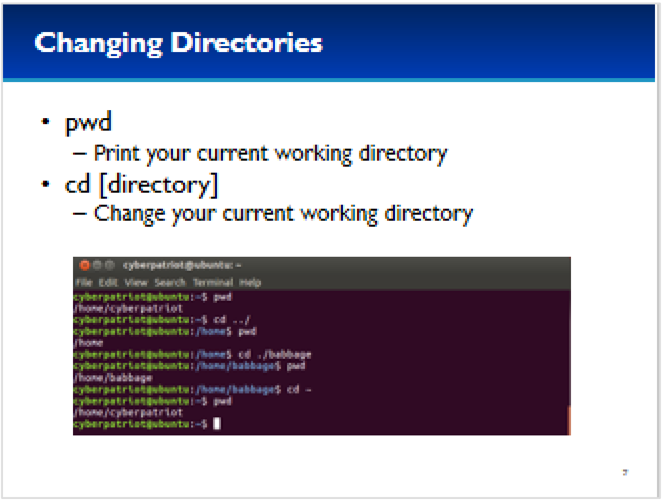
- Every directory has two special directories.

  - The dot directory points to itself, if you begin a path with a dot-slash, you are specifying the current working directory.

  - The dot-dot directory points it's parent, for example the parent of /home is the root directory, if you begin a path with a dot-dot you are specifying the parent of the current working directory.

  - Although they are not directories, some shells have built-in shortcuts, allowing you to use the tilde as a shortcut to your home directory.

Slide 7



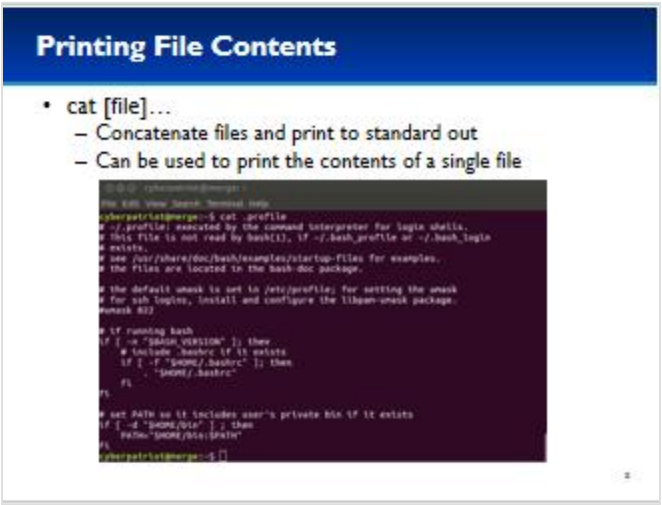
Changing Directories

- pwd
  - Print your current working directory
- cd [directory]
  - Change your current working directory

```
cyberpatriot@ubuntu:~$ pwd
/home/cyberpatriot
cyberpatriot@ubuntu:~$ cd ../
cyberpatriot@ubuntu:/home$ pwd
/home
cyberpatriot@ubuntu:/home$ cd ./babbage
cyberpatriot@ubuntu:/home/babbage$ pwd
/home/babbage
cyberpatriot@ubuntu:/home/babbage$ cd ~
cyberpatriot@ubuntu:~$ pwd
/home/cyberpatriot
cyberpatriot@ubuntu:~$ 
```

- You can print your current working directory using the command **pwd**. On Ubuntu your current working directory is also shown on the right-hand side of your prompt.
- You can change your current working directory by using the **cd** command.

Slide 8



Printing File Contents

- cat [file]…
  - Concatenate files and print to standard out
  - Can be used to print the contents of a single file

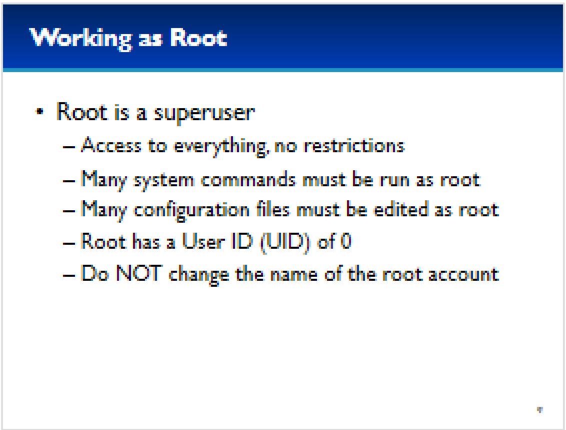
```
cyberpatriot@merge:~$ cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi
cyberpatriot@merge:~$ 
```

8

- The **cat** command is used for concatenating files specified as arguments.

- It is commonly used to print out the contents of a single file.

Slide 9



Working as Root

- Root is a superuser
  - Access to everything, no restrictions
  - Many system commands must be run as root
  - Many configuration files must be edited as root
  - Root has a User ID (UID) of 0
  - Do NOT change the name of the root account

- All Linux systems have a superuser named root.

- Root has access to everything, with no restrictions.

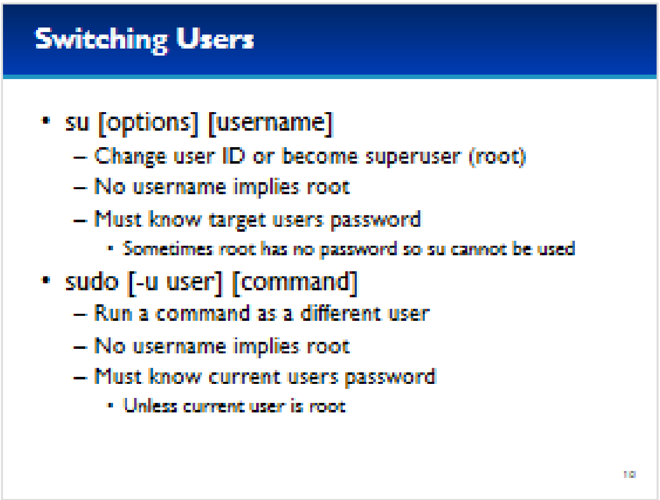
  - Be careful what you do as root, you can permanently destroy your OS with a small typo.

- There are many system commands that can only be run by root, and many system configuration files that must be edited as root.

- Root always has a User ID of 0.

- While technically possible, please don't change the name of the root account; this is not a recommended security practice and will likely break a great many things on your computer.

Slide 10



Switching Users

- su [options] [username]
  - Change user ID or become superuser (root)
  - No username implies root
  - Must know target users password
    - Sometimes root has no password so su cannot be used
- sudo [-u user] [command]
  - Run a command as a different user
  - No username implies root
  - Must know current users password
    - Unless current user is root

10

- When you need to run a command or edit a file as root, or any other user, there are two commands you can use.

- The **su** command allows you to switch to another user, if you don’t specify a username, **su** will assume you want to be root.

  - The **su** command requires you to know the password of the user you are switching to.

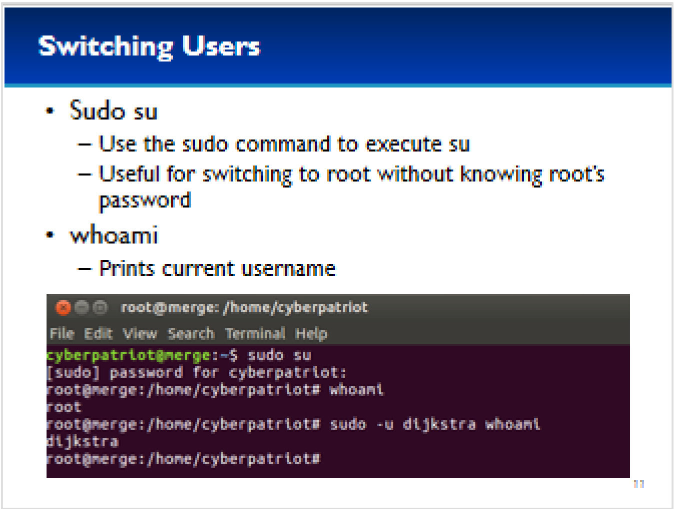
  - Ubuntu does not assign a root password by default as a security feature to prevent anyone from logging in as root, unfortunately this means you can’t use **su** by itself to become root.

- The **sudo** command will allow you to run a specific command as a different user.

  - Again, if you don’t specify a user, **sudo** will assume you want to be root.

  - The **sudo** command however, only requires you to know your own password (and that you are an administrator).

Slide 11



Switching Users

- Sudo su
  - Use the sudo command to execute su
  - Useful for switching to root without knowing root’s password
- whoami
  - Prints current username

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help

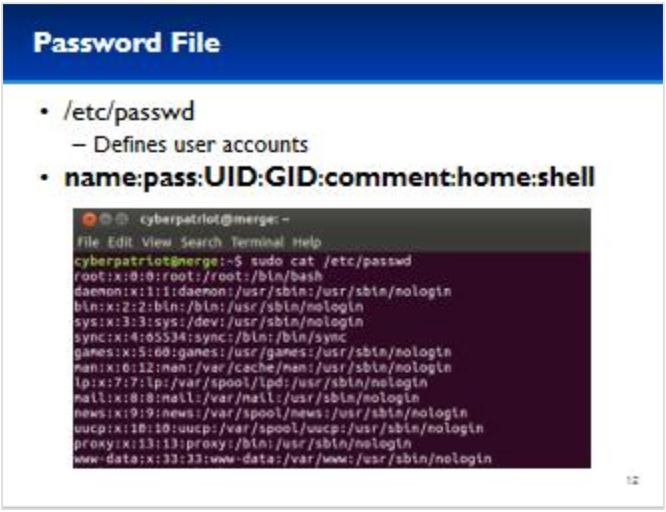
```
cyberpatriot@merge:~$ sudo su
[sudo] password for cyberpatriot:
root@merge:/home/cyberpatriot# whoami
root
root@merge:/home/cyberpatriot# sudo -u dijkstra whoami
dijkstra
root@merge:/home/cyberpatriot#
```

- If you want to become root, but are unable to use **su** because root has no password, you can use **sudo su**.

- This works because **sudo** requires you to know your own password to run **su** as root, and if you run su as root, su doesn’t ask you for a password.

- If you want to see your current username you can use the **whoami** command. Ubuntu also prints your username on the left hand side of your prompt.

Slide 12



Password File

- /etc/passwd
  - Defines user accounts
- **name:pass:UID:GID:comment:home:shell**

```
cyberpatriot@merge:~$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

12

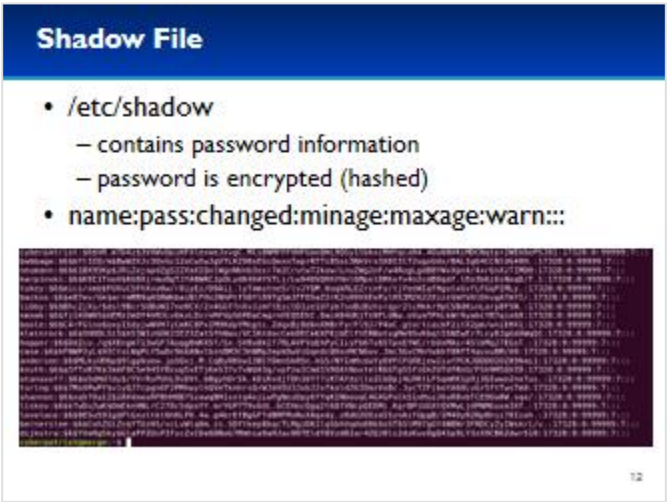
- The /etc/password file contains the list of user accounts.

  - Many of these user accounts are used exclusively by system services.

- The password file format is defined as username, password, User ID, Primary Group ID, comment, home directory, and login shell.

- However, since this file needs to be readable by everyone, passwords are usually stored in the shadow file instead.

Slide 13



Shadow File

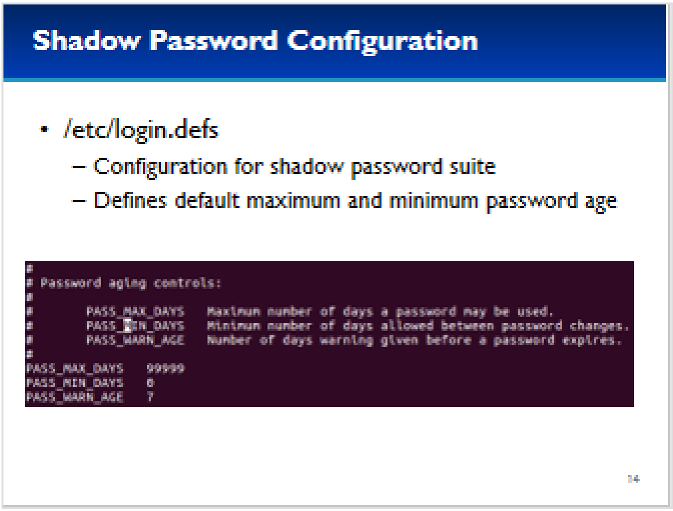
- /etc/shadow
  - contains password information
  - password is encrypted (hashed)
- name:pass:changed:minage:maxage:warn:::

```
[illegible]
```

12

- The shadow file contains the user’s name, encrypted password, when the password was last changed, the user’s minimum password age, the maximum password age, and the number of days before an expiring password generates a warning.

Slide 14



Shadow Password Configuration

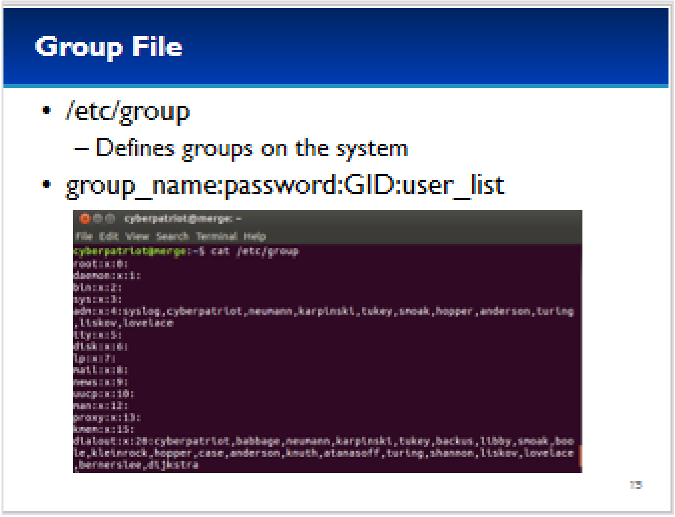
- /etc/login.defs
  - Configuration for shadow password suite
  - Defines default maximum and minimum password age

```
#
# Password aging controls:
#
#         PASS_MAX_DAYS   Maximum number of days a password may be used.
#         PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#         PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

14

- The login.defs file is a configuration file for the shadow password suite.
- Inside this file are many configuration options, including the default maximum and minimum password age for new users.
- Changing these values however does not modify existing user accounts.

Slide 15



Group File

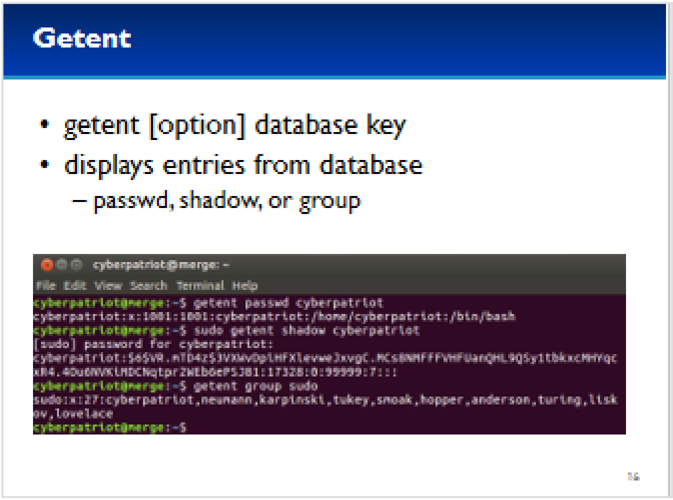
- /etc/group
  - Defines groups on the system
- group_name:password:GID:user_list

```
cyberpatriot@merge:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cyberpatriot,neumann,karpinski,tukey,snoak,hopper,anderson,turing
,liskov,lovelace
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:cyberpatriot,babbage,neumann,karpinski,tukey,backus,libby,snoak,boo
le,kleinrock,hopper,case,anderson,knuth,atanasoff,turing,shannon,liskov,lovelace
,bernerslee,dijkstra
```

15

- The group file defines the user groups on the system.
- The format for the groups file is the group name, password, Group ID, and a list of users in that group.
- Although it is possible to add a password to a group, this feature is generally not used.

Slide 16



Getent

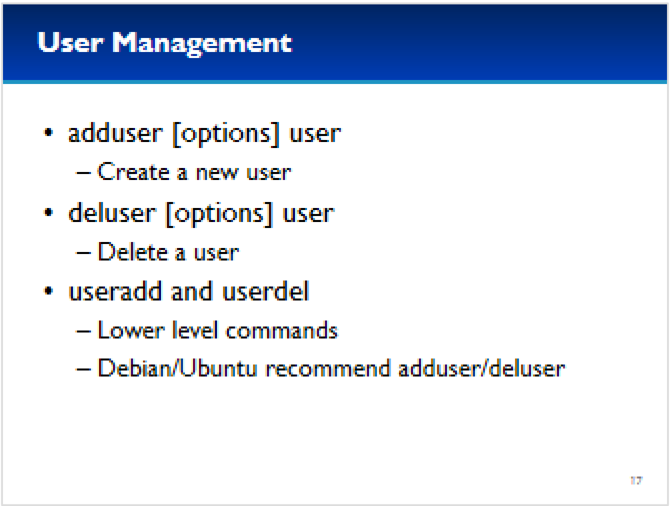
- getent [option] database key
- displays entries from database
  - passwd, shadow, or group

```
cyberpatriot@merge:~$ getent passwd cyberpatriot
cyberpatriot:x:1001:1001:cyberpatriot:/home/cyberpatriot:/bin/bash
cyberpatriot@merge:~$ sudo getent shadow cyberpatriot
[sudo] password for cyberpatriot:
cyberpatriot:$6$VR.mTD4z$3VXWvDplHFXlevweJxvgC.MCs8NMFFFVHFUanQHL9QSy1tbkxcMHYqc
xR4.4Ou6NVKlMDCNqtpr2WEb6eP5J81:17328:0:99999:7:::
cyberpatriot@merge:~$ getent group sudo
sudo:x:27:cyberpatriot,neumann,karpinski,tukey,snoak,hopper,anderson,turing,lisk
ov,lovelace
cyberpatriot@merge:~$
```

16

- If you want to get a line from the password, shadow, or group file you can use the **getent** command.

Slide 17



User Management

- adduser [options] user
  - Create a new user
- deluser [options] user
  - Delete a user
- useradd and userdel
  - Lower level commands
  - Debian/Ubuntu recommend adduser/deluser

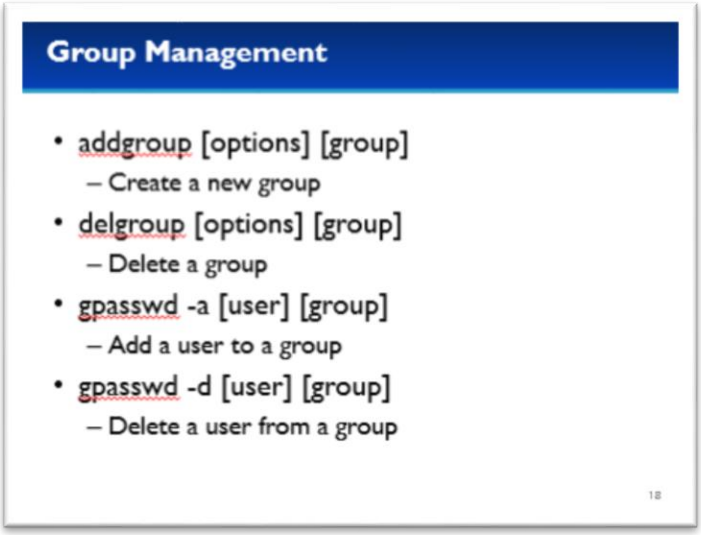
17

- User management from the command line should be performed with the **adduser** and **deluser** commands.

  - These are the recommended commands for Debian and Ubuntu, however they don't exist on all Linux distributions.

- The **useradd** and **userdel** commands are lower-level commands that are more difficult to use, but they exist on all Linux distributions.

Slide 18



Group Management

- addgroup [options] [group]
  - Create a new group
- delgroup [options] [group]
  - Delete a group
- gpasswd -a [user] [group]
  - Add a user to a group
- gpasswd -d [user] [group]
  - Delete a user from a group

18

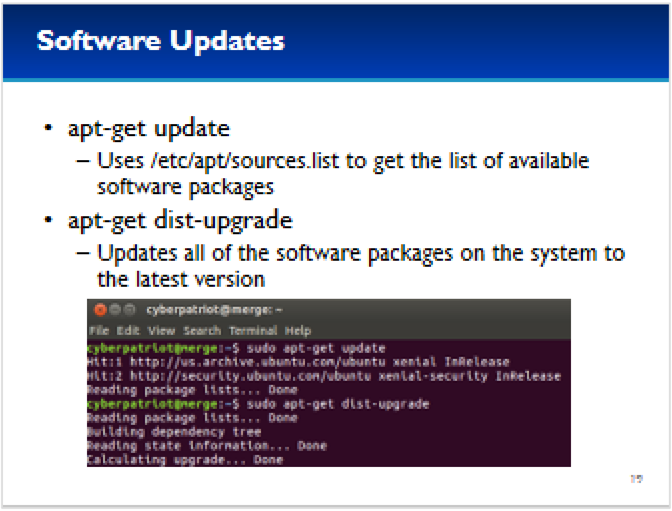
- Similarly, you can create and delete groups with the **addgroup** and **delgroup** commands.

- Group membership can be modified using the **gpasswd** command.

  - The **-a** option adds the specified user to the group.

  - The **-d** option removes the specified user from the group.

Slide 19



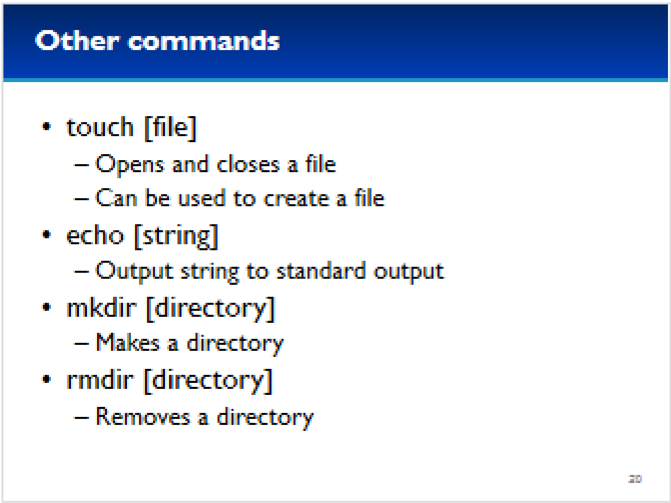
Software Updates

- apt-get update
  - Uses /etc/apt/sources.list to get the list of available software packages
- apt-get dist-upgrade
  - Updates all of the software packages on the system to the latest version

```
cyberpatriot@merge:~$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://security.ubuntu.com/ubuntu xenial-security InRelease
Reading package lists... Done
cyberpatriot@merge:~$ sudo apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
```

- Software updates from the command line are easy.
- You first run **apt-get** update to get the list of latest packages available.
- Then you run **apt-get dist-upgrade** to update the packages on your system to the latest version.
- However, this assumes that your sources.list file is correctly configured.

Slide 20



Other commands

- touch [file]
  - Opens and closes a file
  - Can be used to create a file
- echo [string]
  - Output string to standard output
- mkdir [directory]
  - Makes a directory
- rmdir [directory]
  - Removes a directory

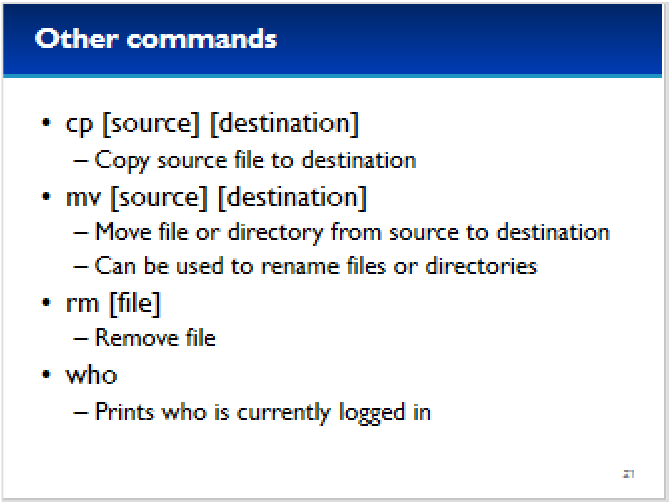
20

- The **touch** command opens and closes a file, but this command is mostly used create a new, empty file.

- The **echo** command prints out its arguments to standard output, we will discuss this more later, but standard output goes to the terminal by default.

- The **mkdir** command can be used to make directories, and the **rmdir** command can be used to delete empty directories.

Slide 21



Other commands

- cp [source] [destination]
  - Copy source file to destination
- mv [source] [destination]
  - Move file or directory from source to destination
  - Can be used to rename files or directories
- rm [file]
  - Remove file
- who
  - Prints who is currently logged in

21

- **cp** stands for copy, and is used to copy files, you can specify a new name for the copied file, or if the destination is a directory, the file will be copied to that directory with the same name.

- **mv** is used to move files, similar to the **cp** command, you can specify a new name for the file, or if the destination is a directory, the file will be moved into that directory with the same name.

- The **rm** command is used to remove a file.

Slide 22

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

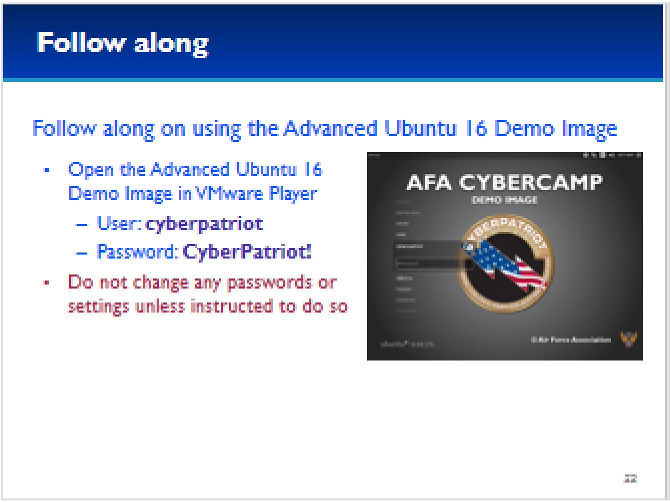
Init Systems

🕒 Devote 30 minutes to slides 23-45. Allow the students 20 minutes to complete the activity on slide 45.

☆Throughout this section, students should follow along in the **Advanced Ubuntu 16 Demo Image**.

☆In this section, we will cover advanced init systems, going into detail about how Linux boots and starts services. You’ll learn the many places to look to identify unwanted services and know how to disable them.

Slide 23



Follow along

Follow along on using the Advanced Ubuntu 16 Demo Image

- Open the Advanced Ubuntu 16 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Do not change any passwords or settings unless instructed to do so

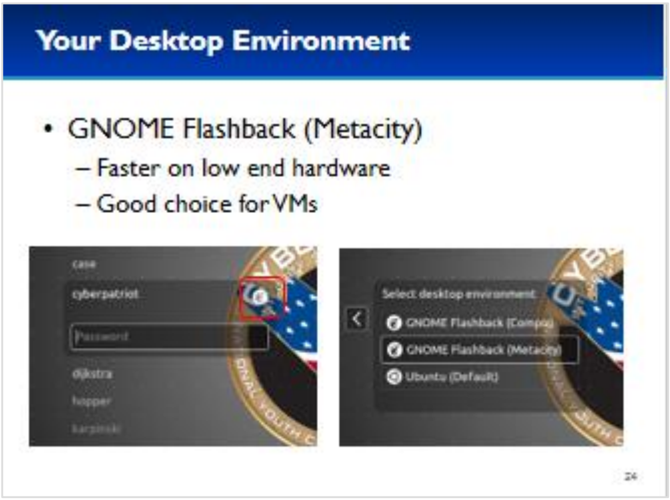
22

☆Have the students follow along if possible and time permits.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so.

☆Users are NOT automatically logged in, they should log in as the user cyberpatriot with the password CyberPatriot!

Slide 24



Your Desktop Environment

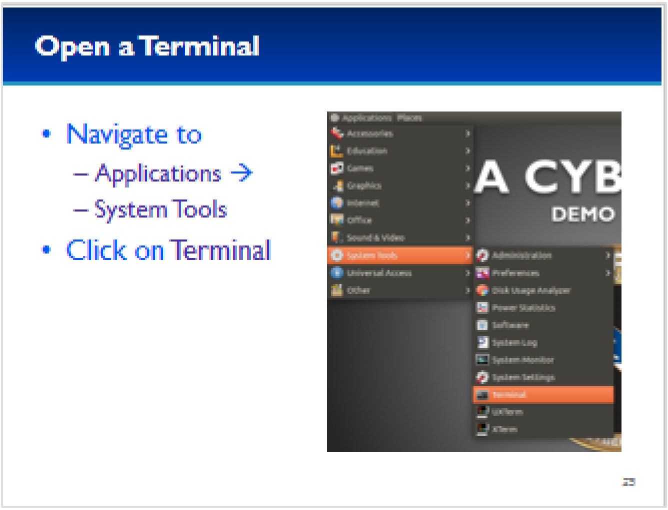
- GNOME Flashback (Metacity)
  - Faster on low end hardware
  - Good choice for VMs

- Before we begin, it’s worth noting that your default desktop environment is GNOME Flashback (Metacity).

  - This looks similar to the traditional GNOME 2 desktop environment.

  - This desktop environment is a good choice for virtual machines since it doesn’t have fancy 3D effects and has low system requirements.

Slide 25

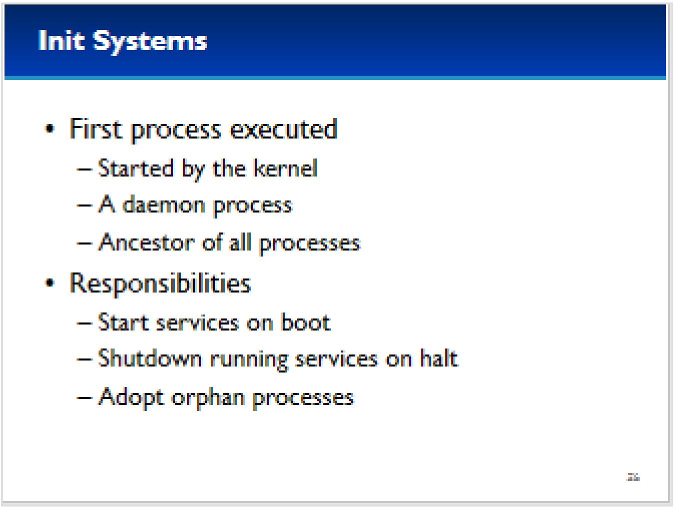


Open a Terminal

- Navigate to
  - Applications →
  - System Tools
- Click on Terminal

- Notice this desktop environment is different from the default Unity desktop environment.
- Open a Terminal now by navigating to Applications → System Tools and clicking on terminal.

Slide 26



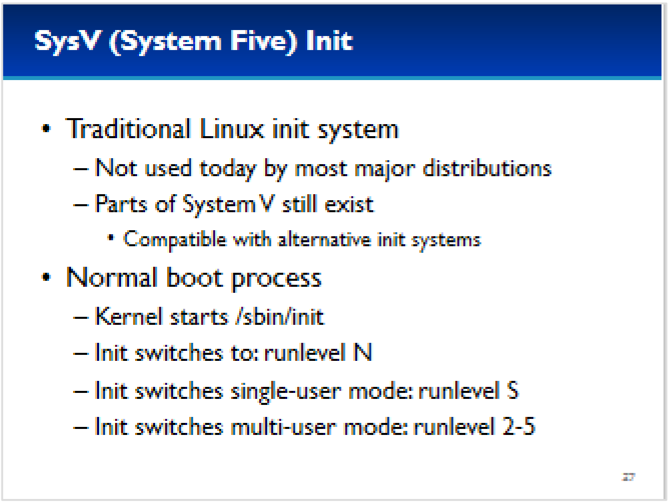
Init Systems

- First process executed
  - Started by the kernel
  - A daemon process
  - Ancestor of all processes
- Responsibilities
  - Start services on boot
  - Shutdown running services on halt
  - Adopt orphan processes

26

- Linux starts with the boot process.
- Init is the first process executed by the kernel.
- It is sometimes referred to as a daemon process because it is running all the time in the background.
- All new processes are created by existing processes, therefore Init is the ancestor of all processes.
- Init traditionally has only a few responsibilities that include starting services on boot, shutting down services on halt, and the adoption of orphaned processes.
  - Although it's not really relevant to our discussion today, when a process' parent dies that process is known as an orphan process, and init becomes the parent of that process.

Slide 27



SysV (System Five) Init

- Traditional Linux init system
  - Not used today by most major distributions
  - Parts of System V still exist
    - Compatible with alternative init systems
- Normal boot process
  - Kernel starts /sbin/init
  - Init switches to: runlevel N
  - Init switches single-user mode: runlevel S
  - Init switches multi-user mode: runlevel 2-5

27

- System V init is the traditional Unix and Linux init system.

  - It's no longer used today by most major distributions, however a large amount of the System V init system still exists on some Linux distributions.

  - Alternatively, init systems are also compatible with System Five, and are therefore still used by many services.

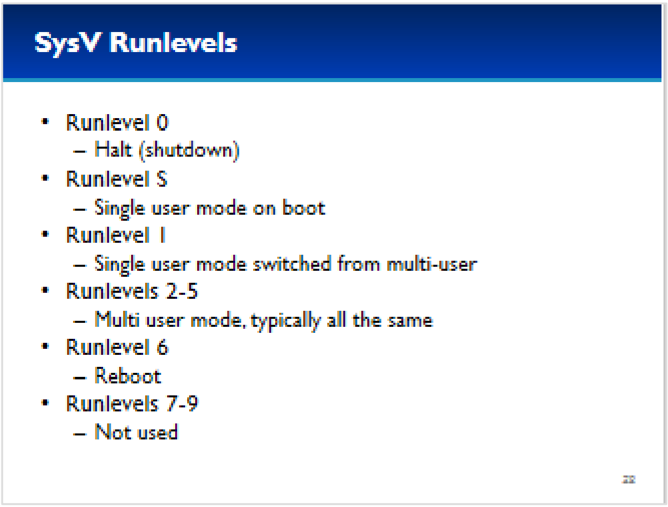
- In the normal System V boot process of Debian and Ubuntu, the kernel starts init.

- Init then immediately switches to runlevel N and initializes the system.

- Then, init switches to runlevel S to initialize the system in single-user mode to complete tasks such as hardware initialization

- After runlevel S, the init switches to a specific multi-user mode; runlevel 2-5. The default is runlevel 3.

Slide 28



SysV Runlevels

- Runlevel 0
  - Halt (shutdown)
- Runlevel S
  - Single user mode on boot
- Runlevel 1
  - Single user mode switched from multi-user
- Runlevels 2-5
  - Multi user mode, typically all the same
- Runlevel 6
  - Reboot
- Runlevels 7-9
  - Not used

- Here is a description of the different runlevels:

  - Runlevel 0 is used to halt the system.

  - Runlevel S is the single-user mode, used to boot the system.

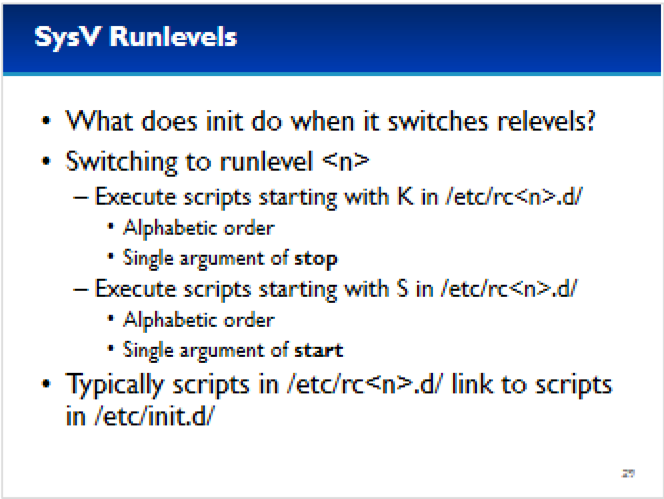
  - Runlevel 1 is the single user mode that can be used to switch from multi-user mode.

  - Runlevels 2 through 5 are multi-user mode runlevels, with 3 being the default. However, on Debian and Ubuntu all these runlevels are the same by default so it doesn’t much matter.

  - Runlevel 6 is used for rebooting the system.

  - Finally, Runlevels 7-9 are technically valid, but not used.

Slide 29



SysV Runlevels

- What does init do when it switches relevels?
- Switching to runlevel <n>
  - Execute scripts starting with K in /etc/rc<n>.d/
    - Alphabetic order
    - Single argument of **stop**
  - Execute scripts starting with S in /etc/rc<n>.d/
    - Alphabetic order
    - Single argument of **start**
- Typically scripts in /etc/rc<n>.d/ link to scripts in /etc/init.d/

29

- I'm sure you are wondering what init does when switching to and from these runlevels.

- It's easy to see for yourself.

- When init switches to runlevel n, it first stops services in it's directory that start with a K, and it does this in alphabetic order.

  - Here, K stands for kill.

  - Init does this by running all the K scripts in /etc/rc<n>.d/ with a single argument of stop

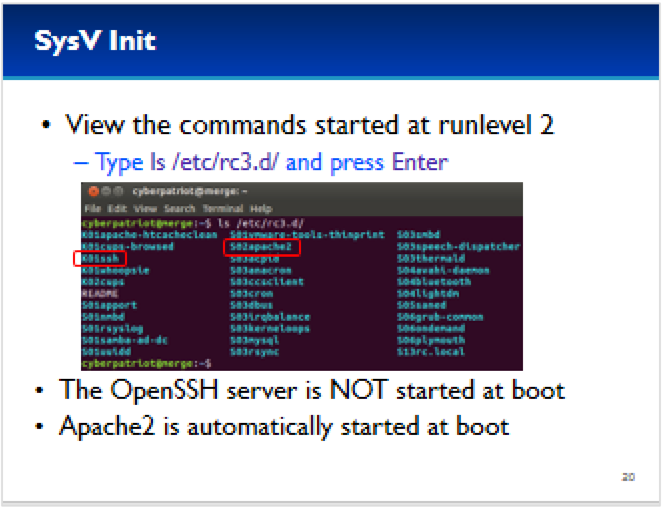
- Then, it starts processes in the same directory that start with an S.

  - S stands for start.

  - Similarly, init accomplishes this by running all the S scripts in /etc/rc<n>.d with a single argument of start.

- We'll talk more about links later, but typically all of the scripts in /etc/rc<n>.d/ are actually just links to scripts in: /etc/init.d/

Slide 30



SysV Init

- View the commands started at runlevel 2
  - Type ls /etc/rc3.d/ and press Enter

```
cyberpatriot@merge:~$ ls /etc/rc3.d/
K01apache-htcacheclean  S01vmware-tools-thinprint  S03smbd
K01cups-browsed         S02apache2                 S03speech-dispatcher
K01ssh                  S03acpid                   S03thermald
K01whoopsie             S03anacron                 S04avahi-daemon
K02cups                 S03ccsclient               S04bluetooth
README                  S03cron                    S04lightdm
S01apport               S03dbus                    S05saned
S01nmbd                 S03irqbalance              S06grub-common
S01rsyslog              S03kerneloops              S06ondemand
S01samba-ad-dc          S03mysql                   S06plymouth
S01uuidd                S03rsync                   S13rc.local
cyberpatriot@merge:~$
```

- The OpenSSH server is NOT started at boot
- Apache2 is automatically started at boot

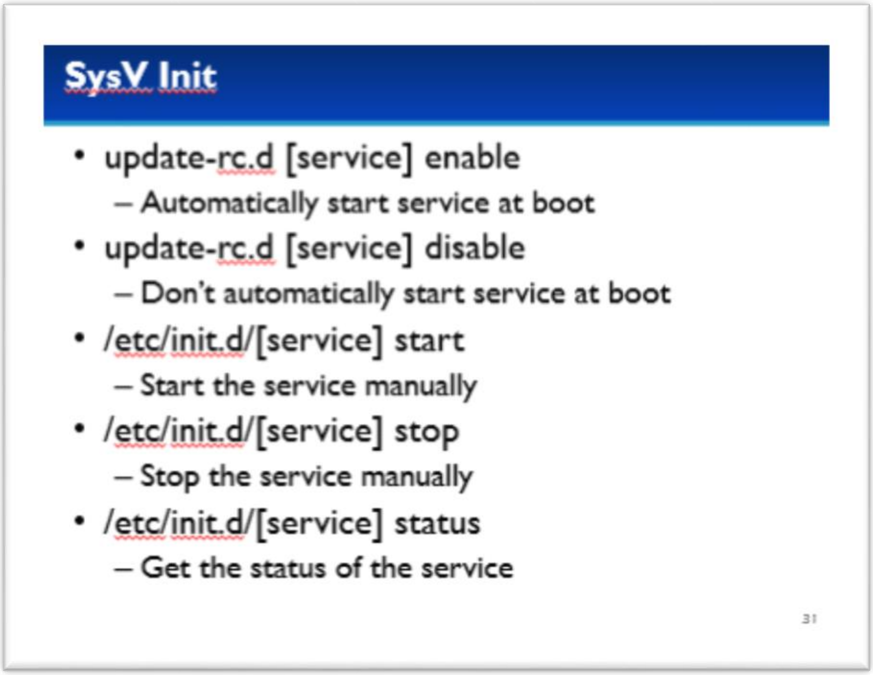
20

- To view the scripts that get started and stopped at runlevel 3, type: **ls /etc/rc3.d/**

  - Here we can see that the OpenSSH server is not configured to start at boot since the link in this directory starts with a K.

  - However, it looks like the Apache2 service is starting at boot since it’s link starts with an S.

Slide 31



SysV Init

- update-rc.d [service] enable
  - Automatically start service at boot
- update-rc.d [service] disable
  - Don’t automatically start service at boot
- /etc/init.d/[service] start
  - Start the service manually
- /etc/init.d/[service] stop
  - Stop the service manually
- /etc/init.d/[service] status
  - Get the status of the service

31

- To define if a service starts at boot, you can use the **update-rc.d** command.

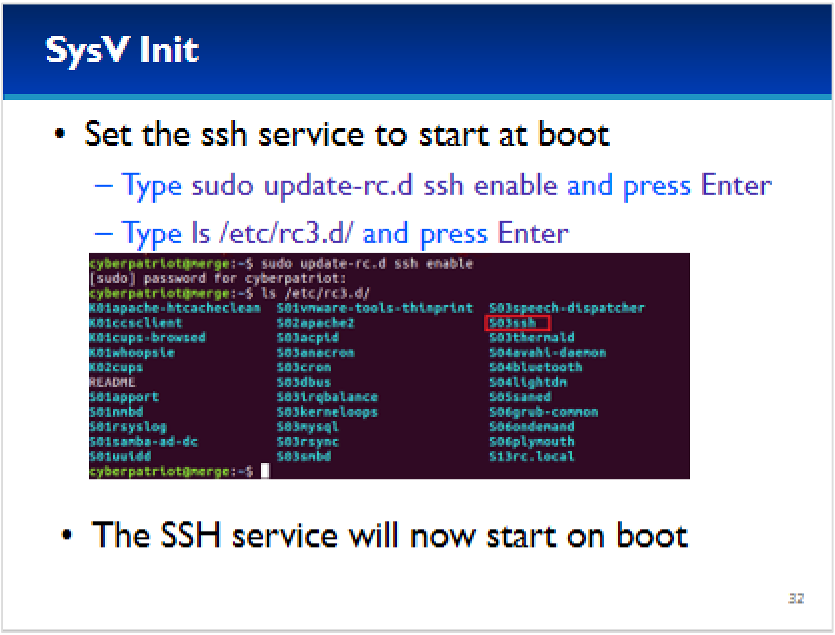
  - The first argument to **update-rc.d** is the name of the service, followed by either enable or disable.

- You can start or stop a service manually by using the init scripts in: /etc/init.d/

  - Just run the script that you want and pass it a single command line argument, either start or stop.

  - You can also use the status argument to print out the status of a service.

Slide 32



SysV Init

- Set the ssh service to start at boot
  - Type sudo update-rc.d ssh enable and press Enter
  - Type ls /etc/rc3.d/ and press Enter

```
cyberpatriot@merge:~$ sudo update-rc.d ssh enable
[sudo] password for cyberpatriot:
cyberpatriot@merge:~$ ls /etc/rc3.d/
K01apache-htcacheclean  S01vmware-tools-thinprint  S03speech-dispatcher
K01ccsclient            S02apache2                 S03ssh
K01cups-browsed         S03acpid                   S03thermald
K01whoopsie             S03anacron                 S04avahi-daemon
K02cups                 S03cron                    S04bluetooth
README                  S03dbus                    S04lightdm
S01apport               S03irqbalance              S05saned
S01nmbd                 S03kerneloops              S06grub-common
S01rsyslog              S03mysql                   S06ondemand
S01samba-ad-dc          S03rsync                   S06plymouth
S01uuidd                S03smbd                    S13rc.local
cyberpatriot@merge:~$
```

- The SSH service will now start on boot

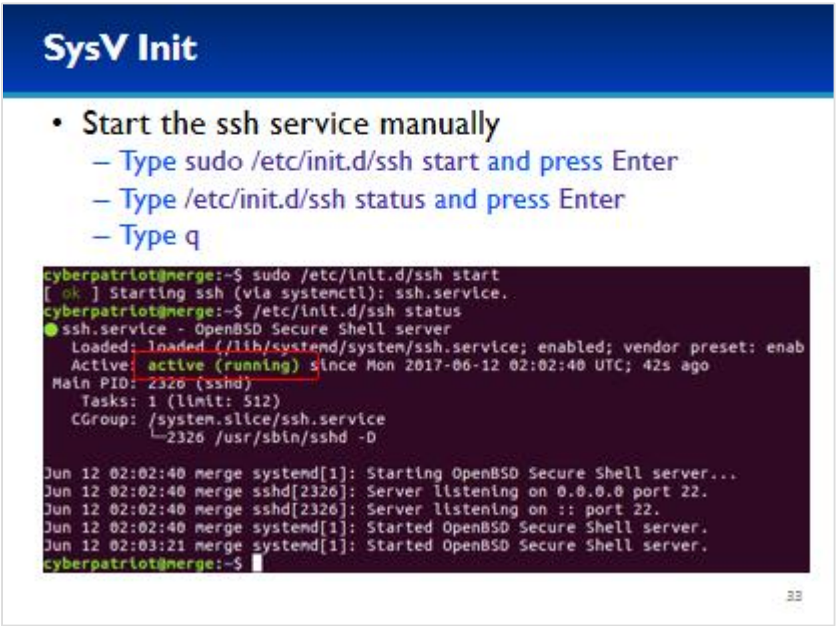
32

- We want the SSH service to automatically start at boot.

☆Have the students run the commands on the screen.

- After running the commands, notice that the ssh link in /etc/rc3.d/ now starts with an S.

Slide 33



SysV Init

- Start the ssh service manually
  - Type sudo /etc/init.d/ssh start and press Enter
  - Type /etc/init.d/ssh status and press Enter
  - Type q

```
cyberpatriot@merge:~$ sudo /etc/init.d/ssh start
[ ok ] Starting ssh (via systemctl): ssh.service.
cyberpatriot@merge:~$ /etc/init.d/ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Mon 2017-06-12 02:02:40 UTC; 42s ago
 Main PID: 2326 (sshd)
    Tasks: 1 (limit: 512)
   CGroup: /system.slice/ssh.service
           └─2326 /usr/sbin/sshd -D

Jun 12 02:02:40 merge systemd[1]: Starting OpenBSD Secure Shell server...
Jun 12 02:02:40 merge sshd[2326]: Server listening on 0.0.0.0 port 22.
Jun 12 02:02:40 merge sshd[2326]: Server listening on :: port 22.
Jun 12 02:02:40 merge systemd[1]: Started OpenBSD Secure Shell server.
Jun 12 02:03:21 merge systemd[1]: Started OpenBSD Secure Shell server.
cyberpatriot@merge:~$ 
```

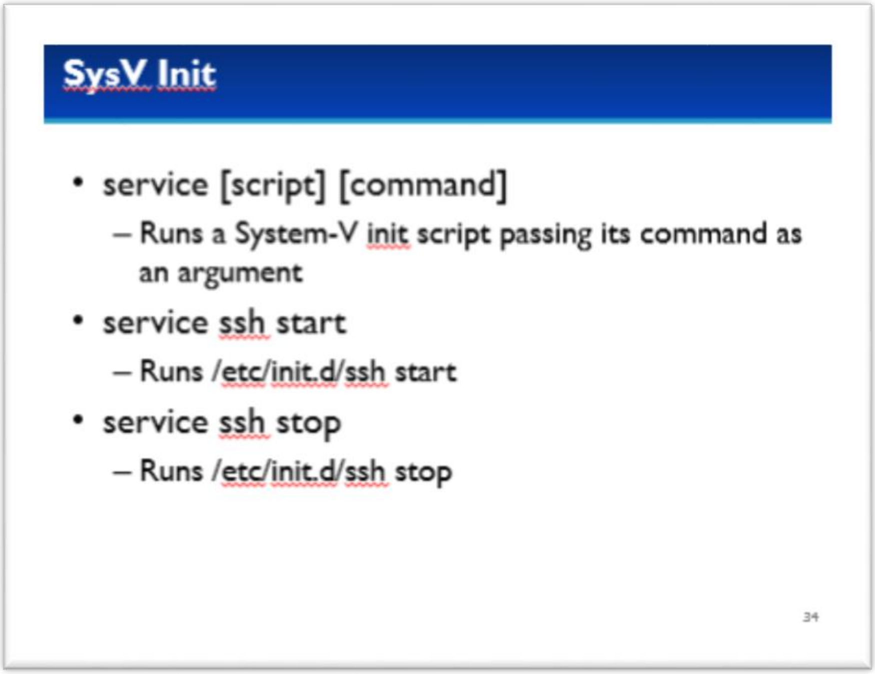
33

- Although we told the ssh service to start at boot, it is not running at the moment.
  - We are going to start the ssh service manually.

☆Have the students run the commands on the screen.

- After starting the ssh service, the status now shows active (running).

Slide 34



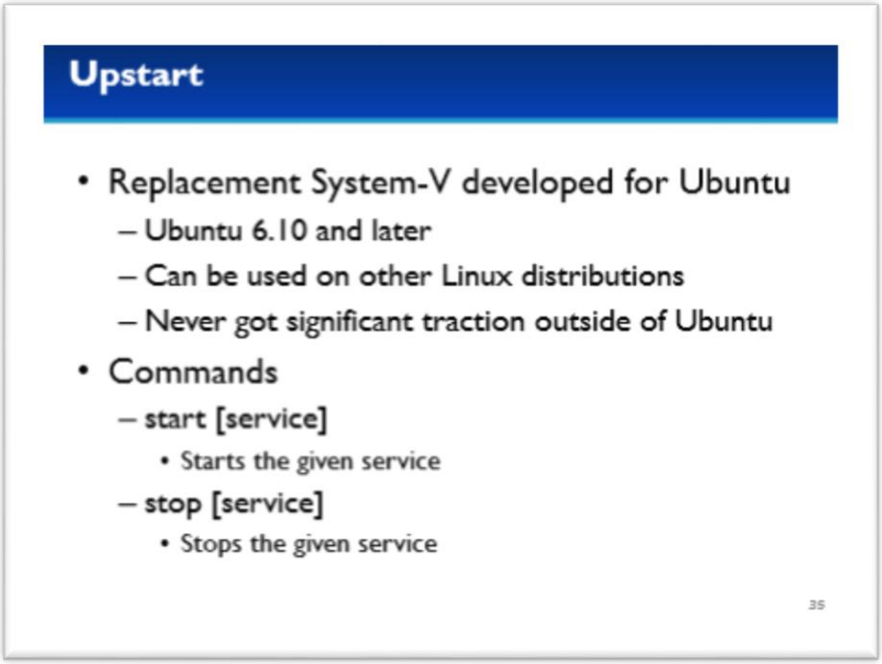
SysV Init

- service [script] [command]
  - Runs a System-V init script passing its command as an argument
- service ssh start
  - Runs /etc/init.d/ssh start
- service ssh stop
  - Runs /etc/init.d/ssh stop

34

- The **service** command can also be used to start and stop services manually, it simply runs the init script with the specified argument.

Slide 35



Upstart

- Replacement System-V developed for Ubuntu
  - Ubuntu 6.10 and later
  - Can be used on other Linux distributions
  - Never got significant traction outside of Ubuntu
- Commands
  - start [service]
    - Starts the given service
  - stop [service]
    - Stops the given service

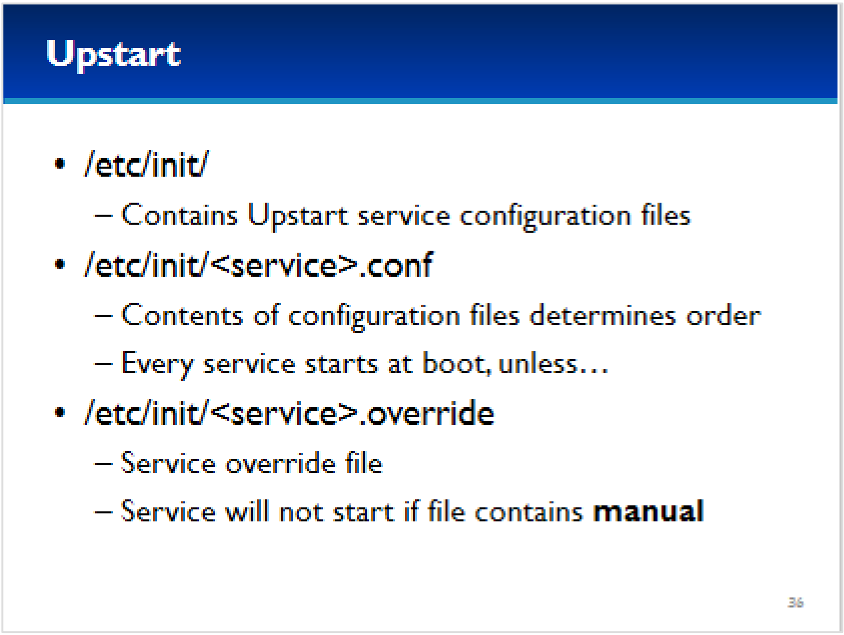
35

- Upstart was an alternative init system initially developed for Ubuntu and works with Ubuntu 6.10 and later.

- It can be used on other Linux distributions but it really never got significant traction outside of Ubuntu.

  - Upstart was made to be backwards-compatible with System-V by being able to run System-V init scripts.

Slide 36



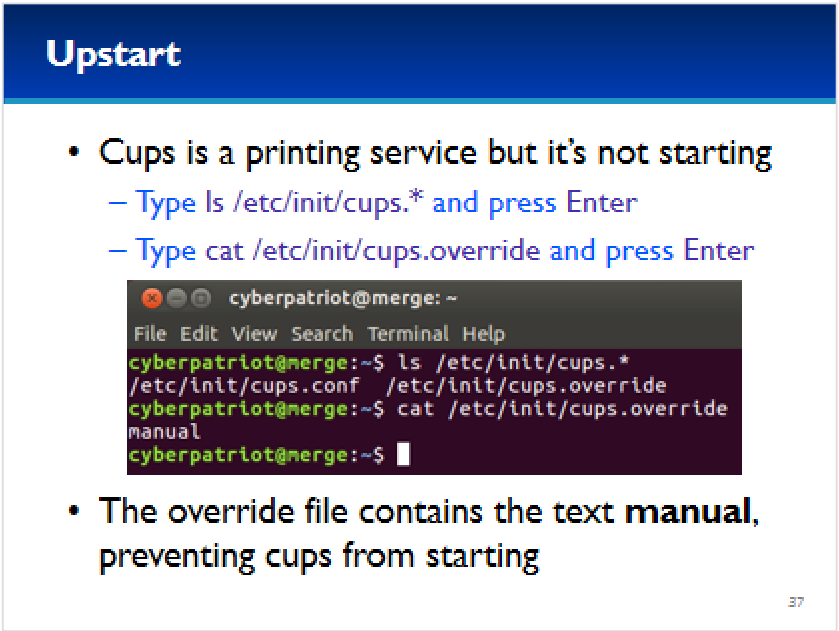
Upstart

- /etc/init/
  - Contains Upstart service configuration files
- /etc/init/<service>.conf
  - Contents of configuration files determines order
  - Every service starts at boot, unless…
- /etc/init/<service>.override
  - Service override file
  - Service will not start if file contains **manual**

36

- Upstart services are specified in the /etc/init directory.
- Each service has its own configuration file ending with .conf.
- Under upstart, every service starts at boot, unless there exists a service.override file containing the text “manual.”

Slide 37



Upstart

- Cups is a printing service but it’s not starting
  - Type ls /etc/init/cups.* and press Enter
  - Type cat /etc/init/cups.override and press Enter

```
cyberpatriot@merge:~$ ls /etc/init/cups.*
/etc/init/cups.conf  /etc/init/cups.override
cyberpatriot@merge:~$ cat /etc/init/cups.override
manual
cyberpatriot@merge:~$ 
```

- The override file contains the text **manual**, preventing cups from starting

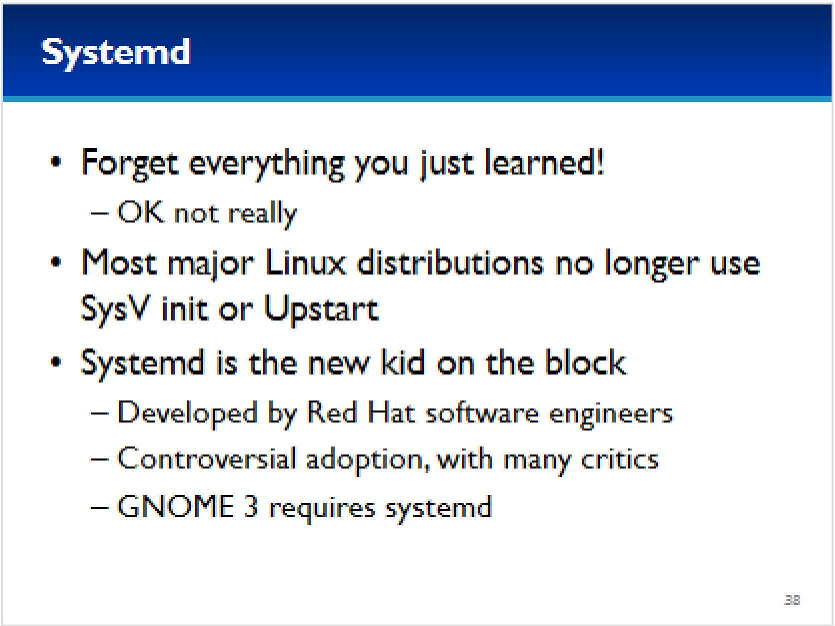
37

- CUPS is a printing service for Linux but it’s not currently starting.

☆Have the students run the commands on the screen.

- As you can see, Upstart won’t start CUPS because of the override file.

Slide 38



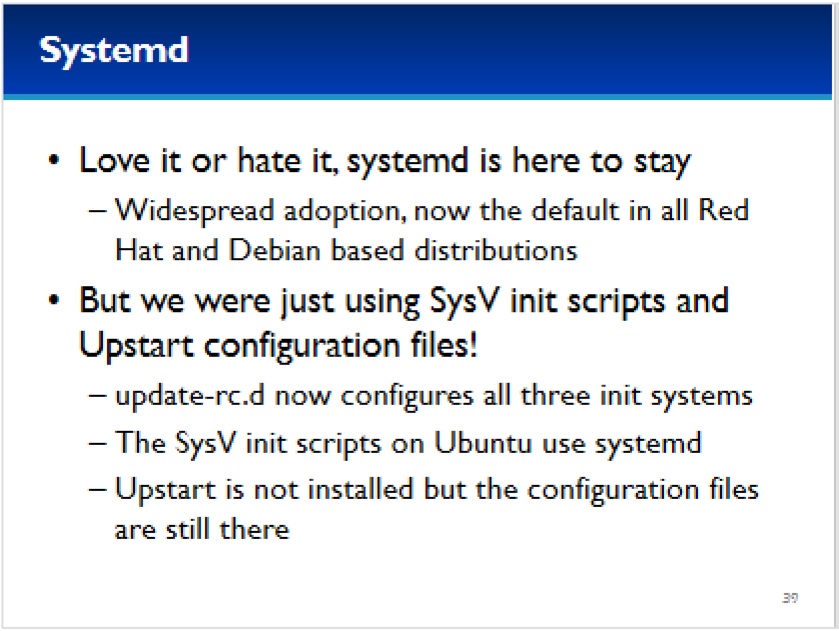
Systemd

- Forget everything you just learned!
  - OK not really
- Most major Linux distributions no longer use SysV init or Upstart
- Systemd is the new kid on the block
  - Developed by Red Hat software engineers
  - Controversial adoption, with many critics
  - GNOME 3 requires systemd

38

- Ok now forget everything you just learned (just kidding, everything you just learned is still relevant and used).
- However as we mentioned before, most major Linux distributions no longer use System V or Upstart as their init systems.
- Currently almost all major Linux distributions, including Ubuntu and Debian now use system.
- Systemd was developed by Red Hat software engineers but it has had a very controversial adoption for many reasons, due in part to the fact that GNOME 3 requires sytemd.
- GNOME 3 is the most widely used Linux desktop environment.

Slide 39



Systemd

- Love it or hate it, systemd is here to stay
  - Widespread adoption, now the default in all Red Hat and Debian based distributions
- But we were just using SysV init scripts and Upstart configuration files!
  - update-rc.d now configures all three init systems
  - The SysV init scripts on Ubuntu use systemd
  - Upstart is not installed but the configuration files are still there

39

- None of this really matters since systemd looks like it is here to stay, and has seen widespread adoption as the default init system in all Red Hat and Debian-based Linux distributions (this encompasses the overwhelming majority of Linux distributions).

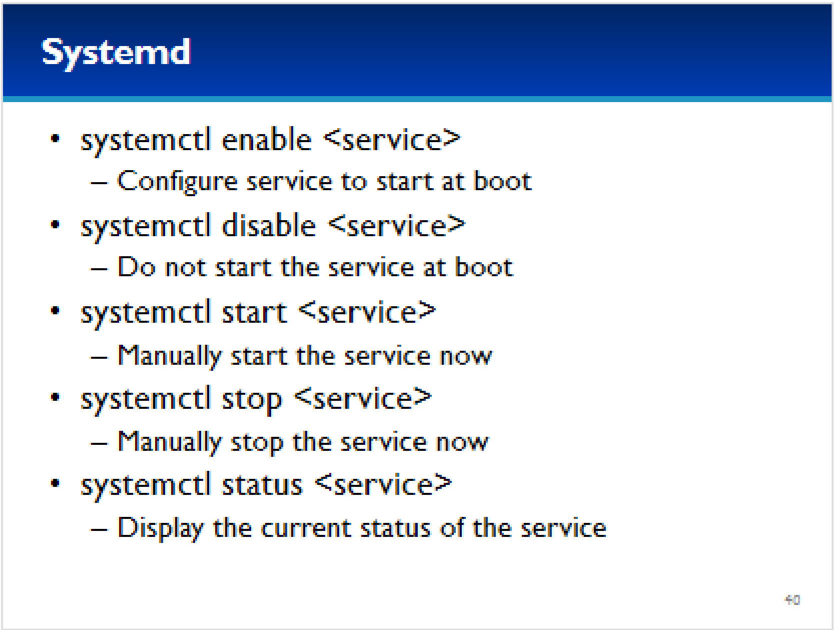
- So how come we just saw all that System-V and Upstart files on our systems if we are now using systemd?

  - **update-rc.d** now configures services for all three init systems.

  - When you run the init scripts manually, most of them actually detect that systemd is being used and instead use systemd to start and stop services.

  - Upstart is not actually currently installed as the default init system either, but it is installed and running on your system for compatibility.

Slide 40



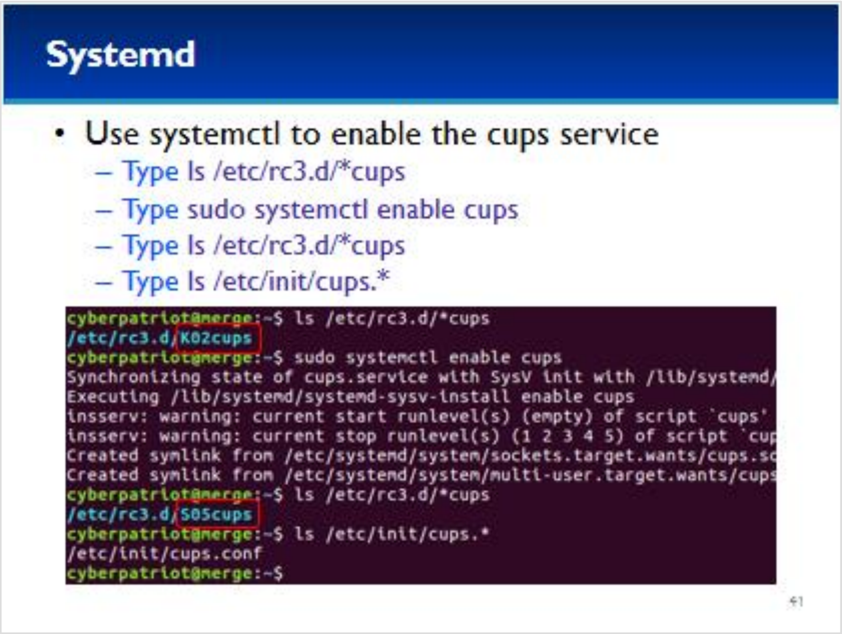
Systemd

- systemctl enable <service>
  - Configure service to start at boot
- systemctl disable <service>
  - Do not start the service at boot
- systemctl start <service>
  - Manually start the service now
- systemctl stop <service>
  - Manually stop the service now
- systemctl status <service>
  - Display the current status of the service

40

- The **systemctl** command is the systemd command for managing services.
- With it, you can configure services to automatically start at boot with the **enable** argument.
- You can stop a service from automatically starting at boot with the **disable** argument.
- If you want to manually start a service, you would use the **start** argument.
- Similarly, the **stop** argument manually stops a service.
- The **status** argument will display the current status of the service.

Slide 41



Systemd

- Use systemctl to enable the cups service
  - Type ls /etc/rc3.d/*cups
  - Type sudo systemctl enable cups
  - Type ls /etc/rc3.d/*cups
  - Type ls /etc/init/cups.*

```
cyberpatriot@merge:~$ ls /etc/rc3.d/*cups
/etc/rc3.d/K02cups
cyberpatriot@merge:~$ sudo systemctl enable cups
Synchronizing state of cups.service with SysV init with /lib/systemd/
Executing /lib/systemd/systemd-sysv-install enable cups
insserv: warning: current start runlevel(s) (empty) of script `cups'
insserv: warning: current stop runlevel(s) (1 2 3 4 5) of script `cup
Created symlink from /etc/systemd/system/sockets.target.wants/cups.so
Created symlink from /etc/systemd/system/multi-user.target.wants/cups
cyberpatriot@merge:~$ ls /etc/rc3.d/*cups
/etc/rc3.d/S05cups
cyberpatriot@merge:~$ ls /etc/init/cups.*
/etc/init/cups.conf
cyberpatriot@merge:~$
```

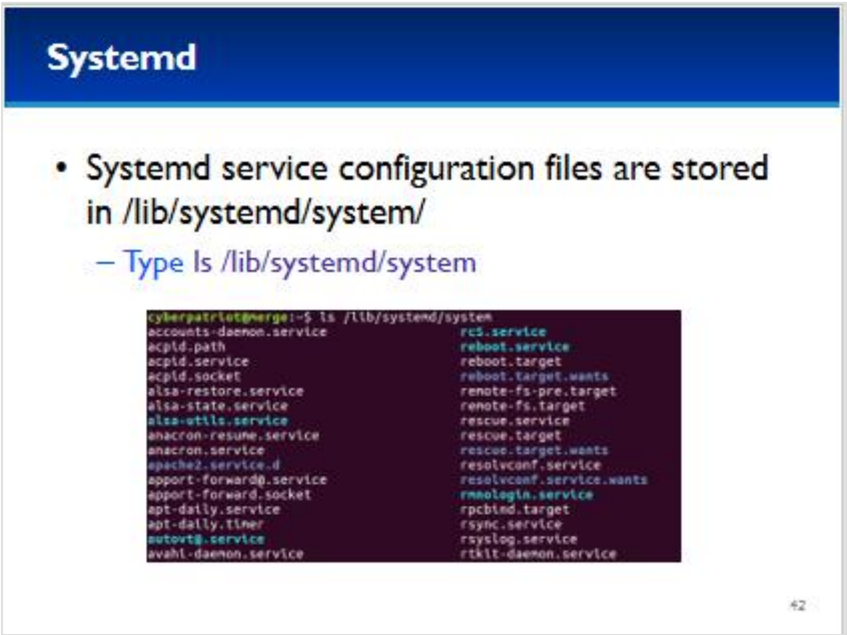
41

- As we saw earlier, the CUPS service was disabled.

☆Have the students run the commands on the screen.
☆Mention that * is a special character that matches any characters (or none).

- After enabling the CUPS service with system, you can see that the System-V and Upstart init systems have been updated as well.

Slide 42



Systemd

- Systemd service configuration files are stored in /lib/systemd/system/
  - Type ls /lib/systemd/system

```
cyberpatriot@merge:~$ ls /lib/systemd/system
accounts-daemon.service                      rc5.service
acpid.path                                   reboot.service
acpid.service                                reboot.target
acpid.socket                                 reboot.target.wants
alsa-restore.service                         remote-fs-pre.target
alsa-state.service                           remote-fs.target
alsa-utils.service                           rescue.service
anacron-resume.service                       rescue.target
anacron.service                              rescue.target.wants
apache2.service.d                            resolvconf.service
apport-forward@.service                      resolvconf.service.wants
apport-forward.socket                        rmnologin.service
apt-daily.service                            rpcbind.target
apt-daily.timer                              rsync.service
autovt@.service                              rsyslog.service
avahi-daemon.service                         rtkit-daemon.service
```

42

- You can find the systemd service in /lib/systemd/system.

☆Have the students run the commands on the screen.

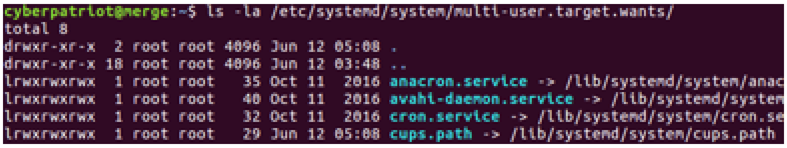
- Most of the services end in .service, however some end in .target or .path, and there are some additional service management files present as well such as sockets.

- The .wants directories specify dependencies of that service.

Slide 43

Systemd

- Systemd services that start at boot are found under /etc/systemd/system/
  - Type **ls -la /etc/systemd/system/multi-user.target.wants/**



```
cyberpatriot@merge:~$ ls -la /etc/systemd/system/multi-user.target.wants/
total 8
drwxr-xr-x  2 root root 4096 Jun 12 05:08 .
drwxr-xr-x 18 root root 4096 Jun 12 03:48 ..
lrwxrwxrwx  1 root root   35 Oct 11  2016 anacron.service -> /lib/systemd/system/anac
lrwxrwxrwx  1 root root   40 Oct 11  2016 avahi-daemon.service -> /lib/systemd/system
lrwxrwxrwx  1 root root   32 Oct 11  2016 cron.service -> /lib/systemd/system/cron.se
lrwxrwxrwx  1 root root   29 Jun 12 05:08 cups.path -> /lib/systemd/system/cups.path
```

43

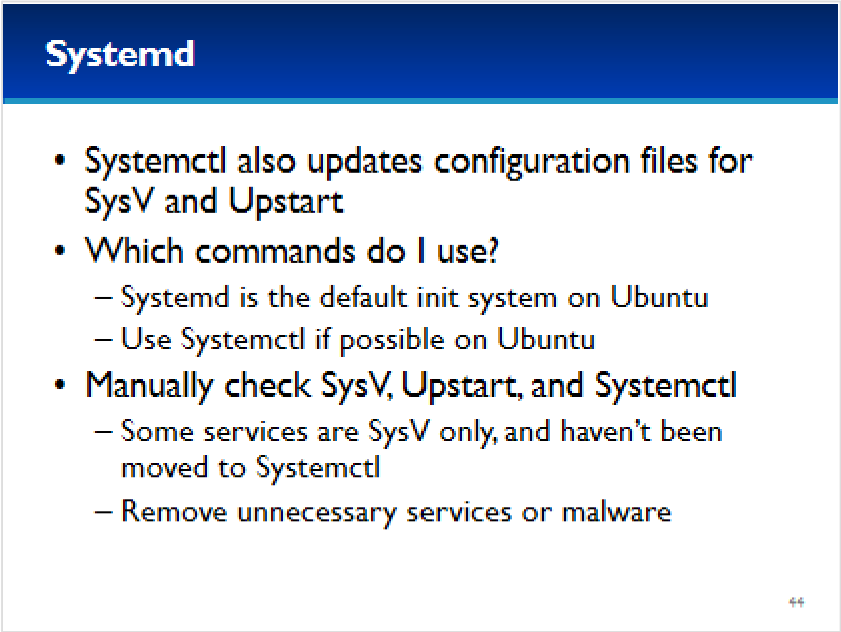
- We just saw the list of services available, but what about the list of services started at boot?

  - The services automatically started at boot are found in /etc/systemd/system and are typically symlinks to the /lib/systemd/system directory.

☆Have the students run the commands on the screen.

- The multi-user.target.wants directory is just one of several directories in /etc/systemd/system/ that specify services to start on boot.

Slide 44



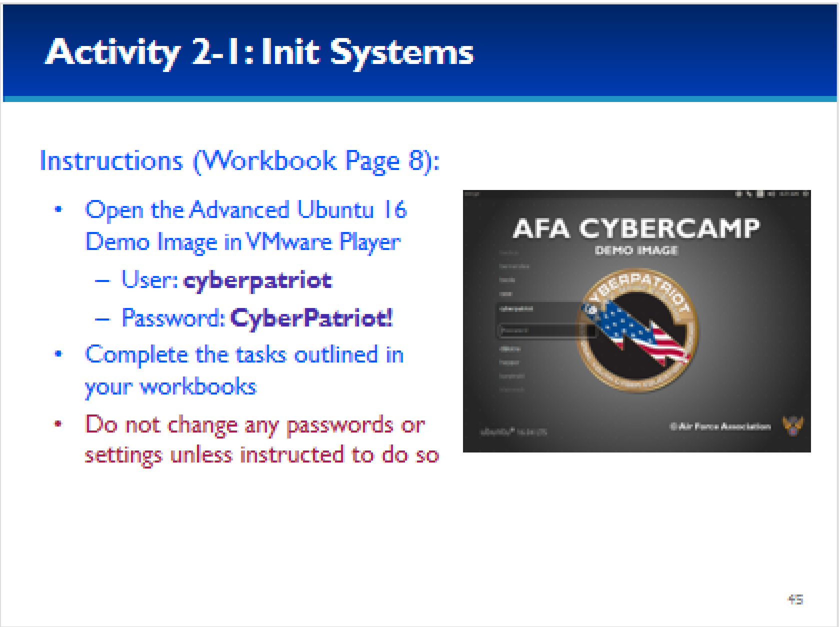
Systemd

- Systemctl also updates configuration files for SysV and Upstart
- Which commands do I use?
  - Systemd is the default init system on Ubuntu
  - Use Systemctl if possible on Ubuntu
- Manually check SysV, Upstart, and Systemctl
  - Some services are SysV only, and haven’t been moved to Systemctl
  - Remove unnecessary services or malware

44

- For the most part it seems like a lot of effort has been put into making all these init systems work with each other.
- So which commands should you use?
- Well, systemd is the default now, so you should use systemctl when possible.
- However a few services do not (yet) work with systemd, so use whatever works for those.
- Since systemd doesn’t yet manage everything, make sure to also check System V and Upstart for the presence of unwanted services.

Slide 45



Activity 2-1: Init Systems

Instructions (Workbook Page 8):

- Open the Advanced Ubuntu 16 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

45

🕒 Give students about 20 minutes to complete the tasks listed on Page 8 of their workbooks.

☆This lab will review the init systems SysV, Upstart, and Systemd.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. -
2. rc.local (or S13rc.local)
3. single (or S02single)
4. cups-browsed, whoopsie
5. -
6. reload
7. Linux 4.4.0-21-generic
8. en_US.UTF-8 (or LANG=en_US.UTF-8)

Slide 46

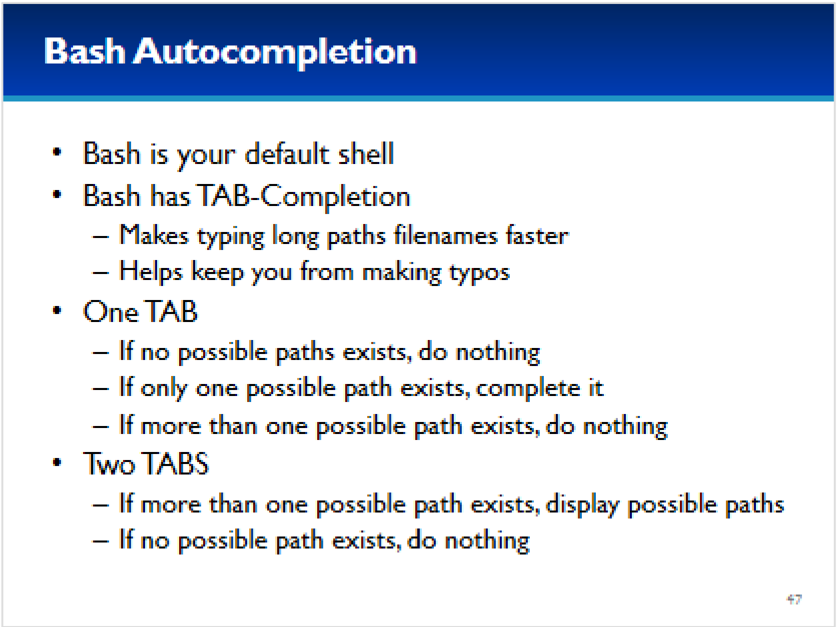
Advanced Command Line

🕒 Devote 30 minutes to slides 47-79. Allow the students 20 minutes to complete the activity on slide 79.

☆ Throughout this section, students should follow along in the **Advanced Ubuntu Demo Image**.

☆ In this section, we’ll cover advanced command line. After this section you should be comfortable on the command line, and know how to preform complex tasks such as finding files or redirecting input and output streams.

Slide 47



Bash Autocompletion

- Bash is your default shell
- Bash has TAB-Completion
  - Makes typing long paths filenames faster
  - Helps keep you from making typos
- One TAB
  - If no possible paths exists, do nothing
  - If only one possible path exists, complete it
  - If more than one possible path exists, do nothing
- Two TABS
  - If more than one possible path exists, display possible paths
  - If no possible path exists, do nothing

47

- When you type commands into the command prompt, you are using your default shell, which is Bash.

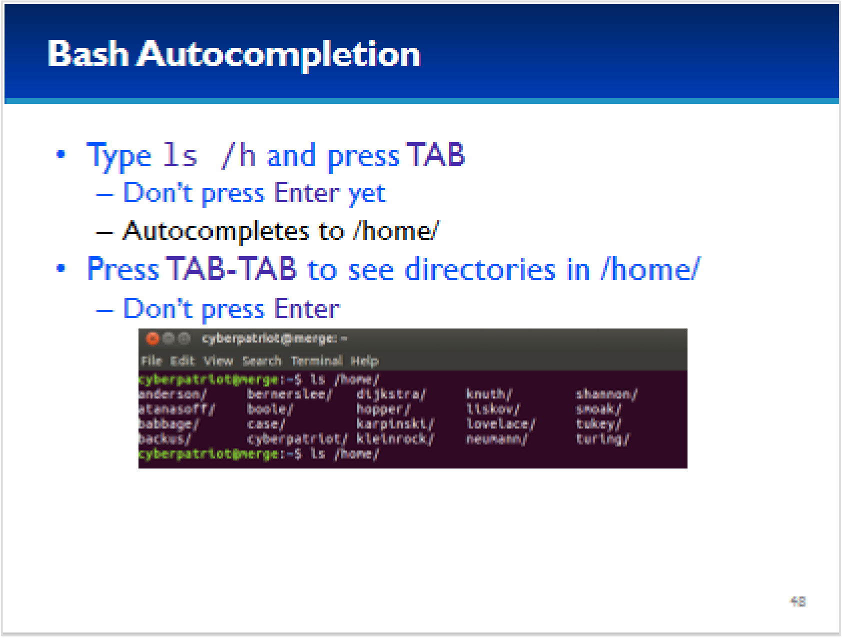
- Bash has some features to help make your life easier, and one of them is Tab-Completion.

- If there is only a single possible file or directory name based on what you have already typed, pressing Tab will automatically complete the name of the file or directory.

- If there are no possible paths, Tab will do nothing.

- If there are more than one possible path, a single tab will do nothing, but pressing Tab twice will display the possibilities based on what you’ve already typed.

Slide 48



Bash Autocompletion

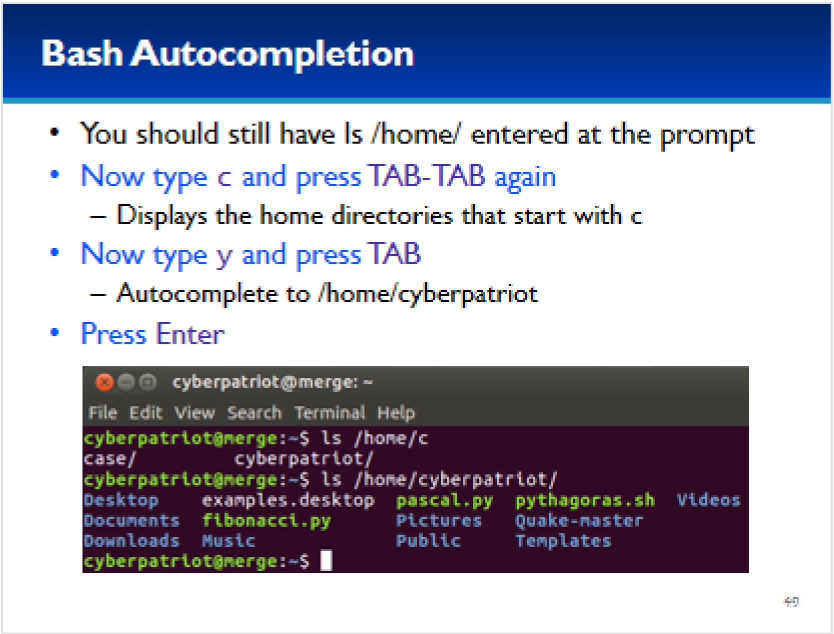
- Type `ls /h` and press TAB
  - Don’t press Enter yet
  - Autocompletes to /home/
- Press TAB-TAB to see directories in /home/
  - Don’t press Enter

```
cyberpatriot@merge:~$ ls /home/
anderson/     bernerslee/   dijkstra/     knuth/        shannon/
atanasoff/    boole/        hopper/       liskov/       smoak/
babbage/      case/         karpinski/    lovelace/     tukey/
backus/       cyberpatriot/ kleinrock/    neumann/      turing/
cyberpatriot@merge:~$ ls /home/
```

48

- For example, type **ls /h** and press Tab.
- You can see that bash automatically types the rest of the directory /home/
- If you then press Tab-Tab, bash will show you all of the directories in /home/
  - Tab-Tab means pressing Tab twice.

Slide 49



Bash Autocompletion

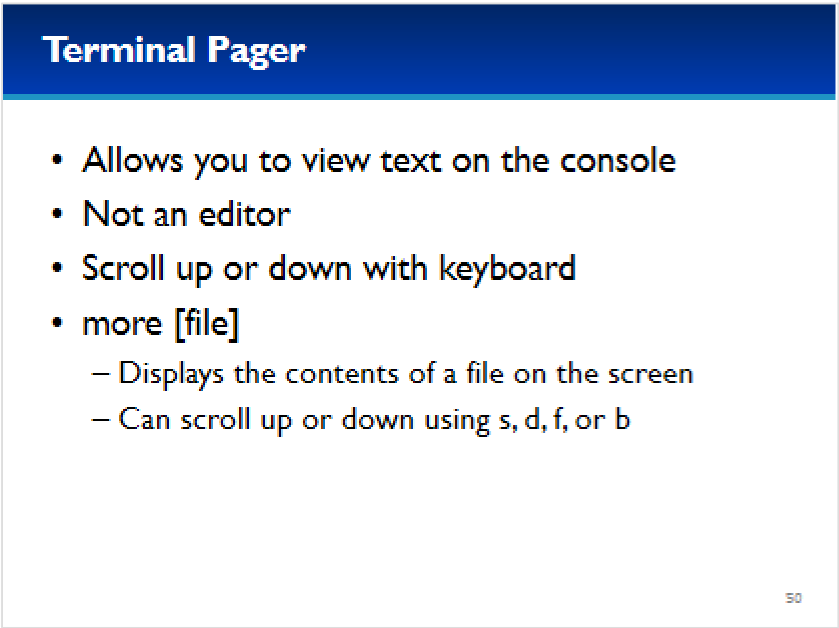
- You should still have ls /home/ entered at the prompt
- Now type c and press TAB-TAB again
  - Displays the home directories that start with c
- Now type y and press TAB
  - Autocomplete to /home/cyberpatriot
- Press Enter

```
cyberpatriot@merge:~$ ls /home/c
case/         cyberpatriot/
cyberpatriot@merge:~$ ls /home/cyberpatriot/
Desktop    examples.desktop  pascal.py  pythagoras.sh  Videos
Documents  fibonacci.py      Pictures   Quake-master
Downloads  Music             Public     Templates
cyberpatriot@merge:~$ 
```

49

- With **ls** /home/ still on the prompt, type c and then press Tab-Tab.
- Bash knows the only two directories that start with a c are case and cyberpatriot, so it displays those options.
- Now type y and press TAB to have bash automatically complete the rest of cyberpatriot.
- Now press Enter to list the contents of your home directory.

Slide 50



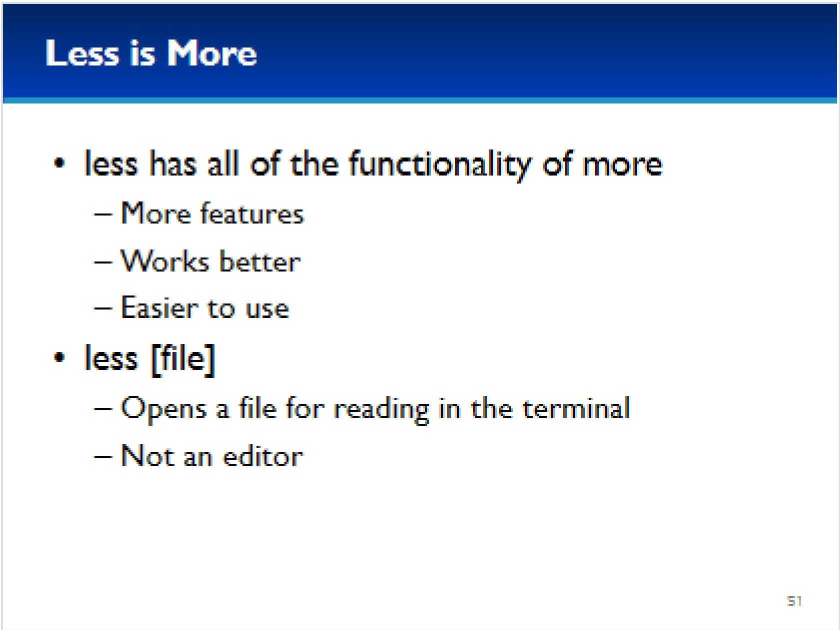
Terminal Pager

- Allows you to view text on the console
- Not an editor
- Scroll up or down with keyboard
- more [file]
  - Displays the contents of a file on the screen
  - Can scroll up or down using s, d, f, or b

50

- A terminal pager allows you to view text files on the console.
- It doesn’t allow you to edit the files by design, but it’s excellent for log files or large configuration files.
- You can scroll up or down using keys on your keyboard.
- The old Linux terminal pager is called **more**. It displayed the contents of a file on the screen.
- Using more you can scroll up or down using **s**, **d**, **f**, or **b**.

Slide 51



Less is More

- less has all of the functionality of more
  - More features
  - Works better
  - Easier to use
- less [file]
  - Opens a file for reading in the terminal
  - Not an editor

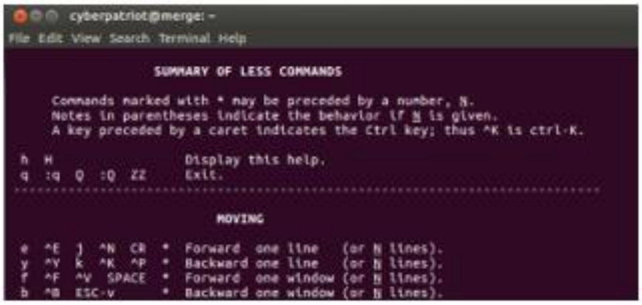
51

- **More** can be a real pain to use sometimes, but there is a much better system pager called **less**.
- The name of **less** is a play on words, but you can remember it by remembering “less is more.”

Slide 52

Less

- Type `less --help` to view the keyboard commands
  - Scroll down by using PgDn, the Down Arrow, or f
  - Scroll up by using PgUp, the Up Arrow, or b
  - Press q to quit



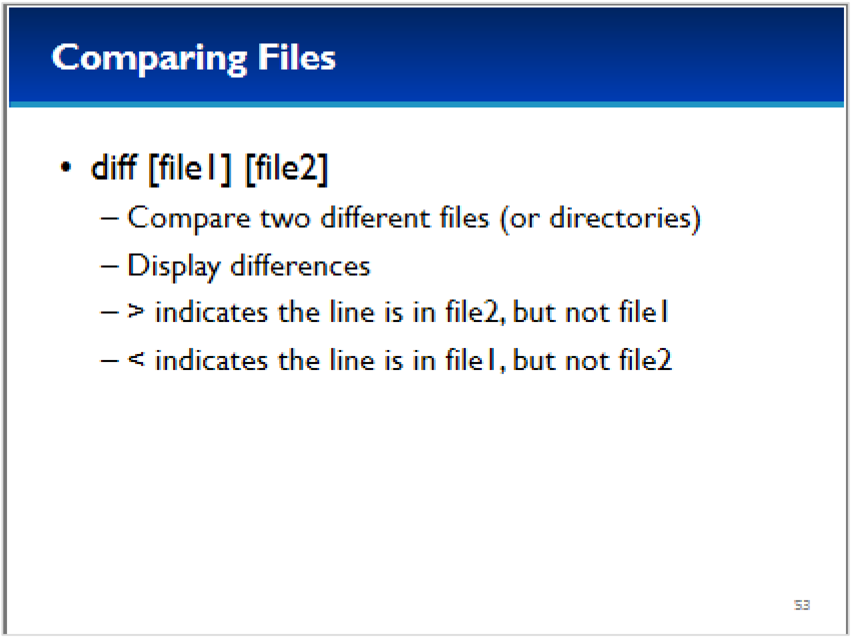
```
                   SUMMARY OF LESS COMMANDS

      Commands marked with * may be preceded by a number, N.
      Notes in parentheses indicate the behavior if N is given.
      A key preceded by a caret indicates the Ctrl key; thus ^K is ctrl-K.

  h  H                 Display this help.
  q  :q  Q  :Q  ZZ     Exit.
 ---------------------------------------------------------------------------

                          MOVING

  e  ^E  j  ^N  CR  *  Forward  one line   (or N lines).
  y  ^Y  k  ^K  ^P  *  Backward one line   (or N lines).
  f  ^F  ^V  SPACE  *  Forward  one window (or N lines).
  b  ^B  ESC-v      *  Backward one window (or N lines).
```

52

☆Have the students run the commands on the screen.

- **Less** is used by the man command for displaying manual pages.

Slide 53



Comparing Files

- diff [file1] [file2]
  - Compare two different files (or directories)
  - Display differences
  - > indicates the line is in file2, but not file1
  - < indicates the line is in file1, but not file2

53

- The **diff** command can compare two different files or directories.

  - It’s mostly useful for comparing files that are similar but may differ slightly.

  - It’s also sometimes helpful to know if two files are exactly the same.

- It displays the differences between the two files by using the greater than (<) or less than (>) sign.

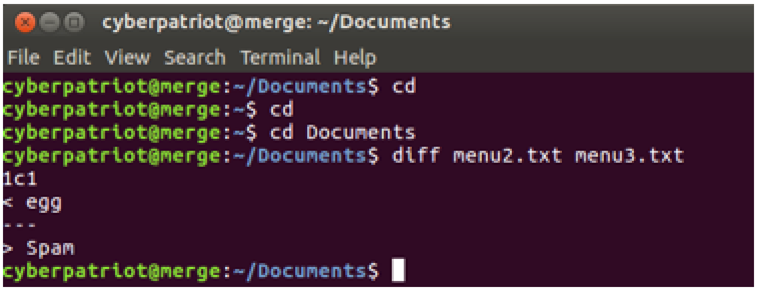
- Greater-than indicates the line is in file2, but not file1.

- Less-than indicates the line is in file1, but not file2.

Slide 54

Comparing Files

- Type cd
- Type cd Documents
- Type diff menu2.txt menu3.txt



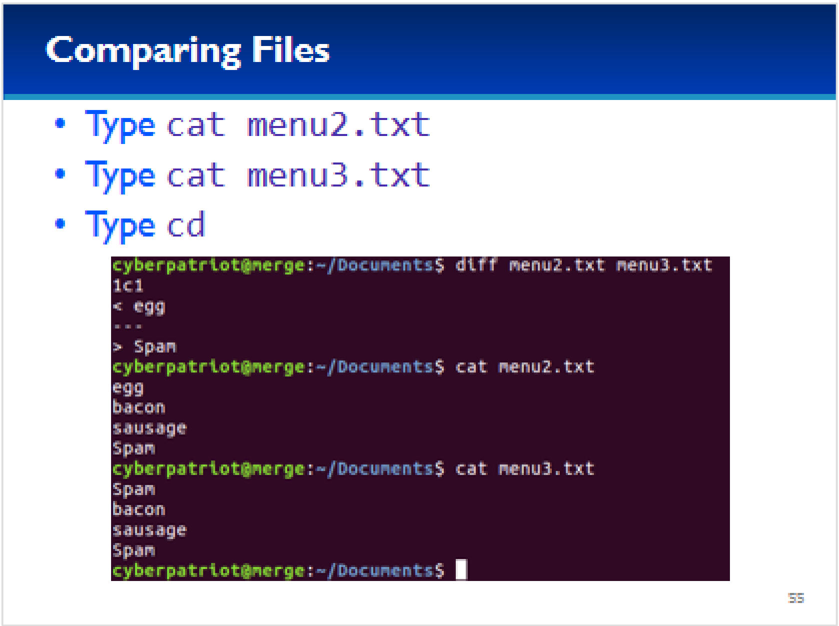
cyberpatriot@merge: ~/Documents
File Edit View Search Terminal Help

```
cyberpatriot@merge:~/Documents$ cd
cyberpatriot@merge:~$ cd
cyberpatriot@merge:~$ cd Documents
cyberpatriot@merge:~/Documents$ diff menu2.txt menu3.txt
1c1
< egg
---
> Spam
cyberpatriot@merge:~/Documents$ 
```

☆Have the students run the commands on the screen.

- As you can see, menu2.txt and menu3.txt are the same, except menu3.txt contains spam instead of egg.

Slide 55



Comparing Files

- Type `cat menu2.txt`
- Type `cat menu3.txt`
- Type `cd`

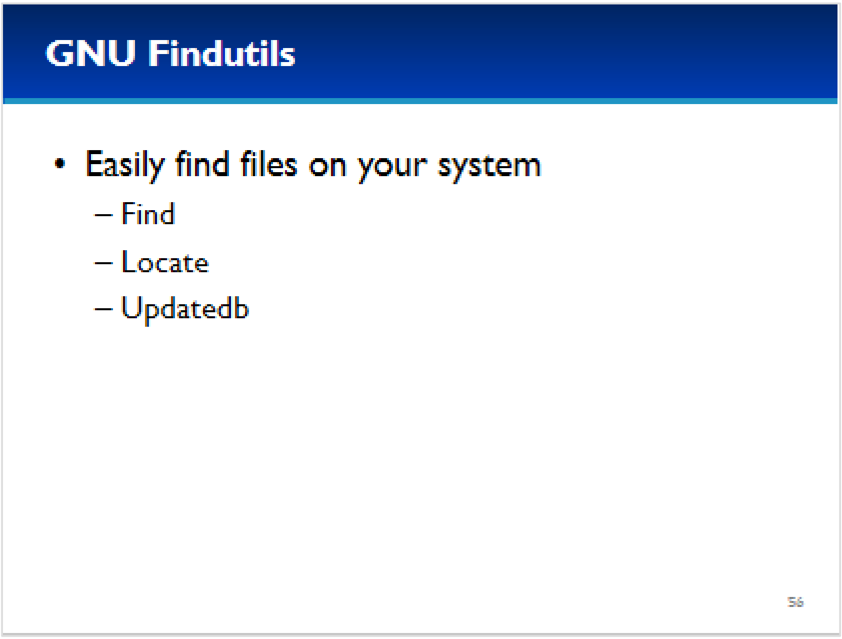
```
cyberpatriot@merge:~/Documents$ diff menu2.txt menu3.txt
1c1
< egg
---
> Spam
cyberpatriot@merge:~/Documents$ cat menu2.txt
egg
bacon
sausage
Spam
cyberpatriot@merge:~/Documents$ cat menu3.txt
Spam
bacon
sausage
Spam
cyberpatriot@merge:~/Documents$ 
```

55

☆Have the students run the commands on the screen.

- **Cat**-ing out the files confirm that the two files are in fact identical except for the first line.

Slide 56



GNU Findutils

- Easily find files on your system
  - Find
  - Locate
  - Updatedb

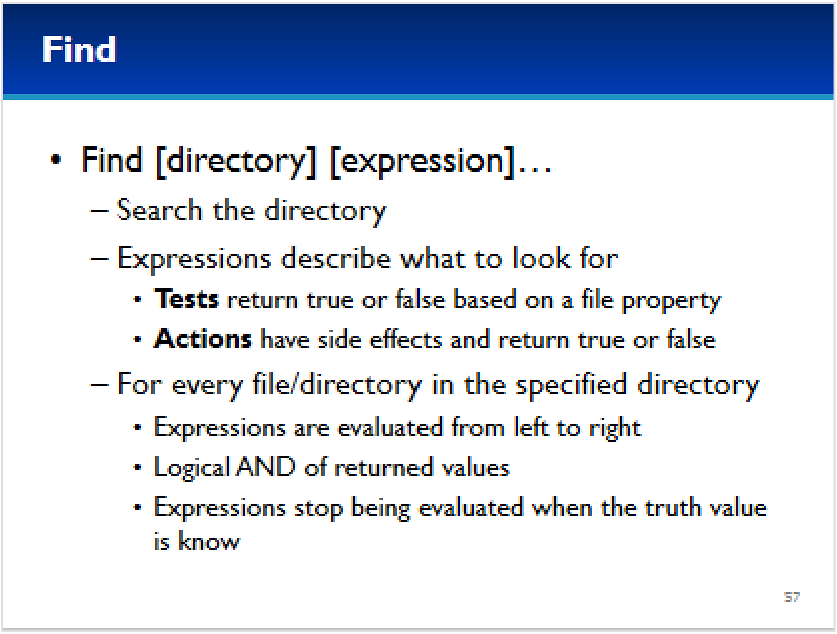
56

- (GNU is officially pronounced like “grew” except with an “n” instead of an “r”, however many people pronounce it like “new”).

- The GNU Findutils is a set of programs to help make it easy to find files on your system, but it lets you do a lot more than that.

  - The three main programs we will cover are **find**, **locate**, and **updateb**.

Slide 57



Find

- Find [directory] [expression]…
  - Search the directory
  - Expressions describe what to look for
    - **Tests** return true or false based on a file property
    - **Actions** have side effects and return true or false
  - For every file/directory in the specified directory
    - Expressions are evaluated from left to right
    - Logical AND of returned values
    - Expressions stop being evaluated when the truth value is know

57

- **Find** is one of the most powerful commands in Linux. The syntax for it can seem rather daunting at first, but most practical operations and examples are easy to understand.

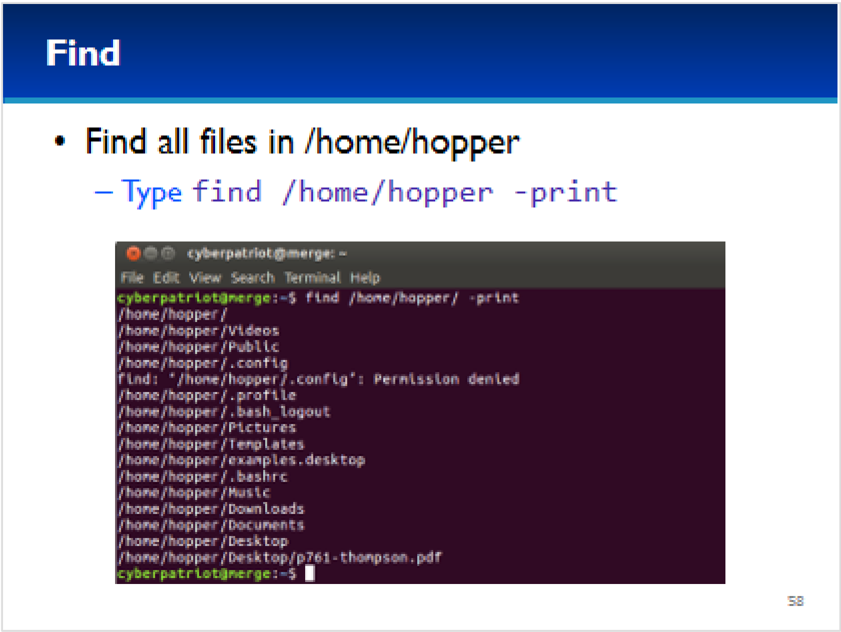
- Expressions may be either tests or actions, both return a truth value; but actions may have additional side effects.

- **Find**, finds every file in a directory and evaluates a list of expressions from left to right.

  - These expressions are evaluated like a logical “and” of the returned values, but the expressions stop being evaluated when the truth value is known.

- This may be confusing at first, so let’s look at some real life examples.

Slide 58



Find

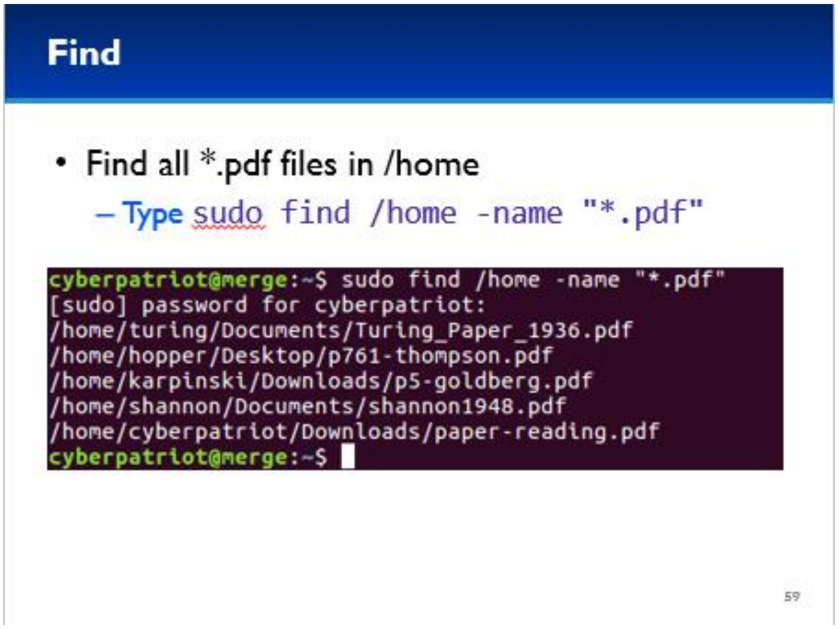
- Find all files in /home/hopper
  - Type `find /home/hopper -print`

```
cyberpatriot@merge:~$ find /home/hopper/ -print
/home/hopper/
/home/hopper/Videos
/home/hopper/Public
/home/hopper/.config
find: '/home/hopper/.config': Permission denied
/home/hopper/.profile
/home/hopper/.bash_logout
/home/hopper/Pictures
/home/hopper/Templates
/home/hopper/examples.desktop
/home/hopper/.bashrc
/home/hopper/Music
/home/hopper/Downloads
/home/hopper/Documents
/home/hopper/Desktop
/home/hopper/Desktop/p761-thompson.pdf
cyberpatriot@merge:~$ 
```

☆Have the students run the commands on the screen.

- This command simply prints out all the files inside the specified directory.
- Here, **-print** is an Action.

Slide 59



Find

- Find all *.pdf files in /home
  - Type sudo find /home -name "*.pdf"

```
cyberpatriot@merge:~$ sudo find /home -name "*.pdf"
[sudo] password for cyberpatriot:
/home/turing/Documents/Turing_Paper_1936.pdf
/home/hopper/Desktop/p761-thompson.pdf
/home/karpinski/Downloads/p5-goldberg.pdf
/home/shannon/Documents/shannon1948.pdf
/home/cyberpatriot/Downloads/paper-reading.pdf
cyberpatriot@merge:~$
```

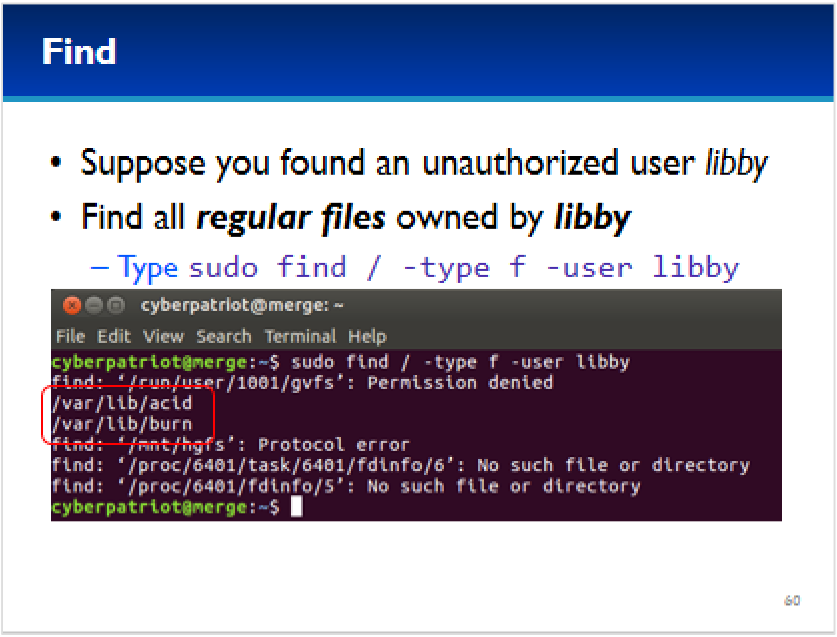
59

- Say you want to find all the files ending in .pdf.

☆Have the students run the commands on the screen.

- The **–name** expression returns true if the filename matches.
- If **–name** returns false, the expression evaluation is terminated and nothing happens.
- If **–name** returns true, it continues on to the next expression.
- Since we didn't specify an Action, find automatically applies the default Action, which is **–print**.

Slide 60



Find

- Suppose you found an unauthorized user *libby*
- Find all ***regular files*** owned by ***libby***
  - Type `sudo find / -type f -user libby`

```
cyberpatriot@merge:~$ sudo find / -type f -user libby
find: '/run/user/1001/gvfs': Permission denied
/var/lib/acid
/var/lib/burn
find: '/mnt/hgfs': Protocol error
find: '/proc/6401/task/6401/fdinfo/6': No such file or directory
find: '/proc/6401/fdinfo/5': No such file or directory
cyberpatriot@merge:~$
```

- Suppose you found an unauthorized user on your computer named Libby, you can use the find command to find all files on the system owned by Libby.

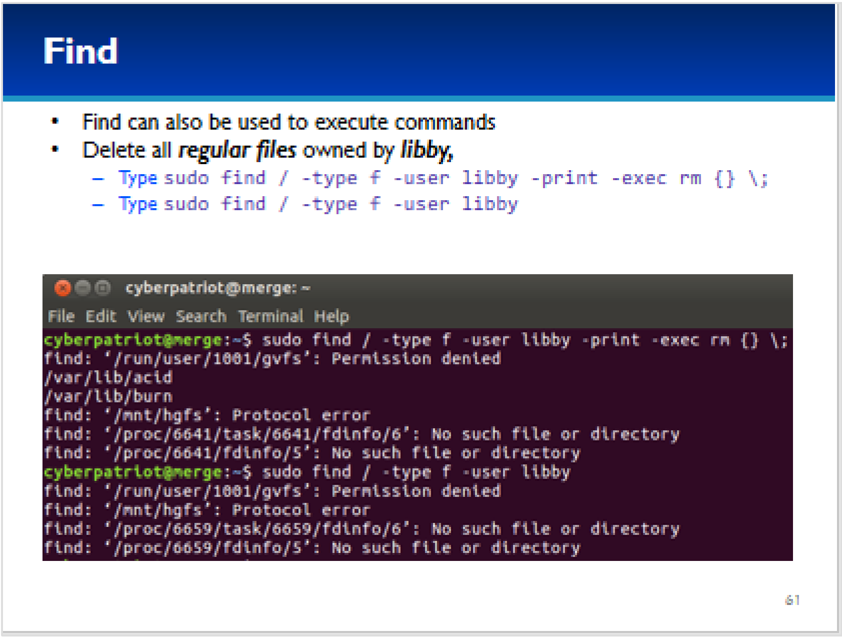
- The **–type f** expression returns true for regular files, and false for everything else.

- The **–user** expression returns true if the file is owned by the user, and false otherwise.

☆Have the students run the commands on the screen.

- Here you can see Libby owns two files on the filesystem.

Slide 61



Find

- Find can also be used to execute commands
- Delete all *regular files* owned by *libby*,
  - Type `sudo find / -type f -user libby -print -exec rm {} \;`
  - Type `sudo find / -type f -user libby`

```
cyberpatriot@merge: ~
File Edit View Search Terminal Help
cyberpatriot@merge:~$ sudo find / -type f -user libby -print -exec rm {} \;
find: ‘/run/user/1001/gvfs’: Permission denied
/var/lib/acid
/var/lib/burn
find: ‘/mnt/hgfs’: Protocol error
find: ‘/proc/6641/task/6641/fdinfo/6’: No such file or directory
find: ‘/proc/6641/fdinfo/5’: No such file or directory
cyberpatriot@merge:~$ sudo find / -type f -user libby
find: ‘/run/user/1001/gvfs’: Permission denied
find: ‘/mnt/hgfs’: Protocol error
find: ‘/proc/6659/task/6659/fdinfo/6’: No such file or directory
find: ‘/proc/6659/fdinfo/5’: No such file or directory
```

61

- **Find** can also be used to execute commands, and will replace open-close-curly-brackets ({}) with the name of the file.

- When using **find** to execute commands, you have to end the command with **\;** (so that find knows when the command ends).

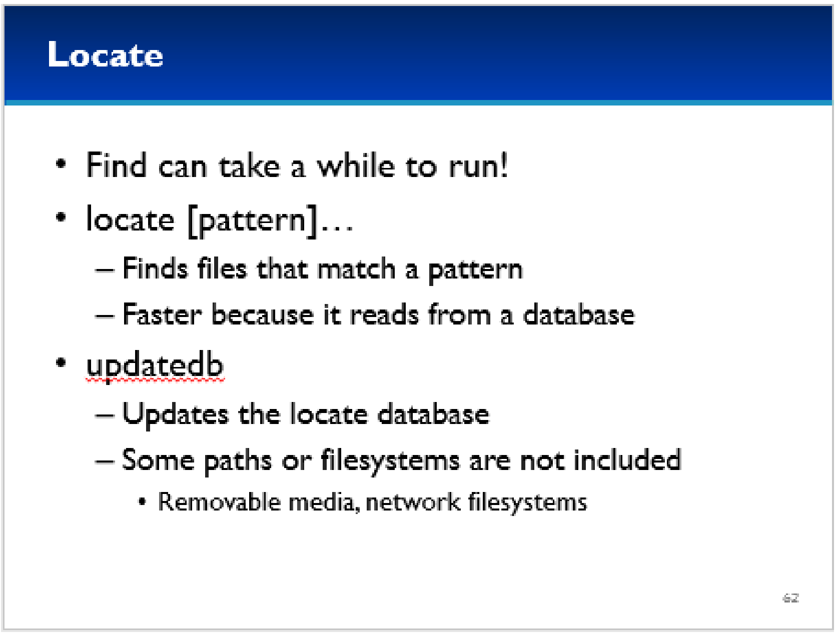
☆Have the students run the commands on the screen.

- The **–type f** expression returns true for regular files, the **–user** Libby expression returns true for files owned by Libby, **-print** is an Action that prints out the filename and returns true, and **–exec** executes the given command substituting the name of the file with {}.

- The **rm** command removes all matching files.

- Searching again for files owned by Libby, you can see that they have indeed been deleted.

Slide 62



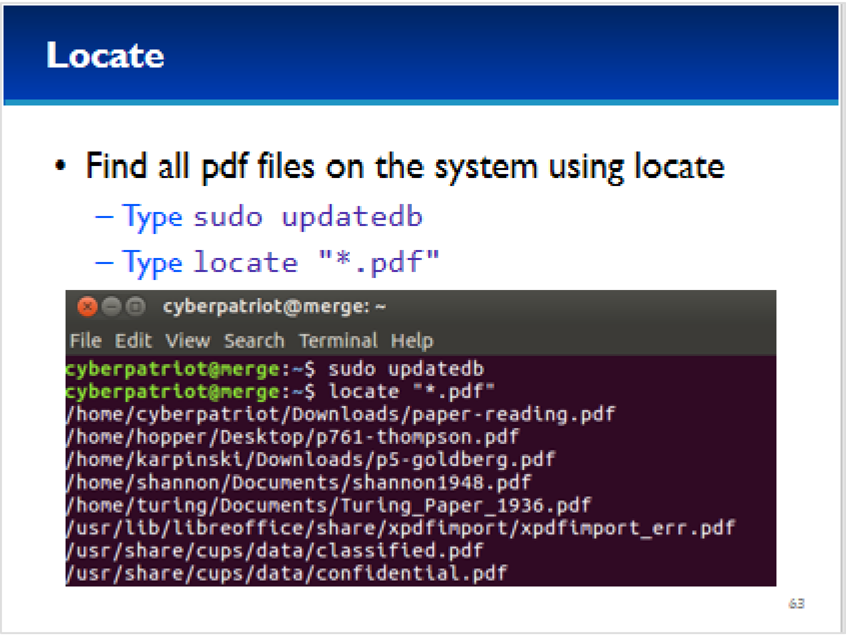
Locate

- Find can take a while to run!
- locate [pattern]…
  - – Finds files that match a pattern
  - – Faster because it reads from a database
- updatedb
  - – Updates the locate database
  - – Some paths or filesystems are not included
    - Removable media, network filesystems

62

- **Find** is very useful, but can take a while to run, which isn’t really necessary when only searching for files by their names.
- For this purpose, **findutils** provides the **locate** and **updatedb** commands.
- **Locate** looks in a database of files on the system to see if it finds a match.
- **Updatedb** updates the database that is used by **locate**.

Slide 63



Locate

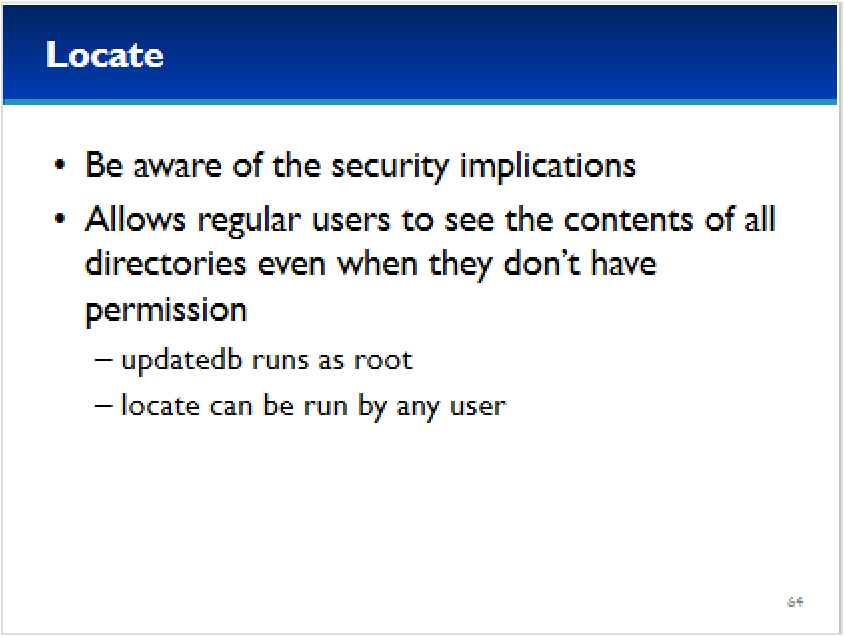
- Find all pdf files on the system using locate
  - Type `sudo updatedb`
  - Type `locate "*.pdf"`

```
cyberpatriot@merge:~$ sudo updatedb
cyberpatriot@merge:~$ locate "*.pdf"
/home/cyberpatriot/Downloads/paper-reading.pdf
/home/hopper/Desktop/p761-thompson.pdf
/home/karpinski/Downloads/p5-goldberg.pdf
/home/shannon/Documents/shannon1948.pdf
/home/turing/Documents/Turing_Paper_1936.pdf
/usr/lib/libreoffice/share/xpdfimport/xpdfimport_err.pdf
/usr/share/cups/data/classified.pdf
/usr/share/cups/data/confidential.pdf
```

- Use locate to find all the files on the system ending with .pdf.

☆Have the students run the commands on the screen.

Slide 64



Locate

- Be aware of the security implications
- Allows regular users to see the contents of all directories even when they don’t have permission
  - updatedb runs as root
  - locate can be run by any user

64

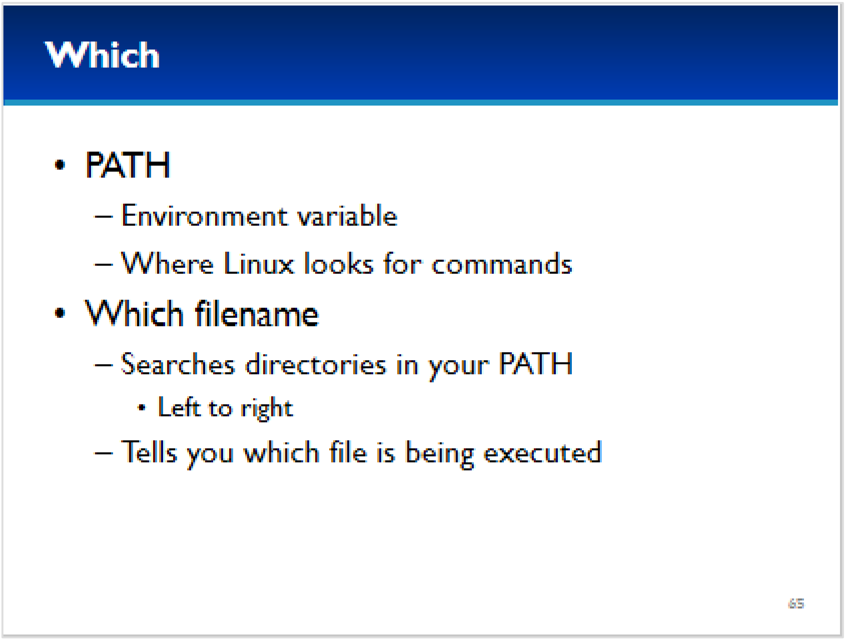
- **Locate** and **updatedb** have security implications that you should be aware of.

- **Updatedb** is usually run automatically as root, so that it can index all of the files on the system.

- However, because **updatedb** runs as root, it is possible that users can use **locate** to learn of the existence of files that may not be otherwise visible to them.

  - This isn’t a critical security vulnerability on its own, but it is something you should be aware of.

Slide 65



Which

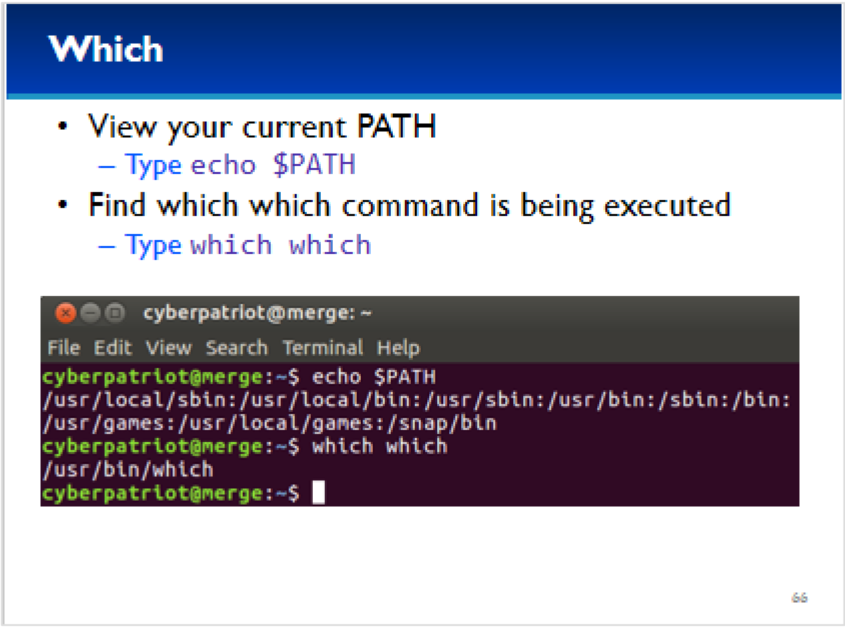
- PATH
  - Environment variable
  - Where Linux looks for commands
- Which filename
  - Searches directories in your PATH
    - Left to right
  - Tells you which file is being executed

65

- When you run a command in Linux, that command exists somewhere on your filesystem, but you don't have to know where because Bash automatically searches directories in your PATH.

- The **which** command searches the directories in your PATH, from left to right, looking for the filename you specified and prints out the first match.

Slide 66



Which

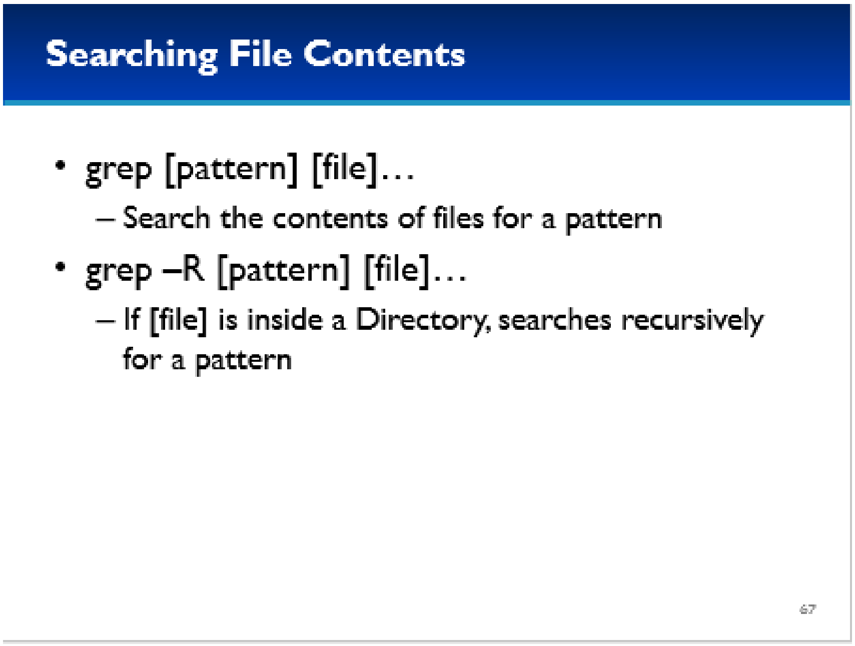
- View your current PATH
  - Type `echo $PATH`
- Find which which command is being executed
  - Type `which which`

```
cyberpatriot@merge:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:
/usr/games:/usr/local/games:/snap/bin
cyberpatriot@merge:~$ which which
/usr/bin/which
cyberpatriot@merge:~$ 
```

66

- PATH is an environment variable.
- To view your current path type **echo $PATH.**
- These are the directories that Bash searches when looking for a command to execute.
- To find the which command is executed when you type **which**, type **which which**.
- You can see the **which** command that is executed is inside the /usr/bin/ directory.
- It’s important to know what your path is, and which commands are executing. If your path is set to an insecure value, an adversary could trick you into executing commands!

Slide 67



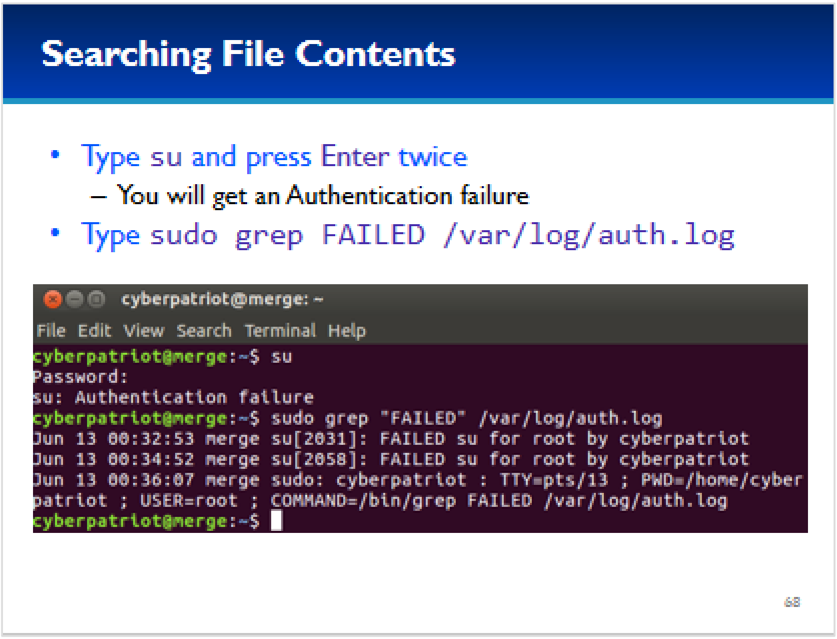
Searching File Contents

- grep [pattern] [file]…
  - Search the contents of files for a pattern
- grep –R [pattern] [file]…
  - If [file] is inside a Directory, searches recursively for a pattern

67

- The **grep** command is used to search for a pattern inside files.
- **Grep** can search recursively inside a directory by using the **–R** option.

Slide 68



Searching File Contents

- Type su and press Enter twice
  - You will get an Authentication failure
- Type sudo grep FAILED /var/log/auth.log

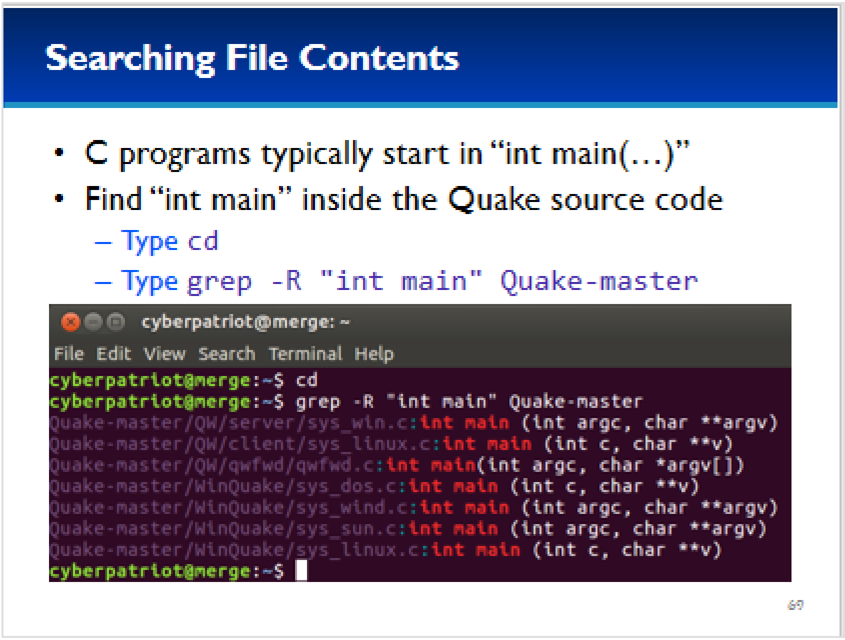
```
cyberpatriot@merge:~$ su
Password:
su: Authentication failure
cyberpatriot@merge:~$ sudo grep "FAILED" /var/log/auth.log
Jun 13 00:32:53 merge su[2031]: FAILED su for root by cyberpatriot
Jun 13 00:34:52 merge su[2058]: FAILED su for root by cyberpatriot
Jun 13 00:36:07 merge sudo: cyberpatriot : TTY=pts/13 ; PWD=/home/cyber
patriot ; USER=root ; COMMAND=/bin/grep FAILED /var/log/auth.log
cyberpatriot@merge:~$ 
```

68

☆Have the students run the commands on the screen.

- This **grep** command searches for FAILED authentication attempts inside the system authorization log.

Slide 69



Searching File Contents

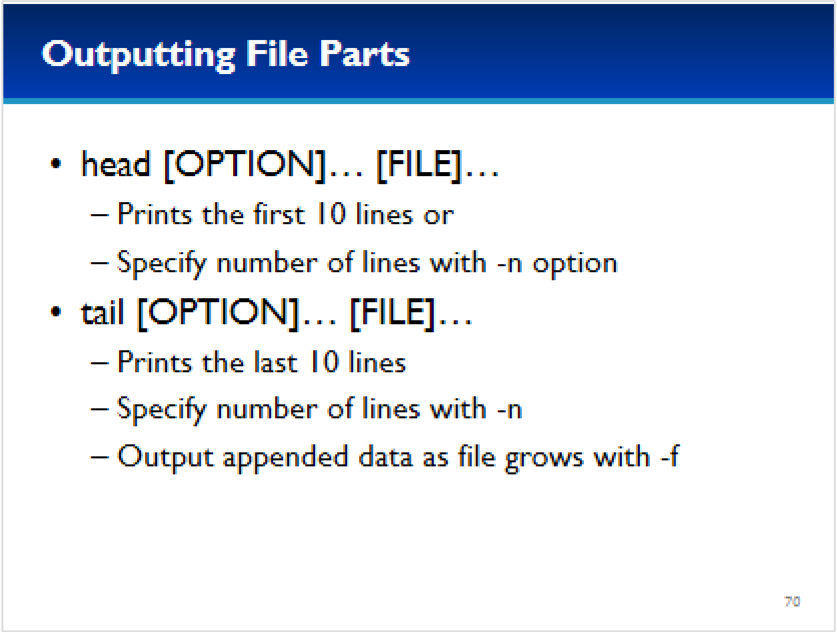
- C programs typically start in “int main(…)”
- Find “int main” inside the Quake source code
  - Type cd
  - Type grep -R "int main" Quake-master

```
cyberpatriot@merge:~$ cd
cyberpatriot@merge:~$ grep -R "int main" Quake-master
Quake-master/QW/server/sys_win.c:int main (int argc, char **argv)
Quake-master/QW/client/sys_linux.c:int main (int c, char **v)
Quake-master/QW/qwfwd/qwfwd.c:int main(int argc, char *argv[])
Quake-master/WinQuake/sys_dos.c:int main (int c, char **v)
Quake-master/WinQuake/sys_wind.c:int main (int argc, char **argv)
Quake-master/WinQuake/sys_sun.c:int main (int argc, char **argv)
Quake-master/WinQuake/sys_linux.c:int main (int c, char **v)
cyberpatriot@merge:~$ 
```

- C programs typically begin in the main function.
- Say you downloaded the Quake source code and wanted to know where it starts.
- You can use **grep** to search recursively for the main function with the following commands.

☆Have the students run the commands on the screen.

Slide 70



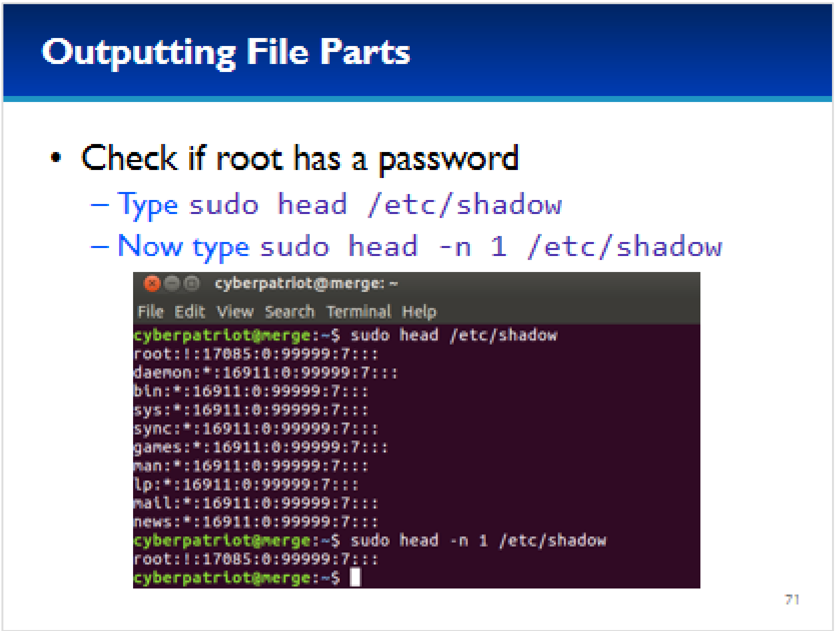
Outputting File Parts

- head [OPTION]… [FILE]…
  - Prints the first 10 lines or
  - Specify number of lines with -n option
- tail [OPTION]… [FILE]…
  - Prints the last 10 lines
  - Specify number of lines with -n
  - Output appended data as file grows with -f

70

- **Head** and **tail** are surprisingly useful commands.
- **Head** prints out the first 10 lines of a file, or you can specify the number of lines to print with the **–n** option.
- Similarly, **tail** prints out the last 10 lines of a file, and again you can specify the number of lines to print with the **–n** option.
- **Tail** can also output lines appended to a file in real time, as the file grows, by specifying the **–f** option.

Slide 71



Outputting File Parts

- Check if root has a password
  - Type sudo head /etc/shadow
  - Now type sudo head -n 1 /etc/shadow

```
cyberpatriot@merge:~$ sudo head /etc/shadow
root:!:17085:0:99999:7:::
daemon:*:16911:0:99999:7:::
bin:*:16911:0:99999:7:::
sys:*:16911:0:99999:7:::
sync:*:16911:0:99999:7:::
games:*:16911:0:99999:7:::
man:*:16911:0:99999:7:::
lp:*:16911:0:99999:7:::
mail:*:16911:0:99999:7:::
news:*:16911:0:99999:7:::
cyberpatriot@merge:~$ sudo head -n 1 /etc/shadow
root:!:17085:0:99999:7:::
cyberpatriot@merge:~$ 
```

71

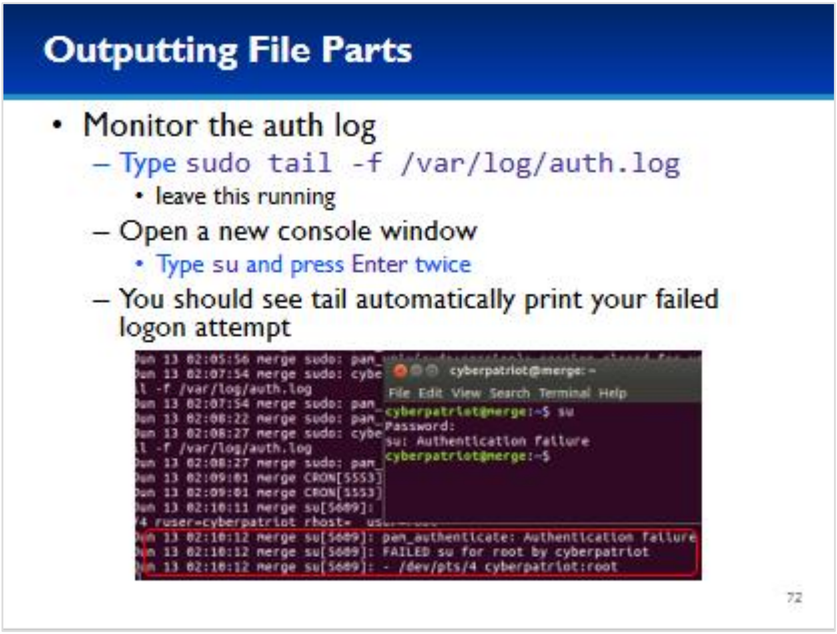
- Let’s use **head** to check if the root user has a password.

☆Have the students run the commands on the screen.

- Root doesn’t have a password, or you would see the encrypted password where the ! Is.

- As you can see, the **–n 1** option prints out only the first line of the file.

Slide 72



Outputting File Parts

- Monitor the auth log
  - Type sudo tail -f /var/log/auth.log
    - leave this running
  - Open a new console window
    - Type su and press Enter twice
  - You should see tail automatically print your failed logon attempt

```
Jun 13 02:05:56 merge sudo: pam_
Jun 13 02:07:54 merge sudo: cybe
il -f /var/log/auth.log
Jun 13 02:07:54 merge sudo: pam_
Jun 13 02:08:22 merge sudo: pam_
Jun 13 02:08:27 merge sudo: cybe
il -f /var/log/auth.log
Jun 13 02:08:27 merge sudo: pam_
Jun 13 02:09:01 merge CRON[5553]
Jun 13 02:09:01 merge CRON[5553]
Jun 13 02:10:11 merge su[5609]:
/4 ruser=cyberpatriot rhost=  user=root
Jun 13 02:10:12 merge su[5609]: pam_authenticate: Authentication failure
Jun 13 02:10:12 merge su[5609]: FAILED su for root by cyberpatriot
Jun 13 02:10:12 merge su[5609]: - /dev/pts/4 cyberpatriot:root
```

```
cyberpatriot@merge:~$ su
Password:
su: Authentication failure
cyberpatriot@merge:~$
```

72

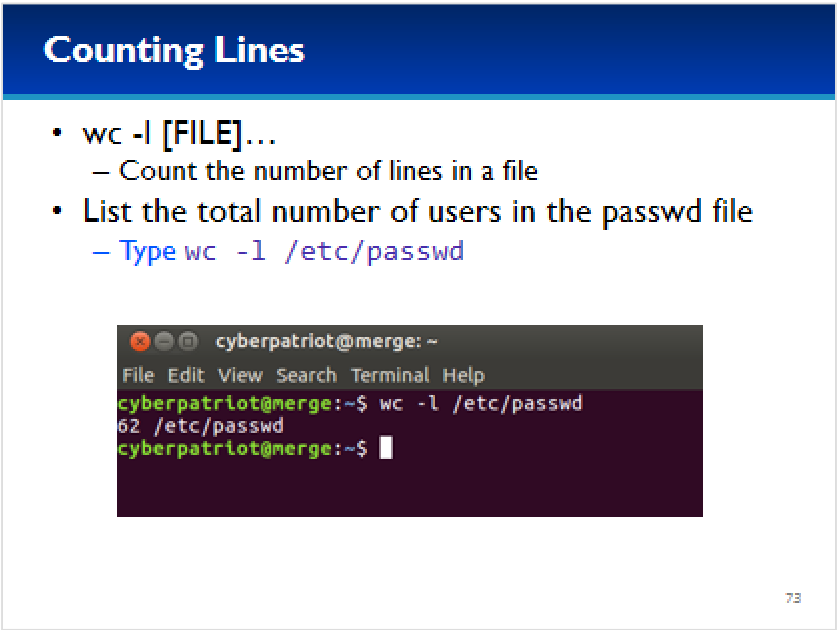
- **Tail** is useful for monitoring log files.

- Type: **sudo tail -f /var/log/auth.log**

- In a new console window, type **su**, but fail the authentication on purpose by pressing **Enter** twice.

- You should see **tail** automatically print out your failed logon attempt.

Slide 73



Counting Lines

- wc -l [FILE]…
  - Count the number of lines in a file
- List the total number of users in the passwd file
  - Type `wc -l /etc/passwd`

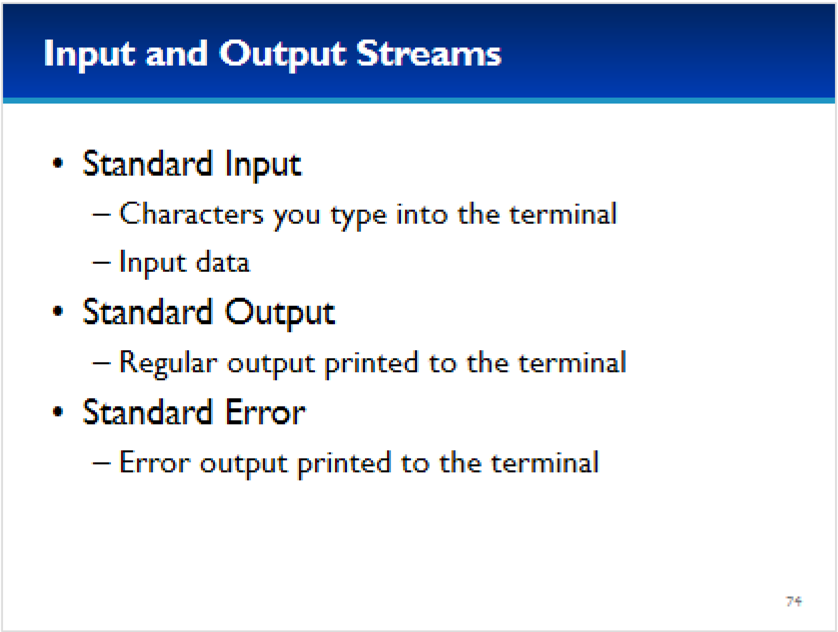
```
cyberpatriot@merge:~$ wc -l /etc/passwd
62 /etc/passwd
cyberpatriot@merge:~$ 
```

- The **wc** command stands for "word count" but can also be used for counting lines in a file with the **–l** option.

- Say you wanted to list total number of user accounts on the system. You can do this by counting the number of lines in the password file.

- There are 62 user accounts on the system.

Slide 74



Input and Output Streams

- Standard Input
  - Characters you type into the terminal
  - Input data
- Standard Output
  - Regular output printed to the terminal
- Standard Error
  - Error output printed to the terminal

74

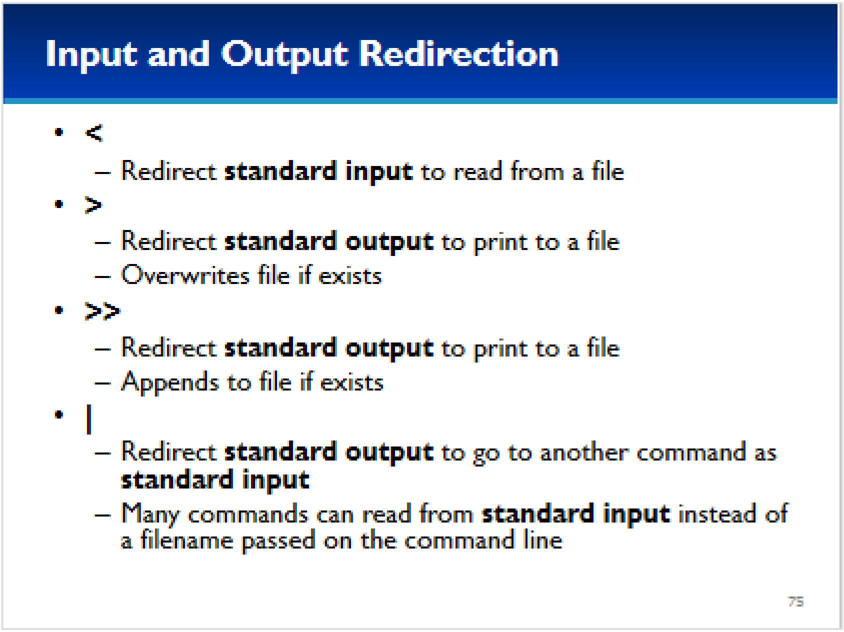
- Let's take a moment to talk about program input and output. All processes are given three open "character streams", one for input, and two for output.

- When a program prompts you for input on the terminal, it is reading from "standard input."

- When a program prints regular information to the terminal it is printing to "standard output."

- When a program prints error information to the terminal is printing to "standard error."

Slide 75



Input and Output Redirection

- **<**
  - Redirect **standard input** to read from a file
- **>**
  - Redirect **standard output** to print to a file
  - Overwrites file if exists
- **>>**
  - Redirect **standard output** to print to a file
  - Appends to file if exists
- **|**
  - Redirect **standard output** to go to another command as **standard input**
  - Many commands can read from **standard input** instead of a filename passed on the command line

75

- These input and output streams can be redirected to and from different locations using the following operators.

- The **less-than** operator redirects standard input to read from a file (instead of the keyboard).

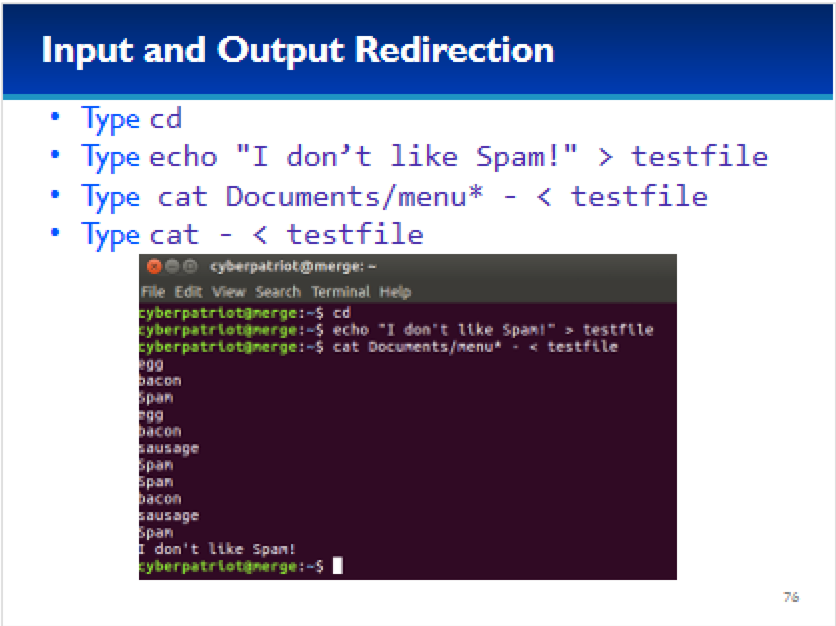
- The **greater-than** operator redirects standard output to print to a file (instead of the screen).

  - Be careful using this because it will Truncate/Overwrite the file if it exists, deleting any existing data.

- The **greater-than greater-than** operator redirects standard output to append to a file (instead of the screen).

- The **pipe** operator is named thusly because it pipes output from the standard output of one command, to the standard input of another command.

Slide 76



Input and Output Redirection

- Type cd
- Type echo "I don't like Spam!" > testfile
- Type cat Documents/menu* - < testfile
- Type cat - < testfile

```
cyberpatriot@merge:~$ cd
cyberpatriot@merge:~$ echo "I don't like Spam!" > testfile
cyberpatriot@merge:~$ cat Documents/menu* - < testfile
egg
bacon
Spam
egg
bacon
sausage
Spam
Spam
bacon
sausage
Spam
I don't like Spam!
cyberpatriot@merge:~$ 
```

- Let's look at some examples.

☆Have the students run the commands on the screen.

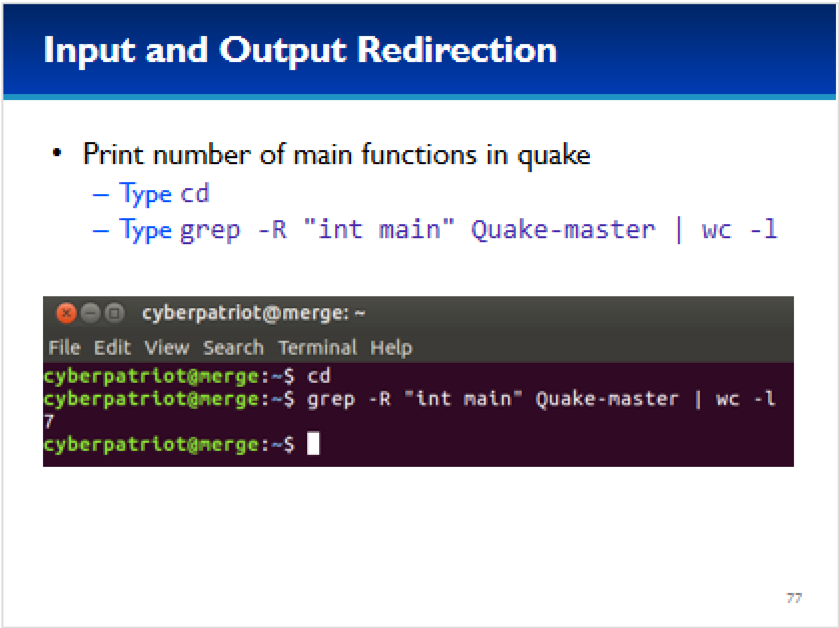
- The **echo** command prints "I don't like Spam!" to standard output, but standard output has been redirected to "testfile" so the text ends up there instead of the screen.

- The **–** argument to the **cat** command tells **cat** to read from standard input.

- Therefore, **cat** concatenates the contents of all files name Documents/menu* and standard input, because standard input has been redirected to come from testfile, it reads from there instead of the keyboard.

- You can see that the contents of testfile are printed to the screen last.

Slide 77



Input and Output Redirection

- Print number of main functions in quake
  - Type `cd`
  - Type `grep -R "int main" Quake-master | wc -l`

```
cyberpatriot@merge:~$ cd
cyberpatriot@merge:~$ grep -R "int main" Quake-master | wc -l
7
cyberpatriot@merge:~$ 
```

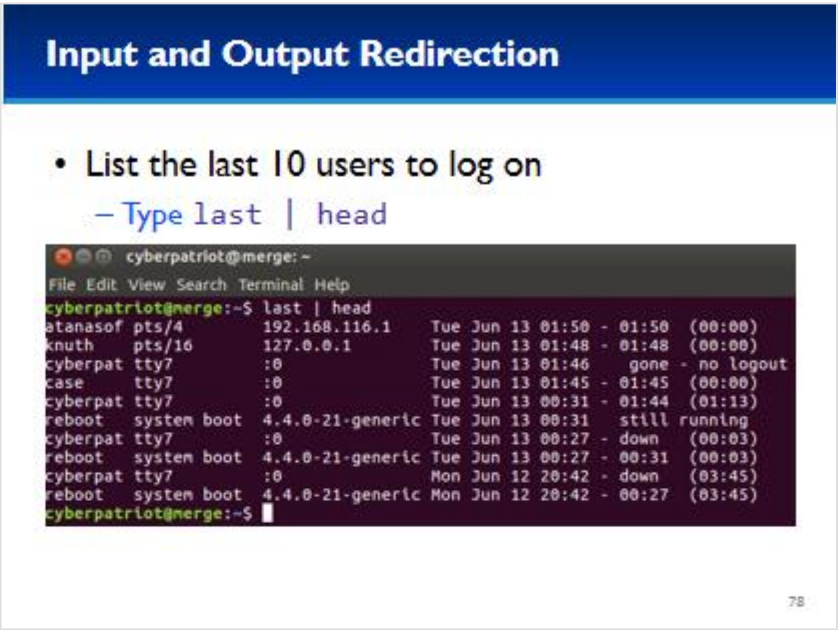
- Many commands will automatically read from standard input if you don’t specify a file argument.

- For example, say you wanted to count the total number of main functions in the Quake source code.

☆Have the students run the commands on the screen.

- The Quake source code has seven different main functions because there are several different programs in the code including clients and servers.

Slide 78



Input and Output Redirection

- List the last 10 users to log on
  - Type `last | head`

cyberpatriot@merge: ~

```
cyberpatriot@merge:~$ last | head
atanasof pts/4        192.168.116.1    Tue Jun 13 01:50 - 01:50  (00:00)
knuth    pts/16       127.0.0.1        Tue Jun 13 01:48 - 01:48  (00:00)
cyberpat tty7         :0               Tue Jun 13 01:46    gone - no logout
case     tty7         :0               Tue Jun 13 01:45 - 01:45  (00:00)
cyberpat tty7         :0               Tue Jun 13 00:31 - 01:44  (01:13)
reboot   system boot  4.4.0-21-generic Tue Jun 13 00:31   still running
cyberpat tty7         :0               Tue Jun 13 00:27 - down   (00:03)
reboot   system boot  4.4.0-21-generic Tue Jun 13 00:27 - 00:31  (00:03)
cyberpat tty7         :0               Mon Jun 12 20:42 - down   (03:45)
reboot   system boot  4.4.0-21-generic Mon Jun 12 20:42 - 00:27  (03:45)
cyberpatriot@merge:~$ 
```

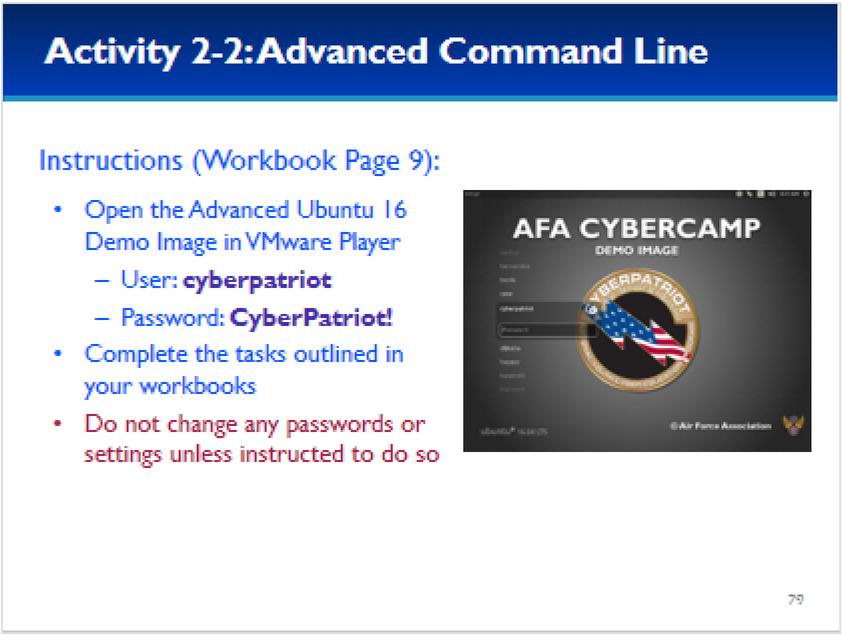
78

- A useful command to view the last ten users to log on is: **last-pipe-head**

☆Have the students run the commands on the screen.

☆The result of the command will not match the screenshot because it is based on the log on activity of each image.

Slide 79



Activity 2-2: Advanced Command Line

Instructions (Workbook Page 9):

- Open the Advanced Ubuntu 16 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

◷ Give students about 20 minutes to complete the tasks listed on Pages 9 of their workbooks.

☆This lab will review the advanced command line commands covered in this section.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. G
2. sausage
3. /home/cyberpatriot/Music/Nutcracker.mp3, /home/kleinrock/Desktop/4.mp3, /home/knuth/Music/1812.mp3
4. /var/spool/
5. /usr/bin/find/
6. 21
7. print the character counts

Slide 80

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

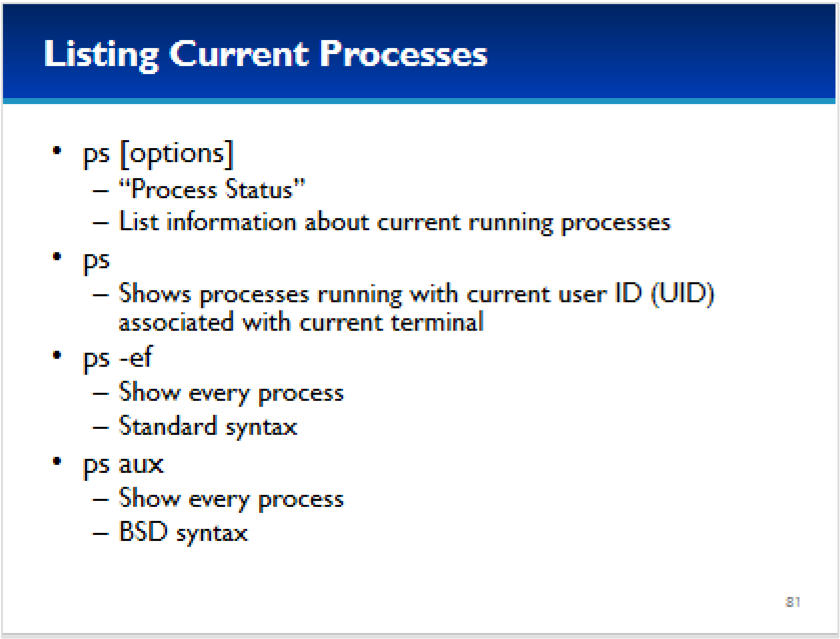
Processes and Scheduled Tasks

🕒 Devote 30 minutes to slides 81-108. Allow the students 20 minutes to complete the activity on slide 108.

☆Throughout this section, students should follow along in the **Advanced Ubuntu Demo Image**.

☆In this section, you will learn multiple methods to determine what processes are being run on your system, how to kill unwanted processes, and methods for bypassing rootkits on a compromised machine.

Slide 81



Listing Current Processes

- ps [options]
  - “Process Status”
  - List information about current running processes
- ps
  - Shows processes running with current user ID (UID) associated with current terminal
- ps -ef
  - Show every process
  - Standard syntax
- ps aux
  - Show every process
  - BSD syntax

81

- The current processes running on your system can be listed using the **ps** command.

- **Ps** by itself with no options is probably not what you want.

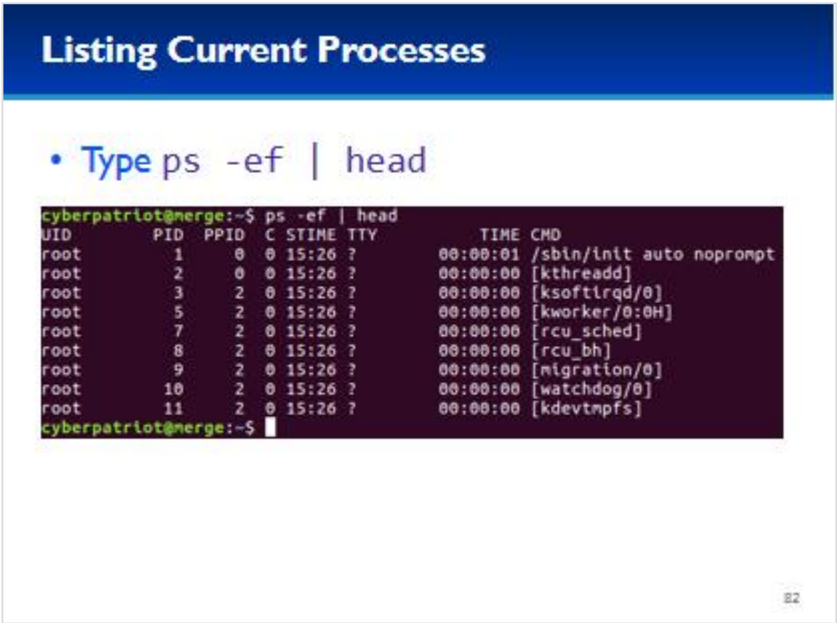
  - By default, it shows only process running as your current user ID and associated with your current terminal.

- There are two ways to list all processes with **ps**, and we’re going to cover them here because you may run into a Linux or Unix distribution that is less friendly and only supports one of these methods.

- **ps –ef** is the standard Linux syntax, **e** lists “every process” and **f** tells it to do a “full-format” listing (which displays more information on each process).

- **pa aux** is the traditional “BSD” style syntax. It displays mostly same thing as **ps –ef** but does display a little bit more information on memory statistics.

Slide 82



Listing Current Processes

- Type ps -ef | head

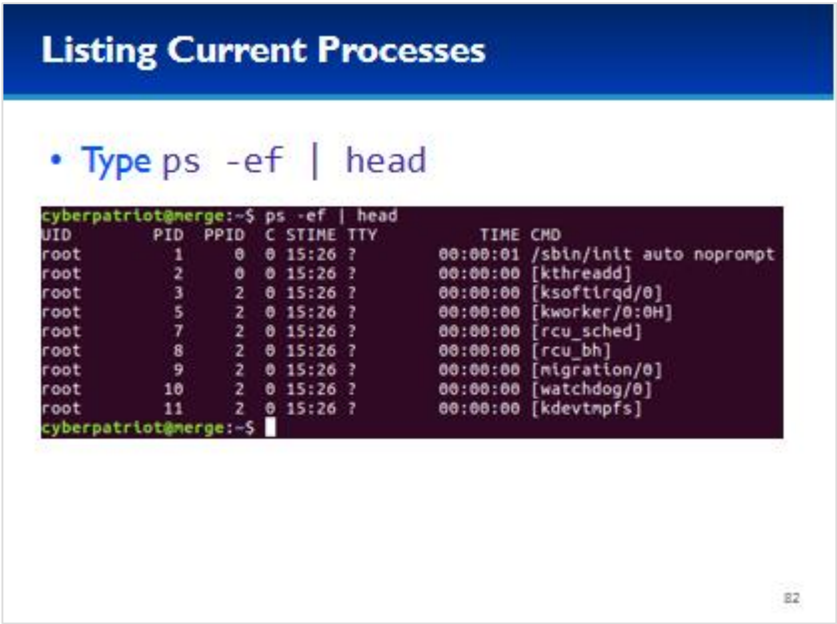
```
cyberpatriot@merge:~$ ps -ef | head
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 15:26 ?        00:00:01 /sbin/init auto noprompt
root         2     0  0 15:26 ?        00:00:00 [kthreadd]
root         3     2  0 15:26 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 15:26 ?        00:00:00 [kworker/0:0H]
root         7     2  0 15:26 ?        00:00:00 [rcu_sched]
root         8     2  0 15:26 ?        00:00:00 [rcu_bh]
root         9     2  0 15:26 ?        00:00:00 [migration/0]
root        10     2  0 15:26 ?        00:00:00 [watchdog/0]
root        11     2  0 15:26 ?        00:00:00 [kdevtmpfs]
cyberpatriot@merge:~$
```

82

- **ps** orders the processes on your computer by PID.
- To view the first 10 lines output by **ps**, type **ps -ef** and pipe it through **head**.

☆Have the students run the commands on the screen.

Slide 82



Listing Current Processes

- Type ps -ef | head

```
cyberpatriot@merge:~$ ps -ef | head
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 15:26 ?        00:00:01 /sbin/init auto noprompt
root         2     0  0 15:26 ?        00:00:00 [kthreadd]
root         3     2  0 15:26 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 15:26 ?        00:00:00 [kworker/0:0H]
root         7     2  0 15:26 ?        00:00:00 [rcu_sched]
root         8     2  0 15:26 ?        00:00:00 [rcu_bh]
root         9     2  0 15:26 ?        00:00:00 [migration/0]
root        10     2  0 15:26 ?        00:00:00 [watchdog/0]
root        11     2  0 15:26 ?        00:00:00 [kdevtmpfs]
cyberpatriot@merge:~$ 
```

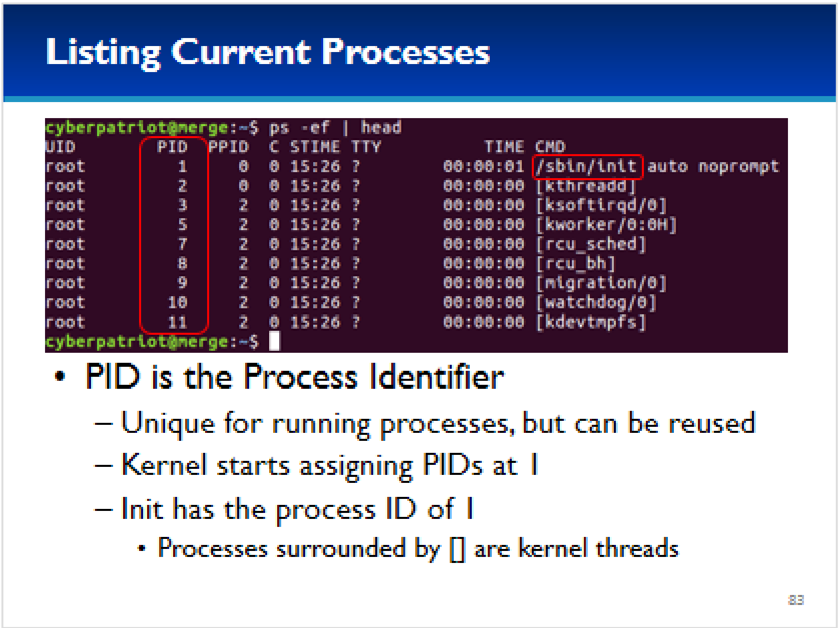
82

- **Ps** orders the processes on your computer by PID.

- To view the first 10 lines output by **ps**, type **ps -ef** and pipe it through **head**.

☆Have the students run the commands on the screen.

Slide 83



Listing Current Processes

```
cyberpatriot@merge:~$ ps -ef | head
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 15:26 ?        00:00:01 /sbin/init auto noprompt
root         2     0  0 15:26 ?        00:00:00 [kthreadd]
root         3     2  0 15:26 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 15:26 ?        00:00:00 [kworker/0:0H]
root         7     2  0 15:26 ?        00:00:00 [rcu_sched]
root         8     2  0 15:26 ?        00:00:00 [rcu_bh]
root         9     2  0 15:26 ?        00:00:00 [migration/0]
root        10     2  0 15:26 ?        00:00:00 [watchdog/0]
root        11     2  0 15:26 ?        00:00:00 [kdevtmpfs]
cyberpatriot@merge:~$
```

- PID is the Process Identifier
  - Unique for running processes, but can be reused
  - Kernel starts assigning PIDs at 1
  - Init has the process ID of 1
    - Processes surrounded by [] are kernel threads

83

- The PID column is where the process identifier or PID is displayed for that process.

- A PID is unique for running processes, but can be reused after a process dies.

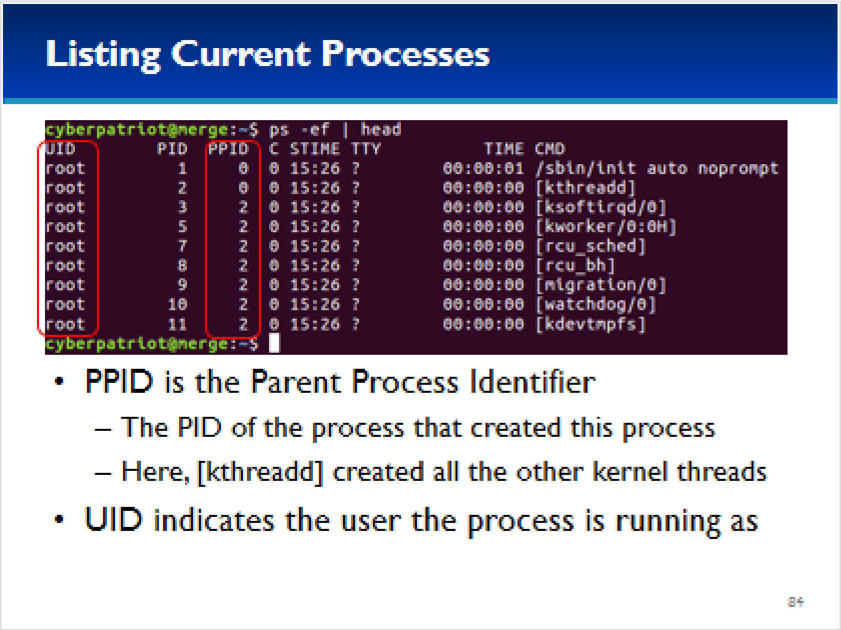
- The Kernel starts assigning PID's starting at 1.

- You can see the first process that was created by the Kernel is init with a PID of 1.

- **Ps** prints out Kernel threads surrounded by square brackets [].

  - These threads are part of the kernel and have different responsibilities such as managing different pieces of hardware.

Slide 84



Listing Current Processes

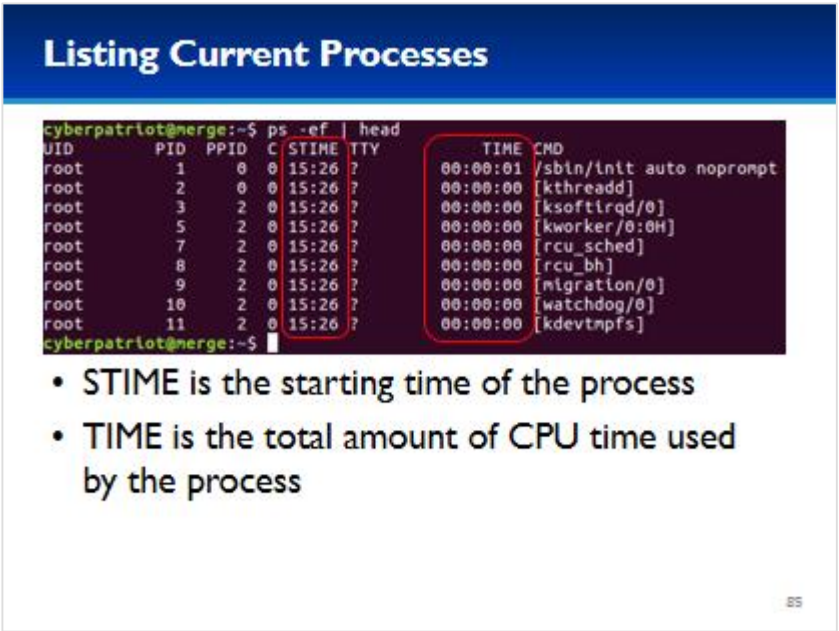
```
cyberpatriot@merge:~$ ps -ef | head
UID          PID  PPID  C STIME TTY          TIME CMD
root           1     0  0 15:26 ?        00:00:01 /sbin/init auto noprompt
root           2     0  0 15:26 ?        00:00:00 [kthreadd]
root           3     2  0 15:26 ?        00:00:00 [ksoftirqd/0]
root           5     2  0 15:26 ?        00:00:00 [kworker/0:0H]
root           7     2  0 15:26 ?        00:00:00 [rcu_sched]
root           8     2  0 15:26 ?        00:00:00 [rcu_bh]
root           9     2  0 15:26 ?        00:00:00 [migration/0]
root          10     2  0 15:26 ?        00:00:00 [watchdog/0]
root          11     2  0 15:26 ?        00:00:00 [kdevtmpfs]
cyberpatriot@merge:~$
```

- PPID is the Parent Process Identifier
  - The PID of the process that created this process
  - Here, [kthreadd] created all the other kernel threads
- UID indicates the user the process is running as

84

- The PPID is the parent PID. This is the PID of the process that created this process.
- The PPID of init and [kthreadd] is 0, indicating that the kernel created this process on it's own.
- kthreadd is the kernel thread daemon that manages the kernel threads.
- UID is the user the process is running as, this determines what the process is allowed to do.

Slide 85



Listing Current Processes

```
cyberpatriot@merge:~$ ps -ef | head
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 15:26 ?        00:00:01 /sbin/init auto noprompt
root         2     0  0 15:26 ?        00:00:00 [kthreadd]
root         3     2  0 15:26 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 15:26 ?        00:00:00 [kworker/0:0H]
root         7     2  0 15:26 ?        00:00:00 [rcu_sched]
root         8     2  0 15:26 ?        00:00:00 [rcu_bh]
root         9     2  0 15:26 ?        00:00:00 [migration/0]
root        10     2  0 15:26 ?        00:00:00 [watchdog/0]
root        11     2  0 15:26 ?        00:00:00 [kdevtmpfs]
cyberpatriot@merge:~$
```

- STIME is the starting time of the process
- TIME is the total amount of CPU time used by the process

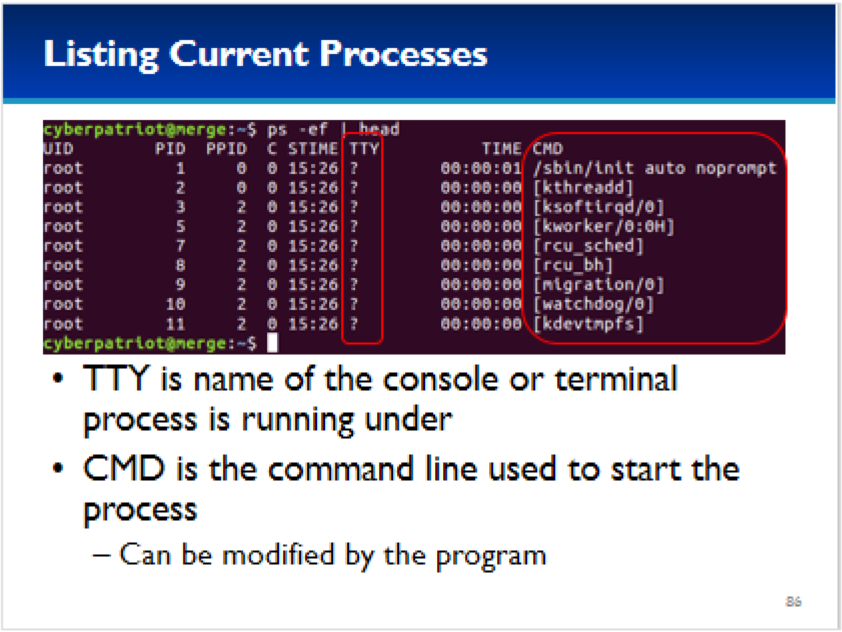
85

- STIME is the starting time of the process, in this example the virtual machine was booted at 3:26, hence init and all the kernel threads were started at 3:26 as well.

- TIME is the cpu time that this process has used, this is not the time that the process has been alive, but rather the total time that the process has been actively using the CPU.

  - You can see that most of these processes are fairly lightweight and in this example the init thread has used about one second of CPU time since we powered on the system.

Slide 86



Listing Current Processes

```
cyberpatriot@merge:~$ ps -ef | head
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 15:26 ?        00:00:01 /sbin/init auto noprompt
root         2     0  0 15:26 ?        00:00:00 [kthreadd]
root         3     2  0 15:26 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 15:26 ?        00:00:00 [kworker/0:0H]
root         7     2  0 15:26 ?        00:00:00 [rcu_sched]
root         8     2  0 15:26 ?        00:00:00 [rcu_bh]
root         9     2  0 15:26 ?        00:00:00 [migration/0]
root        10     2  0 15:26 ?        00:00:00 [watchdog/0]
root        11     2  0 15:26 ?        00:00:00 [kdevtmpfs]
cyberpatriot@merge:~$ 
```

- TTY is name of the console or terminal process is running under
- CMD is the command line used to start the process
  - Can be modified by the program

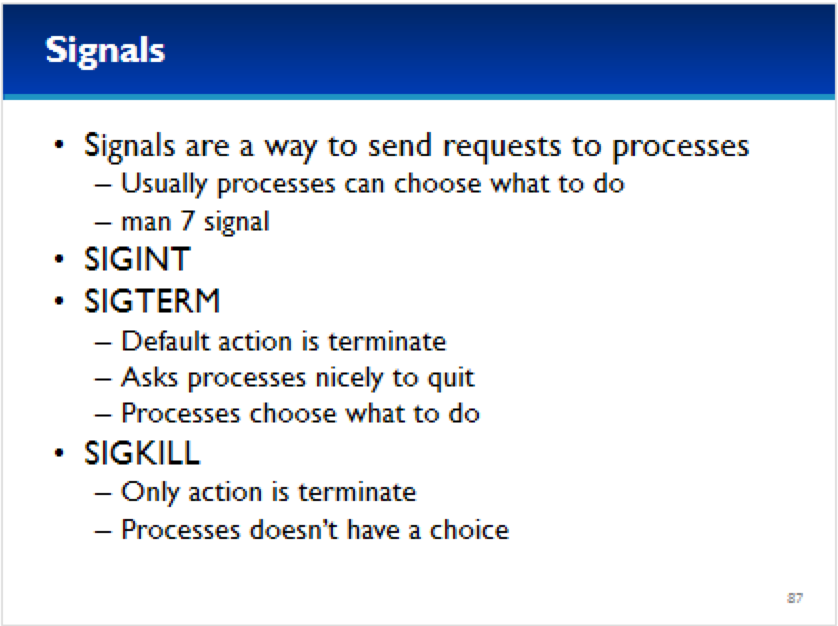
86

- TTY is the name of the console or terminal the process is running under, in this case these processes have no associated terminal.

- CMD is the command line used to start the process.

  - However, this can be changed by programs for various reasons – some . For example, you might want to prevent users from seeing potentially sensitive command line options that were passed to your program.

Slide 87



Signals

- Signals are a way to send requests to processes
  - Usually processes can choose what to do
  - man 7 signal
- SIGINT
- SIGTERM
  - Default action is terminate
  - Asks processes nicely to quit
  - Processes choose what to do
- SIGKILL
  - Only action is terminate
  - Processes doesn't have a choice

87

- How do you kill a process?

- If a process is running in the foreground, you can often kill it by typing **Ctrl+C**.

  - **Ctrl** is often represented by a **caret** (**^**).

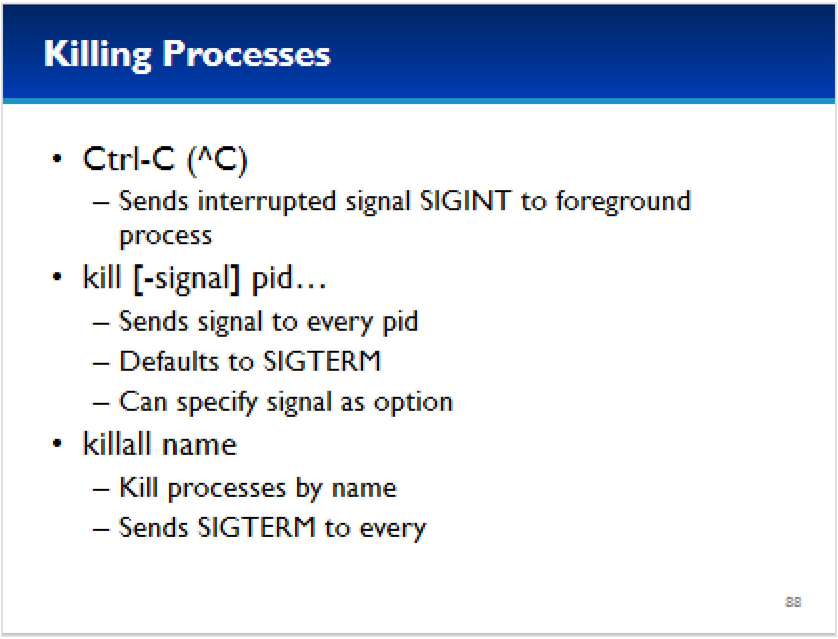
- The **kill** command does more than just kill processes, it will send the signal to every PID you specify on the command line.

  - It defaults to **SIGTERM**, but you could specify **SIGKILL** as the signal if the program isn't dying with SIGTERM.

- **Kill** can be tedious to use because you must specify the PID on the command line.

  - The **killall** command can help with that by killing <u>all</u> processes that match a specific name.

Slide 88



Killing Processes

- Ctrl-C (^C)
  - Sends interrupted signal SIGINT to foreground process
- kill [-signal] pid…
  - Sends signal to every pid
  - Defaults to SIGTERM
  - Can specify signal as option
- killall name
  - Kill processes by name
  - Sends SIGTERM to every

88

- So how do you kill a process?

- If a process is running in the foreground, you can often kill it by typing **Ctrl+C** (lowercase c).

  - Ctrl is often represented by a caret.

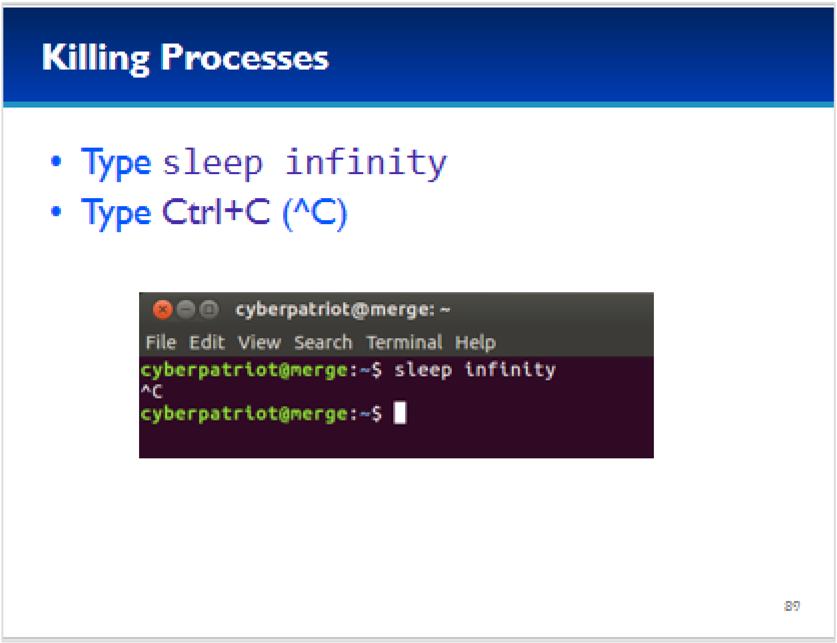
- The **kill** command does more than just kill processes, it will send the specified signal to every PID you specify on the command line.

  - It defaults to **-SIGTERM**, but you could specify **–SIGKILL** as the signal if the program isn't dying with **SIGTERM**.

- Kill can be tedious to use sometimes because you have to specify the PID on the command line.

  - The **killall** command can help with that by killing ALL processes that match a specific name.

Slide 89



Killing Processes

- Type `sleep infinity`
- Type Ctrl+C (^C)

```
cyberpatriot@merge:~$ sleep infinity
^C
cyberpatriot@merge:~$ █
```

- Here's an example of how to use **Ctrl+C** to kill a program in the foreground.

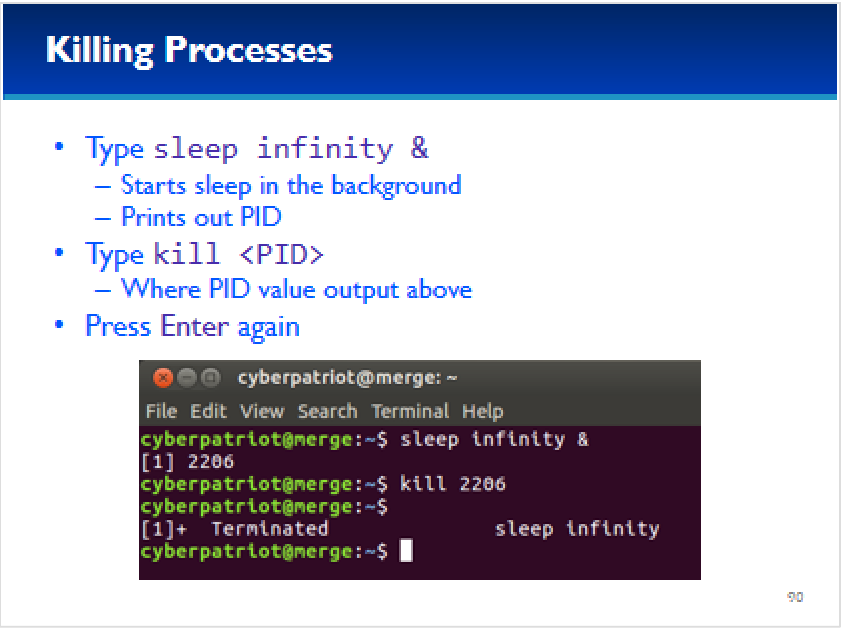
- The **sleep infinity** command will do nothing forever.

☆Have the students run the commands on the screen.

- You can see that the command will hang forever until you kill it.

  - In this case, we killed it with **Ctrl+C**.

Slide 90



Killing Processes

- Type `sleep infinity &`
  - Starts sleep in the background
  - Prints out PID
- Type `kill <PID>`
  - Where PID value output above
- Press Enter again

```
cyberpatriot@merge:~$ sleep infinity &
[1] 2206
cyberpatriot@merge:~$ kill 2206
cyberpatriot@merge:~$
[1]+  Terminated              sleep infinity
cyberpatriot@merge:~$ 
```

90

- If you want to start a program, but you don’t want your console to wait for it to die, you can start that process in the background with an **&**.

- When you start a process in the background, the PID of that process is printed on the screen.

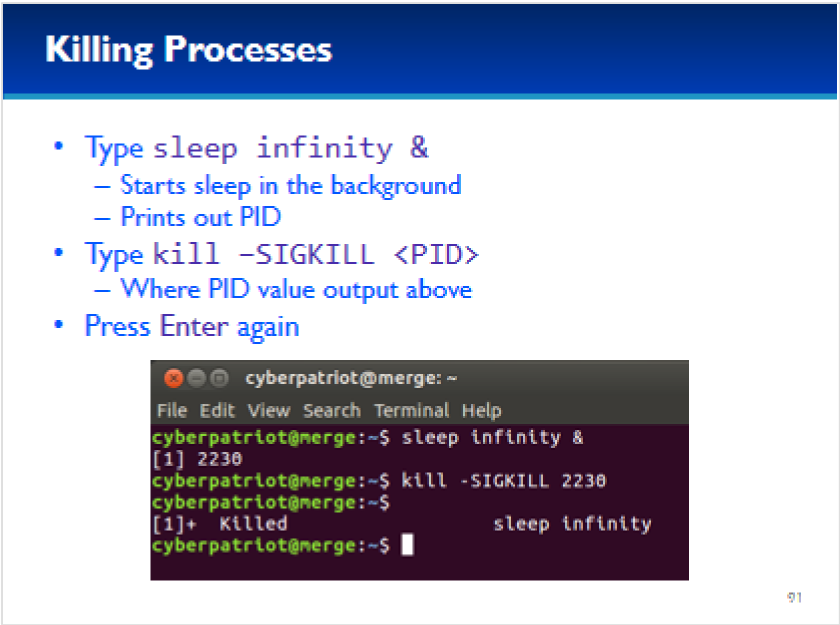
☆Have the students run the commands on the screen.

- In this example, the PID of sleep is 2206.

- By typing **kill 2206**, we are killing the **sleep** process we just started.

- We don’t get a notification that the process died right away because our shell doesn’t want to interrupt us while we type a command, so we have to press **Enter** again before we are notified.

Slide 91



Killing Processes

- Type `sleep infinity &`
  - Starts sleep in the background
  - Prints out PID
- Type `kill -SIGKILL <PID>`
  - Where PID value output above
- Press Enter again

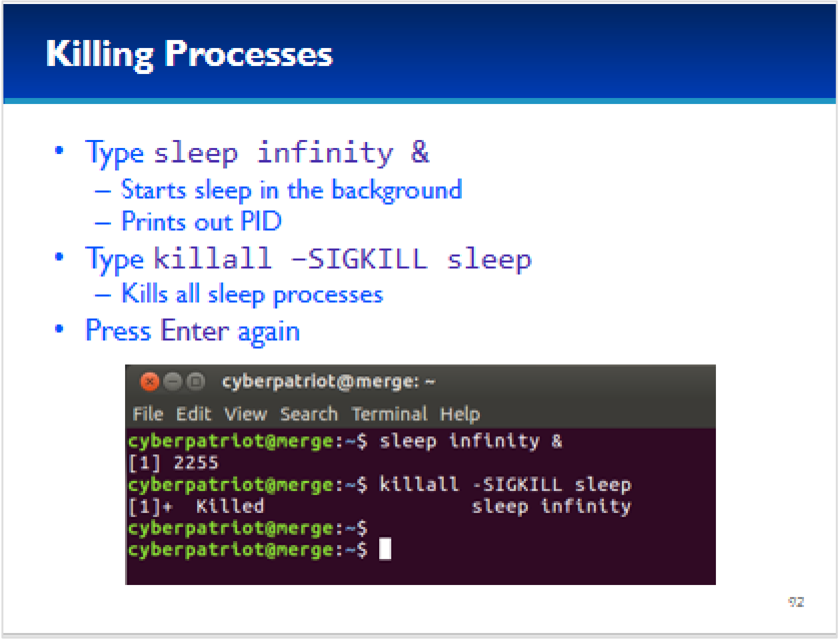
```
cyberpatriot@merge:~$ sleep infinity &
[1] 2230
cyberpatriot@merge:~$ kill -SIGKILL 2230
cyberpatriot@merge:~$
[1]+  Killed                  sleep infinity
cyberpatriot@merge:~$ 
```

91

- Sometimes a process won’t die with the default **SIGTERM**.
- In this case you need to specify a signal of **SIGKILL**.

☆Have the students run the commands on the screen.

Slide 92



Killing Processes

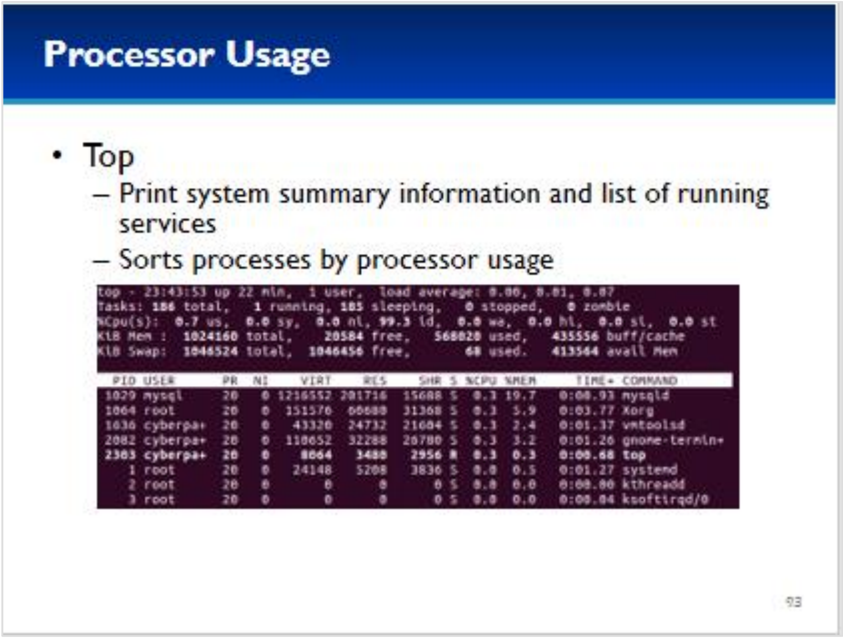
- Type `sleep infinity &`
  - Starts sleep in the background
  - Prints out PID
- Type `killall -SIGKILL sleep`
  - Kills all sleep processes
- Press Enter again

```
cyberpatriot@merge:~$ sleep infinity &
[1] 2255
cyberpatriot@merge:~$ killall -SIGKILL sleep
[1]+  Killed                  sleep infinity
cyberpatriot@merge:~$
cyberpatriot@merge:~$
```

- The **killall** command works just like **kill**, except you specify a process name instead of PID.

- **Killall** is very useful, but be careful when running it because it is possible to unintentionally kill important processes.

Slide 93



Processor Usage

- Top
  - Print system summary information and list of running services
  - Sorts processes by processor usage

```
top - 23:43:53 up 22 min,  1 user,  load average: 0.00, 0.01, 0.07
Tasks: 186 total,   1 running, 185 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.0 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1024160 total,    20584 free,   568020 used,   435556 buff/cache
KiB Swap:  1046524 total,  1046456 free,       68 used.   413564 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1029 mysql     20   0 1216552 201716  15688 S  0.3 19.7   0:00.93 mysqld
 1064 root      20   0  151576  60680  31368 S  0.3  5.9   0:03.77 Xorg
 1036 cyberpa+  20   0   43320  24732  21004 S  0.3  2.4   0:01.37 vmtoolsd
 2082 cyberpa+  20   0  110652  32288  26780 S  0.3  3.2   0:01.26 gnome-termin+
 2303 cyberpa+  20   0    8064   3480   2956 R  0.3  0.3   0:00.68 top
    1 root      20   0   24148   5208   3836 S  0.0  0.5   0:01.27 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.04 ksoftirqd/0
```

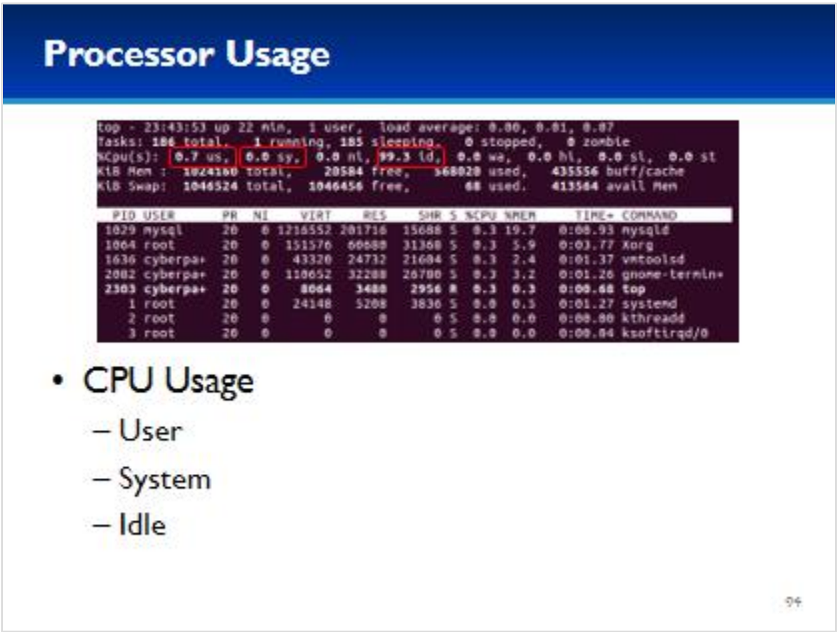
93

- Sometimes you want a real-time view of resource utilization and what processes are running on your system.

- In that case, the **top** command is what you need.

- By default, **top** sorts processes by CPU usage, so you can easily see which processes might be hung, slowing down your system, or where any bottlenecks might be.

Slide 94



Processor Usage

```
top - 23:43:53 up 22 min,  1 user,  load average: 0.00, 0.01, 0.07
Tasks: 186 total,   1 running, 185 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.0 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1024160 total,    20584 free,   568020 used,   435556 buff/cache
KiB Swap:  1046524 total,  1046456 free,       68 used.   413564 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1029 mysql     20   0 1216552 201716  15688 S  0.3 19.7   0:00.93 mysqld
 1064 root      20   0  151576  60688  31368 S  0.3  5.9   0:03.77 Xorg
 1636 cyberpa+  20   0   43320  24732  21604 S  0.3  2.4   0:01.37 vmtoolsd
 2082 cyberpa+  20   0  110652  32288  26700 S  0.3  3.2   0:01.26 gnome-termin+
 2303 cyberpa+  20   0    8064   3480   2956 R  0.3  0.3   0:00.68 top
    1 root      20   0   24148   5208   3836 S  0.0  0.5   0:01.27 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.04 ksoftirqd/0
```

- CPU Usage
  - User
  - System
  - Idle

94

- The overall CPU usage is displayed here and is divided into three main parts.

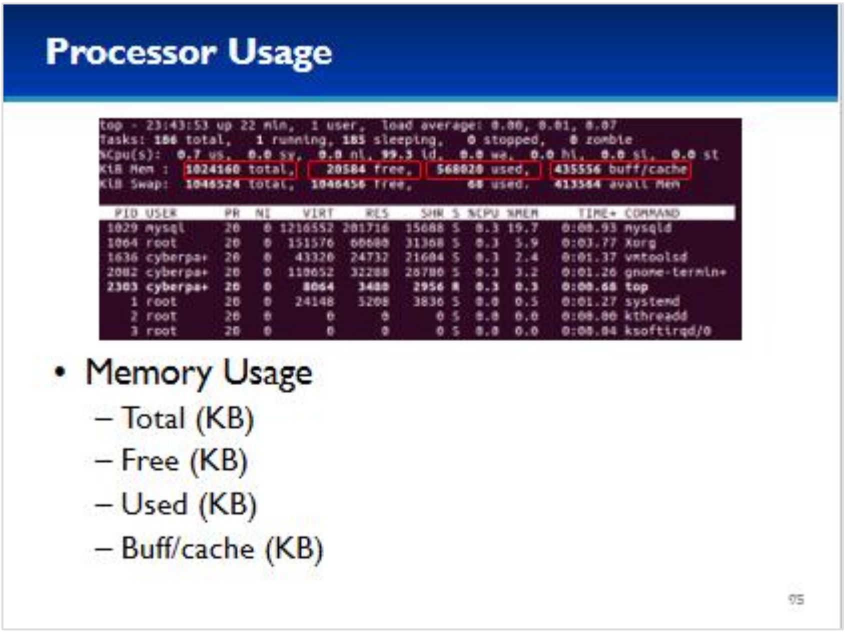
- The user usage is the % of CPU cycles spent on "user space" applications.

- The system usage is the % of CPU usage spent on "kernel space."

  - A lot of the actions that applications take are performed in "kernel space" such as file input and output.

- The idle CPU usage is the % that is not being used; this is probably the first number you want to look at when determining if your CPU is under heavy load.

Slide 95



Processor Usage

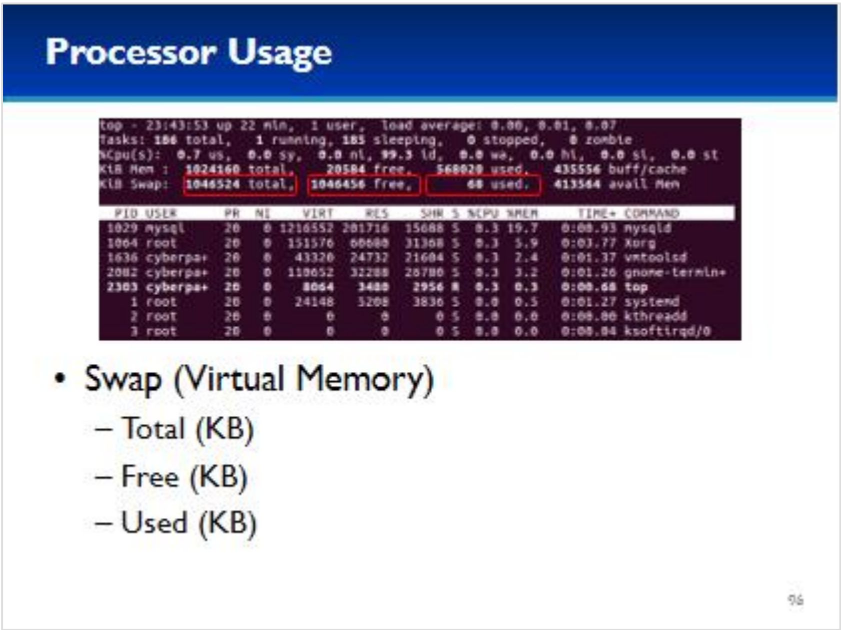
```
top - 23:43:53 up 22 min,  1 user,  load average: 0.00, 0.01, 0.07
Tasks: 186 total,   1 running, 185 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.0 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1024160 total,    20584 free,   568020 used,   435556 buff/cache
KiB Swap:  1046524 total,  1046456 free,       68 used.   413564 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1029 mysql     20   0 1216552 201716  15688 S  0.3 19.7   0:00.93 mysqld
 1064 root      20   0  151576  60600  31368 S  0.3  5.9   0:03.77 Xorg
 1636 cyberpa+  20   0   43320  24732  21604 S  0.3  2.4   0:01.37 vmtoolsd
 2082 cyberpa+  20   0  110652  32288  28780 S  0.3  3.2   0:01.26 gnome-termin+
 2303 cyberpa+  20   0    8064   3480   2956 R  0.3  0.3   0:00.68 top
    1 root      20   0   24148   5208   3836 S  0.0  0.5   0:01.27 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.04 ksoftirqd/0
```

- Memory Usage
  - Total (KB)
  - Free (KB)
  - Used (KB)
  - Buff/cache (KB)

95

- System memory usage information is shown as well.
- The total amount of memory in kilobytes is shown on the left; here we have one gigabyte of system memory.
- Next the amount of free memory is shown; but here it says we only have 20 megabytes free.
- After that, the amount of memory that is used by applications is shown. Here we are using about 560 megabytes of memory.
- Those numbers don’t exactly add up, so where is the rest of the memory going?
- The rest of the memory is being used by the kernel to cache recently used files on the filesystem, so if we need to use those files again, they will be readily available.

Slide 96



Processor Usage

```
top - 23:43:53 up 22 min,  1 user,  load average: 0.00, 0.01, 0.07
Tasks: 186 total,   1 running, 185 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.0 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1024160 total,    20584 free,   568020 used,   435556 buff/cache
KiB Swap:  1046524 total,  1046456 free,       68 used.   413544 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1029 mysql     20   0 1216552 201716  15688 S  0.3 19.7   0:00.93 mysqld
 1064 root      20   0  151576  60680  31368 S  0.3  5.9   0:03.77 Xorg
 1636 cyberpa+  20   0   43320  24732  21604 S  0.3  2.4   0:01.37 vmtoolsd
 2082 cyberpa+  20   0  110652  32288  28780 S  0.3  3.2   0:01.26 gnome-termin+
 2303 cyberpa+  20   0    8064   3480   2956 R  0.3  0.3   0:00.68 top
    1 root      20   0   24148   5208   3836 S  0.0  0.5   0:01.27 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.04 ksoftirqd/0
```

- Swap (Virtual Memory)
  - Total (KB)
  - Free (KB)
  - Used (KB)

96

- The next line of **top** shows the swap space.

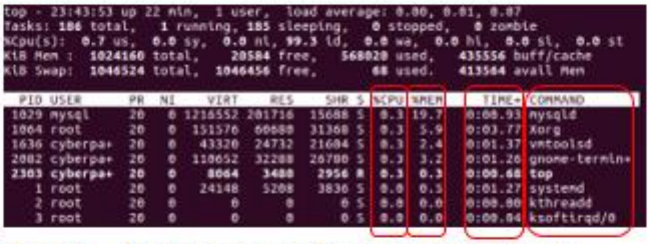
- Swap space is virtual memory, and the kernel will move infrequently accessed memory there to free up more memory in case we need it.

- Here we can see swap statistics including the total amount of swap space, the amount of swap space free, and the amount of used swap space.

  - We’re not using much swap space since we have plenty of memory available to be used (even though that memory is currently allocated to caching files).

Slide 97

Processor Usage



```
top - 23:43:53 up 22 min,  1 user,  load average: 0.00, 0.01, 0.07
Tasks: 186 total,   1 running, 185 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.0 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1024160 total,    20584 free,   568020 used,   435556 buff/cache
KiB Swap:  1046524 total,  1046456 free,       68 used.   413564 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1029 mysql     20   0 1216552 201716  15688 S  0.3 19.7   0:00.93 mysqld
 1064 root      20   0  151576  60680  31368 S  0.3  5.9   0:03.77 Xorg
 1636 cyberpa+  20   0   43320  24732  21604 S  0.3  2.4   0:01.37 vmtoolsd
 2082 cyberpa+  20   0  110652  32288  26700 S  0.3  3.2   0:01.26 gnome-termin+
 2303 cyberpa+  20   0    8064   3480   2956 R  0.3  0.3   0:00.68 top
    1 root      20   0   24148   5208   3836 S  0.0  0.3   0:01.27 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.04 ksoftirqd/0
```

- %CPU – Percentage of processor used
- %MEM – Percentage of memory used
- TIME+ – CPU time process has used
- COMMAND – Name of the process

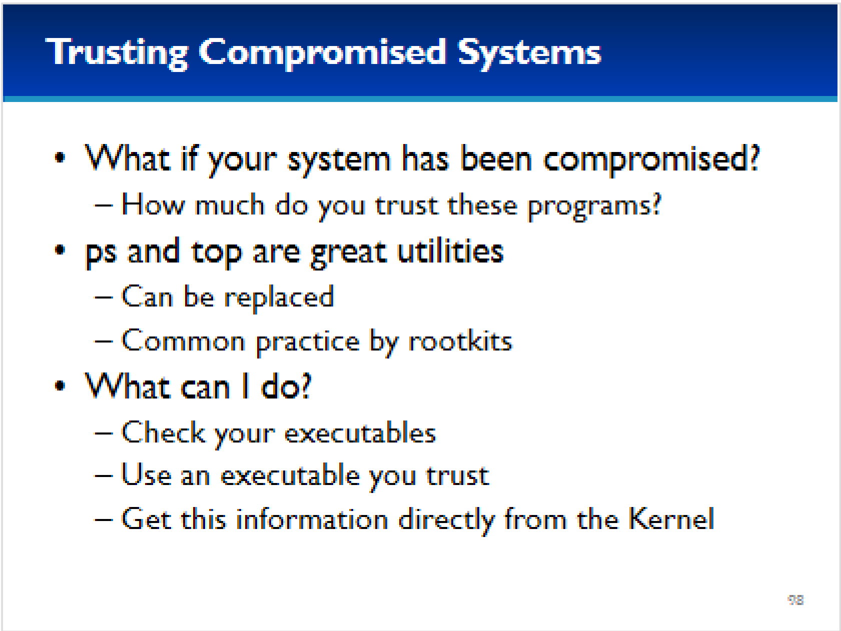
97

- **Top** also shows the percentages of CPU capacity and memory that a process is using, and the amount of CPU time it has used.

  - Remember CPU time is the total amount of time that the process has been actively running on the CPU.

  - Each logical core of a CPU can only run one process at a time, so it needs to quickly switch between processes to make it appear like they are all running simultaneously.

Slide 98



Trusting Compromised Systems

- What if your system has been compromised?
  - How much do you trust these programs?
- ps and top are great utilities
  - Can be replaced
  - Common practice by rootkits
- What can I do?
  - Check your executables
  - Use an executable you trust
  - Get this information directly from the Kernel

98

- What if your system has been compromised?

- Can you trust these programs?

Click to reveal answer.

- **ps** and **top** are extremely useful programs, but an adversary that has compromised your computer can easily replace these (and other) programs.

- What can you do about it?

  - You can check your executables to see if they match the executables on a trusted computer.

  - You can run trusted executables from a removable drive that is preferably read-only.

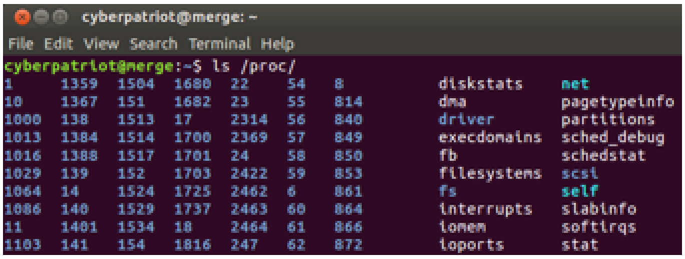
  - You could get this information directly from the kernel.

- These are all good starting strategies; however, it's important to note that you cannot fully trust anything on a system that has been compromised, so an offline analysis using a trusted computer is sometimes required.

Slide 99

Proc Filesystem

- Pseudo-filesystem
  - Interface to kernel data structures
  - Provides process information
  - Much harder to hide processes
- Type `ls /proc`



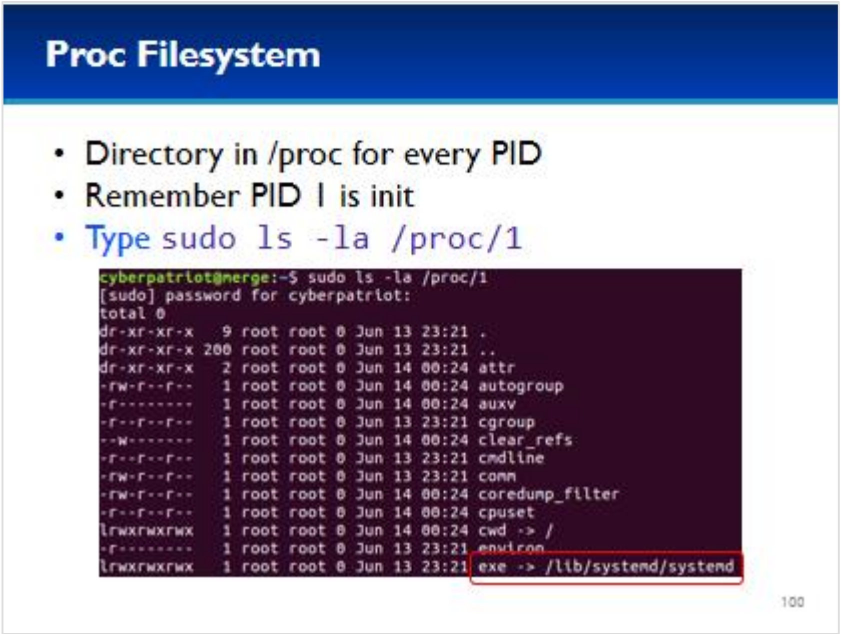
```
cyberpatriot@merge:~$ ls /proc/
1      1359  1504  1680  22    54   8            diskstats    net
10     1367  151   1682  23    55   814          dma          pagetypeinfo
1000   138   1513  17    2314  56   840          driver       partitions
1013   1384  1514  1700  2369  57   849          execdomains  sched_debug
1016   1388  1517  1701  24    58   850          fb           schedstat
1029   139   152   1703  2422  59   853          filesystems  scsi
1064   14    1524  1725  2462  6    861          fs           self
1086   140   1529  1737  2463  60   864          interrupts   slabinfo
11     1401  1534  18    2464  61   866          iomem        softirqs
1103   141   154   1816  247   62   872          ioports      stat
```

99

- How do we get this information directly from the kernel?
- The kernel provides the proc filesystem for this purpose.
- Let's take a look at the proc filesystem.

☆Have the students run the commands on the screen.

Slide 100



Proc Filesystem

- Directory in /proc for every PID
- Remember PID 1 is init
- Type `sudo ls -la /proc/1`

```
cyberpatriot@merge:~$ sudo ls -la /proc/1
[sudo] password for cyberpatriot:
total 0
dr-xr-xr-x   9 root root 0 Jun 13 23:21 .
dr-xr-xr-x 200 root root 0 Jun 13 23:21 ..
dr-xr-xr-x   2 root root 0 Jun 14 00:24 attr
-rw-r--r--   1 root root 0 Jun 14 00:24 autogroup
-r--------   1 root root 0 Jun 14 00:24 auxv
-r--r--r--   1 root root 0 Jun 13 23:21 cgroup
--w-------   1 root root 0 Jun 14 00:24 clear_refs
-r--r--r--   1 root root 0 Jun 13 23:21 cmdline
-rw-r--r--   1 root root 0 Jun 13 23:21 comm
-rw-r--r--   1 root root 0 Jun 14 00:24 coredump_filter
-r--r--r--   1 root root 0 Jun 14 00:24 cpuset
lrwxrwxrwx   1 root root 0 Jun 14 00:24 cwd -> /
-r--------   1 root root 0 Jun 13 23:21 environ
lrwxrwxrwx   1 root root 0 Jun 13 23:21 exe -> /lib/systemd/systemd
```

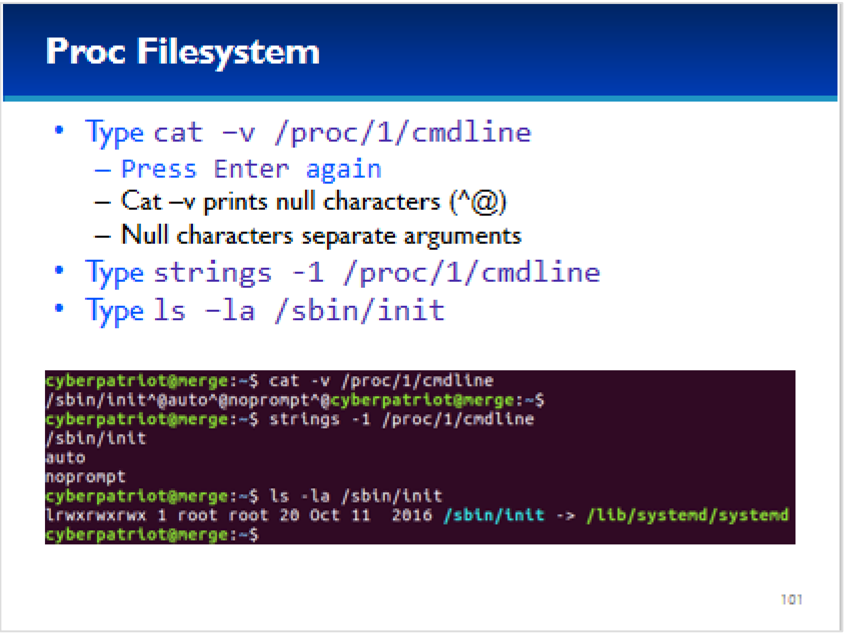
100

- Inside the proc filesystem, there are many numbered directories.
- There is a numbered directory for every PID running on the system.
- We know that PID 1 is init, so let's look inside that directory.

☆Have the students run the commands on the screen.

- You can see there are lots of files in this directory that represent parts of the process that you can view or even modify if you have permissions.
- For example, the exe file in this directory points to the actual process executable which is: /lib/systemd/systemd
- Remember how **ps** said that PID 1 was: /sbin/init
  - /sbin/init is actually just a symlink to /lib/systemd/systemd

Slide 101



Proc Filesystem

- Type `cat –v /proc/1/cmdline`
  - `Press Enter again`
  - Cat –v prints null characters (^@)
  - Null characters separate arguments
- Type `strings -1 /proc/1/cmdline`
- Type `ls –la /sbin/init`

```
cyberpatriot@merge:~$ cat -v /proc/1/cmdline
/sbin/init^@auto^@noprompt^@cyberpatriot@merge:~$
cyberpatriot@merge:~$ strings -1 /proc/1/cmdline
/sbin/init
auto
noprompt
cyberpatriot@merge:~$ ls -la /sbin/init
lrwxrwxrwx 1 root root 20 Oct 11  2016 /sbin/init -> /lib/systemd/systemd
cyberpatriot@merge:~$
```

101

- Exploring the proc filesystem more, the cmdline file contains the command line that was used to execute the program.

- However, the command line arguments are separated by null characters which don’t print to the screen, making the output hard to read.

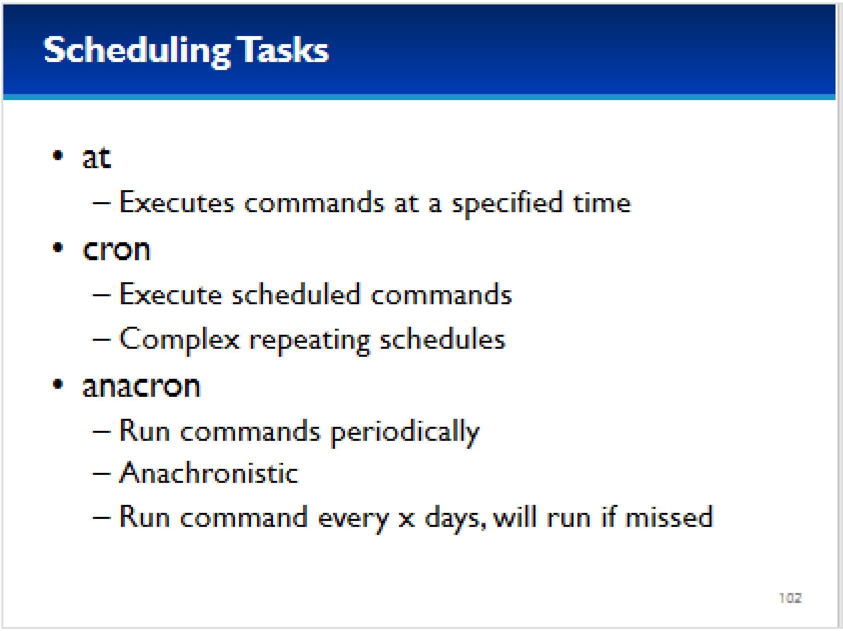
- To get around this you can use **cat –v** to print the null characters as ^@

- Or you can use **strings -1** to print each argument on a different line.

☆Have the students run the commands on the screen.

- You can see **systemd** was started as /sbin/init with the auto and noprompt command line arguments.

Slide 102



Scheduling Tasks

- at
  - Executes commands at a specified time
- cron
  - Execute scheduled commands
  - Complex repeating schedules
- anacron
  - Run commands periodically
  - Anachronistic
  - Run command every x days, will run if missed

102

- How do scheduled tasks get executed in Linux?

- All processes get spawned by an existing process, and scheduled tasks are no different. These are started by services such as **at**, **cron**, and **anacron**.

- **At** is no longer installed on most Linux distributions by default, but it can be used to execute a program at a specified time.

- **Cron** is designed for running tasks on a regularly repeating schedule, and is very configurable allowing you to specify complex schedules to fit most needs.

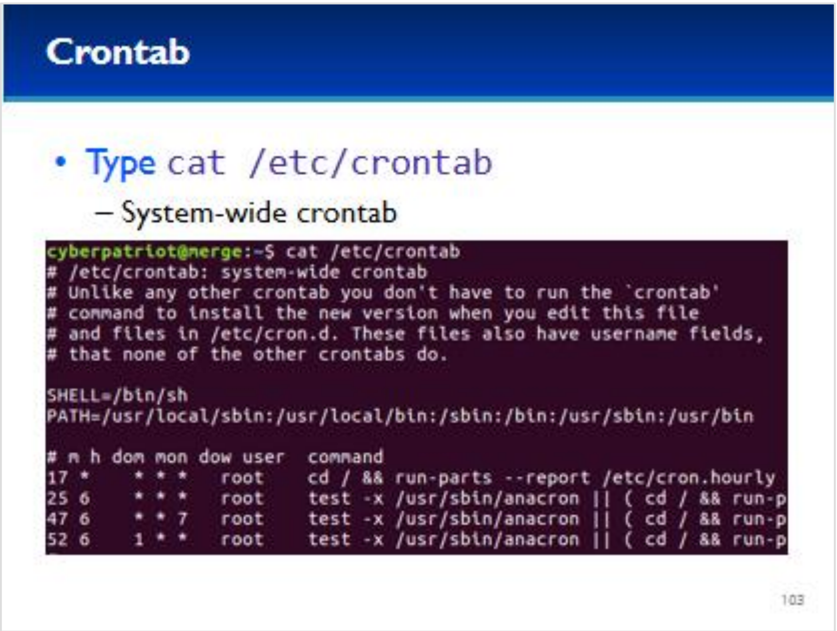
- **Cron** is an important system service, so it's usually not a good idea to remove it.

- **Anacron** is another system service that can work in conjunction with **cron**.

  - Designed to run programs on a schedule that is specified in days. Unlike **cron** you can't specify times.

  - What makes **anacron** special is that it will run tasks if they were previously missed, which often happens when a system is powered off.

Slide 103



Crontab

- Type `cat /etc/crontab`
  - System-wide crontab

```
cyberpatriot@merge:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-p
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-p
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-p
```

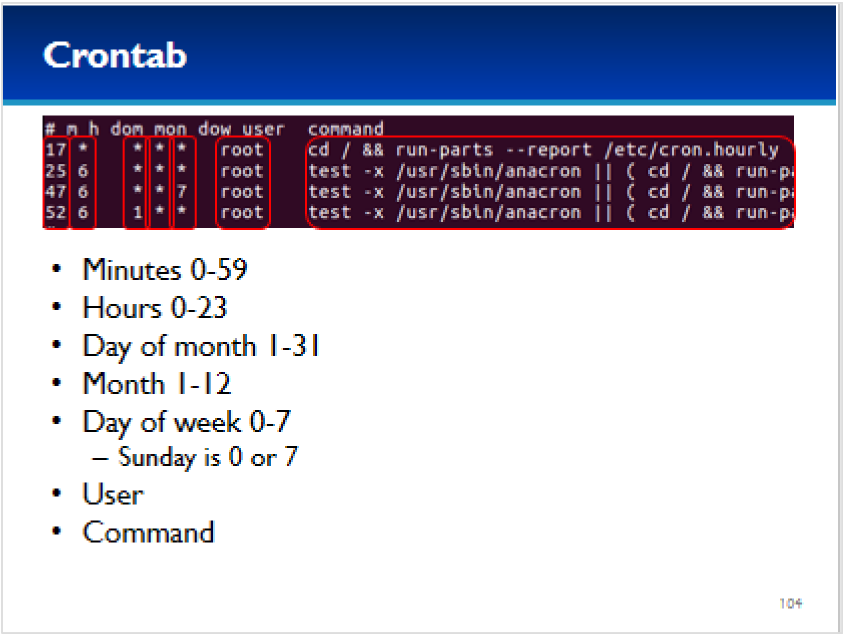
103

- The primary **cron** configuration file that tells **cron** what to run is located at: /etc/crontab

- Lines that begin with # are comments and are ignored by **cron**.

- Let’s examine this file more closely on the next slides.

Slide 104



Crontab

```
# m h dom mon dow user   command
17 *     * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6     * * *   root    test -x /usr/sbin/anacron || ( cd / && run-p
47 6     * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-p
52 6     1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-p
```

- Minutes 0-59
- Hours 0-23
- Day of month 1-31
- Month 1-12
- Day of week 0-7
  - Sunday is 0 or 7
- User
- Command

104

- The first column is minutes; specifies the minutes portion of the day and time that the command will be run.

Click to reveal Hours.

- The second column is hours, and specifies the hours portion.
- A star means the command will be executed for any value.

Click to reveal day of month.

- The next column is the day of the month, as a number, from 1-31.

Click to reveal month.

- The next column is the month, specified as a number, from 1-12.

Click to reveal day of week.

- The next column is the day of week, specified as a number from 0-7; Sunday is represented by either 0 or 7.

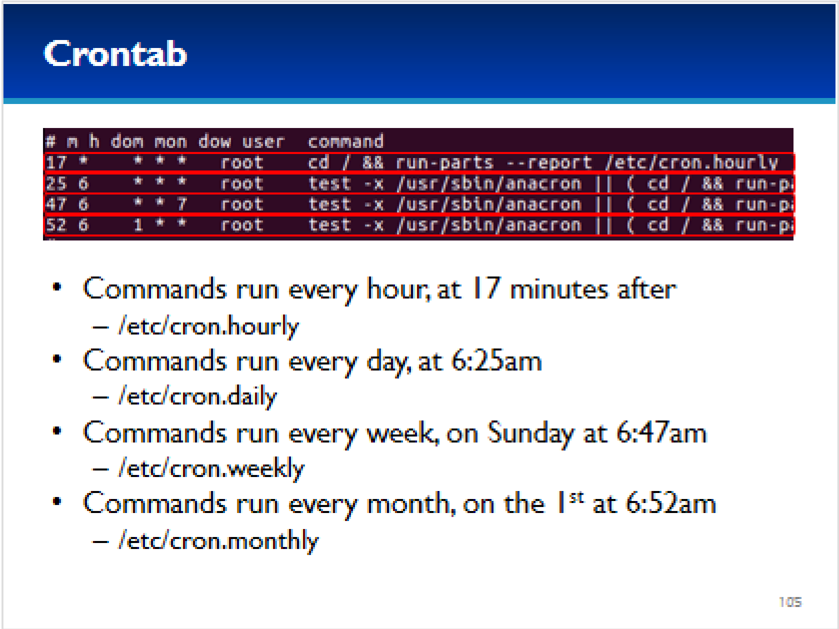
Click to reveal user.

- User displays name of user that initiated a process.

Click to reveal Command.

- Finally, the last column is the command that is run.

Slide 105



Crontab

```
# m h dom mon dow user  command
17 *     * * *  root    cd / && run-parts --report /etc/cron.hourly
25 6     * * *  root    test -x /usr/sbin/anacron || ( cd / && run-pa
47 6     * * 7  root    test -x /usr/sbin/anacron || ( cd / && run-pa
52 6     1 * *  root    test -x /usr/sbin/anacron || ( cd / && run-pa
```

- Commands run every hour, at 17 minutes after
  - /etc/cron.hourly
- Commands run every day, at 6:25am
  - /etc/cron.daily
- Commands run every week, on Sunday at 6:47am
  - /etc/cron.weekly
- Commands run every month, on the 1st at 6:52am
  - /etc/cron.monthly

105

- The first line runs the specified command every hour of every day at 17 minutes after the top of the hour.

- This command runs all of the commands in: /etc/cron.hourly

Click to reveal cron.daily.

- The next line runs all commands in /etc/cron.daily everyday at 6:25 a.m.

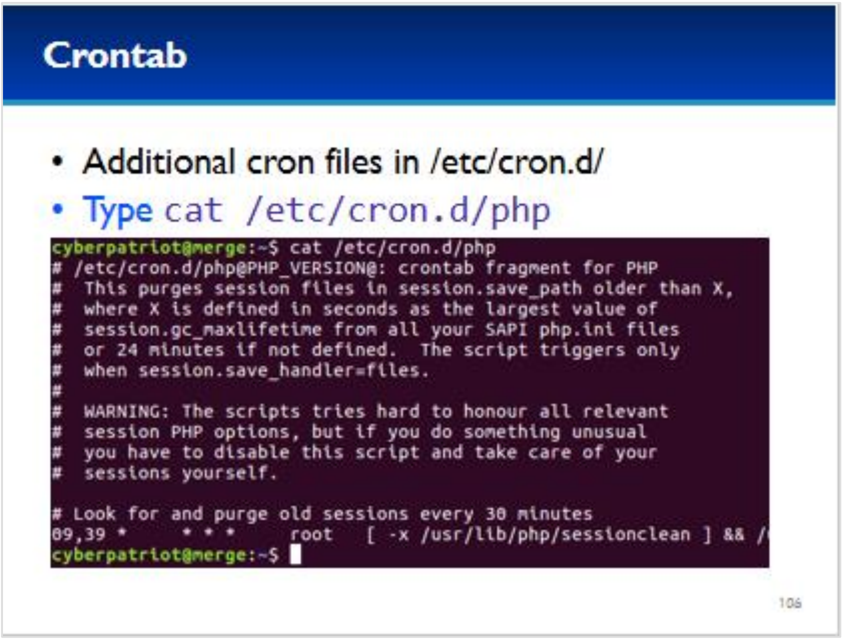
Click to reveal cron.weekly.

- The next line runs all commands in /etc/cron.weekly every Sunday at 6:47 a.m.

Click to reveal cron.monthly.

- The last line runs all commands in /etc/cron.monthly on the first of every month at 6:52 a.m.

Slide 106



Crontab

- Additional cron files in /etc/cron.d/
- Type `cat /etc/cron.d/php`

```
cyberpatriot@merge:~$ cat /etc/cron.d/php
# /etc/cron.d/php@PHP_VERSION@: crontab fragment for PHP
#  This purges session files in session.save_path older than X,
#  where X is defined in seconds as the largest value of
#  session.gc_maxlifetime from all your SAPI php.ini files
#  or 24 minutes if not defined.  The script triggers only
#  when session.save_handler=files.
#
#  WARNING: The scripts tries hard to honour all relevant
#  session PHP options, but if you do something unusual
#  you have to disable this script and take care of your
#  sessions yourself.

# Look for and purge old sessions every 30 minutes
09,39 *     * * *     root   [ -x /usr/lib/php/sessionclean ] && /
cyberpatriot@merge:~$ 
```

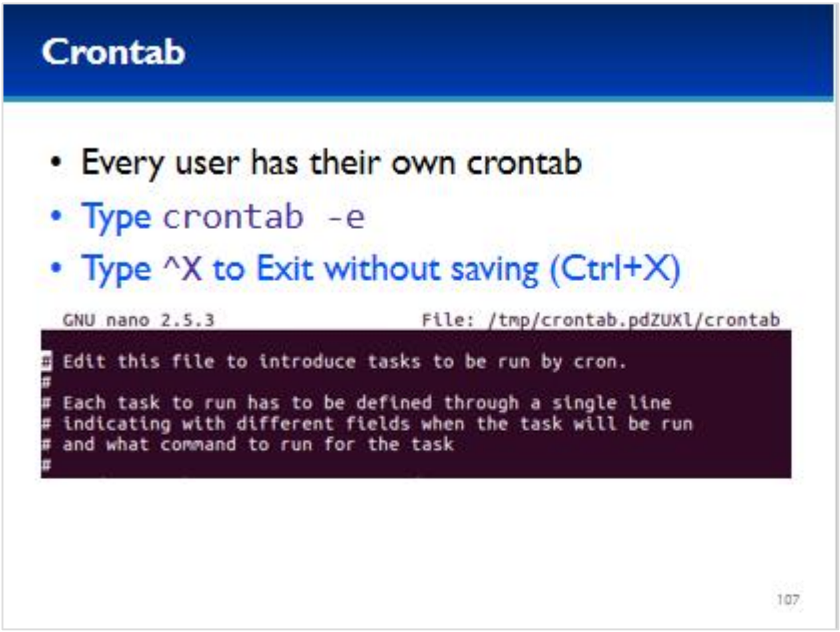
106

- Additional cron files are located in: /etc/cron.d/

☆Have the students run the commands on the screen.

- Here, the **php sessionclean** command is run twice every hour, at nine minutes after, and 39 minutes after.

Slide 107



Crontab

- Every user has their own crontab
- Type `crontab -e`
- Type ^X to Exit without saving (Ctrl+X)

```
  GNU nano 2.5.3                  File: /tmp/crontab.pdZUXl/crontab

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
```

107

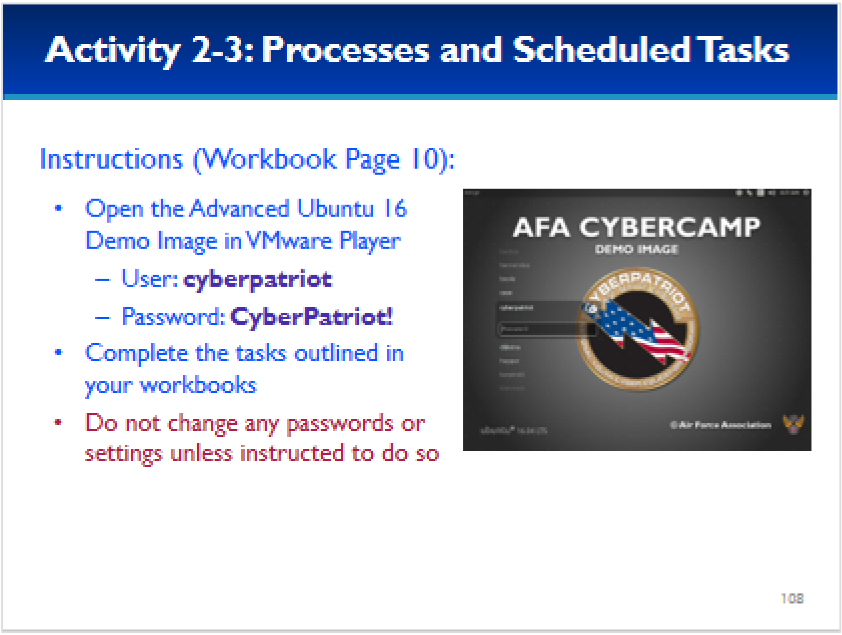
- Additionally, every user has their own crontab that can be edited by typing the command: **crontab –e**

  - User **crontab** files don’t specify a user to run the command, since they will always run as the user that the crontab belongs to.

☆Have the students run the commands on the screen.

- This is a default blank crontab that does nothing. Note: All the lines that begin with # are comments and are ignored.

Slide 108



Activity 2-3: Processes and Scheduled Tasks

Instructions (Workbook Page 10):

- Open the Advanced Ubuntu 16 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

108

◷ Give students about 20 minutes to complete the tasks listed on page 10 of their workbooks.

☆This lab will review processes and scheduled tasks.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. -r
2. /usr/bin/nc -k -l -p 1337 -w 300 -e /bin/bash
3. Every minute
4. -
5. -
6. 3
7. --no-debug
8. /bin/ls

Slide 109

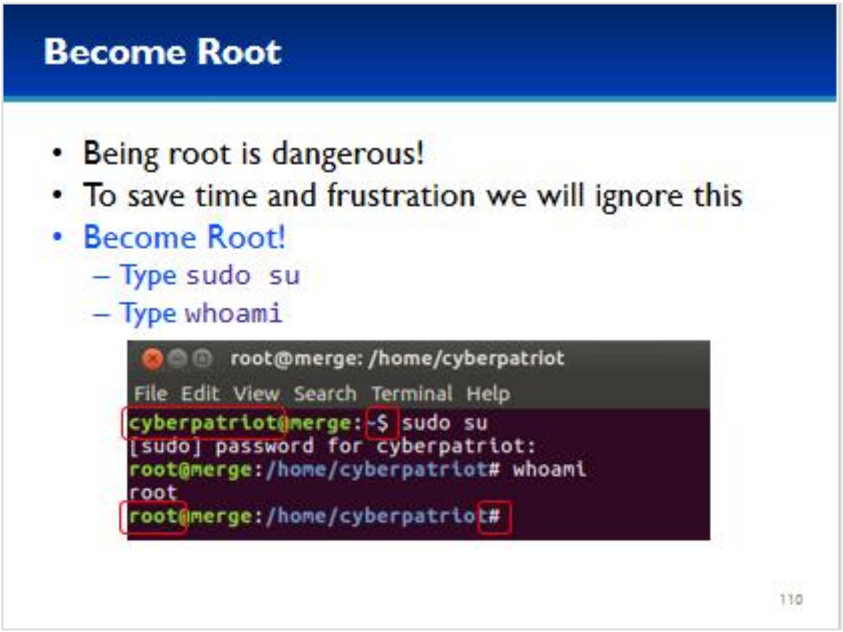
Security Policies and PAM

🕒 Devote 40 minutes to slides 110-149. Allow the students 20 minutes to complete the activity on slide 149.

☆ Throughout this section, students should follow along in the **Advanced Ubuntu 16 Demo Image**.

☆ In this section we’ll take a long look at a few of the many Kernel parameters that can affect the security of your system, and the best way to modify them. In the second part of this section we will break down PAM and explain how it works step-by-step so you know how to enable secure account and password policies.

Slide 110



Become Root

- Being root is dangerous!
- To save time and frustration we will ignore this
- Become Root!
  - Type sudo su
  - Type whoami

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help

```
cyberpatriot@merge:~$ sudo su
[sudo] password for cyberpatriot:
root@merge:/home/cyberpatriot# whoami
root
root@merge:/home/cyberpatriot#
```

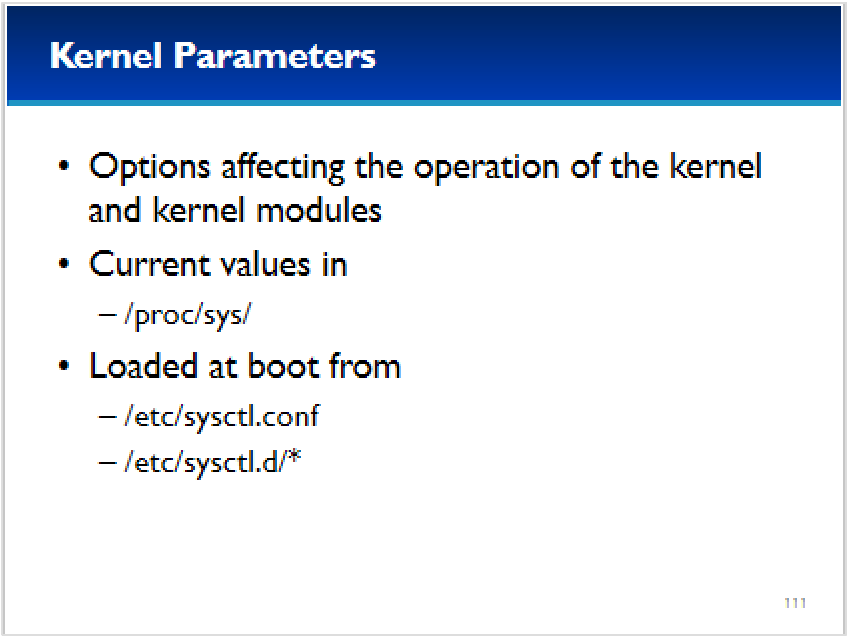
110

- Some of the commands in this section are harder to execute if you're not root; in particular, output redirection is more complicated using **sudo**.
- For this purpose we are going to be root for the remaining sections.
- In order to become root, type **sudo su** and type your password if prompted.

☆Have the students run the commands on the screen.

- When you're root, you can see that your username to the left side of your prompt changes to root, and the symbol on the right side if your prompt changes to a #.
- This is done to help you know if you're root or not.

Slide 111



Kernel Parameters

- Options affecting the operation of the kernel and kernel modules
- Current values in
  - /proc/sys/
- Loaded at boot from
  - /etc/sysctl.conf
  - /etc/sysctl.d/*

111

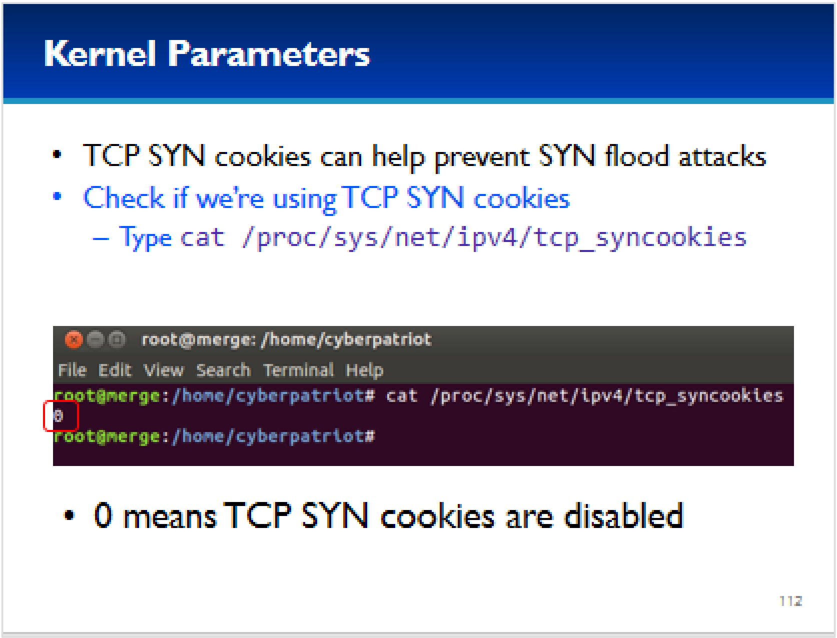
- Kernel parameters are options that affect many parts Linux, including kernel modules.

- The parameters are accessible in: /proc/sys

  - Many parameters can be directly changed through the /proc/ filesystem.

- These values are loaded on boot from the file /etc/sysctl.conf, and all of the files in the directory: /etc/sysctl.d/

Slide 112



Kernel Parameters

- TCP SYN cookies can help prevent SYN flood attacks
- Check if we're using TCP SYN cookies
  - Type `cat /proc/sys/net/ipv4/tcp_syncookies`

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help

```
root@merge:/home/cyberpatriot# cat /proc/sys/net/ipv4/tcp_syncookies
0
root@merge:/home/cyberpatriot#
```

- 0 means TCP SYN cookies are disabled

112

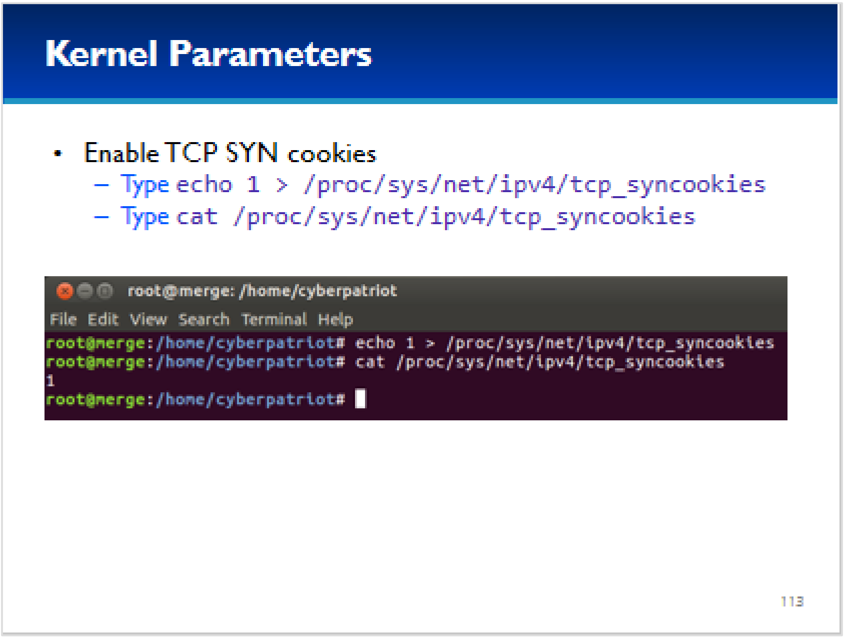
- There are many security-related kernel parameters, and we can’t cover them all. That’s up to you to research on your own, but we will cover a few prominent examples.

- TCP Syncookies is a technique that can help prevent SYN flood attacks.

- To check if we are using TCP SYN cookies, enter: **cat /proc/sys/net/ipv4/tcp_syncookies**

- This isn’t a “real” file on the hard drive, but rather an interface to the Linux kernel that can be accessed the same way as a file.

Slide 113



Kernel Parameters

- Enable TCP SYN cookies
  - Type `echo 1 > /proc/sys/net/ipv4/tcp_syncookies`
  - Type `cat /proc/sys/net/ipv4/tcp_syncookies`

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help

```
root@merge:/home/cyberpatriot# echo 1 > /proc/sys/net/ipv4/tcp_syncookies
root@merge:/home/cyberpatriot# cat /proc/sys/net/ipv4/tcp_syncookies
1
root@merge:/home/cyberpatriot# 
```

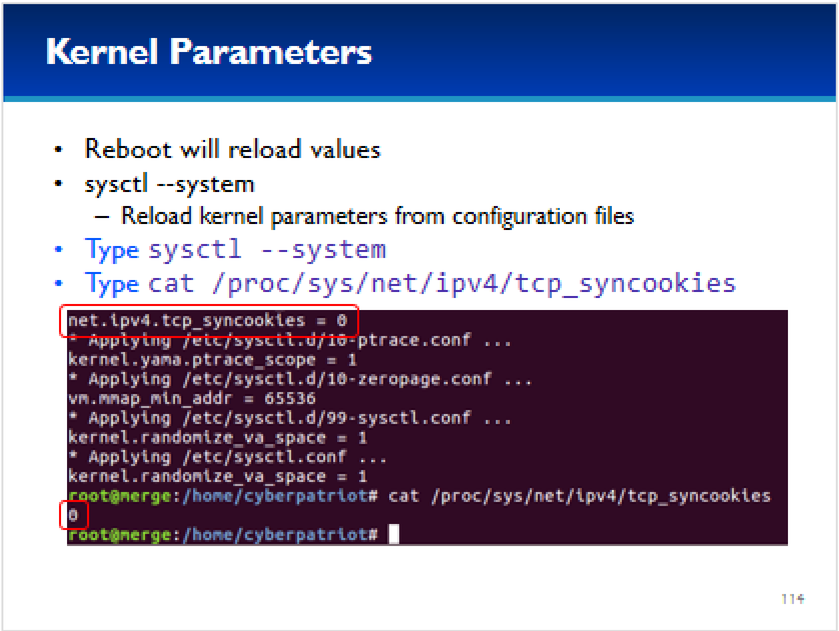
113

- In order to enable TCP SYN cookies, all we have to do is write 1 to the tcp_syncookies file.

☆Have the students run the commands on the screen.

- You can see that now the file contains a 1 and the Linux kernel is now using TCP SYN cookies to protect your computer against SYN flood attacks.

Slide 114



Kernel Parameters

- Reboot will reload values
- sysctl --system
  - Reload kernel parameters from configuration files
- Type `sysctl --system`
- Type `cat /proc/sys/net/ipv4/tcp_syncookies`

```
net.ipv4.tcp_syncookies = 0
* Applying /etc/sysctl.d/10-ptrace.conf ...
kernel.yama.ptrace_scope = 1
* Applying /etc/sysctl.d/10-zeropage.conf ...
vm.mmap_min_addr = 65536
* Applying /etc/sysctl.d/99-sysctl.conf ...
kernel.randomize_va_space = 1
* Applying /etc/sysctl.conf ...
kernel.randomize_va_space = 1
root@merge:/home/cyberpatriot# cat /proc/sys/net/ipv4/tcp_syncookies
0
root@merge:/home/cyberpatriot# 
```

114

- Unfortunately, our changes are not persistent. The next time the computer is shut off or rebooted, tcp_syncookies will go back to its default value.

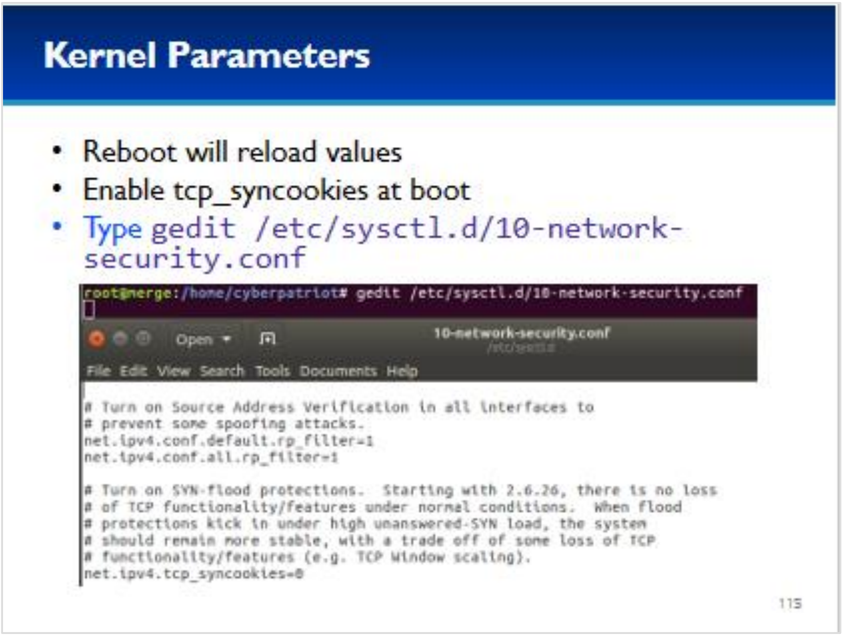
- To simulate this, we can use the **sysctl** command, which reloads the values stored in the sysctl configuration files.

- Side note: the **sysctl** command is completely unrelated to **systemctl** and **systemd**.

☆Have the students run the commands on the screen.

- After running **sysctl --system** we can see that the tcp_syncookies value was restored to 0.

Slide 115



Kernel Parameters

- Reboot will reload values
- Enable tcp_syncookies at boot
- Type `gedit /etc/sysctl.d/10-network-security.conf`

```
root@merge:/home/cyberpatriot# gedit /etc/sysctl.d/10-network-security.conf
```

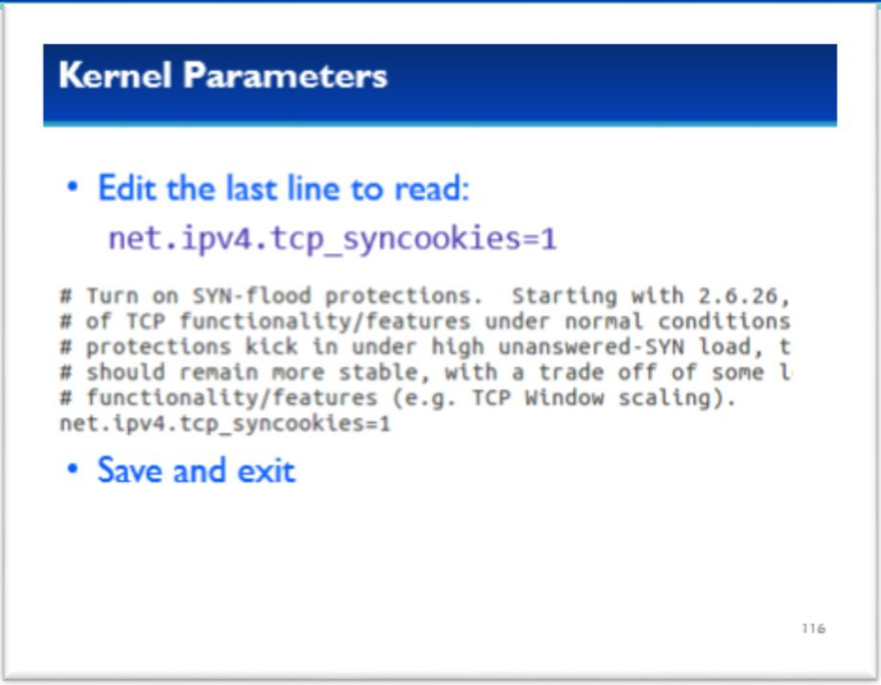
```
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks.
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

# Turn on SYN-flood protections.  Starting with 2.6.26, there is no loss
# of TCP functionality/features under normal conditions.  When flood
# protections kick in under high unanswered-SYN load, the system
# should remain more stable, with a trade off of some loss of TCP
# functionality/features (e.g. TCP Window scaling).
net.ipv4.tcp_syncookies=0
```

115

- All we have to do is set this parameter in the **sysctl** configuration files.
- Before setting a kernel parameter, you should check if and where it is currently being set in /etc/sysctl.conf or /etc/sysctl.d/
  - Using **grep –R** can help with this.
- In this case, tcp_syncookies is being set in the file /etc/sysctl.d/10-network-security.conf
- As root, use **gedit** to edit this file.

☆Have the students run the commands on the screen.

Slide 116



Kernel Parameters

- Edit the last line to read:

  net.ipv4.tcp_syncookies=1

```
# Turn on SYN-flood protections.  Starting with 2.6.26,
# of TCP functionality/features under normal conditions
# protections kick in under high unanswered-SYN load, t
# should remain more stable, with a trade off of some l
# functionality/features (e.g. TCP Window scaling).
net.ipv4.tcp_syncookies=1
```

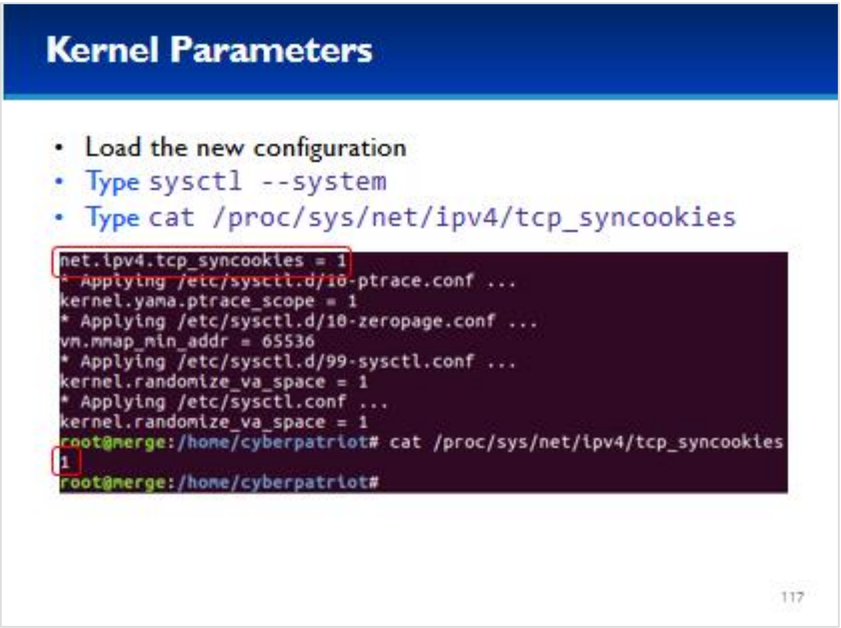
- Save and exit

116

- Change the last line in the file to set tcp_syncookies to 1 instead of 0.

- Now save the file and exit.

Slide 117



Kernel Parameters

- Load the new configuration
- Type `sysctl --system`
- Type `cat /proc/sys/net/ipv4/tcp_syncookies`

```
net.ipv4.tcp_syncookies = 1
* Applying /etc/sysctl.d/10-ptrace.conf ...
kernel.yama.ptrace_scope = 1
* Applying /etc/sysctl.d/10-zeropage.conf ...
vm.mmap_min_addr = 65536
* Applying /etc/sysctl.d/99-sysctl.conf ...
kernel.randomize_va_space = 1
* Applying /etc/sysctl.conf ...
kernel.randomize_va_space = 1
root@merge:/home/cyberpatriot# cat /proc/sys/net/ipv4/tcp_syncookies
1
root@merge:/home/cyberpatriot#
```

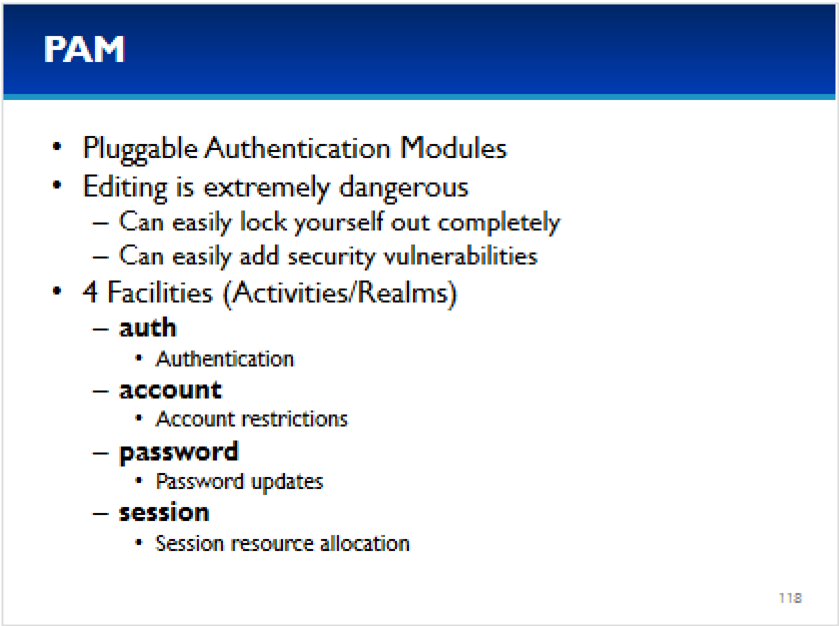
117

- Reload the **sysctl** settings again using the **sysctl --system** command.

☆Have the students run the commands on the screen.

- You can see that tcp_syncookies is set to 1 by **sysctl**, which tells the kernel to use TCP SYN cookies.

Slide 118



PAM

- Pluggable Authentication Modules
- Editing is extremely dangerous
  - Can easily lock yourself out completely
  - Can easily add security vulnerabilities
- 4 Facilities (Activities/Realms)
  - **auth**
    - Authentication
  - **account**
    - Account restrictions
  - **password**
    - Password updates
  - **session**
    - Session resource allocation

118

- PAM stands for Pluggable Authentication Modules, and is used for authentication by almost all Linux distributions.

  - The only notable Linux distribution that does not currently use PAM is Slackware.

- PAM is extremely complicated and any typo, no matter how small, can lock you out of your system permanently.

- It’s also very easy to accidentally make your computer less secure if you don’t know precisely what you are doing.

- Pam defines four facilities for managing four different activities (or realms).

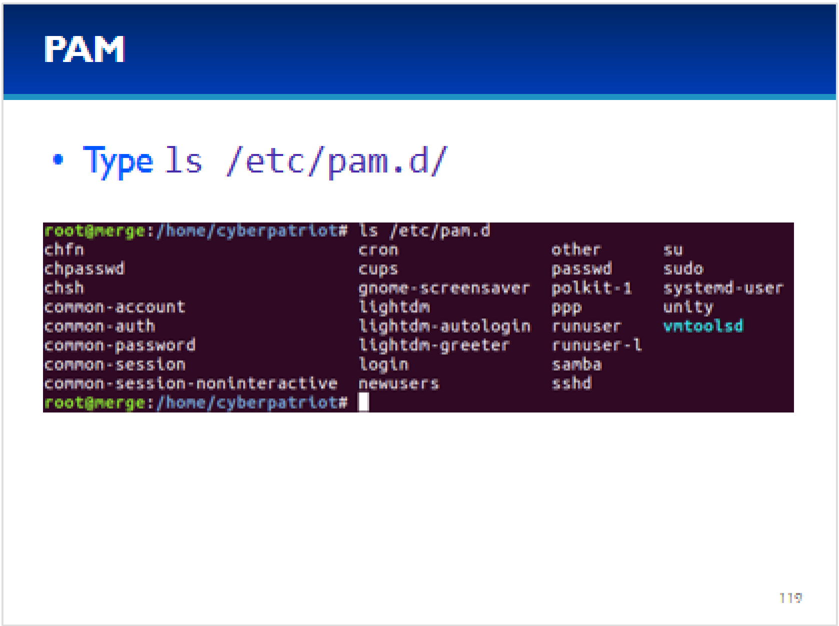
- The **auth** facility handles authentication.

- The **account** facility handles account restrictions, such as time of day a user is allowed to be logged in.

- The **password** facility handles password updates.

- And the **session** facility handles various session resources that need to be allocated when a user logs on.

Slide 119



PAM

- Type `ls /etc/pam.d/`

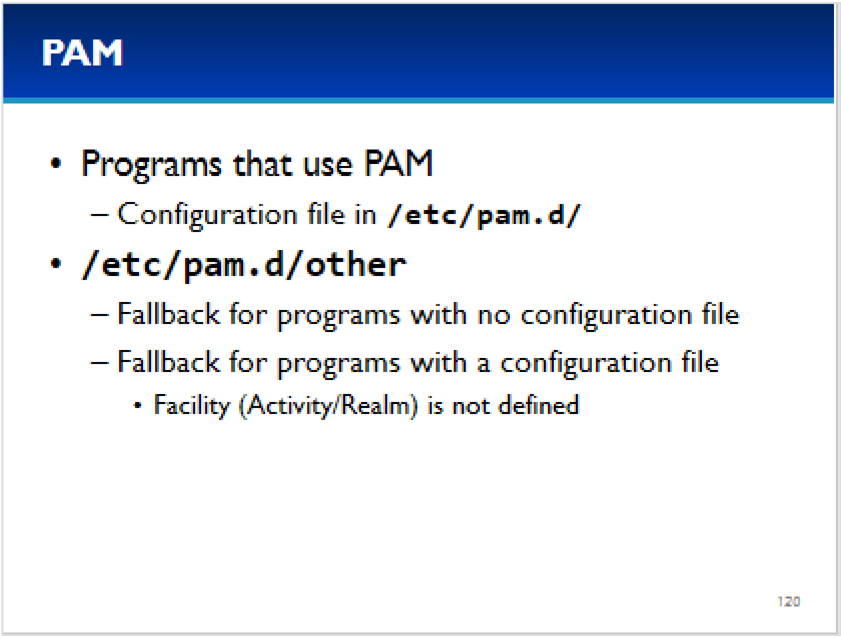
```
root@merge:/home/cyberpatriot# ls /etc/pam.d
chfn                           cron                  other      su
chpasswd                       cups                  passwd     sudo
chsh                           gnome-screensaver     polkit-1   systemd-user
common-account                 lightdm               ppp        unity
common-auth                    lightdm-autologin     runuser    vmtoolsd
common-password                lightdm-greeter       runuser-l
common-session                 login                 samba
common-session-noninteractive  newusers              sshd
root@merge:/home/cyberpatriot# 
```

119

- Before we go on, let’s look at the different PAM configuration files.

☆Have the students run the commands on the screen.

Slide 120



PAM

- Programs that use PAM
  - Configuration file in `/etc/pam.d/`
- `/etc/pam.d/other`
  - Fallback for programs with no configuration file
  - Fallback for programs with a configuration file
    - Facility (Activity/Realm) is not defined

120

- You probably recognize some of the file names in the pam.d directory as program names.

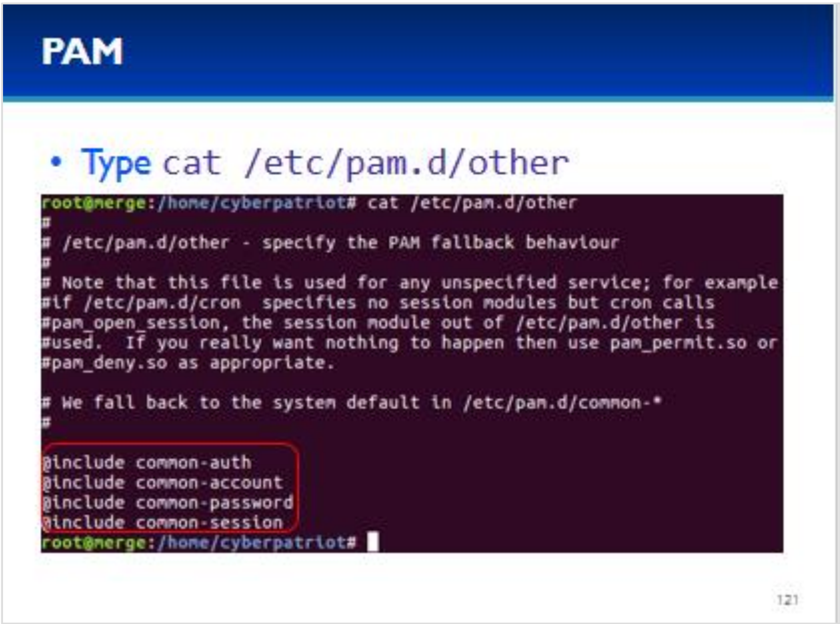
  - This is because every program that makes use of PAM, has its own configuration file in: /etc/pam.d/

- What if a program doesn't have a configuration file?

  - In that case, it uses the configuration file named other.

  - Other is also a fallback for programs that have a configuration file, but don't define the requested facility.

Slide 121



PAM

- Type cat /etc/pam.d/other

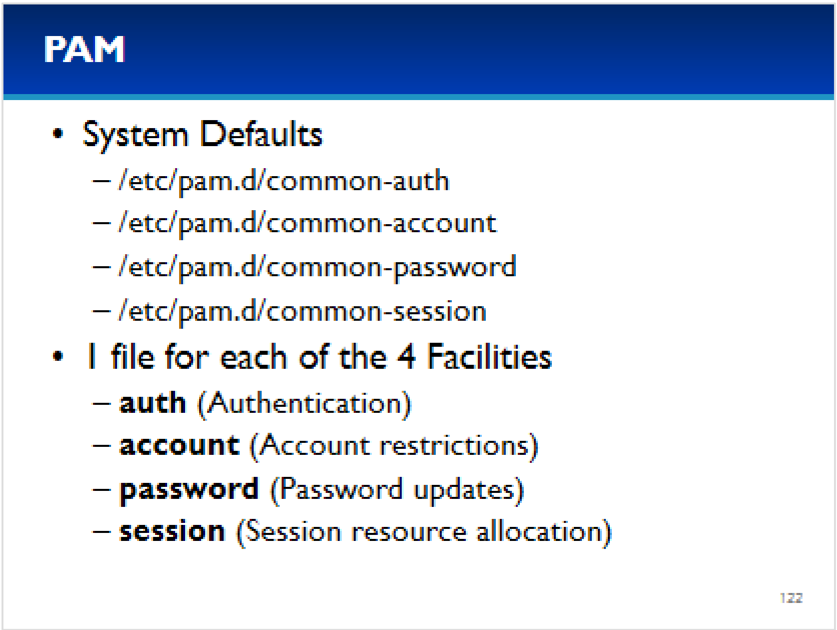
```
root@merge:/home/cyberpatriot# cat /etc/pam.d/other
#
# /etc/pam.d/other - specify the PAM fallback behaviour
#
# Note that this file is used for any unspecified service; for example
#if /etc/pam.d/cron  specifies no session modules but cron calls
#pam_open_session, the session module out of /etc/pam.d/other is
#used.  If you really want nothing to happen then use pam_permit.so or
#pam_deny.so as appropriate.

# We fall back to the system default in /etc/pam.d/common-*
#

@include common-auth
@include common-account
@include common-password
@include common-session
root@merge:/home/cyberpatriot# 
```

121

☆Have the students run the commands on the screen.

- Lines beginning with # are comments and are ignored.

Slide 122



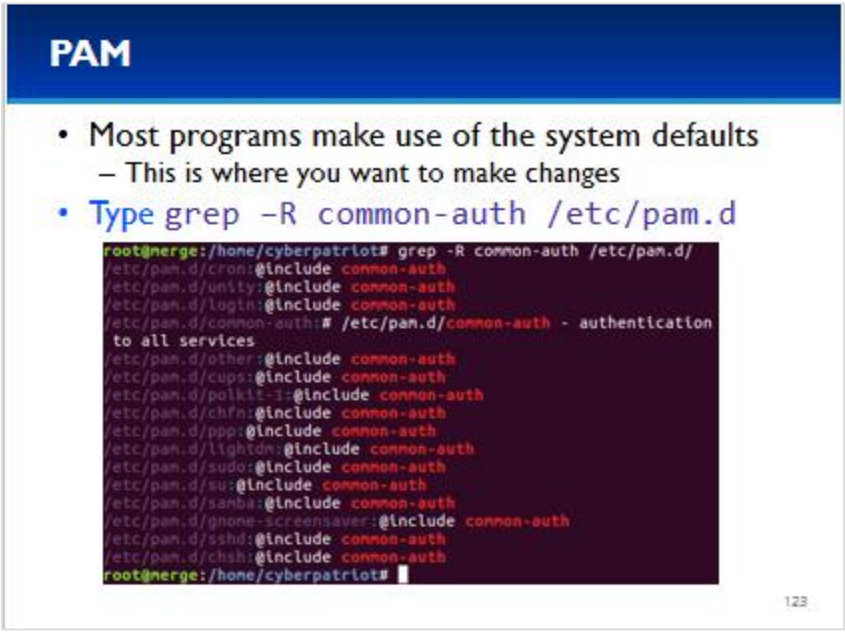
PAM

- System Defaults
  - /etc/pam.d/common-auth
  - /etc/pam.d/common-account
  - /etc/pam.d/common-password
  - /etc/pam.d/common-session
- 1 file for each of the 4 Facilities
  - **auth** (Authentication)
  - **account** (Account restrictions)
  - **password** (Password updates)
  - **session** (Session resource allocation)

122

- Looking at the “other” PAM configuration file, you can see that it includes four different configuration files, one for each facility.

Slide 123



PAM

- Most programs make use of the system defaults
  - This is where you want to make changes
- Type `grep -R common-auth /etc/pam.d`

```
root@merge:/home/cyberpatriot# grep -R common-auth /etc/pam.d/
/etc/pam.d/cron:@include common-auth
/etc/pam.d/unity:@include common-auth
/etc/pam.d/login:@include common-auth
/etc/pam.d/common-auth:# /etc/pam.d/common-auth - authentication
 to all services
/etc/pam.d/other:@include common-auth
/etc/pam.d/cups:@include common-auth
/etc/pam.d/polkit-1:@include common-auth
/etc/pam.d/chfn:@include common-auth
/etc/pam.d/ppp:@include common-auth
/etc/pam.d/lightdm:@include common-auth
/etc/pam.d/sudo:@include common-auth
/etc/pam.d/su:@include common-auth
/etc/pam.d/samba:@include common-auth
/etc/pam.d/gnome-screensaver:@include common-auth
/etc/pam.d/sshd:@include common-auth
/etc/pam.d/chsh:@include common-auth
root@merge:/home/cyberpatriot# 
```

123

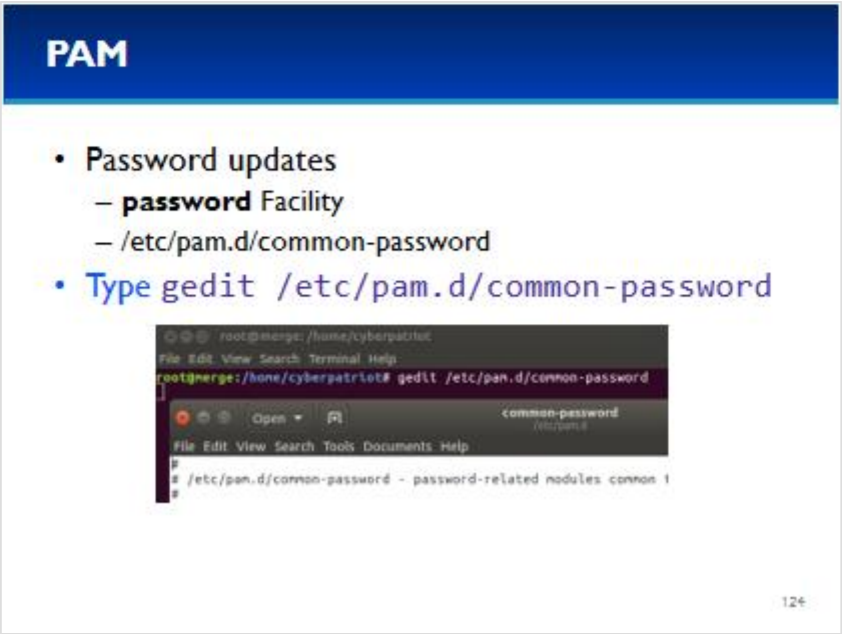
- These included files aren't just used by programs without a configuration file.

- In fact, these included files are also used by most programs in their configuration files.

☆Have the students run the commands on the screen.

- You can see that common-auth appears in many configuration files including **sudo**, **su**, and **sshd.**

Slide 124



PAM

- Password updates
  - **password** Facility
  - /etc/pam.d/common-password
- Type `gedit /etc/pam.d/common-password`

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help

```
root@merge:/home/cyberpatriot# gedit /etc/pam.d/common-password
```

Open
common-password
/etc/pam.d
File Edit View Search Tools Documents Help

```
#
# /etc/pam.d/common-password - password-related modules common t
#
```

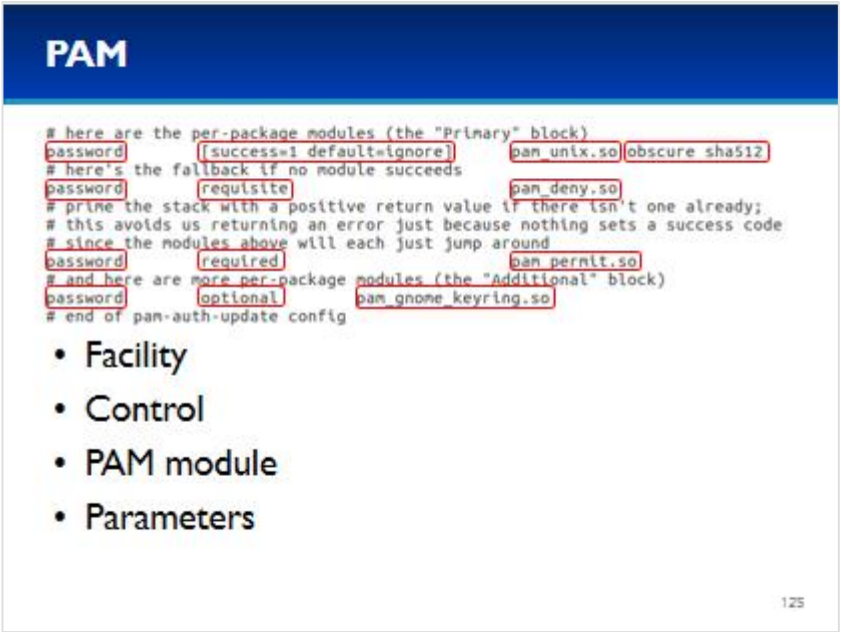
124

- Password updates are performed by the password facility.
- To see how password updates are handled, open the common-password file.

☆Have the students run the commands on the screen.

- Be careful not to make any changes to this file unless directed to.

Slide 125



PAM

```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

- Facility
- Control
- PAM module
- Parameters

125

- Again, all the lines beginning with # are comments and are ignored.

- The first column is the facility; this defines the facility that the rule applies to.

Click to reveal Control.

- The second column is the control. Control determines what to do based on the return value of the PAM module.

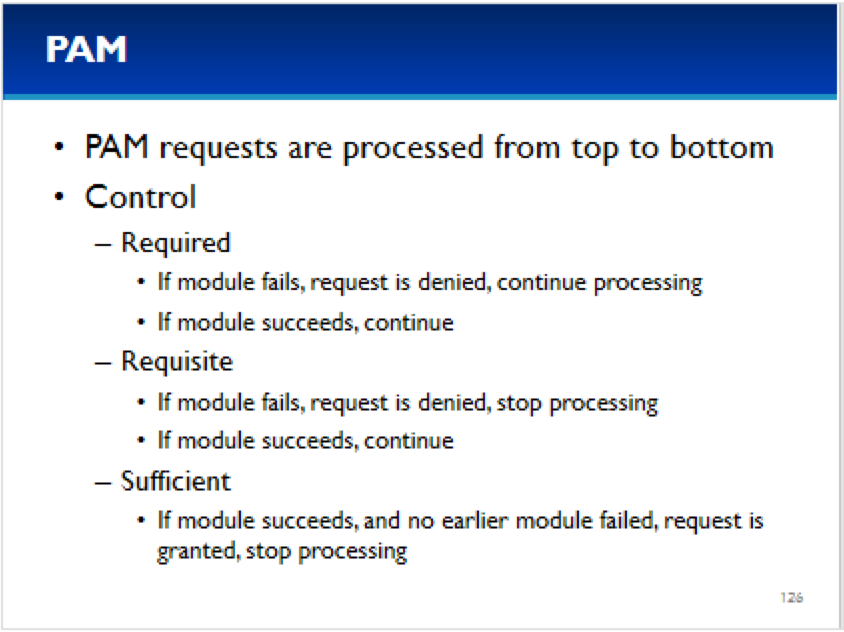
Click to reveal PAM module.

- The PAM module is the shared object (.so) file that executes code.

Click to reveal Parameters.

- The last column, if it exists, specifies parameters to pass to the PAM module.

Slide 126



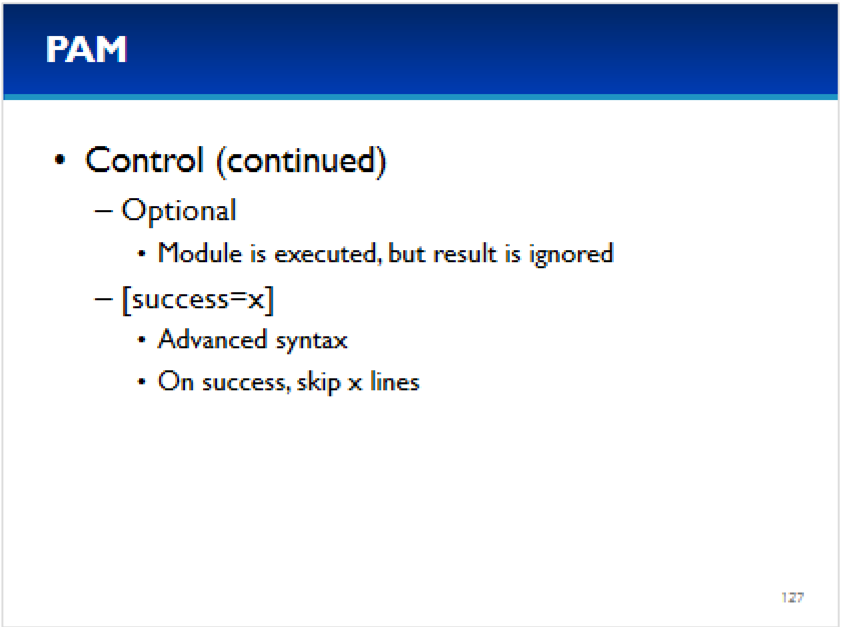
PAM

- PAM requests are processed from top to bottom
- Control
  - Required
    - If module fails, request is denied, continue processing
    - If module succeeds, continue
  - Requisite
    - If module fails, request is denied, stop processing
    - If module succeeds, continue
  - Sufficient
    - If module succeeds, and no earlier module failed, request is granted, stop processing

126

- PAM requests are processed from top to bottom in their respective configuration files.
- The Control column may have different values, and we will cover the five main ones
- If control is set to required, and the PAM module returns “failure,” then the request will ultimately be denied, but the request is allowed to continue processing in case more work needs to be done.
- If control is set to requisite, and the PAM module returns “failure,” then the request is immediately denied and stops processing.
- If control is set to sufficient and the module succeeds, and no earlier module failed, then the request is granted and immediately stops processing.

Slide 127



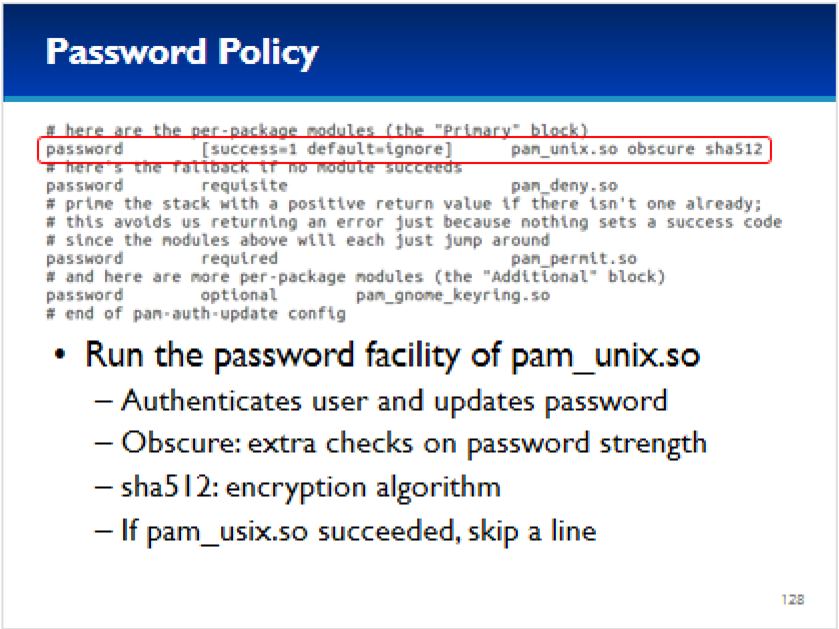
PAM

- Control (continued)
  - Optional
    - Module is executed, but result is ignored
  - [success=x]
    - Advanced syntax
    - On success, skip x lines

127

- If control is set to option, then the module is executed, but the return value is ignore.
- If control is surrounded by square brackets [], then this is the advanced syntax, and it is commonly used to tell PAM to skip x number of lines when the module returns success.

Slide 128



Password Policy

```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

- Run the password facility of pam_unix.so
  - Authenticates user and updates password
  - Obscure: extra checks on password strength
  - sha512: encryption algorithm
  - If pam_usix.so succeeded, skip a line

128

- Let’s go through the password policy PAM file line by line.

- The first line runs the password facility of pam_unix.so.

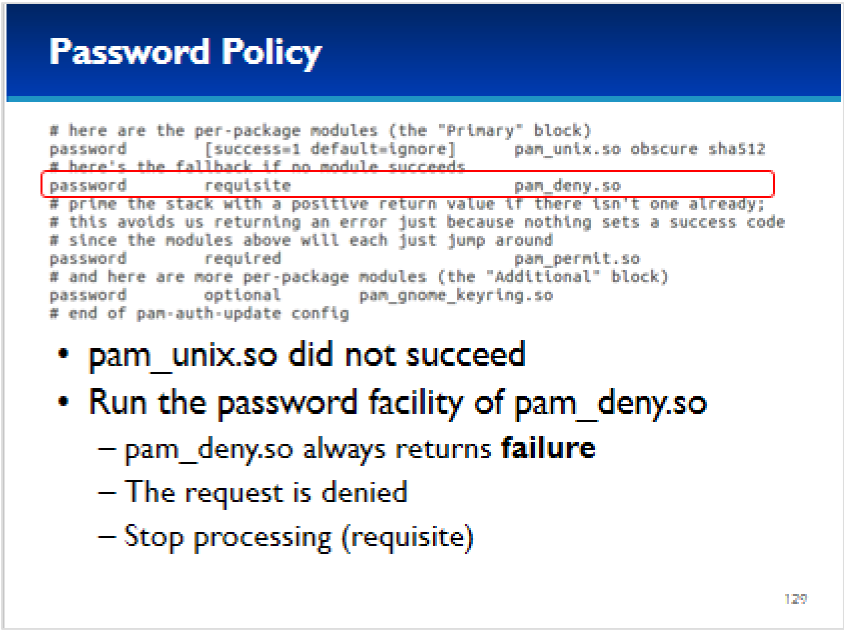
  - Authenticates user by asking for their current password, and asks them enter a new password.

  - The obscure option tells pam_unix to apply some additional checks to improve the password strength.

  - The sha512 option specifies the encryption (or hash) algorithm used to encrypt passwords

- The control of success=1 specifies, that if pam_unix succeeds, then skip the next (1) line

Slide 129



Password Policy

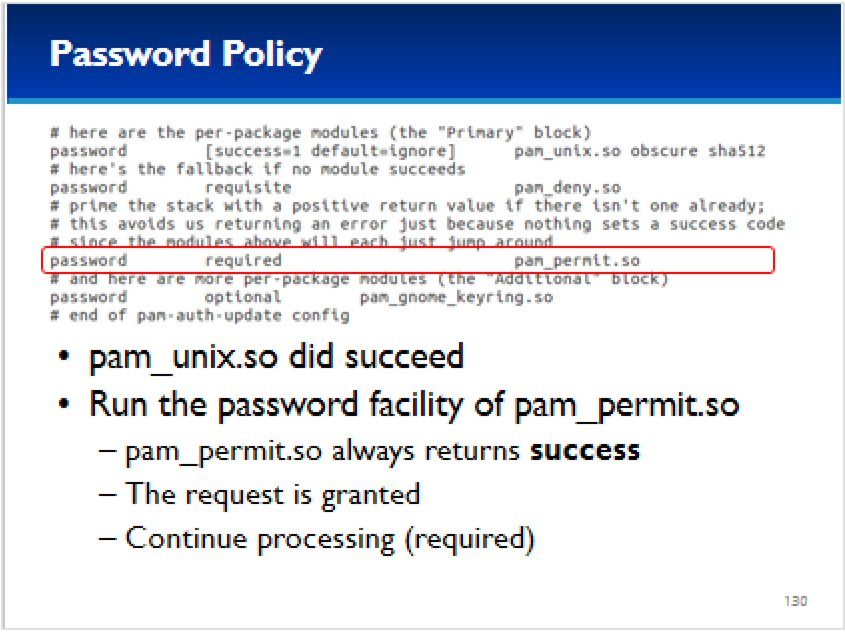
```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

- pam_unix.so did not succeed
- Run the password facility of pam_deny.so
  - pam_deny.so always returns **failure**
  - The request is denied
  - Stop processing (requisite)

129

- This line skipped if pam_unix succeded.
- Therefore, we know if this line is executed, then pam_unix failed.
- Pam_deny always returns failure.
- Since the control is set to requisite, the request is immediately denied, and processing immediately stops.

Slide 130



Password Policy

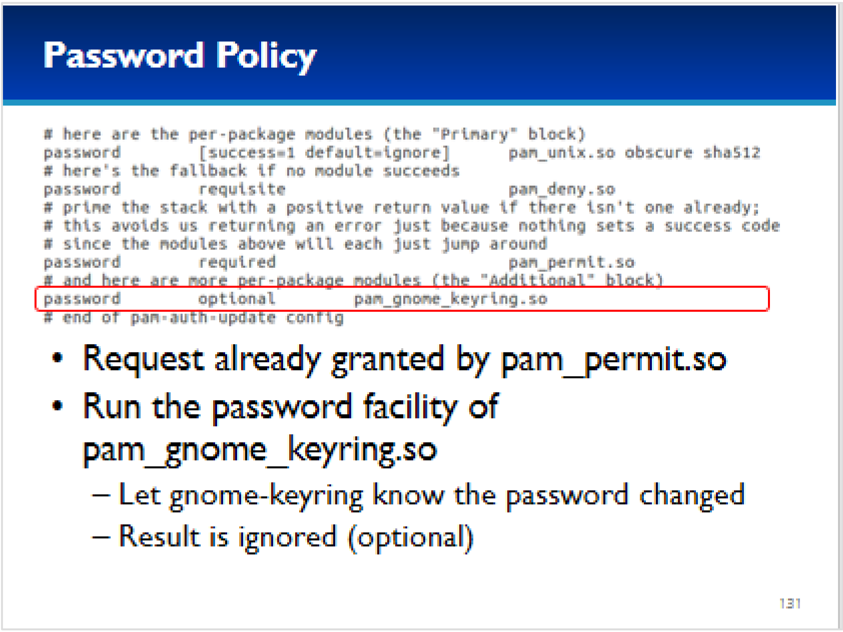
```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

- pam_unix.so did succeed
- Run the password facility of pam_permit.so
  - pam_permit.so always returns **success**
  - The request is granted
  - Continue processing (required)

130

- If we get to this line, then we know that pam_unix succeeded, since the line above this (pam_deny) stops processing.
- This line runs the password facility of the pam_permit module, which always returns success.
- Since the control is listed as required the request will eventually be granted, but we continue processing in case more work needs to be done.

Slide 131



Password Policy

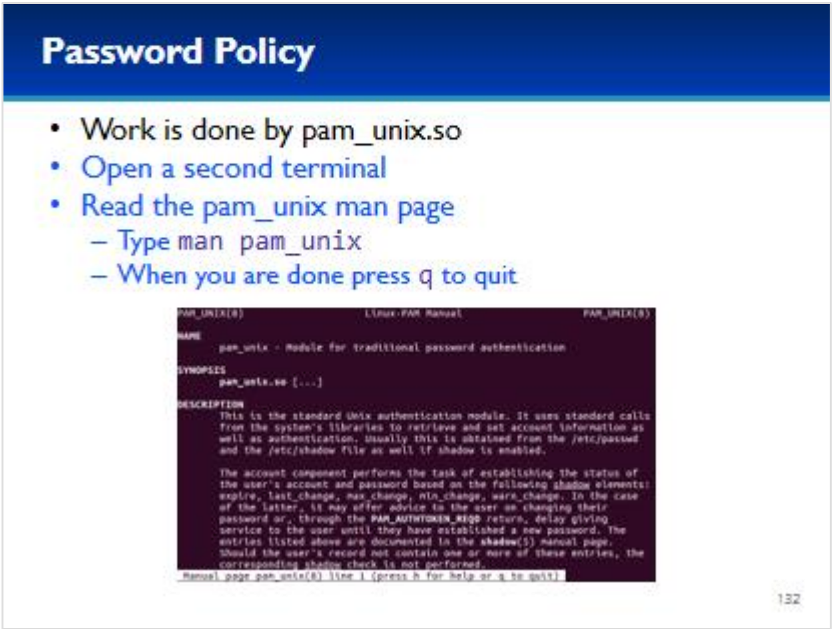
```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

- Request already granted by pam_permit.so
- Run the password facility of pam_gnome_keyring.so
  - Let gnome-keyring know the password changed
  - Result is ignored (optional)

131

- The last line uses a control of optional, which means the return of pam_gnome_keyring module is ignored.
- The purpose of this line is to notify the GNOME keyring that a password has been updated.

Slide 132



Password Policy

- Work is done by pam_unix.so
- Open a second terminal
- Read the pam_unix man page
  - Type `man pam_unix`
  - When you are done press q to quit

```
PAM_UNIX(8)                    Linux-PAM Manual                    PAM_UNIX(8)

NAME
       pam_unix - Module for traditional password authentication

SYNOPSIS
       pam_unix.so [...]

DESCRIPTION
       This is the standard Unix authentication module. It uses standard calls
       from the system's libraries to retrieve and set account information as
       well as authentication. Usually this is obtained from the /etc/passwd
       and the /etc/shadow file as well if shadow is enabled.

       The account component performs the task of establishing the status of
       the user's account and password based on the following shadow elements:
       expire, last_change, max_change, min_change, warn_change. In the case
       of the latter, it may offer advice to the user on changing their
       password or, through the PAM_AUTHTOKEN_REQD return, delay giving
       service to the user until they have established a new password. The
       entries listed above are documented in the shadow(5) manual page.
       Should the user's record not contain one or more of these entries, the
       corresponding shadow check is not performed.
 Manual page pam_unix(8) line 1 (press h for help or q to quit)
```

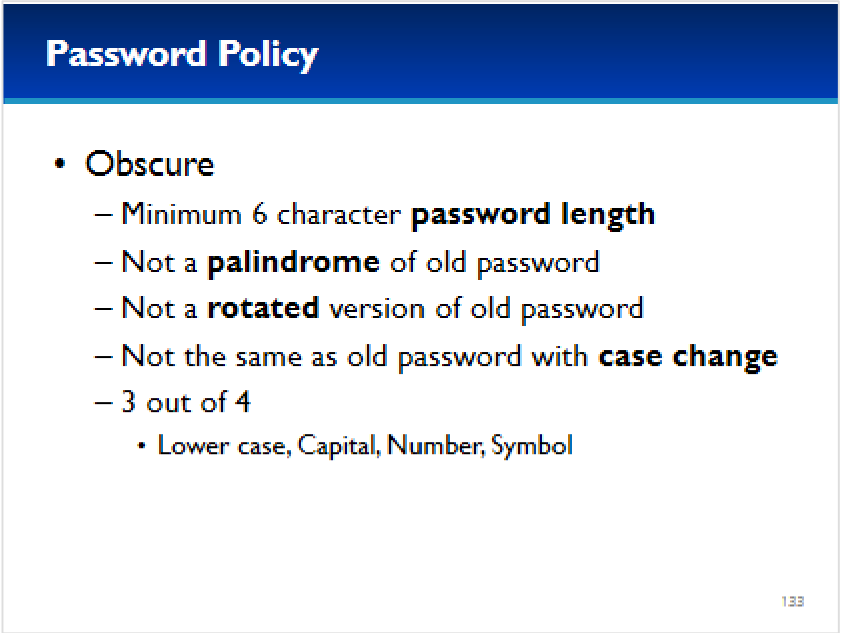
132

- As you can see, the majority of the work in common-password is done by the pam_unix module.

- In order to learn more about the pam_unix module.

☆Have the students run the commands on the screen.

Slide 133



Password Policy

- Obscure
  - Minimum 6 character **password length**
  - Not a **palindrome** of old password
  - Not a **rotated** version of old password
  - Not the same as old password with **case change**
  - 3 out of 4
    - Lower case, Capital, Number, Symbol

133

- The man page states that **obscure** enables some extra checks on password strength, which ensure that the password:

  - Is at least six characters in length.

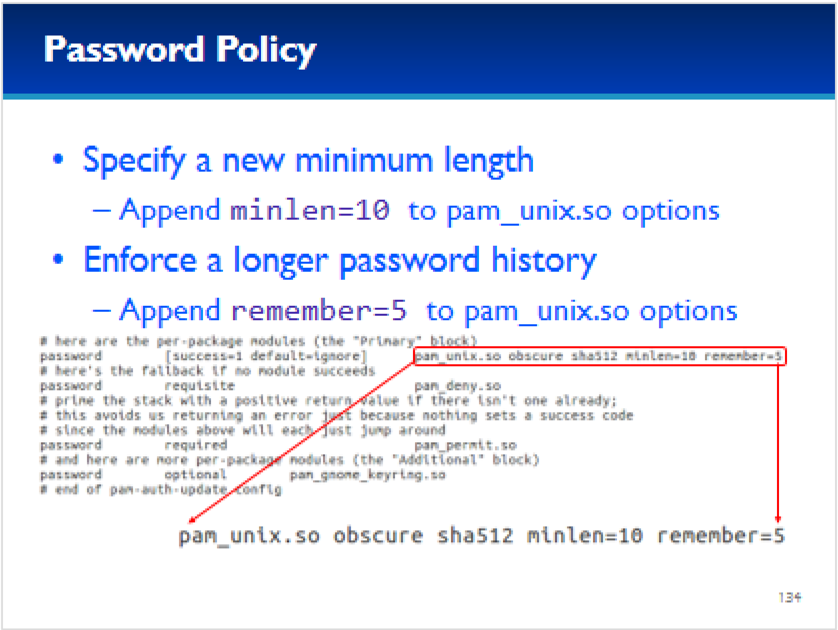
  - Is not a palindrome (or reversal) of the old password.

  - Is not a rotated version of the old password.

  - Is not just a case change of the previous password.

  - Has at least three of four of the following character types: lower-case, upper-case, number, and symbol.

Slide 134



Password Policy

- Specify a new minimum length
  - Append minlen=10 to pam_unix.so options
- Enforce a longer password history
  - Append remember=5 to pam_unix.so options

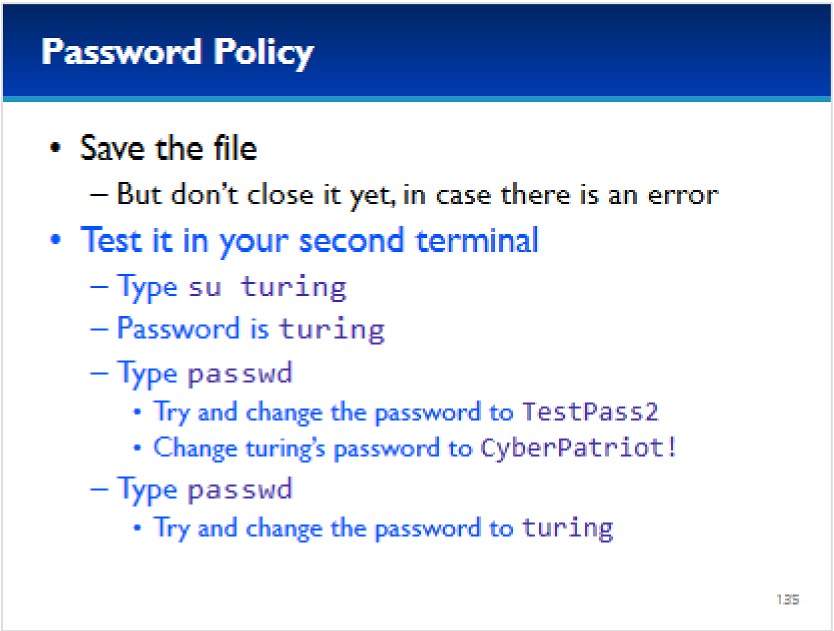
```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512 minlen=10 remember=5
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

```
pam_unix.so obscure sha512 minlen=10 remember=5
```

134

- Don’t close **gedit** until you are instructed to.
- A minimum password length of six isn’t very good, let’s change it to 10.
  - Append **minlen=10** to the pam_unix option.
- There is currently no password history being enforced, let’s institute one now.
  - Append **remember=5** to the pam_unix option.

Slide 135



Password Policy

- Save the file
  - But don't close it yet, in case there is an error
- Test it in your second terminal
  - Type `su turing`
  - Password is `turing`
  - Type `passwd`
    - Try and change the password to `TestPass2`
    - Change turing's password to `CyberPatriot!`
  - Type `passwd`
    - Try and change the password to `turing`

135

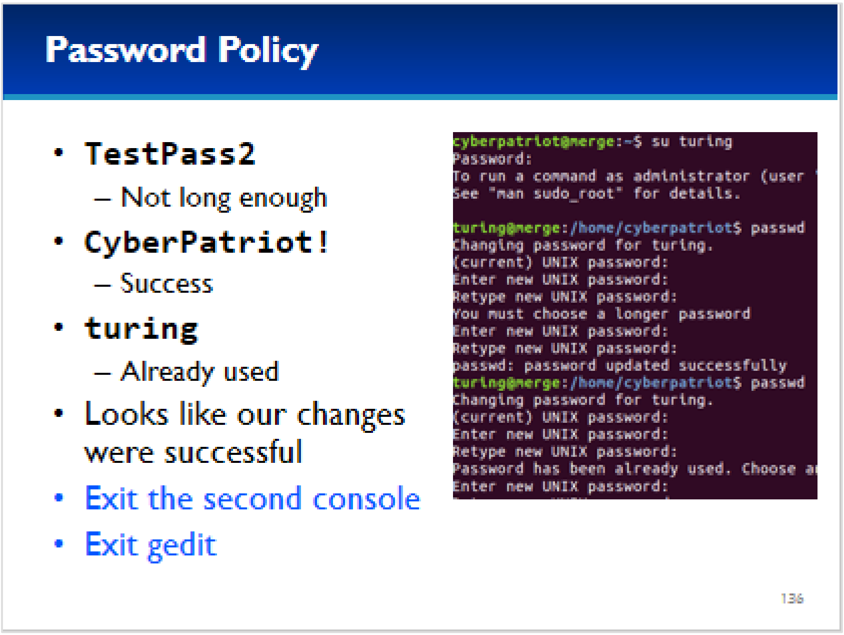
- Now save the file, but don't close **gedit** yet.

  - We need to test it first to make sure there is not an error.

  - Testing it before we close the file will ensure we don't lock ourselves out.

☆Have the students run the commands on the screen.

Slide 136



Password Policy

- TestPass2
  - Not long enough
- CyberPatriot!
  - Success
- turing
  - Already used
- Looks like our changes were successful
- Exit the second console
- Exit gedit

```
cyberpatriot@merge:~$ su turing
Password:
To run a command as administrator (user "
See "man sudo_root" for details.

turing@merge:/home/cyberpatriot$ passwd
Changing password for turing.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
You must choose a longer password
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
turing@merge:/home/cyberpatriot$ passwd
Changing password for turing.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
Password has been already used. Choose a
Enter new UNIX password:
```

136

- As you can see, **passwd** wouldn't let us change our password to TesPass2 because it is not long enough.

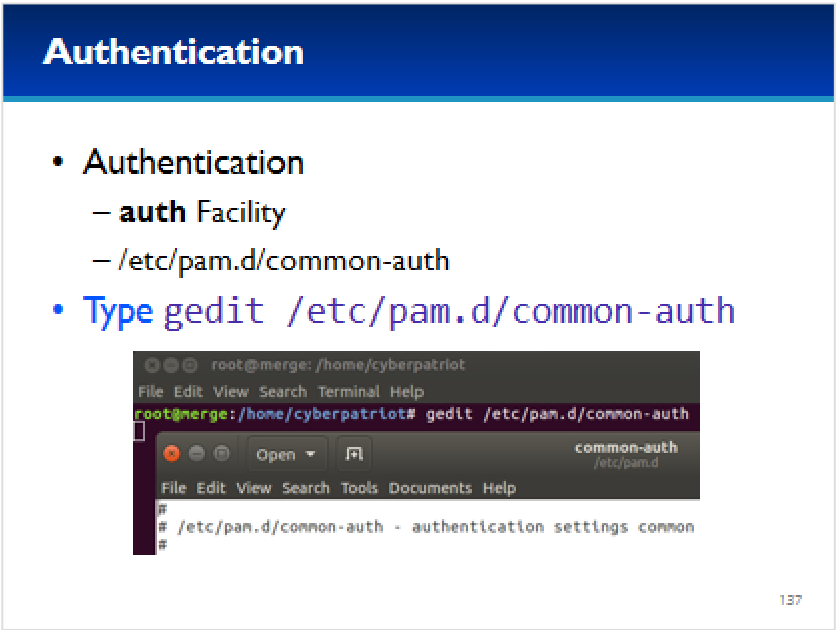
- However, the password CyberPatriot! was acceptable.

- Trying to change turing's password back to turing results in the request denial because a password history is being enforced.

- Close the second terminal instance.

- It's also now safe to exit **gedit**.

Slide 137



Authentication

- Authentication
  - **auth** Facility
  - /etc/pam.d/common-auth
- Type `gedit /etc/pam.d/common-auth`

```
root@merge:/home/cyberpatriot# gedit /etc/pam.d/common-auth
```

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help
Open
common-auth
/etc/pam.d
File Edit View Search Tools Documents Help

```
#
# /etc/pam.d/common-auth - authentication settings common
#
```

137

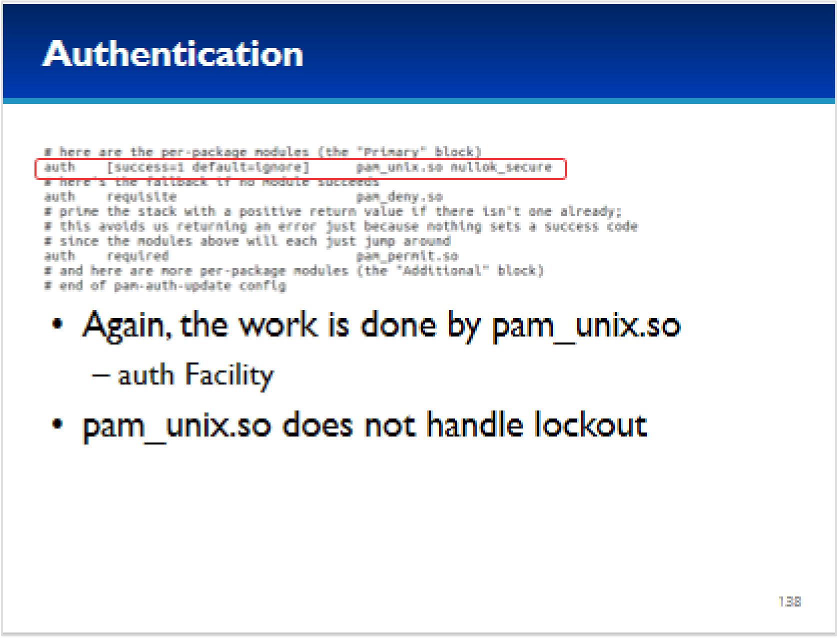
- Authentication is handled by the auth facility.

- The default configuration for this facility is in the common-auth file.

- Open the common-auth file with **gedit**.

☆Have the students run the commands on the screen.

Slide 138



Authentication

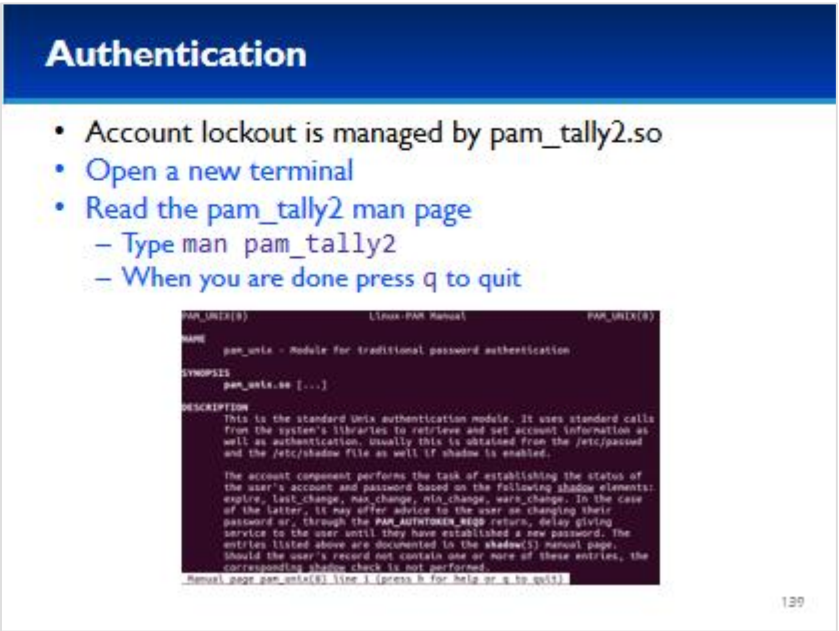
```
# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

- Again, the work is done by pam_unix.so
  - auth Facility
- pam_unix.so does not handle lockout

138

- In common-auth you can see that all of the work is again done by using the auth facility of the the pam_unix module.
- However, the pam_unix module is not capable of handling account lockout functions.

Slide 139



Authentication

- Account lockout is managed by pam_tally2.so
- Open a new terminal
- Read the pam_tally2 man page
  - Type `man pam_tally2`
  - When you are done press q to quit

```
PAM_UNIX(8)                    Linux-PAM Manual                    PAM_UNIX(8)

NAME
       pam_unix - Module for traditional password authentication

SYNOPSIS
       pam_unix.so [...]

DESCRIPTION
       This is the standard Unix authentication module. It uses standard calls
       from the system's libraries to retrieve and set account information as
       well as authentication. Usually this is obtained from the /etc/passwd
       and the /etc/shadow file as well if shadow is enabled.

       The account component performs the task of establishing the status of
       the user's account and password based on the following shadow elements:
       expire, last_change, max_change, min_change, warn_change. In the case
       of the latter, it may offer advice to the user on changing their
       password or, through the PAM_AUTHTOKEN_REQD return, delay giving
       service to the user until they have established a new password. The
       entries listed above are documented in the shadow(5) manual page.
       Should the user's record not contain one or more of these entries, the
       corresponding shadow check is not performed.
 Manual page pam_unix(8) line 1 (press h for help or q to quit)
```

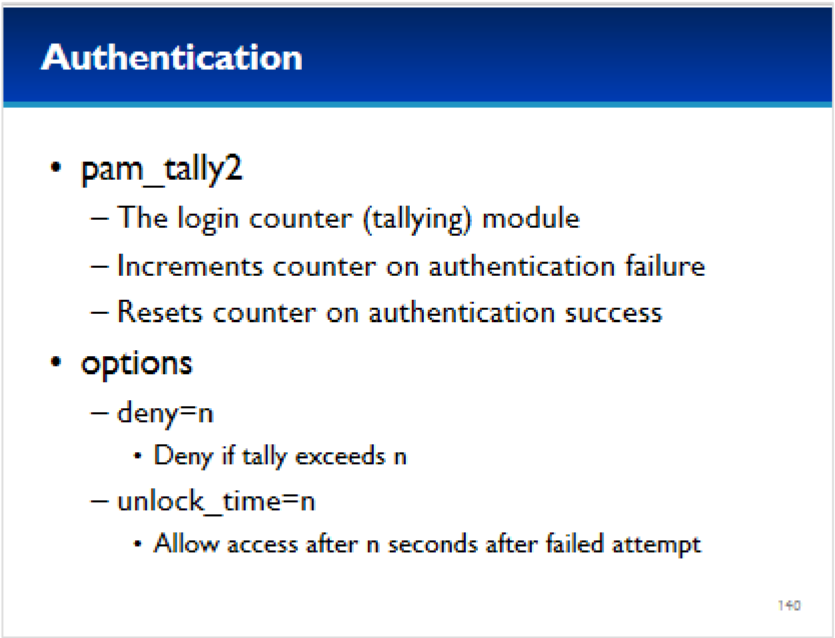
139

- In order to handle account lockout functionality we are going to use the pam_tally2 module.

- First, read the manual page of pam_tally2.

☆Have the students run the commands on the screen.

Slide 140



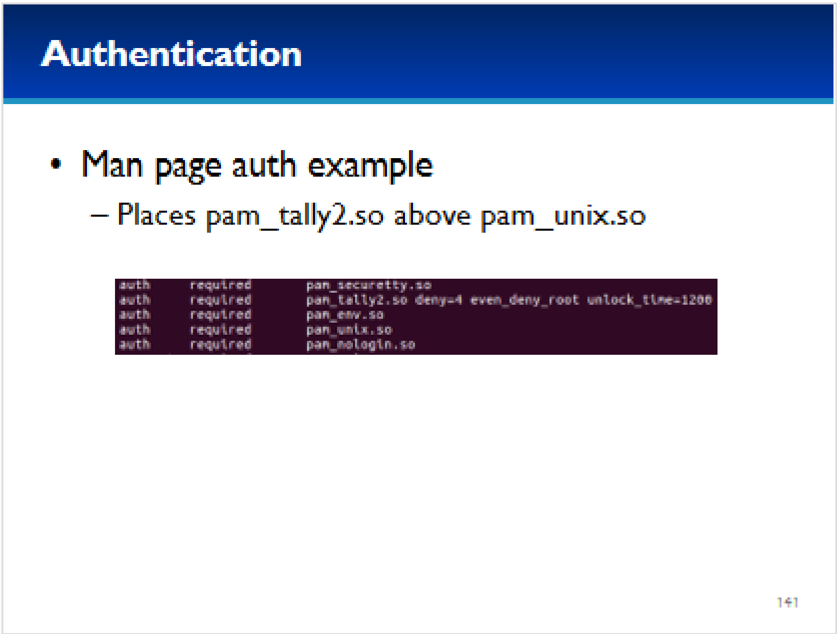
Authentication

- pam_tally2
  - The login counter (tallying) module
  - Increments counter on authentication failure
  - Resets counter on authentication success
- options
  - deny=n
    - Deny if tally exceeds n
  - unlock_time=n
    - Allow access after n seconds after failed attempt

140

- Pam_tally2 is described as a login counter module.
- When a request is denied, the counter is incremented.
- When a request is granted, the counter is reset to 0.
- Looking at the pam_tally2 manual, there are also some important options.
- The deny option will automatically deny the authentication request if the counter exceeds n.
- The unlock time option will allow a single additional authentication attempt after a specified number of seconds.

Slide 141



Authentication

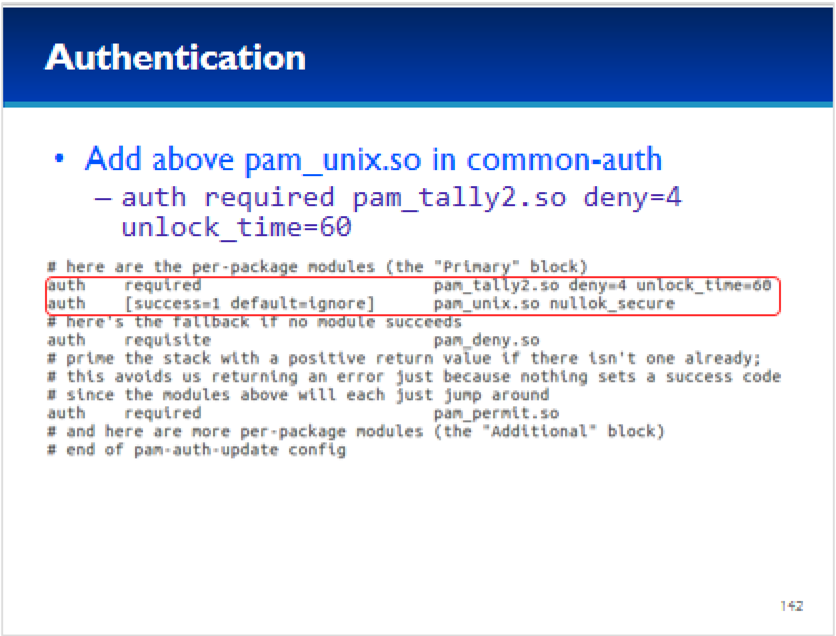
- Man page auth example
  - Places pam_tally2.so above pam_unix.so

```
auth      required      pam_securetty.so
auth      required      pam_tally2.so deny=4 even_deny_root unlock_time=1200
auth      required      pam_env.so
auth      required      pam_unix.so
auth      required      pam_nologin.so
```

141

- Further down on the pam_tally2 manual page, it shows an example implementation which places pam_tally2 module above the pam_unix module.

Slide 142



Authentication

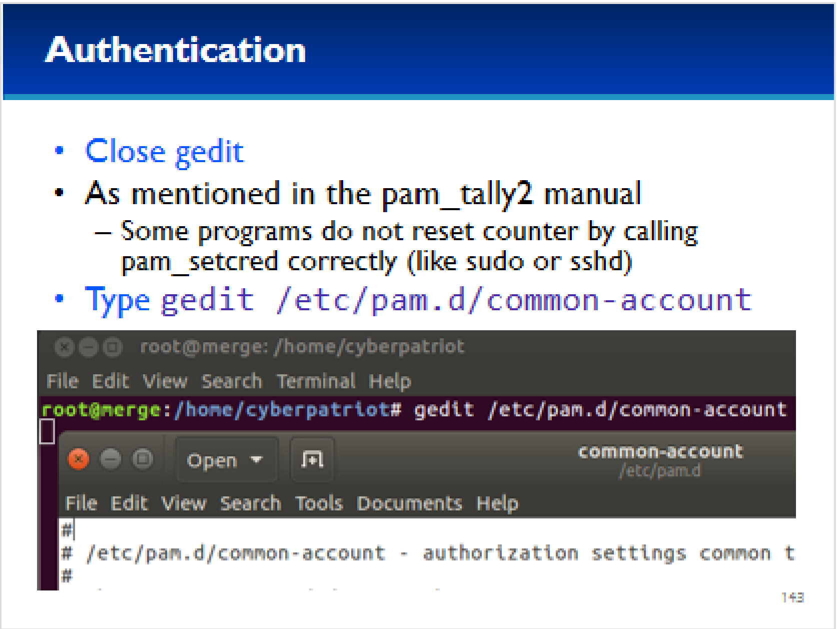
- Add above pam_unix.so in common-auth
  - auth required pam_tally2.so deny=4 unlock_time=60

```
# here are the per-package modules (the "Primary" block)
auth    required                        pam_tally2.so deny=4 unlock_time=60
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

142

- Add the pam_tally2 module directly above the pam_unix module.
  - Using the auth facility.
  - And a control of: required
- A deny value of four is a little low, but it will allow us to test our configuration more easily.
- An unlock_time of 60 is generally acceptable since it will only allow 1 additional logon attempt every minute, but a more secure value would be a little higher.

Slide 143



Authentication

- Close gedit
- As mentioned in the pam_tally2 manual
  - Some programs do not reset counter by calling pam_setcred correctly (like sudo or sshd)
- Type `gedit /etc/pam.d/common-account`

root@merge: /home/cyberpatriot
File Edit View Search Terminal Help

```
root@merge:/home/cyberpatriot# gedit /etc/pam.d/common-account
```

Open
common-account
/etc/pam.d
File Edit View Search Tools Documents Help

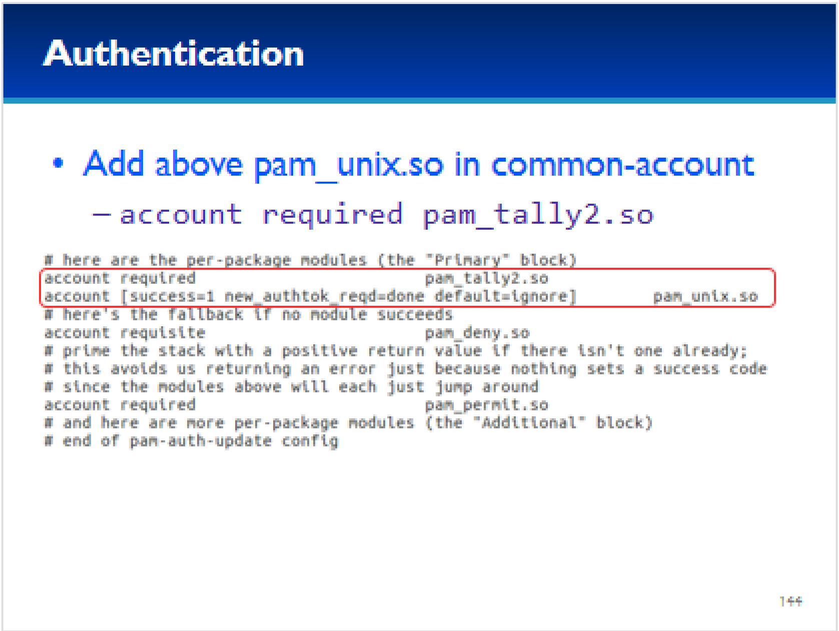
```
#
# /etc/pam.d/common-account - authorization settings common t
#
```

143

- Unfortunately, as mentioned in the pam_tally2 module, some programs do not call pam_setcred correctly, thus resetting the lockout counter.
  - Some of these programs include **sudo** and **sshd**.
- In order to prevent these programs from locking you out, we have to edit the common-account file.

☆Have the students run the commands on the screen.

Slide 144



Authentication

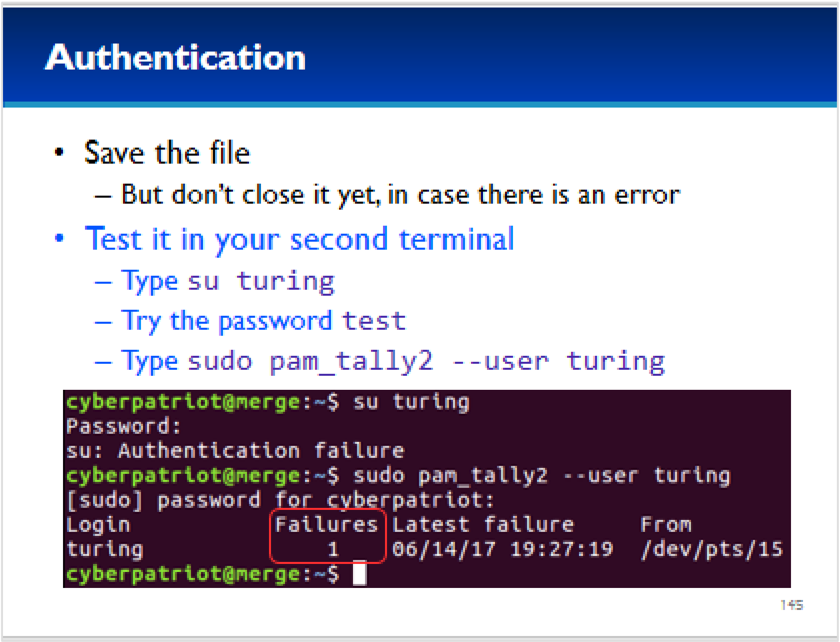
- Add above pam_unix.so in common-account
  - account required pam_tally2.so

```
# here are the per-package modules (the "Primary" block)
account required                         pam_tally2.so
account [success=1 new_authtok_reqd=done default=ignore]        pam_unix.so
# here's the fallback if no module succeeds
account requisite                        pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
account required                         pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

144

- Add the pam_tally2 module directly above the pam_unix module.
  - Using the account facility and a control of required.
- No options are necessary this time.
- This will ensure the lockout counter is reset after a successful authentication.

Slide 145



Authentication

- Save the file
  - But don’t close it yet, in case there is an error
- Test it in your second terminal
  - Type `su turing`
  - Try the password `test`
  - Type `sudo pam_tally2 --user turing`

```
cyberpatriot@merge:~$ su turing
Password:
su: Authentication failure
cyberpatriot@merge:~$ sudo pam_tally2 --user turing
[sudo] password for cyberpatriot:
Login           Failures Latest failure     From
turing              1    06/14/17 19:27:19  /dev/pts/15
cyberpatriot@merge:~$ 
```

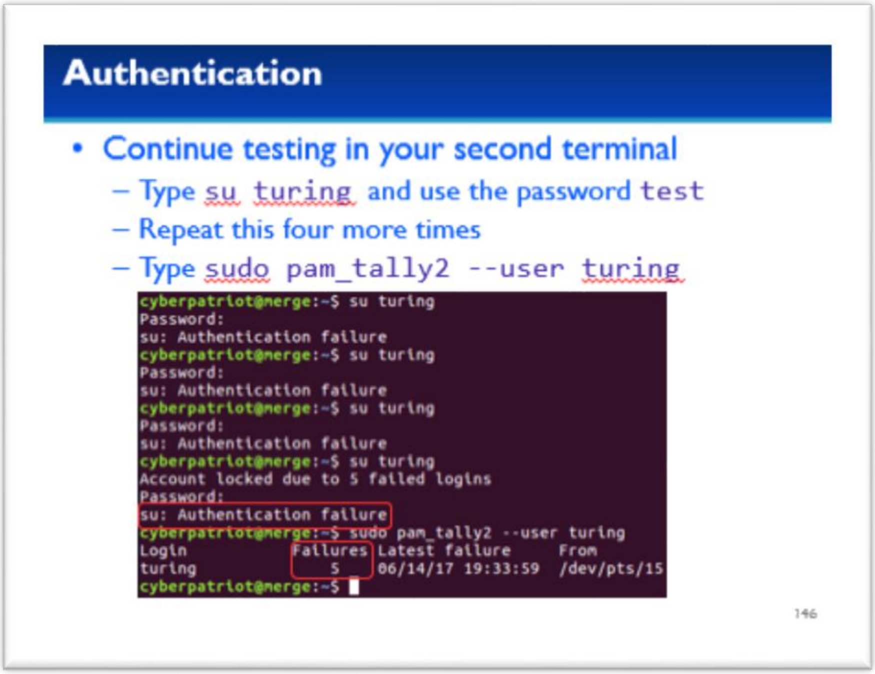
145

- Save the file in **gedit**, but don’t close it in case there is an error.

☆Have the students run the commands on the screen.

- The **pam_tally2** command tells us that the user turing has 1 failed login.

Slide 146



Authentication

- Continue testing in your second terminal
  - Type su turing and use the password test
  - Repeat this four more times
  - Type sudo pam_tally2 --user turing

```
cyberpatriot@merge:~$ su turing
Password:
su: Authentication failure
cyberpatriot@merge:~$ su turing
Password:
su: Authentication failure
cyberpatriot@merge:~$ su turing
Password:
su: Authentication failure
cyberpatriot@merge:~$ su turing
Account locked due to 5 failed logins
Password:
su: Authentication failure
cyberpatriot@merge:~$ sudo pam_tally2 --user turing
Login           Failures Latest failure     From
turing              5    06/14/17 19:33:59  /dev/pts/15
cyberpatriot@merge:~$
```

146

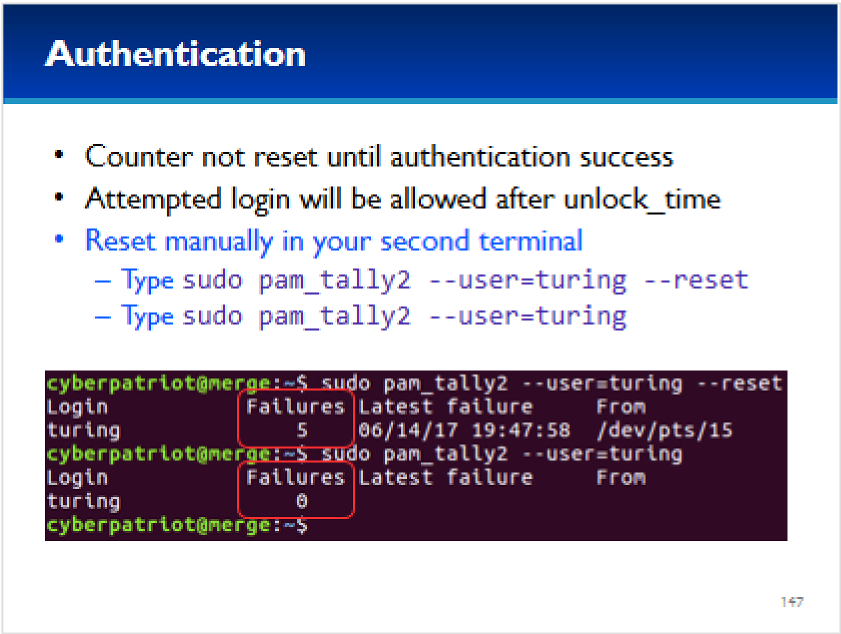
- Go ahead and fail authentication four more times.

☆Have the students run the commands on the screen.

- Your last authentication attempt should give you an account lockout warning message.

- The **pam_tally2** command now shows that we have five failed login attempts.

Slide 147



Authentication

- Counter not reset until authentication success
- Attempted login will be allowed after unlock_time
- Reset manually in your second terminal
  - Type `sudo pam_tally2 --user=turing --reset`
  - Type `sudo pam_tally2 --user=turing`

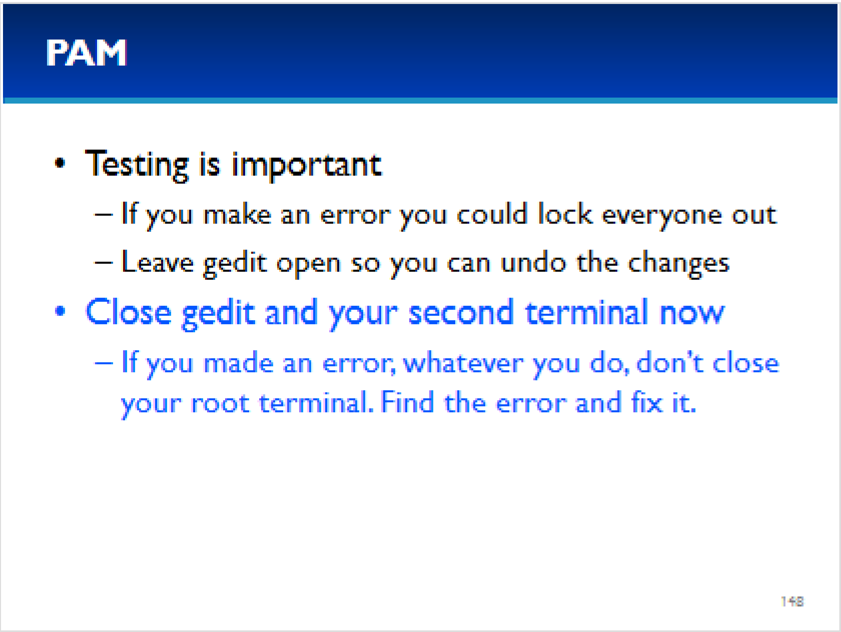
```
cyberpatriot@merge:~$ sudo pam_tally2 --user=turing --reset
Login           Failures Latest failure     From
turing              5    06/14/17 19:47:58  /dev/pts/15
cyberpatriot@merge:~$ sudo pam_tally2 --user=turing
Login           Failures Latest failure     From
turing              0
cyberpatriot@merge:~$
```

147

- The counter will not be reset for that user until a successful authentication, but a single authentication attempt will be allowed after unlock_time.

- You can manually reset the account lockout counters (as root) with the **pam_tally2** module.

Slide 148



PAM

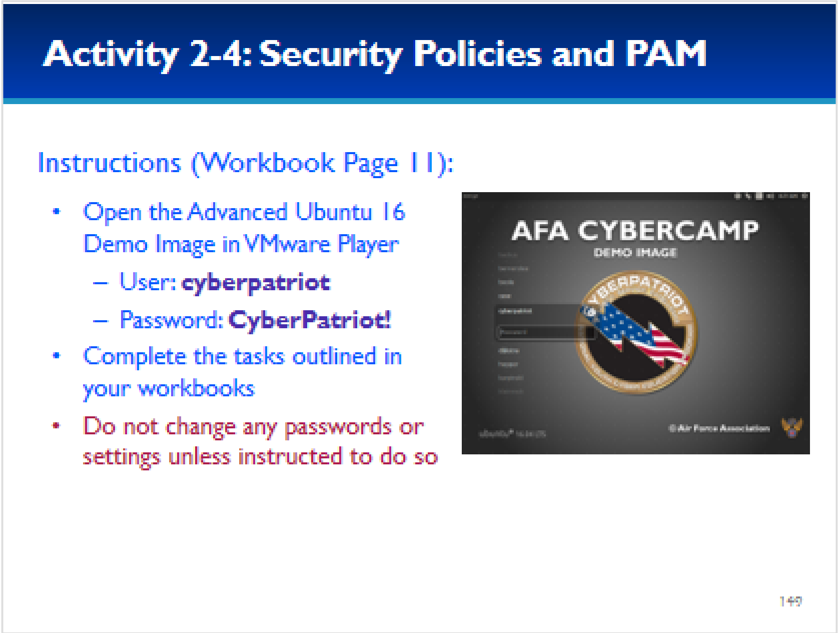
- Testing is important
  - If you make an error you could lock everyone out
  - Leave gedit open so you can undo the changes
- Close gedit and your second terminal now
  - If you made an error, whatever you do, don't close your root terminal. Find the error and fix it.

148

- It is extremely important that you always test your changes before closing your editor. That way, if you made an error, you can quickly undo all the changes you made and easily restore your system to a working state.

- It looks like we didn't break anything so go ahead and close gedit and your second terminal now.

Slide 149



AFA CYBERCAMP
DEMO IMAGE
CYBERPATRIOT
©Air Force Association

Activity 2-4: Security Policies and PAM

Instructions (Workbook Page 11):

- Open the Advanced Ubuntu 16 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

149

🕒 Give students about 20 minutes to complete the tasks listed on page 11 of their workbooks.

☆This lab will review security policies and PAM.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. 1
2. /etc/sysctl.conf
3. -
4. 4.4.0-21-generic
5. /etc/security/opasswd
6. pam_wheel (or pam_wheel.so)
7. Even_deny_root
8. -
9. -

Slide 150

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

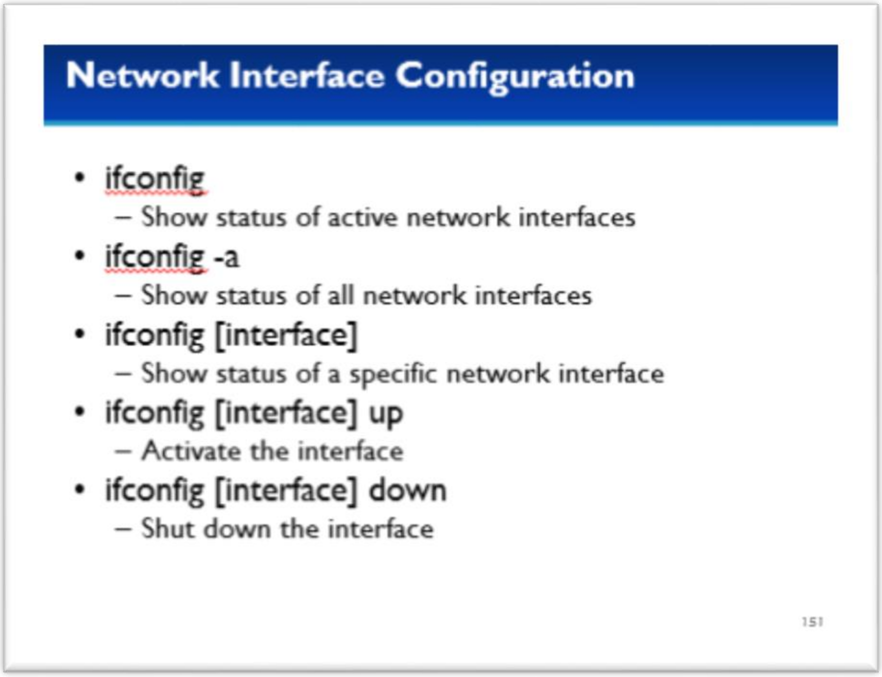
Networking

🕒 Devote 30 minutes to slides 151-167. Allow the students 20 minutes to complete the activity on slide 167.

☆Throughout this section, students should follow along in the **Advanced Ubuntu Demo Image**.

☆In this section, we'll wrap things up by looking at two different sets of networking utilities available on most modern Linux systems, and discuss how to easily enable the firewall and modify firewall rules from the command line.

Slide 151



Network Interface Configuration

- ifconfig
  - Show status of active network interfaces
- ifconfig -a
  - Show status of all network interfaces
- ifconfig [interface]
  - Show status of a specific network interface
- ifconfig [interface] up
  - Activate the interface
- ifconfig [interface] down
  - Shut down the interface

151

- The traditional Linux command for configuring your network interface is the **ifconfig** command.

  - Any changes made with **ifconfig** are not persistent and will be reset to their default configured values upon reboot.

- The **ifconfig** command with no arguments will show the status of active network interfaces.

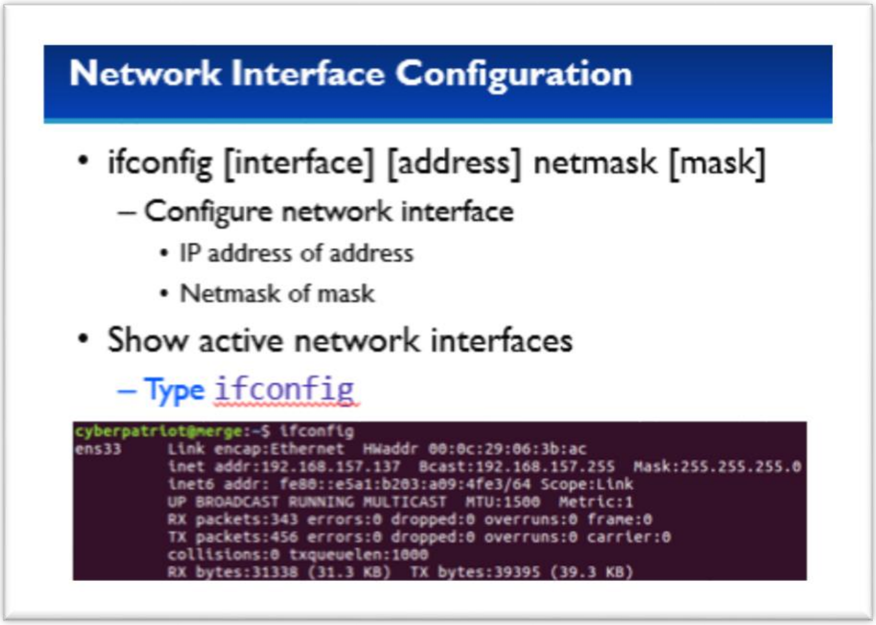
- **Ifconfig –a** will show the status of all network interfaces, not just active ones.

- **Ifconfig** can show the status of a specific network interface by using the **interface** name as an argument.

- **Ifconfig** can also activate a network interface by specifying the interface name followed by **up**.

- Similarly, specifying the interface name followed by **down** will shut down the network interface.

Slide 152



Network Interface Configuration

- ifconfig [interface] [address] netmask [mask]
  - Configure network interface
    - IP address of address
    - Netmask of mask
- Show active network interfaces
  - Type ifconfig

```
cyberpatriot@merge:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:06:3b:ac
          inet addr:192.168.157.137  Bcast:192.168.157.255  Mask:255.255.255.0
          inet6 addr: fe80::e5a1:b203:a09:4fe3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:343 errors:0 dropped:0 overruns:0 frame:0
          TX packets:456 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31338 (31.3 KB)  TX bytes:39395 (39.3 KB)
```

- You can configure network interface by first specifying the interface name, followed by the desired IP address, then the word **netmask** followed by the desired netmask.

- Show the active connections now by typing **ifconfig**.

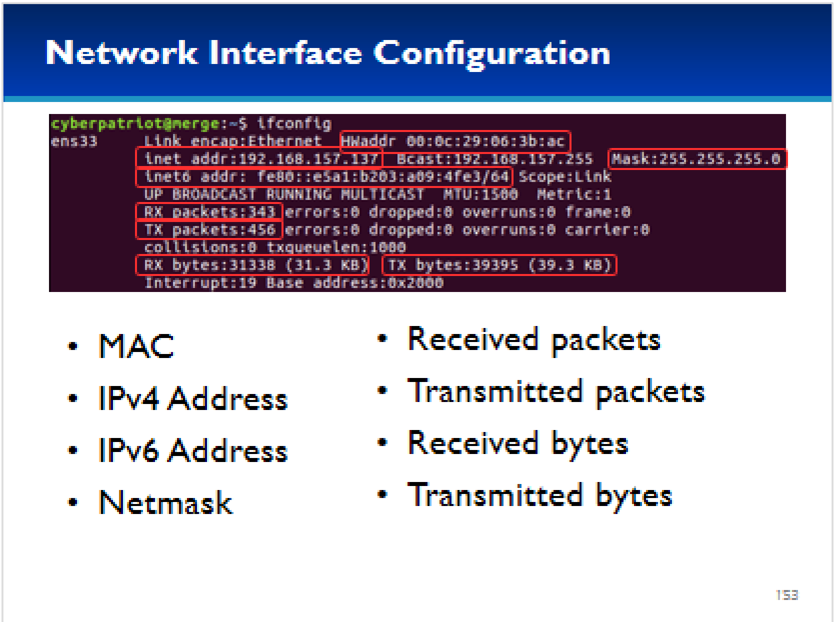
☆Have the students run the commands on the screen.

- The first interface in this example is named "ens33" and is our physical network interface.

- The second interface labeled "lo" is your "loopback" device.

  - This is a virtual network interface that is used by your computer to communicate with itself.

Slide 153



Network Interface Configuration

```
cyberpatriot@merge:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:06:3b:ac
          inet addr:192.168.157.137  Bcast:192.168.157.255  Mask:255.255.255.0
          inet6 addr: fe80::e5a1:b203:a09:4fe3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:343 errors:0 dropped:0 overruns:0 frame:0
          TX packets:456 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31338 (31.3 KB)  TX bytes:39395 (39.3 KB)
          Interrupt:19 Base address:0x2000
```

- MAC
- IPv4 Address
- IPv6 Address
- Netmask

- Received packets
- Transmitted packets
- Received bytes
- Transmitted bytes

153

- Let’s take a closer look at the output of **ifconfig**.
- **Ifconfig** displays the MAC address, which is hardcoded into the device and not normally intended to be changed.

Click to reveal IPv4 Address.

- Your IPv4 address is shown by the label inet addr.

Click to reveal IPv6 Address.

- The IPv6 address is shown by the label inet6 addr.
- IPv6 is a replacement for IPv4 that does not yet have widespread adoption.

Click to reveal Netmask.

- Netmask is shown by the mask label, and specifies the range of IP addresses you can (and can’t) talk to directly.

Click to reveal Received packets.

- Ifconfig also shows the number of received packets; RX is an abbreviation for received.

Click to reveal Transmitted packets.

- The number of transmitted packets; TX is an abbreviation for transmitted.

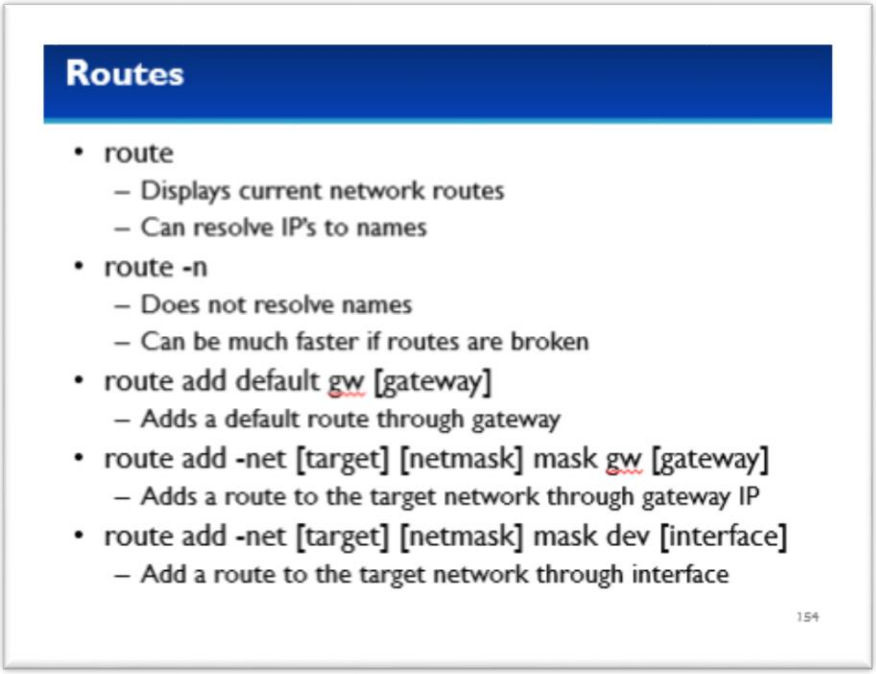
Click to reveal Received bytes.

- The number of received bytes is shown.

Click to reveal Transmitted bytes.

- Displays the number of transmitted bytes.

Slide 154



Routes

- route
  - Displays current network routes
  - Can resolve IP's to names
- route -n
  - Does not resolve names
  - Can be much faster if routes are broken
- route add default gw [gateway]
  - Adds a default route through gateway
- route add -net [target] [netmask] mask gw [gateway]
  - Adds a route to the target network through gateway IP
- route add -net [target] [netmask] mask dev [interface]
  - Add a route to the target network through interface

154

- The **route** command is used to display or modify routes.

- **Route** without any options will display the current routes.

- The **–n** option tells route to not resolve IP addresses to names, which can significantly speed up route if you have incorrect routes.

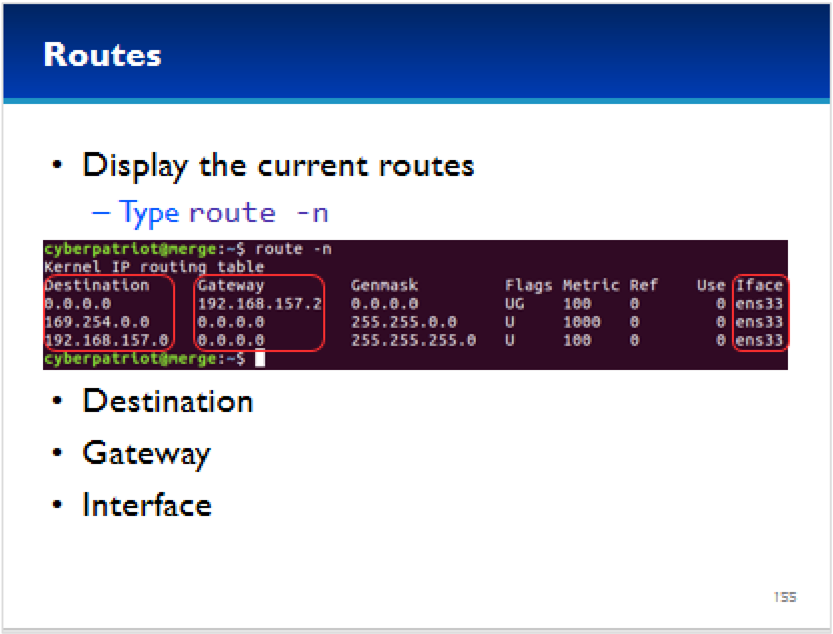
- You can use **route** to set a default gateway by running the command **route add default gw** followed by the IP address of the default gateway you want to use.

- You can also set routes to networks by using **route add –net**.

  - Here the target is the network you want to add a route to, and mask is the netmask of the target network.

  - You can specify the route by specifying an IP address with **gw** or a network interface with **dev**.

Slide 155



Routes

- Display the current routes
  - Type route -n

```
cyberpatriot@merge:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.157.2   0.0.0.0         UG    100    0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.157.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
cyberpatriot@merge:~$
```

- Destination
- Gateway
- Interface

155

- Let’s look at your current routes.

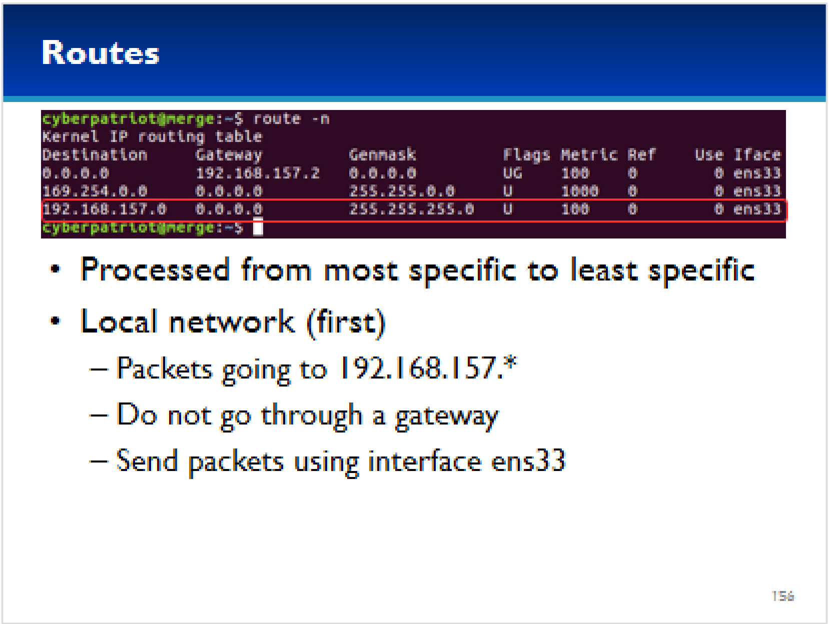
☆Have the students run the commands on the screen.

- Your values will be different, since VMware uses different IP address ranges on different computers.
- The destination is the network that is the destination of this route.
- A value of 0.0.0.0 indicates this is the default route.

☆Have the students run the commands on the screen.

- The gateway is the IP that our packets must go through to get to the destination network.
- A gateway of 0.0.0.0 indicates that the network is directly reachable without going through a gateway.
- The interface is the network interface used to reach the destination network.

Slide 156



Routes

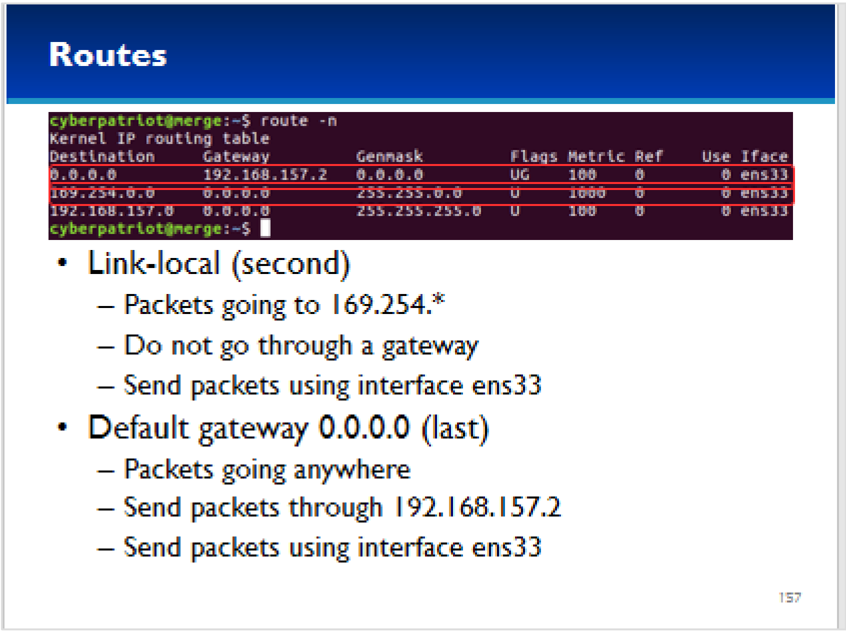
```
cyberpatriot@merge:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.157.2   0.0.0.0         UG    100    0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.157.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
cyberpatriot@merge:~$ 
```

- Processed from most specific to least specific
- Local network (first)
  - Packets going to 192.168.157.*
  - Do not go through a gateway
  - Send packets using interface ens33

156

- Routes are processed from most specific to least specific.
- In this example, the bottom line is evaluated first and specifies that we do not need to go through a gateway to get to our local network.

Slide 157



Routes

```
cyberpatriot@merge:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.157.2   0.0.0.0         UG    100    0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.157.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
cyberpatriot@merge:~$ 
```

- Link-local (second)
  - Packets going to 169.254.*
  - Do not go through a gateway
  - Send packets using interface ens33
- Default gateway 0.0.0.0 (last)
  - Packets going anywhere
  - Send packets through 192.168.157.2
  - Send packets using interface ens33

157

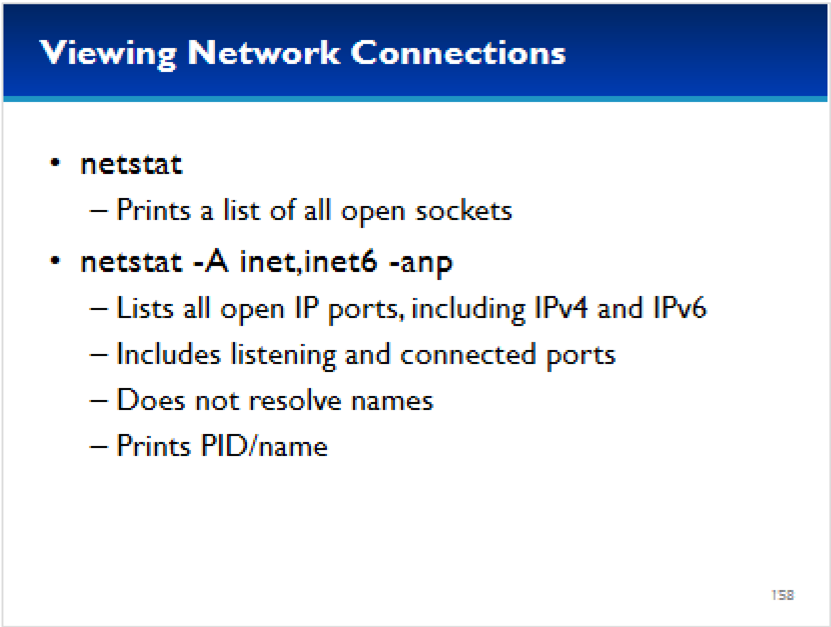
- The next line is the link-local address, which is used to communicate with any devices that did not receive a DHCP address.

- This defines another local network with a different IP address range.

Click to reveal default gateway.

- The default gateway says that all remaining packets must go through our default gateway (192.168.157.2) in order to go anywhere (0.0.0.0).

Slide 158



Viewing Network Connections

- netstat
  - Prints a list of all open sockets
- netstat -A inet,inet6 -anp
  - Lists all open IP ports, including IPv4 and IPv6
  - Includes listening and connected ports
  - Does not resolve names
  - Prints PID/name

158

- The **netstat** command can be used to display open sockets or current routes.

- The **netstat** command by itself prints all open sockets. This contains a lot of information you may not be interested in, such as UNIX domain sockets.

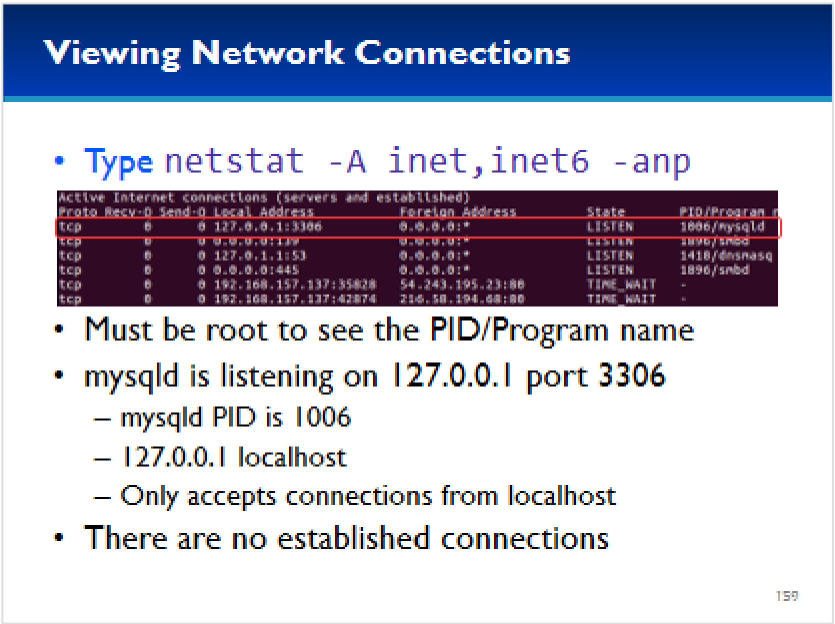
- An example set of netstat options: **–A inet,inet6 –anp**

  - This shows all IPv4 and IPv6 sockets, including established connections and listening ports.

  - Does not resolve addresses to names.

  - Prints out the PID/process name associated with this socket.

Slide 159



Viewing Network Connections

- Type `netstat -A inet,inet6 -anp`

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program n
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1006/mysqld
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1896/smbd
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN      1418/dnsmasq
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1896/smbd
tcp        0      0 192.168.157.137:35828   54.243.195.23:80        TIME_WAIT   -
tcp        0      0 192.168.157.137:42874   216.58.194.68:80        TIME_WAIT   -
```

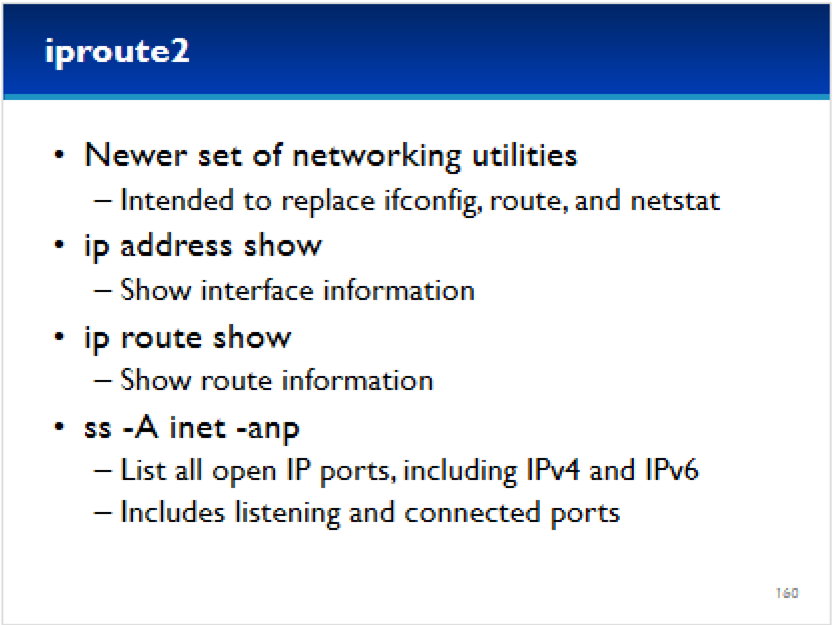
- Must be root to see the PID/Program name
- mysqld is listening on 127.0.0.1 port 3306
  - mysqld PID is 1006
  - 127.0.0.1 localhost
  - Only accepts connections from localhost
- There are no established connections

159

☆Have the students run the commands on the screen.

- In this example you can see that the mysqld process, with a PID of 1006 is listening on port 3306 on the local address: 127.0.0.1
- Since it is listening on localhost, only programs running on this computer can connect to it.

Slide 160



iproute2

- Newer set of networking utilities
  - Intended to replace ifconfig, route, and netstat
- ip address show
  - Show interface information
- ip route show
  - Show route information
- ss -A inet -anp
  - List all open IP ports, including IPv4 and IPv6
  - Includes listening and connected ports

160

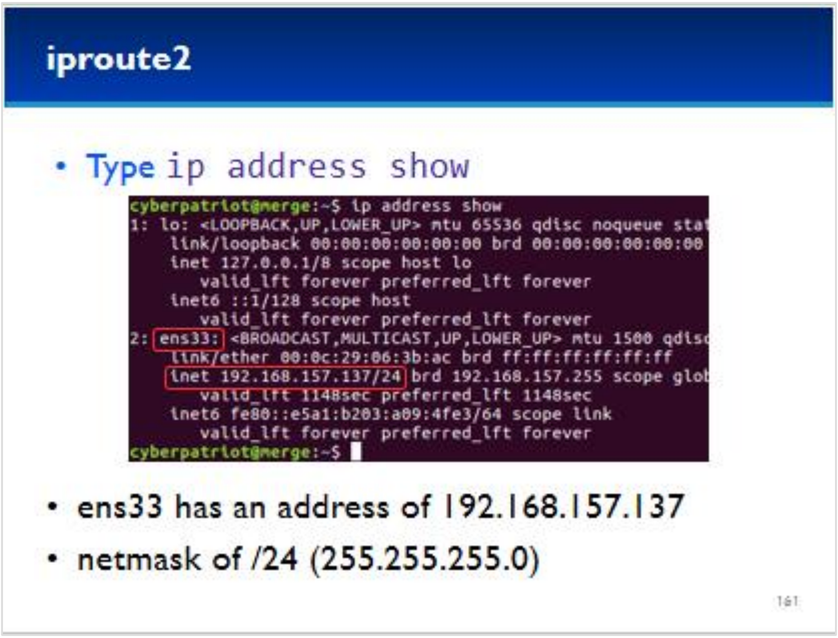
- The **ifconfig** and **netstat** commands are a bit older and don’t incorporate some newer functionality and features.

- There is a newer set of commands intended to replace **ifconfig** and **netstat** called the **iproute2** utility suite.

- The **ip** command can be used to show interface or route configuration, or configure network interfaces.

- The **ss** command is similar to **netstat**.

Slide 161



iproute2

- Type `ip address show`

```
cyberpatriot@merge:~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue stat
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether 00:0c:29:06:3b:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.157.137/24 brd 192.168.157.255 scope glob
       valid_lft 1148sec preferred_lft 1148sec
    inet6 fe80::e5a1:b203:a09:4fe3/64 scope link
       valid_lft forever preferred_lft forever
cyberpatriot@merge:~$ 
```

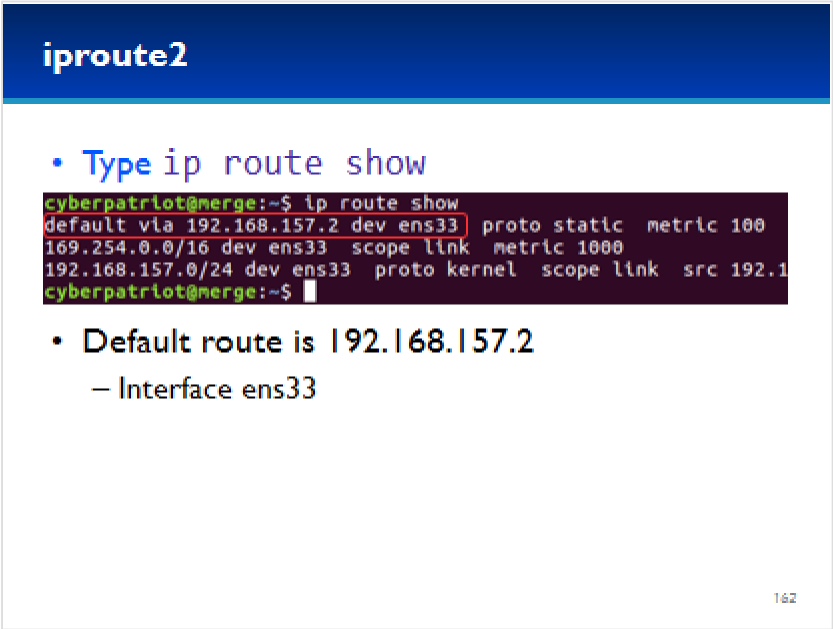
- ens33 has an address of 192.168.157.137
- netmask of /24 (255.255.255.0)

161

☆Have the students run the commands on the screen.

- Here you can see the IP address and netmask of the interface ens33, as well as a lot of the same information printed out by **ifconfig**.

Slide 162



iproute2

- Type ip route show

```
cyberpatriot@merge:~$ ip route show
default via 192.168.157.2 dev ens33  proto static  metric 100
169.254.0.0/16 dev ens33  scope link  metric 1000
192.168.157.0/24 dev ens33  proto kernel  scope link  src 192.1
cyberpatriot@merge:~$ 
```

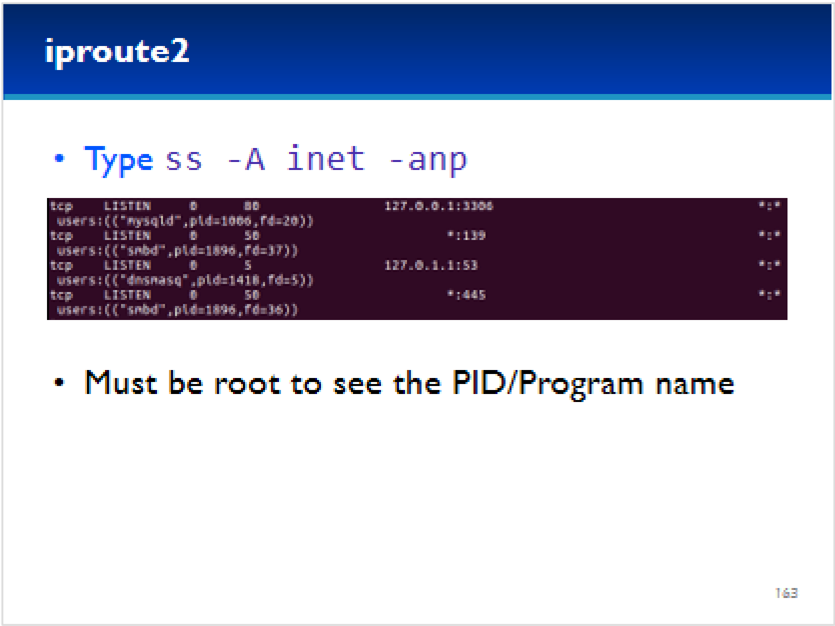
- Default route is 192.168.157.2
  - Interface ens33

162

☆Have the students run the commands on the screen.

- Here we can see network routes, which is basically the same information printed by the **route** command.

Slide 163



iproute2

- Type `ss -A inet -anp`

```
tcp    LISTEN     0      80                  127.0.0.1:3306                  *:*
 users:(("mysqld",pid=1006,fd=20))
tcp    LISTEN     0      50                         *:139                    *:*
 users:(("smbd",pid=1896,fd=37))
tcp    LISTEN     0      5                   127.0.1.1:53                    *:*
 users:(("dnsmasq",pid=1418,fd=5))
tcp    LISTEN     0      50                         *:445                    *:*
 users:(("smbd",pid=1896,fd=36))
```

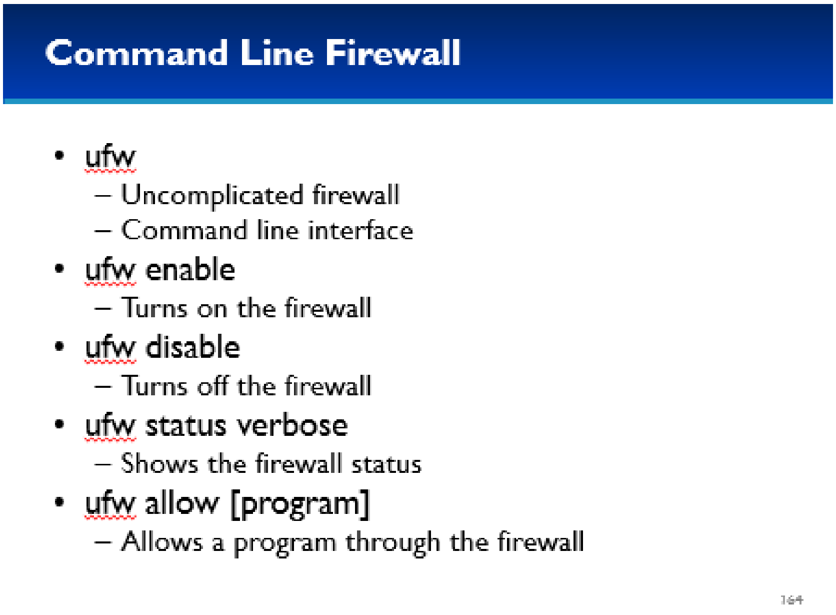
- Must be root to see the PID/Program name

163

☆Have the students run the commands on the screen.

- The **ss** command for printing network connections is a little simpler than **netstat**, but the output is harder to read if you include the **-p** option.

Slide 164



Command Line Firewall

- ufw
  - Uncomplicated firewall
  - Command line interface
- ufw enable
  - Turns on the firewall
- ufw disable
  - Turns off the firewall
- ufw status verbose
  - Shows the firewall status
- ufw allow [program]
  - Allows a program through the firewall

164

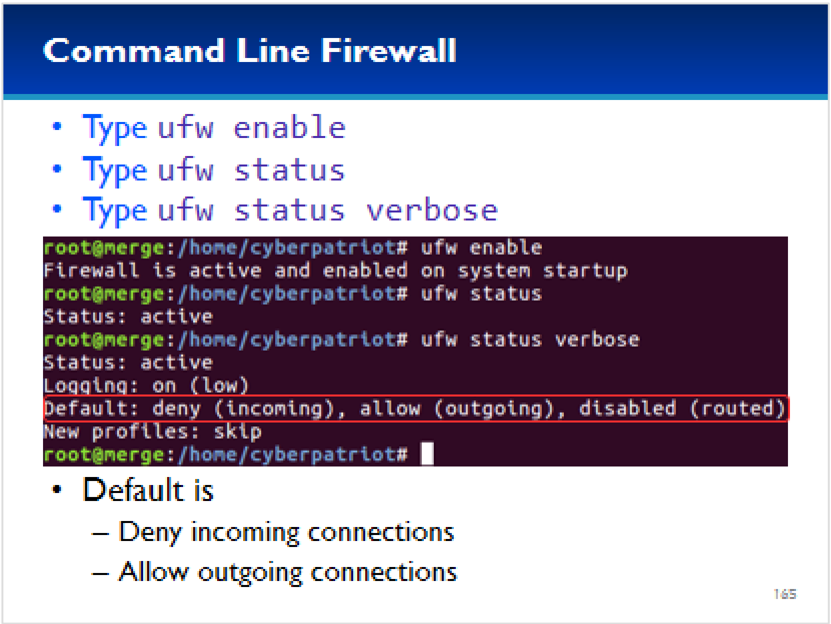
- Ubuntu comes with the uncomplicated firewall which is easily configurable from the command line.

- To turn on the firewall, type: **ufw enable**

- To turn off the firewall, type: **ufw disable**

- **Ufw** status shows the status of the firewall. Can be configured to allow programs or ports through the firewall using **ufw allow**.

Slide 165



Command Line Firewall

- Type `ufw enable`
- Type `ufw status`
- Type `ufw status verbose`

```
root@merge:/home/cyberpatriot# ufw enable
Firewall is active and enabled on system startup
root@merge:/home/cyberpatriot# ufw status
Status: active
root@merge:/home/cyberpatriot# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
root@merge:/home/cyberpatriot# 
```

- Default is
  - Deny incoming connections
  - Allow outgoing connections

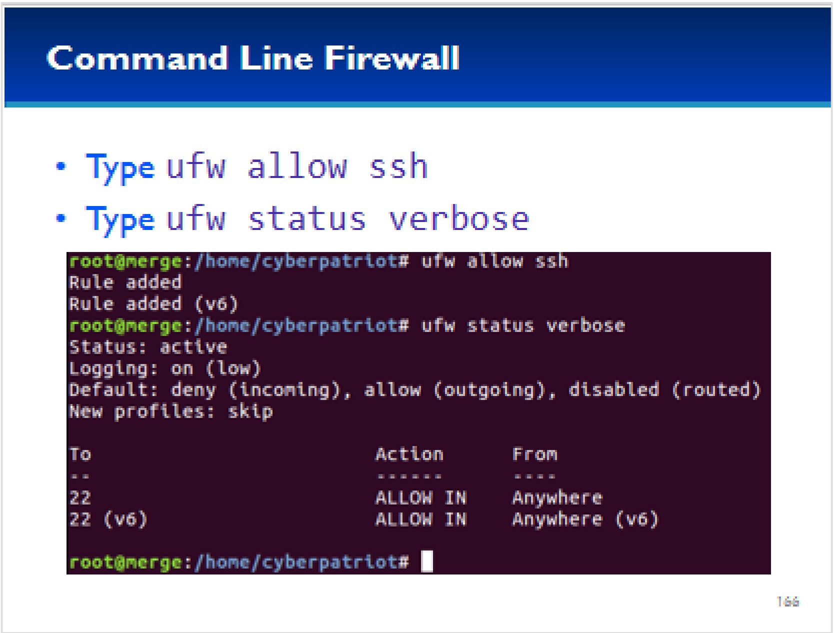
165

☆Have the students run the commands on the screen.

- After enabling the firewall you can see that the default rule is to deny all incoming connections and allow all outgoing connections.

- This is a good default rule for workstations.

Slide 166



Command Line Firewall

- Type `ufw allow ssh`
- Type `ufw status verbose`

```
root@merge:/home/cyberpatriot# ufw allow ssh
Rule added
Rule added (v6)
root@merge:/home/cyberpatriot# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)

root@merge:/home/cyberpatriot# 
```

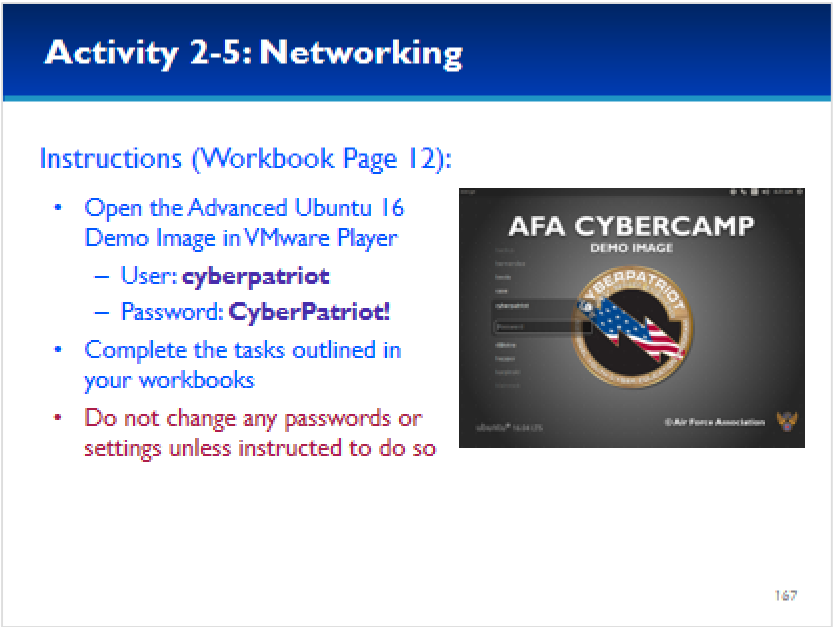
166

- We enabled the ssh service at the beginning of this module, let's make sure let it through the firewall.

☆Have the students run the commands on the screen.

- Now you can see that port 22 is allowed through the firewall.

Slide 167



Activity 2-5: Networking

Instructions (Workbook Page 12):

- Open the Advanced Ubuntu 16 Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or settings unless instructed to do so

167

🕒 Give students about 20 minutes to complete the tasks listed on page 12 of their workbooks.

☆This lab will review networking and firewalls.

☆Stress that the students should not change any passwords or settings unless they are expressly directed to do so in the activity.

☆The students should not need to use any other user names or passwords to complete the activities. Here are the passwords to some administrative accounts just in case.

Username: neumann
Password: vN_@rchit3cture

Username: hopper
Password: ENIAC.TurC0mp

☆Answers:

1. 127.0.0.1, 255.0.0.0 (or 8)
2. 139, 445
3. 68
4. 127.0.1.1
5. ufw logging on
6. -
7. 139, 145
8. 137, 138

Instructor’s Guide Table of Contents

Cisco Networking

Student Workbook Activities

Slide 0

2018 AFA Advanced CyberCamp

cisco Networking

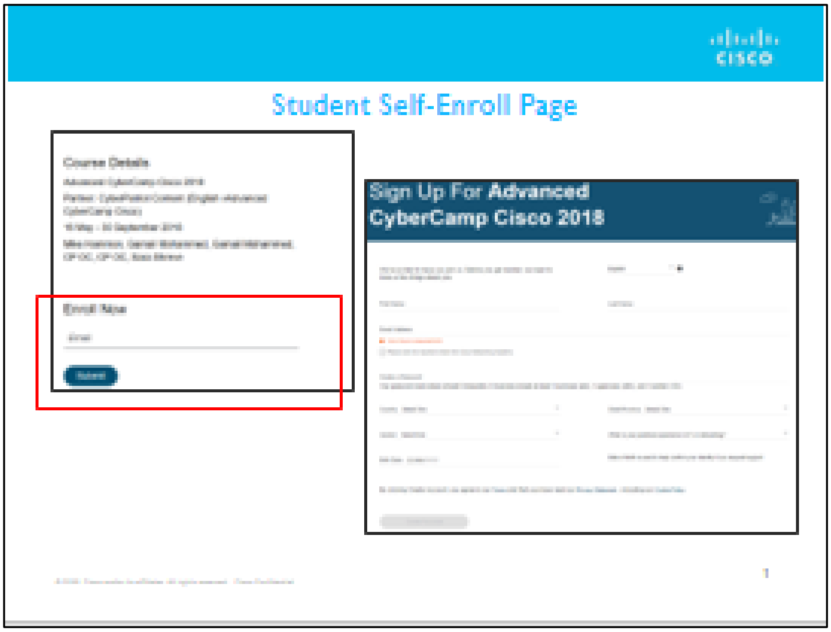
Cisco Networking

Three modules

- Hyperlinks connect Instructor to NetAcademy diagrams and example.
- Separate files to be downloaded to student computers beforehand:
  - Packet Tracer file https://www.netacad.com/group/offerings/packet-tracer
  - Packet Tracer Wireless Configuration
  - Packet Tracer Final Competition

Instructors should be logged into Cisco NetAcad before starting Module 1.

Slide 1



Student Self-Enroll Page

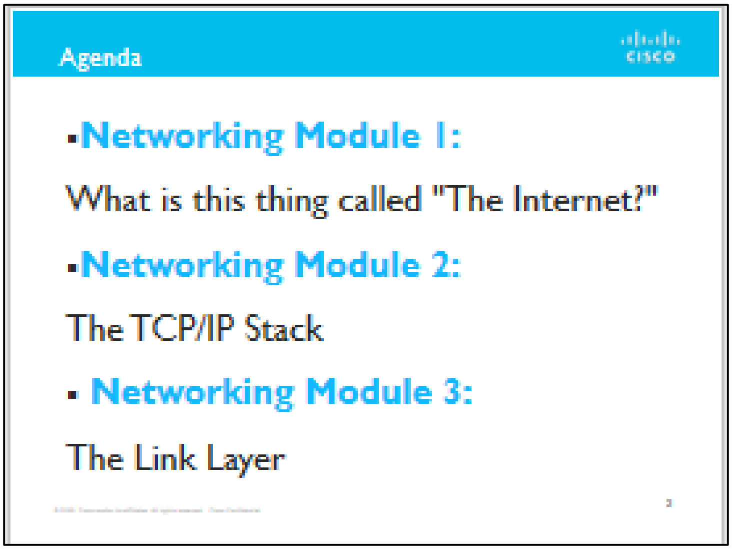
Course Details

Enroll Now

Sign Up For Advanced CyberCamp Cisco 2018

- Instructors should be logged into Cisco NetAcad before starting Module 1.
- Instructors will need to send each student attending the advanced camp a link to the self-enroll page found at the following link. Link: https://www.netacad.com/web/self-enroll/course-671717
- Ideally, students should be sent this self-enroll page before the first day of the camp session. Students should have their parent or guardian sign and return the Parental Permission form **(which can be found on the Camp Coordinator dashboard**) when they arrive for the first day of camp and ideally students should self-enroll before the first day to save time.
- The Parental Permission form can be found on the Camp Coordinator dashboard and should be emailed or passed along in a hard copy to students before utilizing the Cisco Networking portion of the AFA Advanced CyberCamps.
- Parental Permission forms are to be kept on file with the camp instructor for the site and DO NOT get returned to CyberPatriot.
- Students can follow the diagrams and examples on their individual computers as instructors lead OR the instructor can utilize the NetAcad portions as a teaching tool only.

Slide 2



Agenda

- Networking Module 1:

What is this thing called "The Internet?"

- Networking Module 2:

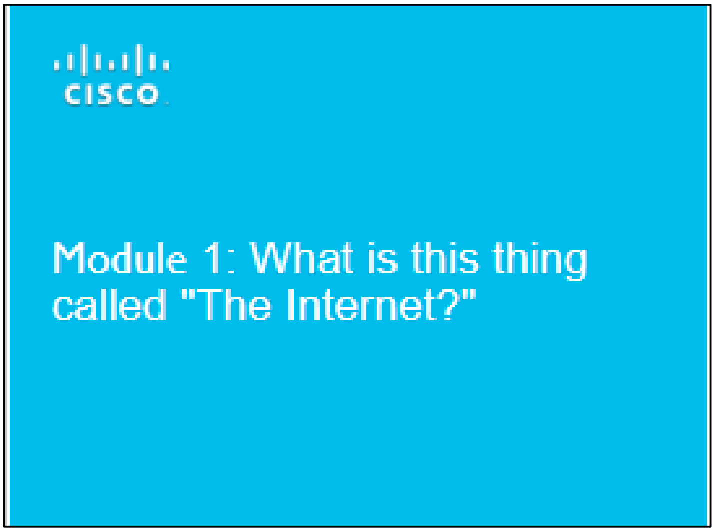
The TCP/IP Stack

- Networking Module 3:

The Link Layer

- There are three modules in the Cisco Networking portion of AFA Advanced CyberCamps:
- Networking Module 1: What is this thing called “The Internet”
- Networking Module 2: The TCP/IP Stack
- Networking Module 3: The Link Layer

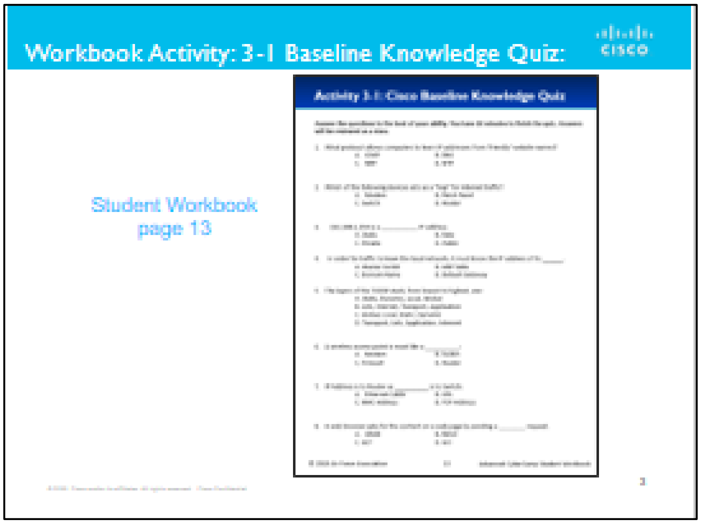
Slide 3



Module 1: What is this thing called "The Internet?"

Module 1: What is this thing called “The Internet?”

Slide 4



Workbook Activity: 3-1 Baseline Knowledge Quiz:

Student Workbook page 13

Activity 3-1: Cisco Baseline Knowledge Quiz

- On page 13 of your Student Workbook answer each question to the best of your abilities. You will have 10 minutes to answer the baseline quiz. After everyone has finished, we will go over the answers as a group.

Answer Key:

1. What protocol allows computers to learn IP addresses from ‘friendly’ website names?

    b. DNS

2. Which of the following devices acts as a “hop” for internet traffic?

    d. Router

3. 192.168.1.254 is a ___________ IP address.

    c. Private

4. In order for traffic to leave the local network, it must know the IP address of its ______.

    d. Default Gateway

5. The layers of the TCP/IP stack, from lowest to highest, are:

    b. Link, Internet, Transport, Application

6. A wireless access point is most like a __________:

    b. Switch

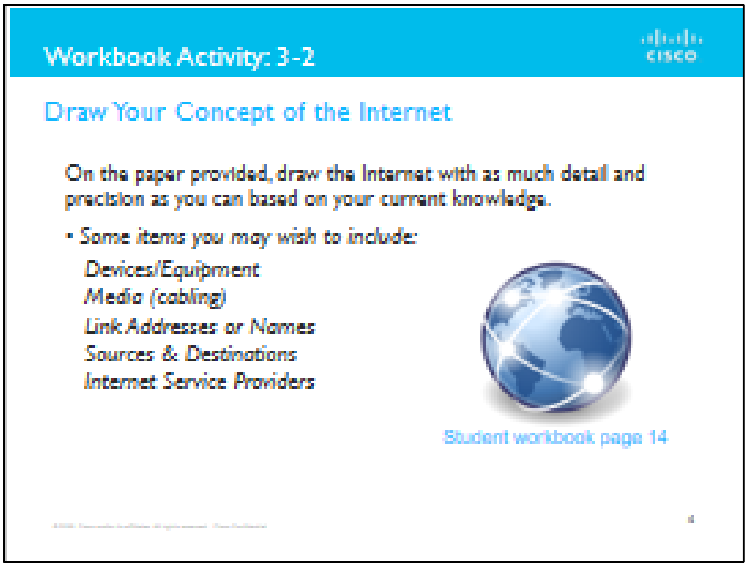
7. IP Address is to Router as __________ is to Switch:

    c. MAC Address

8. A web browser asks for the content on a web page by sending a ________ request.

    c. GET

Slide 5



Workbook Activity: 3-2

Draw Your Concept of the Internet

On the paper provided, draw the Internet with as much detail and precision as you can based on your current knowledge.

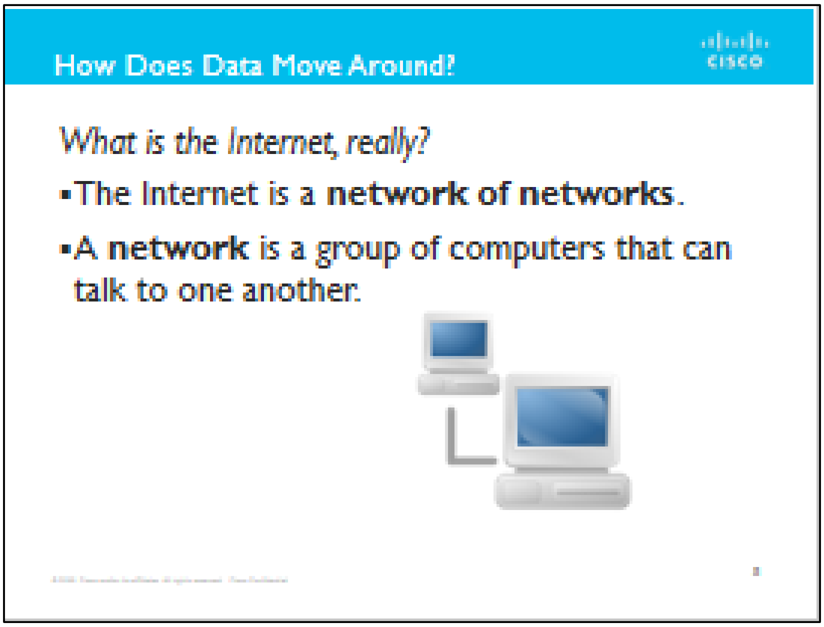
- *Some items you may wish to include:*

Devices/Equipment
Media (cabling)
Link Addresses or Names
Sources & Destinations
Internet Service Providers

Student workbook page 14

- On page 14 of the Student Workbook, students will draw their idea of the Internet in as much detail as possible.
- Items should include: devices, equipment, media (cabling), link addresses or names, sources and destinations, and Internet service providers.
- Students should be prepared to explain some of the reasoning they used. A few students should be selected to share their drawings.
- The goal of today is for every student to gain a detailed understanding of what the Internet is and how it works.

Slide 6



How Does Data Move Around?

What is the Internet, really?

- The Internet is a **network of networks**.
- A **network** is a group of computers that can talk to one another.

- The Internet is a network or networks. Simply put, a network is a group of computers that can talk to one another.
- But how does data get from one computer to another?
  - On a local network?
  - On the Internet?

Slide 7

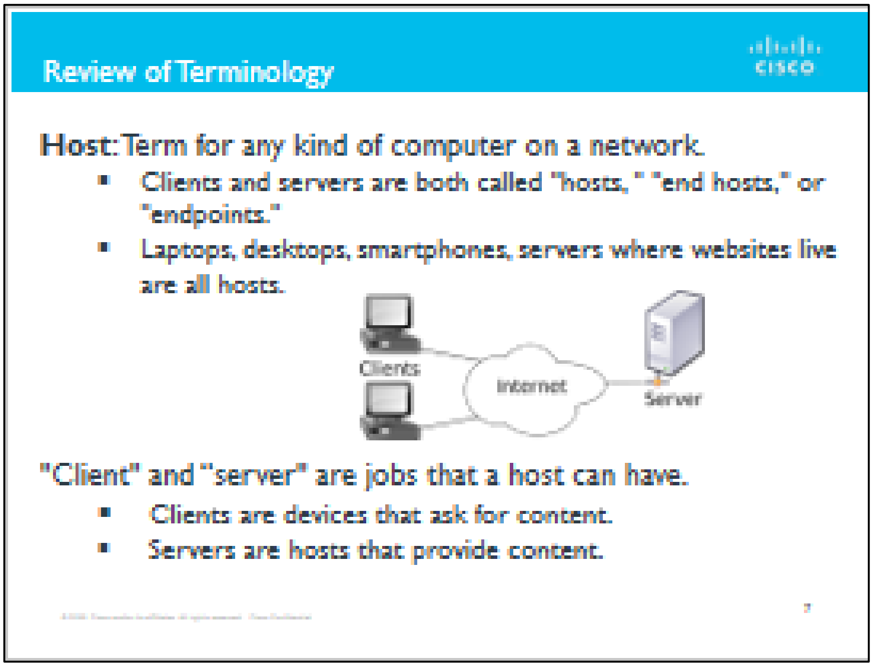
Video

Internet Overview

- Click on the screenshot to launch video: 3:29 minutes

https://www.youtube.com/watch?v=ewrBalT_eBM

Slide 8



Review of Terminology

Host: Term for any kind of computer on a network.

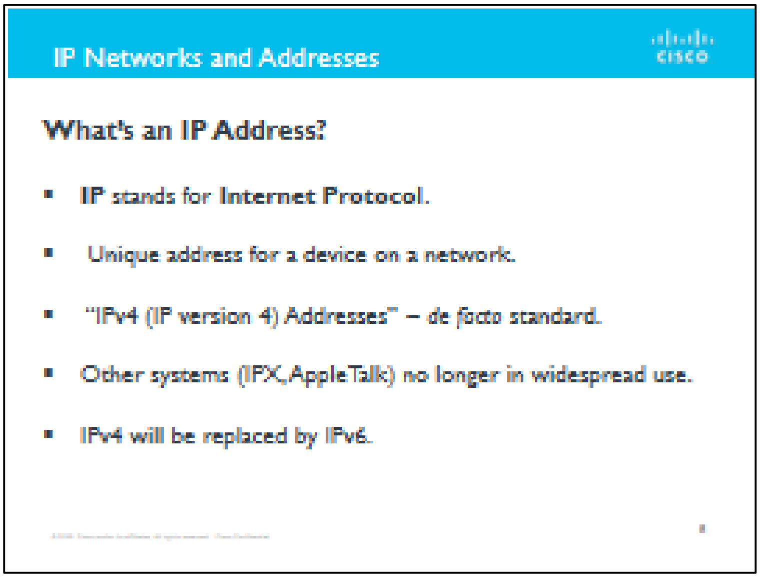
- Clients and servers are both called "hosts," "end hosts," or "endpoints."
- Laptops, desktops, smartphones, servers where websites live are all hosts.

"Client" and "server" are jobs that a host can have.

- Clients are devices that ask for content.
- Servers are hosts that provide content.

- "Host" is a general term for any kind of computer on a network.
  - Clients and servers are both called “hosts,” “end hosts,” or “endpoints.”
  - Hosts are computers that use the network.
  - Laptops, desktops, smartphones, servers where websites live—these are all hosts.
- ”Client” and “server” are jobs that a host can have.
  - Clients are devices that ask for content.
  - Servers are hosts that provide content.

Slide 9



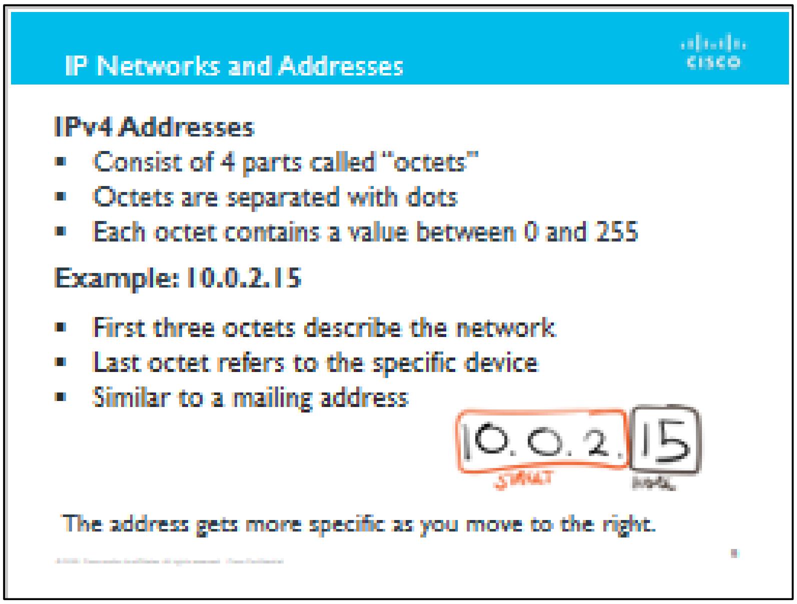
IP Networks and Addresses

What's an IP Address?

- IP stands for Internet Protocol.
- Unique address for a device on a network.
- "IPv4 (IP version 4) Addresses" – de facto standard.
- Other systems (IPX, AppleTalk) no longer in widespread use.
- IPv4 will be replaced by IPv6.

- In order for hosts to communicate across the networks, it's important that they have unique addresses.
- Similar to how you send and receive mail; you need a unique address yourself, and you must know the address of the recipient.
- IP stands for Internet Protocol.
- You'll sometimes see IP addresses referred to as "IPv4 Addresses."
- IPv4 (Internet Protocol version 4) is the most common system of so-called "logical addressing," and is currently the de facto standard.
- Other systems such as IPX and AppleTalk used to be major competitors to IPv4, but are no longer in widespread use.

Slide 10



IP Networks and Addresses

IPv4 Addresses

- Consist of 4 parts called "octets"
- Octets are separated with dots
- Each octet contains a value between 0 and 255

Example: 10.0.2.15

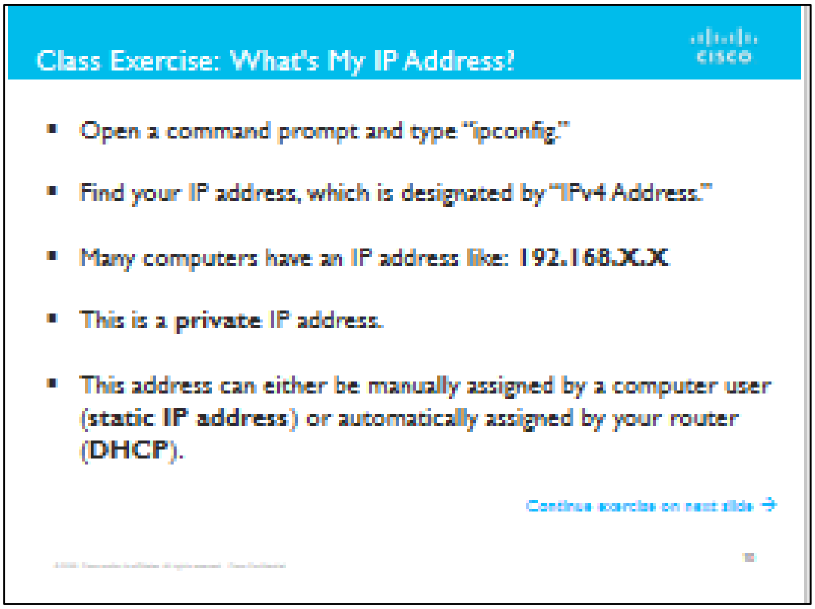
- First three octets describe the network
- Last octet refers to the specific device
- Similar to a mailing address

10.0.2.
15
STREET

The address gets more specific as you move to the right.

- In the future, IPv4 will be replaced by IPv6 because we have started to run out of free IPv4 addresses!
- An IPv4 address consists of four parts called "octets." Octets are separated by dots and each can contain a value between 0 and 255.
- Example: 10.0.2.15
    - First three octets describe the network.
    - Last octet refers to the specific device.
- Similar to a mailing address.
    - On most networks, the first three octets describe the network, and the last octet refers to the specific device.
    - Like a home address, The IP address is kind of like a home address (where the first three octets are like a street, followed by the last octet, which is like a house number).
- The address gets more specific as you move to the right.

Slide 11



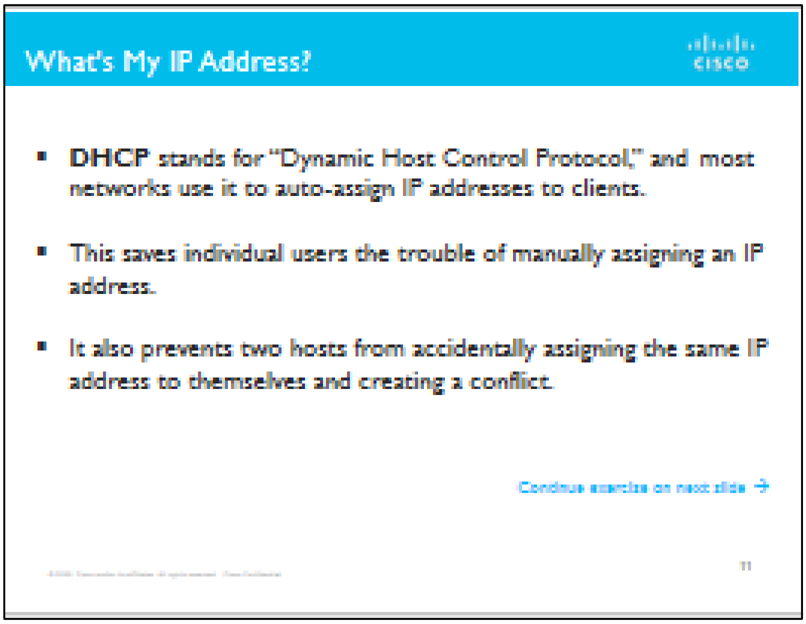
Class Exercise: What's My IP Address?

- Open a command prompt and type "ipconfig."
- Find your IP address, which is designated by "IPv4 Address."
- Many computers have an IP address like: 192.168.X.X
- This is a private IP address.
- This address can either be manually assigned by a computer user (static IP address) or automatically assigned by your router (DHCP).

Continue exercise on next slide →

- Students: open a command prompt and type: ipconfig
- Find your IP address, which is designated by “IPv4 Address.”
- This might look familiar—you’ll see a lot of computers with IP addresses like 192.168.X.X. This is a private IP address.
- This address can either be manually assigned by a computer user (static IP address) or automatically assigned by your router (DHCP).

Slide 12



What's My IP Address?

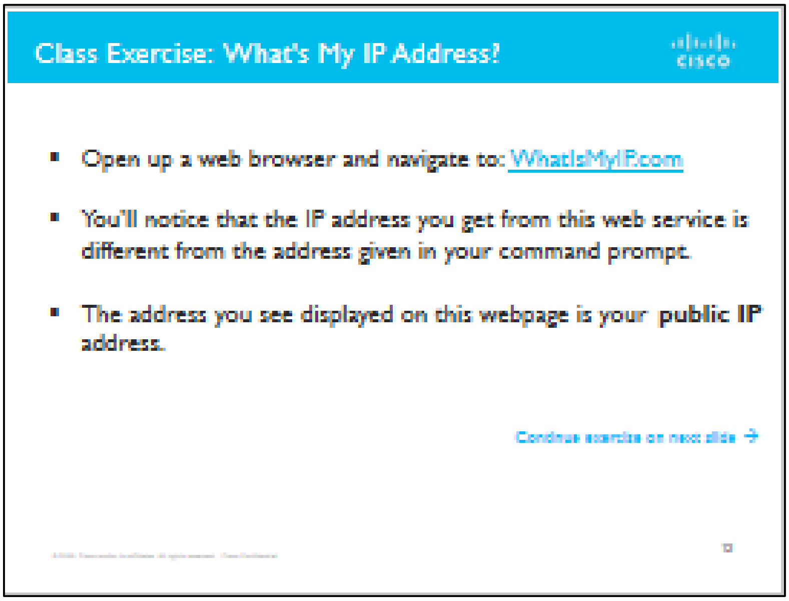
- DHCP stands for "Dynamic Host Control Protocol," and most networks use it to auto-assign IP addresses to clients.
- This saves individual users the trouble of manually assigning an IP address.
- It also prevents two hosts from accidentally assigning the same IP address to themselves and creating a conflict.

Continue exercise on next slide →

11

- DHCP stands for “Dynamic Host Control Protocol,” and most networks use DHCP to auto-assign IP addresses to clients.
- This saves individual users the trouble of manually assigning an IP address.
- It also prevents two hosts from accidentally assigning the same IP address to themselves and creating a conflict.

Slide 13



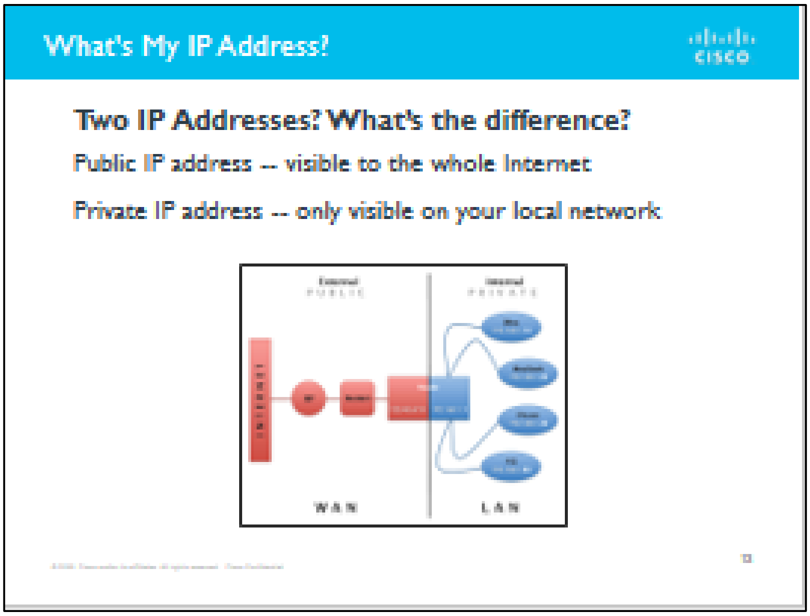
Class Exercise: What's My IP Address?

- Open up a web browser and navigate to: WhatIsMyIP.com
- You'll notice that the IP address you get from this web service is different from the address given in your command prompt.
- The address you see displayed on this webpage is your **public IP** address.

Continue exercise on next slide →

- Open up a web browser and navigate to WhatIsMyIP.com or click the hyperlink in the slide to launch the site directly.
- You’ll notice that the IP address you get from this web service is different from the address given in your command prompt.
- The address you see displayed on this webpage is your public IP address.

Slide 14



What's My IP Address?

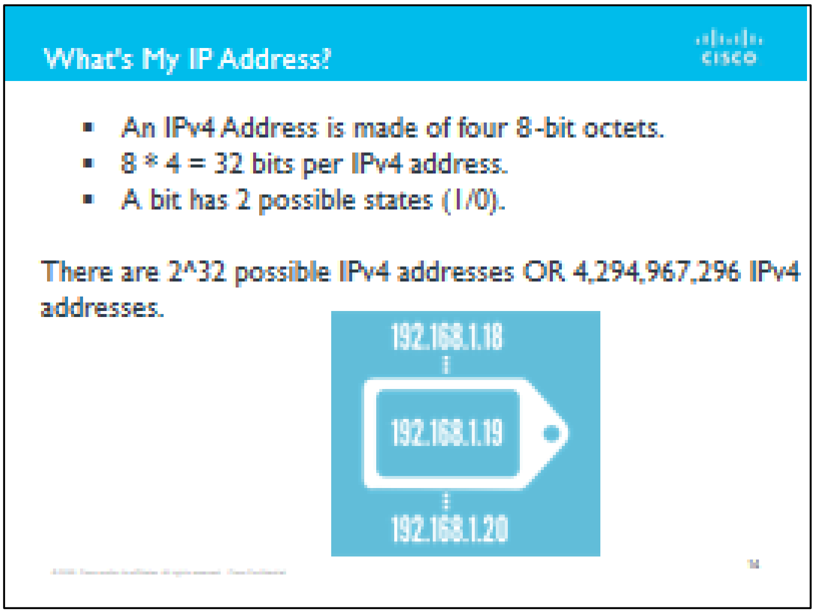
Two IP Addresses? What's the difference?

Public IP address -- visible to the whole Internet

Private IP address -- only visible on your local network

- Public IP address -- visible to the whole Internet.
- Private IP address -- only visible on your local network.

Slide 15



What's My IP Address?

- An IPv4 Address is made of four 8-bit octets.
- 8 * 4 = 32 bits per IPv4 address.
- A bit has 2 possible states (1/0).

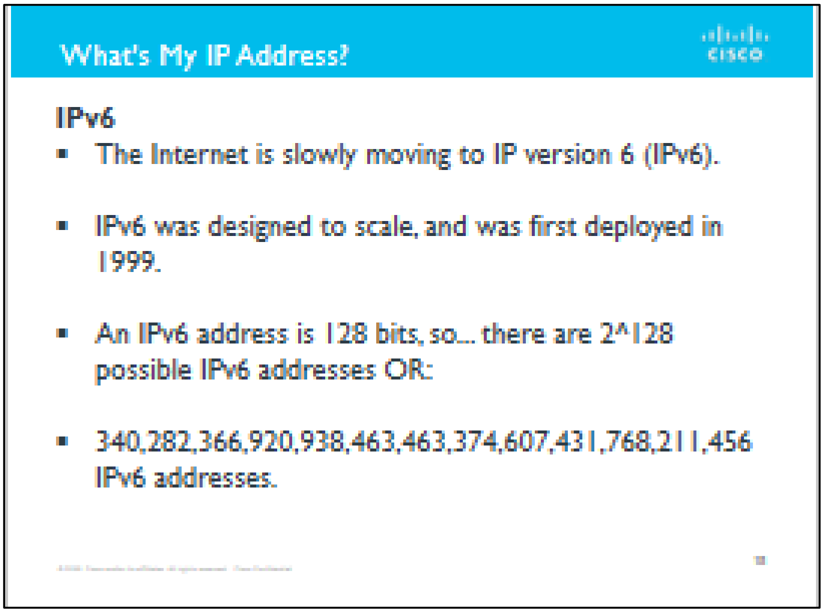
There are 2^32 possible IPv4 addresses OR 4,294,967,296 IPv4 addresses.

192.168.1.18
192.168.1.19
192.168.1.20

- An IPv4 Address is made of four 8-bit octets.
- 8*4=32 bits per IPv4 address.
- A bit has 2 possible states (1/0).
- There are 2^32 possible Ipv$ addresses or 4,294,967,296 IPv4 addresses.

- Did you know?
  - IPv4 was deployed in 1981.
  - Not enough unique IPv4 addresses for all of the devices in the world. The United States IP Address Registry exhausted on September 24, 2015.

Slide 16



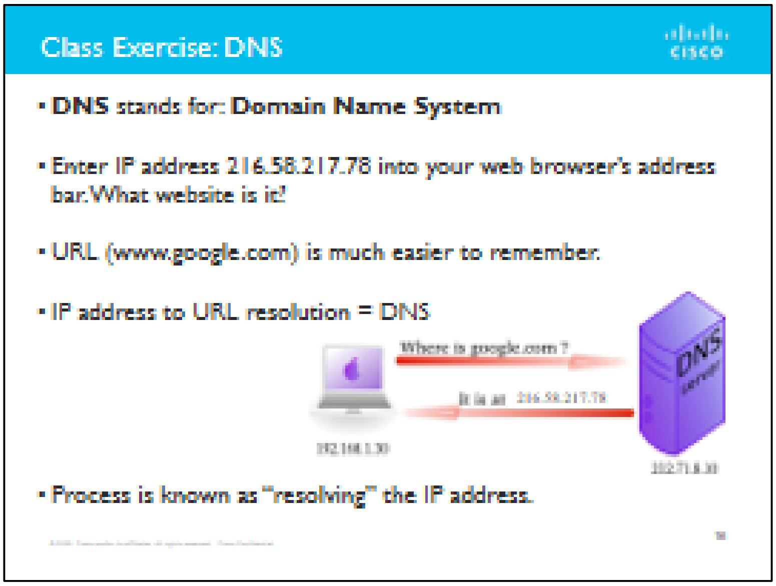
What's My IP Address?

IPv6

- The Internet is slowly moving to IP version 6 (IPv6).
- IPv6 was designed to scale, and was first deployed in 1999.
- An IPv6 address is 128 bits, so... there are 2^128 possible IPv6 addresses OR:
- 340,282,366,920,938,463,463,374,607,431,768,211,456 IPv6 addresses.

- Slowly, the internet moving to IP version 6 (IPv6).
- IPv6 was designed to scale, and was first deployed in 1999.
- An IPv6 address is 128 bits, so... there are 2^128 possible IPv6 addresses.
  OR 340,282,366,920,938,463,463,374,607,431,768,211,456 IPv6 addresses.

Slide 17



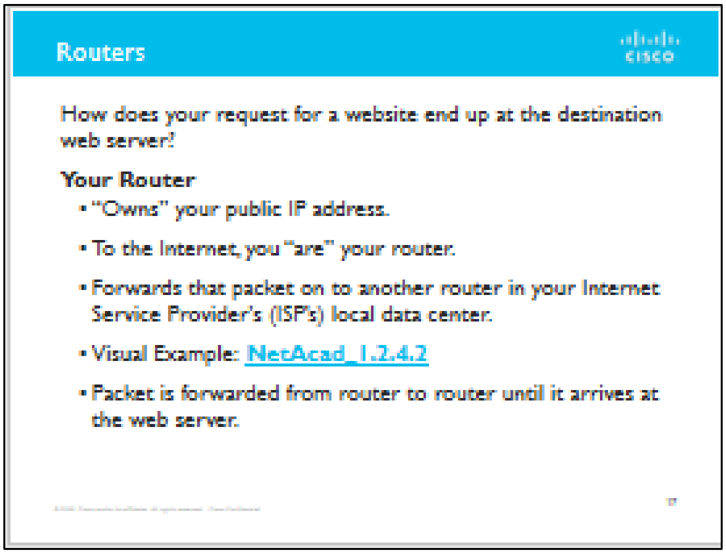
Class Exercise: DNS

- DNS stands for: Domain Name System
- Enter IP address 216.58.217.78 into your web browser's address bar. What website is it?
- URL (www.google.com) is much easier to remember.
- IP address to URL resolution = DNS

- Process is known as "resolving" the IP address.

- As we just discussed, IP addresses are used to indicate where something is located on the Internet so we can send traffic to it.
- [Mini-exercise]: You can get to a website just by entering its IP address into your web browser's address bar.
  - Open a browser and type in: 216.58.217.78
  - What site did it bring you to?
  - Answer: www.google.com.
- But we hardly ever type IP addresses into web browsers; it's much more common to type a website's URL, because a URL is much easier to remember.
- How does my laptop know to go to 216.58.217.78 when I put http://www.google.com in my browser?
- Your computer needs an IP address for its destination—there's no getting around this requirement.
- The solution is **Domain Name System** or **DNS**.
- DNS servers store mappings of IP addresses to "friendly" web addresses.
- Anytime you navigate to a URL in your browser's address bar, your computer automatically sends a DNS request to a DNS server to get the IP address for that URL.
- Even when you enter a "friendly" name, your computer gets the IP address of the destination—this process is known as "resolving" the IP address.

Slide 18



Routers

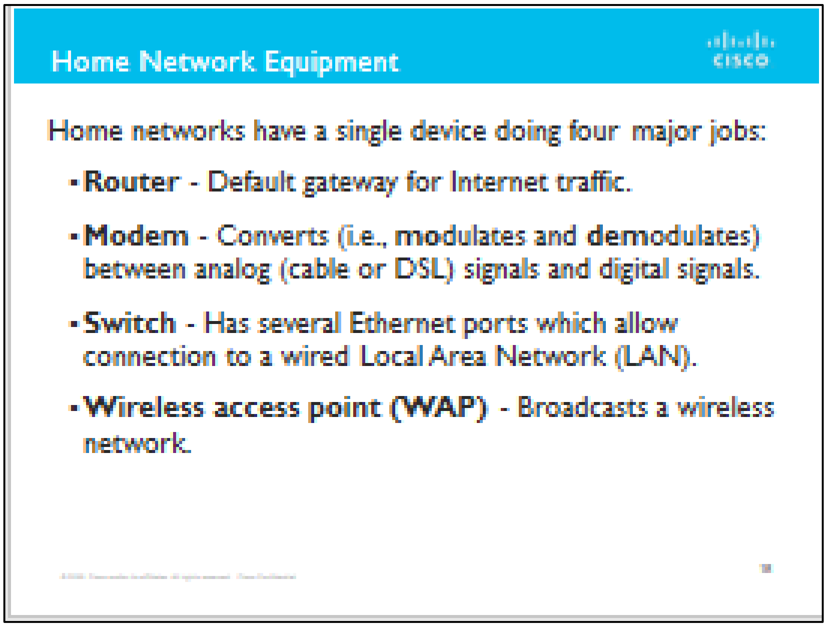
How does your request for a website end up at the destination web server?

Your Router

- "Owns" your public IP address.
- To the Internet, you "are" your router.
- Forwards that packet on to another router in your Internet Service Provider's (ISP's) local data center.
- Visual Example: NetAcad_1.2.4.2
- Packet is forwarded from router to router until it arrives at the web server.

- When you send request for the data that makes up a website, where does that request go?
  - Ultimately, it ends up at the destination web server.
  - But how does it get there?
- When you request a web page from your house, your computer first sends that request to your home router.
  - Reminder: Your router is the device in your home which "owns" your public IP address. To the Internet, you "are" your router.
- Your router then forwards that packet on to another router in your Internet Service Provider's (ISP's) local data center.
  - Take a look at this visualization: **1.2.4.2 (Links to an external site)** NetAcad example.
  - That router forwards your request to another router, and another, and another after that, until the packet eventually arrives at the web server.
- Link: https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#1.2.4.2

Slide 19



Home Network Equipment

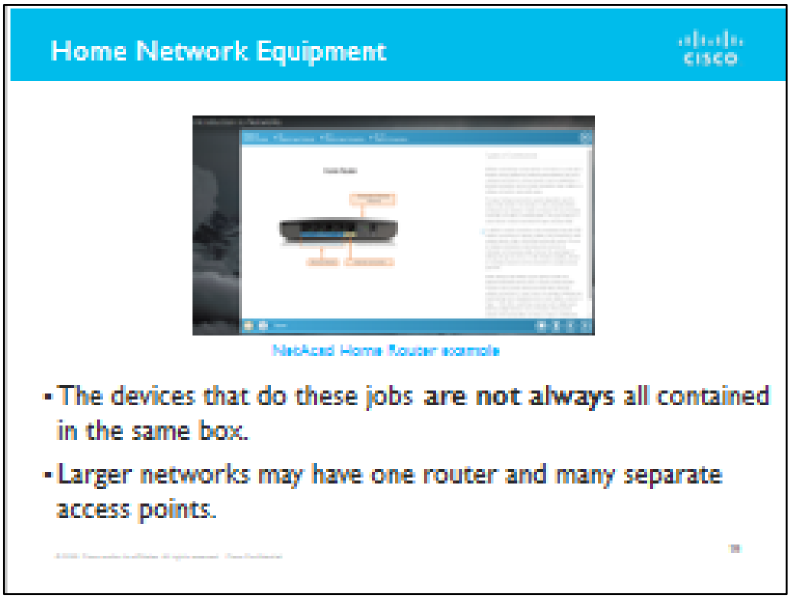
Home networks have a single device doing four major jobs:

- **Router** - Default gateway for Internet traffic.
- **Modem** - Converts (i.e., **mod**ulates and **dem**odulates) between analog (cable or DSL) signals and digital signals.
- **Switch** - Has several Ethernet ports which allow connection to a wired Local Area Network (LAN).
- **Wireless access point (WAP)** - Broadcasts a wireless network.

- Most homes have a single device doing four major jobs for the home network.
- This device, usually provided by your ISP, is acting as a **modem**, a **router**, a **switch**, and a **wireless access point**.
    - This device is a **router** in that it serves as the default gateway for traffic on the home network and forwards that traffic over the Internet.
    - This device is a **modem** in that it does conversion (i.e., **mod**ulates and **dem**odulates) between analog (cable or DSL) signal and digital signal (0’s and 1’s, the language packets are written in).
    - This device is a **switch** in that it has several ethernet ports which allow connection to a wired Local Area Network (LAN).
    - This device is a **wireless access point (WAP)** in that it broadcasts a wireless network which clients can connect to.

Source: https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#4.1.1.1

Slide 20



Home Network Equipment

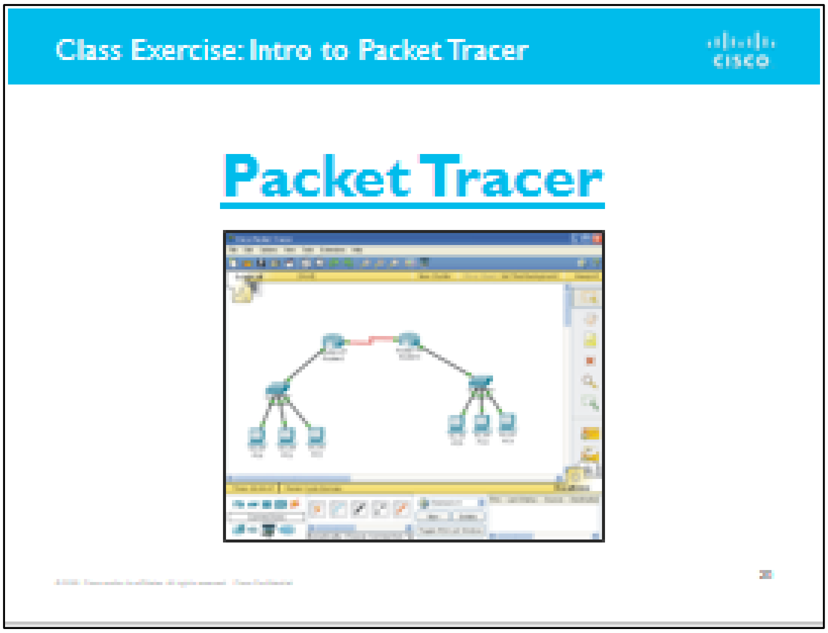
NetAcad Home Router example

- The devices that do these jobs are not always all contained in the same box.
- Larger networks may have one router and many separate access points.

Click on the screenshot to launch the NetAcad Home Router example or copy and paste: https://www.netacad.com/?p_p_id=58&p_p_lifecycle=0&p_p_state=normal&saveLastPath=false&_58_struts_action=%2Flogin%2Flogin&redirect=%2Fc%2Fportal%2Fsaml%2Fsso

- Home networking devices **are not always** all contained in the same piece of hardware.
- Example: In a large office building with dozens of employees spread across many floors, there may be one router and multiple wireless access points.
  - Why do you think this is?

Slide 21

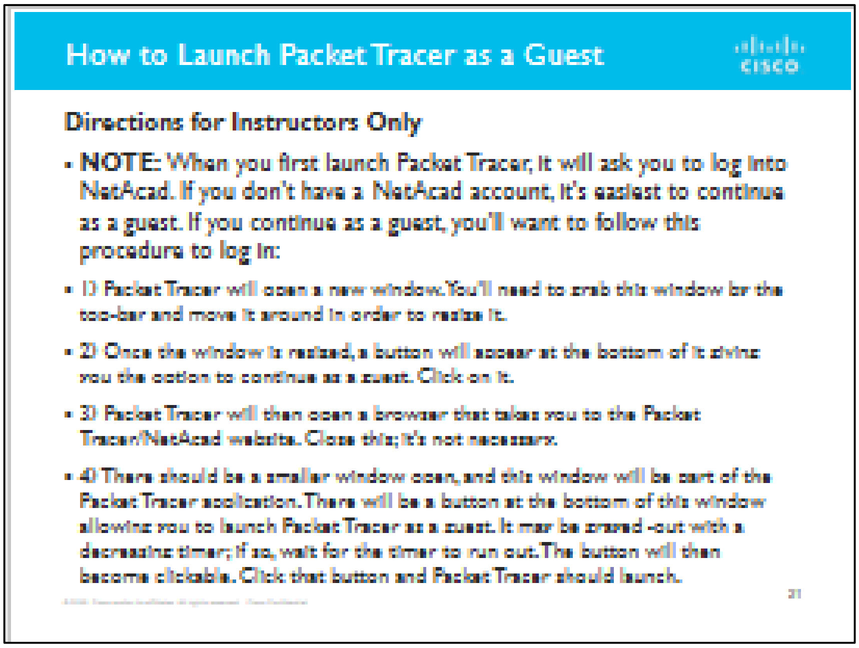


Class Exercise: Intro to Packet Tracer

Packet Tracer

- If the class needs additional background on Packet Tracer, cover the following course, which will take about 60 minutes to complete.
- Click on the phrase Packet Tracer to go directly to the site or cut and paste the following URL: https://www.netacad.com/courses/packet-tracer
- NOTE: NetAcad login required.

Slide 22



How to Launch Packet Tracer as a Guest

Directions for Instructors Only

- **NOTE:** When you first launch Packet Tracer, it will ask you to log into NetAcad. If you don't have a NetAcad account, it's easiest to continue as a guest. If you continue as a guest, you'll want to follow this procedure to log in:
- 1) Packet Tracer will open a new window. You'll need to grab this window by the top-bar and move it around in order to resize it.
- 2) Once the window is resized, a button will appear at the bottom of it giving you the option to continue as a guest. Click on it.
- 3) Packet Tracer will then open a browser that takes you to the Packet Tracer/NetAcad website. Close this; it's not necessary.
- 4) There should be a smaller window open, and this window will be part of the Packet Tracer application. There will be a button at the bottom of this window allowing you to launch Packet Tracer as a guest. It may be grayed -out with a decreasing timer; if so, wait for the timer to run out. The button will then become clickable. Click that button and Packet Tracer should launch.

21

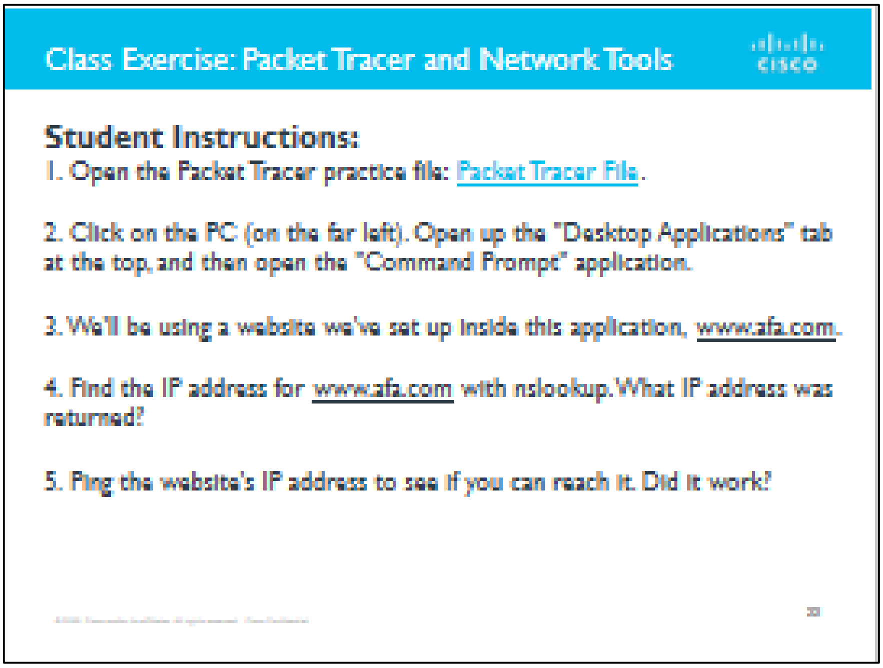
1) Packet Tracer will open a new window. You'll need to grab this window by the top-bar and move it around in order to resize it.

2) Once the window is resized, a button will appear at the bottom of it giving you the option to continue as a guest. Click on it.

3) Packet Tracer will then open a browser that takes you to the Packet Tracer/Netacad website. Close this; it's not necessary.

4) There should be a smaller window open, and this window will be part of the Packet Tracer application. There will be a button at the bottom of this window allowing you to launch Packet Tracer as a guest. It may be grayed-out with a decreasing timer; if so, wait for the timer to run out. The button will then become clickable. Click that button and Packet Tracer should launch.

Slide 23



Class Exercise: Packet Tracer and Network Tools

Student Instructions:

1. Open the Packet Tracer practice file: Packet Tracer File.

2. Click on the PC (on the far left). Open up the "Desktop Applications" tab at the top, and then open the "Command Prompt" application.

3. We'll be using a website we've set up inside this application, www.afa.com.

4. Find the IP address for www.afa.com with nslookup. What IP address was returned?

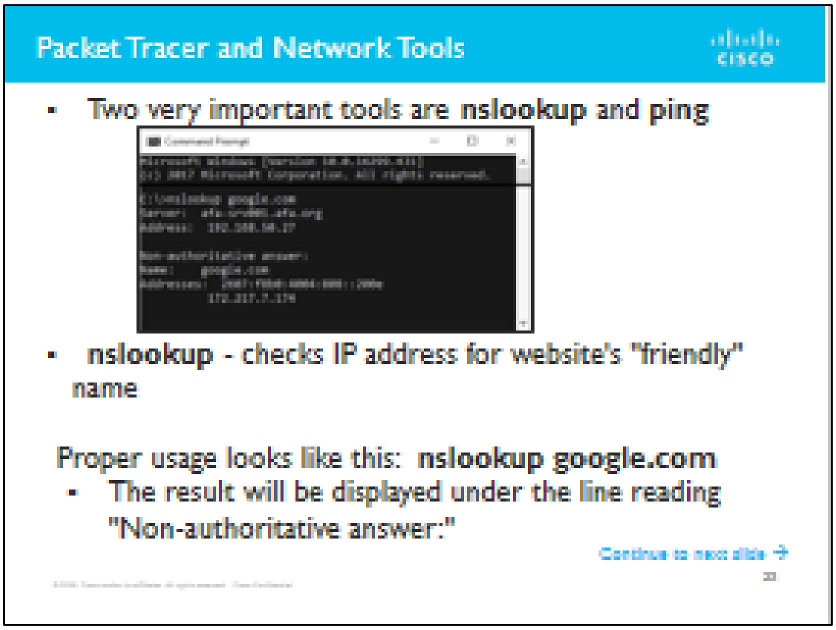
5. Ping the website's IP address to see if you can reach it. Did it work?

To download the Packet Tracer practice file, click on the hyperlink on the slide, or cut and paste the following URL into your browser’s address bar:

https://150566673.netacad.com/courses/487683/files/46796296/download?wrap=1

Instructions:
1. Open the Packet Tracer practice file on your laptop.
2. Click on the PC (on the far left). Open the "Desktop Applications" tab at the top, and then open the "Command Prompt" application.
3. We will use a website we've set up inside this application, www.afa.com.
4. Find the IP address for www.afa.com with nslookup. What IP address was returned?
5. Ping the website's IP address to see if you can reach it. Did it work?

Slide 24



Packet Tracer and Network Tools

- Two very important tools are **nslookup** and **ping**

```
Microsoft Windows [Version 10.0.16299.431]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\>nslookup google.com
Server:  afa-srv001.afa.org
Address:  192.168.50.27

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4004:808::200e
          172.217.7.174
```

- **nslookup** - checks IP address for website's "friendly" name

Proper usage looks like this: **nslookup google.com**

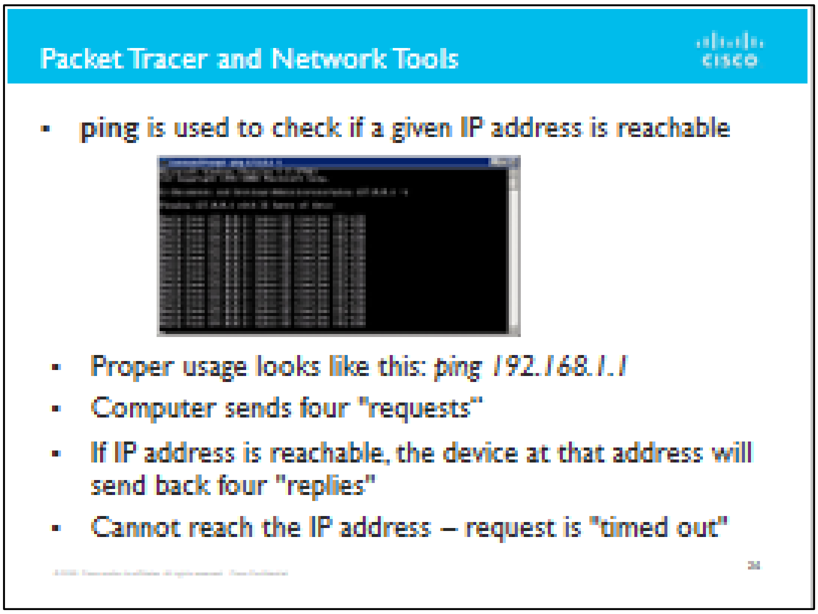
- The result will be displayed under the line reading "Non-authoritative answer:"

Continue to next slide →

23

- Two very important tools for network engineers are **nslookup** and **ping**.
- nslookup is used to check what the IP address is for a website's "friendly" name.
  - Proper usage looks like this: **nslookup google.com**
    - The result will be displayed under the line reading "Non-authoritative answer:"

Slide 25

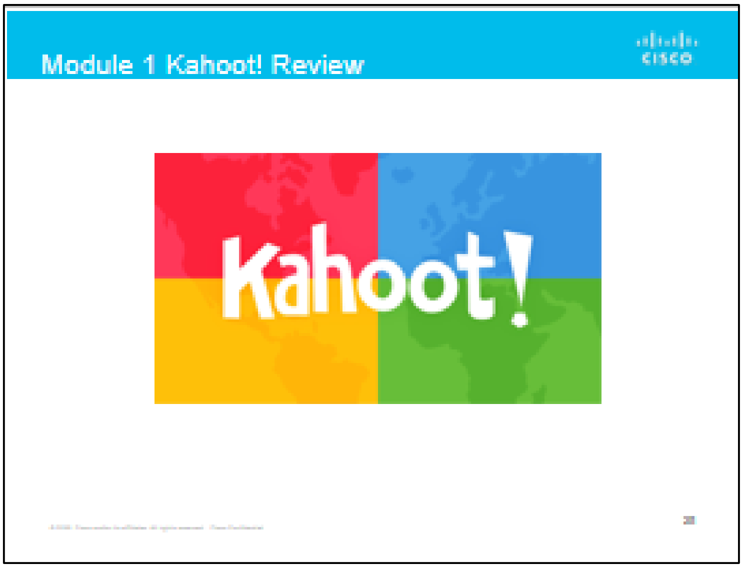


Packet Tracer and Network Tools

- ping is used to check if a given IP address is reachable
  - Proper usage looks like this: ping *192.168.1.1*
  - Computer sends four "requests"
  - If IP address is reachable, the device at that address will send back four "replies"
  - Cannot reach the IP address – request is "timed out"

- ping is used to check if a given IP address is reachable.
  - Proper usage looks like this: **ping 192.168.1.1**
  - Your computer will send four "requests." If the IP address is reachable, the device at the destination address will send back four "replies."
  - If your computer cannot reach the IP address you ping, then you will usually see that the requests "timed out."

Slide 26



Module 1 Kahoot! Review

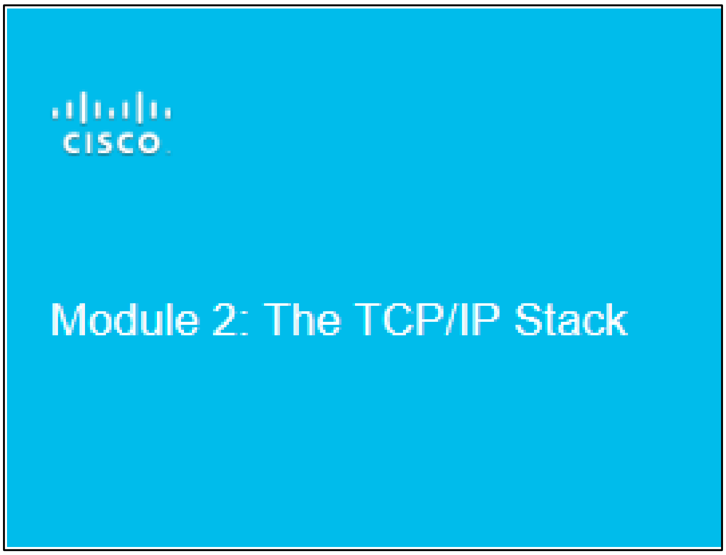
Click on the logo to go directly to the site or cut and paste the following URL:

https://goo.gl/g2R3F4

- When you click on the logo a start screen will appear.
- Instructor will have the option to choose 1:1 playing where students use their individual devices or shared devices for small groups.

For more information on how to play Kahoot! visit: https://files.getkahoot.com/academy/Kahoot_Academy_Getting_Started_Guide_2nd_Ed_-_June_2016.pdf

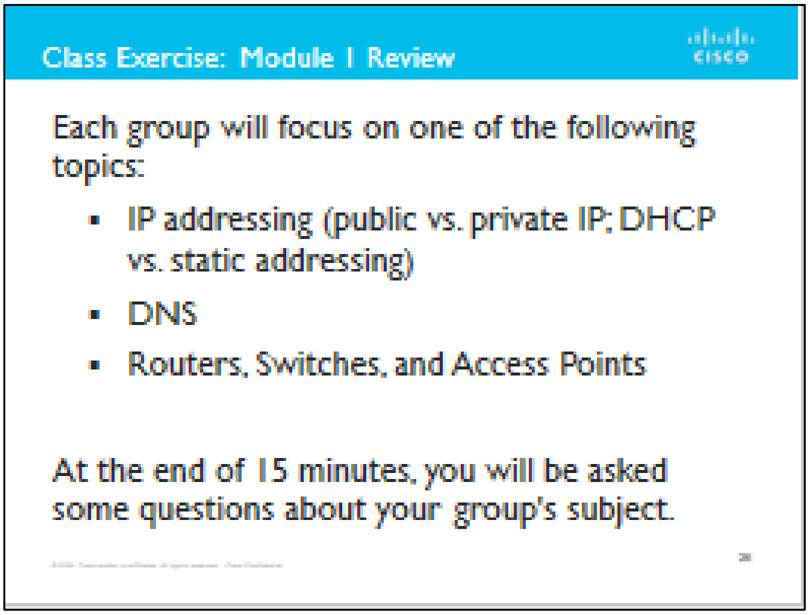
Slide 27



Module 2: The TCP/IP Stack

Module 2: The TCP/IP Stack

Slide 28



Class Exercise: Module 1 Review

Each group will focus on one of the following topics:

- IP addressing (public vs. private IP; DHCP vs. static addressing)
- DNS
- Routers, Switches, and Access Points

At the end of 15 minutes, you will be asked some questions about your group's subject.

- Break into three even groups.
- Take 15 minutes to review yesterday's material. Each group will focus on one of the following topics:
  - IP addressing (public/private IP addresses, DHCP vs. static addressing)
  - Domain Name System (DNS)
  - Routers, Switches, and Access Points
- At the end of 15 minutes, you will be asked some questions about your group's subject. Don't be afraid to ask questions if you're having a hard time remembering things.

Slide 29

Video

What is an IP Address (Review)

- Click on the screenshot to launch video: 3:33 minutes

https://youtu.be/7_-qWlvQQtY

Slide 30

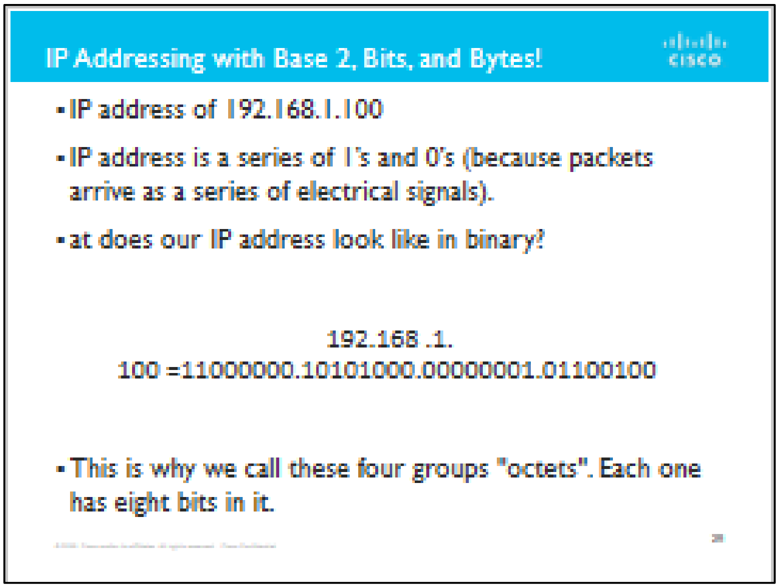
Video

Base 2 Counting

- Click on the screenshot to launch video: 5:20 minutes

https://youtu.be/LpuPe81bc2w

Slide 31



IP Addressing with Base 2, Bits, and Bytes!

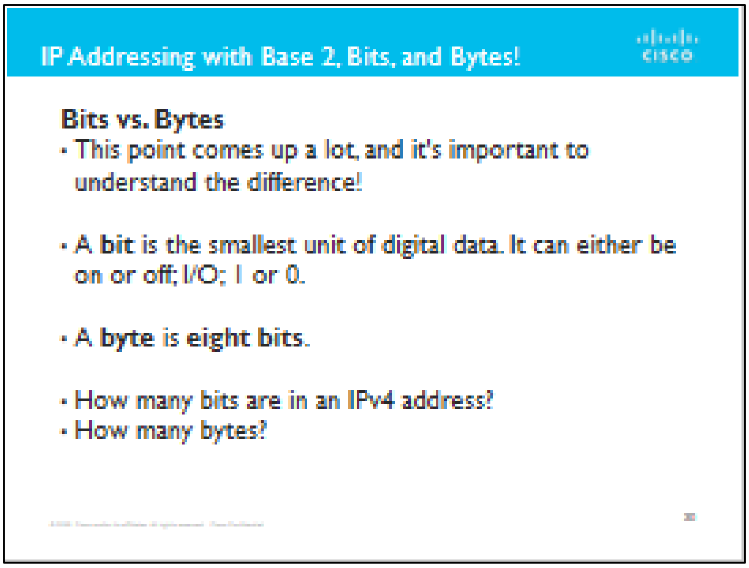
- IP address of 192.168.1.100
- IP address is a series of 1's and 0's (because packets arrive as a series of electrical signals).
- at does our IP address look like in binary?

192.168 .1.
100 =11000000.10101000.00000001.01100100

- This is why we call these four groups "octets". Each one has eight bits in it.

- Say we have an IP address of: 192.168.1.100
- As we saw in some of the review videos, computers and routers read an IP address as a series of 1’s and 0’s (because a packet arrives as a series of electrical signals).
- What does our IP address look like in binary? Work it out for yourself. Did you get it right?
  - 192.168.1.100 = 11000000.10101000.00000001.01100100
- This is why we call these four groups "octets." Each one has eight bits in it.

Slide 32



IP Addressing with Base 2, Bits, and Bytes!

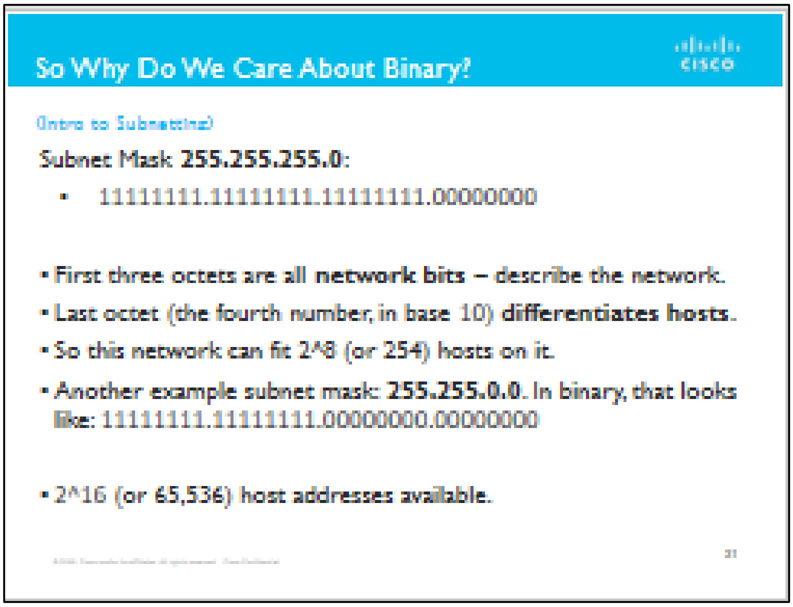
Bits vs. Bytes

- This point comes up a lot, and it's important to understand the difference!
- A bit is the smallest unit of digital data. It can either be on or off; I/O; 1 or 0.
- A byte is eight bits.
- How many bits are in an IPv4 address?
- How many bytes?

Bits vs. Bytes

- This point comes up a lot, and it's important to understand the difference!
- A **bit** is the smallest unit of digital data. It can either be on or off; I/O; 1 or 0.
- A **byte** is **eight bits**.
- How many bits in an IPv4 address?
- How many bytes?

Slide 33



So Why Do We Care About Binary?

(Intro to Subnetting)

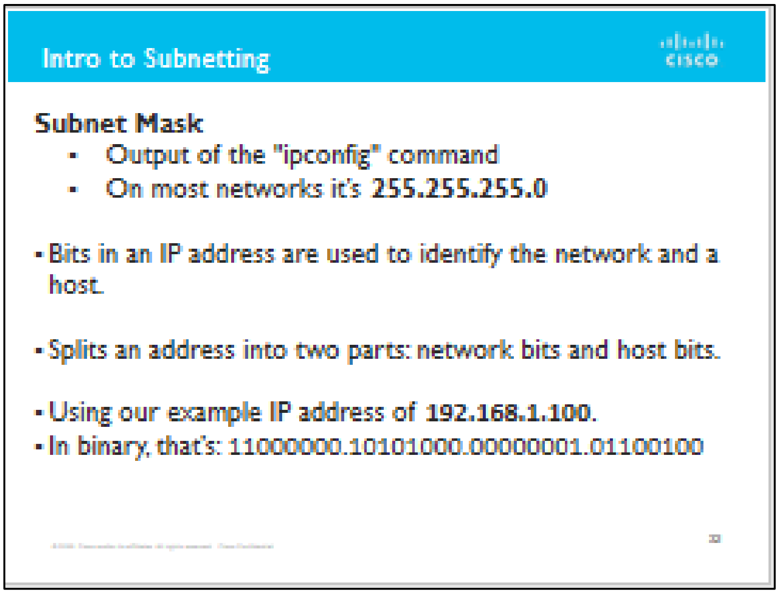
Subnet Mask **255.255.255.0**:

- 11111111.11111111.11111111.00000000

- First three octets are all **network bits** – describe the network.
- Last octet (the fourth number, in base 10) **differentiates hosts**.
- So this network can fit 2^8 (or 254) hosts on it.
- Another example subnet mask: **255.255.0.0**. In binary, that looks like: 11111111.11111111.00000000.00000000
- 2^16 (or 65,536) host addresses available.

- Now, let's look at an example subnet mask: 255.255.255.0
  - 11111111.11111111.11111111.00000000
- The **first three octets** are **Network bits**.
- What does that mean?
  - It means that only the **last octet** (the fourth number, in base 10) is used to **differentiate hosts**. The **first three octets**, taken together, **describe the network**.
- This network can fit 2^8 (or 254) hosts on it.
- Another example subnet mask: 255.255.0.0. In binary, that is:
  - 11111111.11111111.00000000.00000000
- This means that there are 2^16 (or 65,536) host addresses available in a network with this mask.

Slide 34



Intro to Subnetting

Subnet Mask

- Output of the "ipconfig" command
- On most networks it's **255.255.255.0**

- Bits in an IP address are used to identify the network and a host.

- Splits an address into two parts: network bits and host bits.

- Using our example IP address of **192.168.1.100**.
- In binary, that's: 11000000.10101000.00000001.01100100

- You've probably noticed the “subnet mask" in the output of the ipconfig command, or seen it elsewhere.
- On most networks you've probably been on, it's likely: **255.255.255.0**

    - What does this mean?

- A Subnet Mask tells us which bits in an IP address are used to identify the Network, and which bits are used to identify a Host.
- It splits an address into two parts: the Network bits and the Host bits.
- Using our example IP address of **192.168.1.100**. In binary, that’s:

    - 11000000.10101000.00000001.01100100

Slide 35

Module 2 Subnetting Kahoot!

https://play.kahoot.it/#/k/28e548e1-62ba-46de-992c-f972235377a1

- When you click on the logo a start screen will appear.
- Instructor will have the option to choose 1:1 playing where students use their individual devices or shared devices for small groups.

For more information on how to play Kahoot! visit: https://files.getkahoot.com/academy/Kahoot_Academy_Getting_Started_Guide_2nd_Ed_-_June_2016.pdf

Slide 36

Video

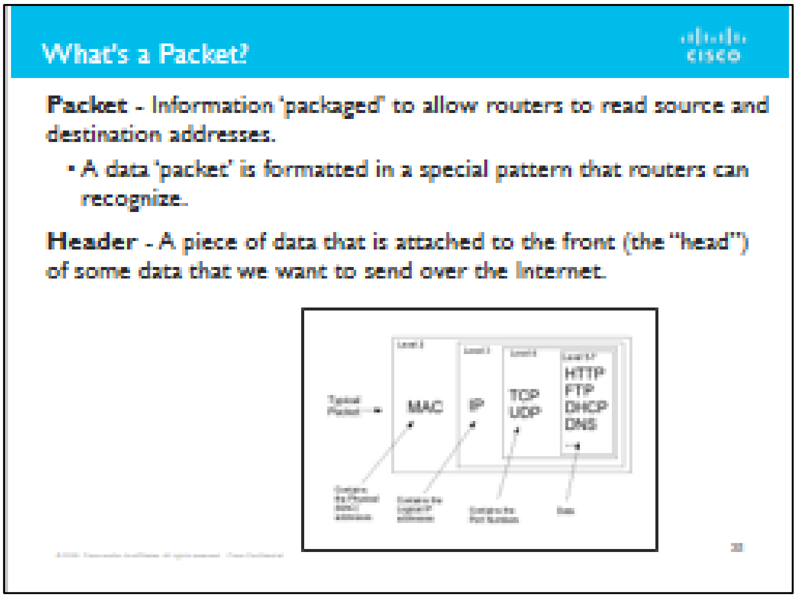
Internet Packets Review

36

Click on the screenshot to launch video: 4:48 minutes

https://youtu.be/7_LPdttKXPc

Slide 37



What's a Packet?

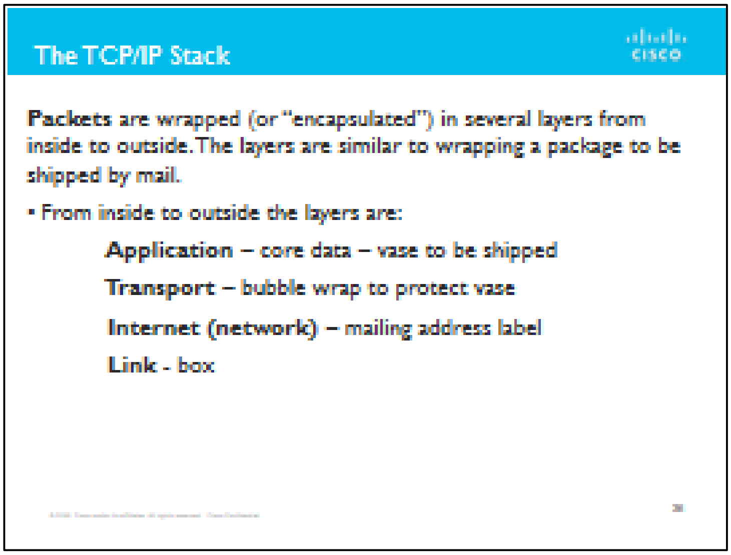
Packet - Information 'packaged' to allow routers to read source and destination addresses.

- A data 'packet' is formatted in a special pattern that routers can recognize.

Header - A piece of data that is attached to the front (the "head") of some data that we want to send over the Internet.

- Have you heard the term “**packet**” before? What do you think it means?
- When we send information across a network (including the Internet), it must be ‘packaged’ into a format that allows routers to read its source and destination addresses along the way.
    - Remember: Every time your request gets sent to a new ‘hop’ in the route, that hop needs to read the source and destination addresses.
- Similar to mailing a letter: You ‘package’ the letter in an envelope which displays the destination and return addresses so the Post Office knows where to send it and where to return it if necessary.
- Routers are just specialized computers:
    - Computers are good at recognizing predefined patterns.
    - To say that data is in a ‘packet’ means that it’s been formatted in a special pattern that routers recognize.
- This formatting is in the form of a “**header**,” a piece of data that is attached to the front (the “head”) of some data that we want to send over the internet.

Slide 38



The TCP/IP Stack

Packets are wrapped (or “encapsulated”) in several layers from inside to outside. The layers are similar to wrapping a package to be shipped by mail.

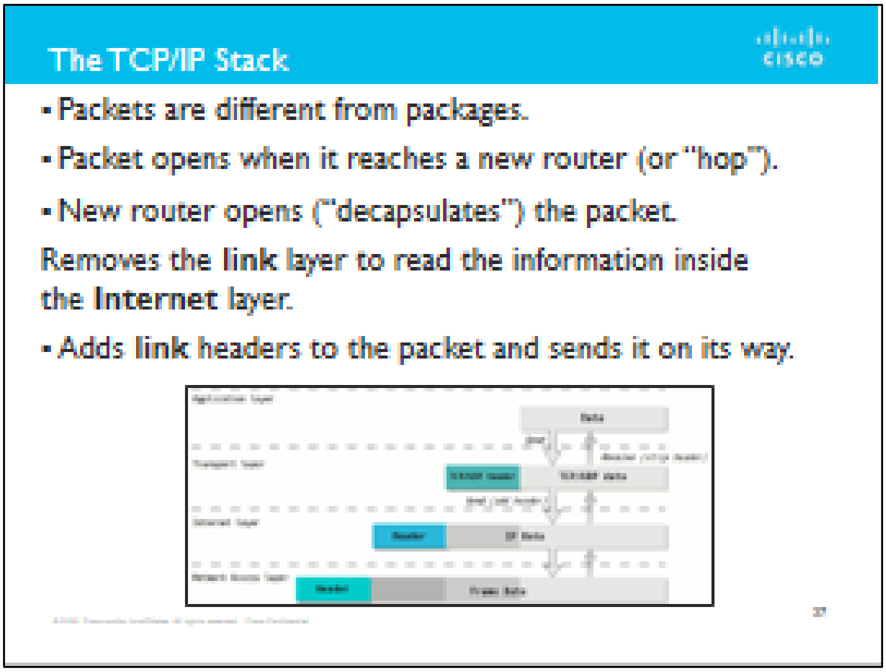
- From inside to outside the layers are:
  - **Application** – core data – vase to be shipped
  - **Transport** – bubble wrap to protect vase
  - **Internet (network)** – mailing address label
  - **Link** - box

- Any time we send a **packet** over a network, it’s wrapped (or “encapsulated”) in several **layers**; from inside to outside, these are:
  - **Application**
  - **Transport**
  - **Internet (aka Network)**
  - **Link**
- Each layer serves a specific purpose.

- The following example compares sending a data packet to shipping a valuable, fragile vase through the mail.

  - The vase is the core data which necessitates packaging. In this example, the **application** layer; the substantive data being transmitted in the packet.
  - Since the vase is fragile, you would likely want to protect it with bubble-wrap. The protection provided is the **transport** layer, which protects the sensitive contents of the packet.
  - The Post Office needs to know where the vase is going and where it came from, so you affix a shipping label with the destination and return addresses. This is how the **Internet (network)** layer tells a router where to direct a packet.
  - To contain the vase and its packing materials, you put everything in a box. This is like the **link** layer that contains and protects the preceding three layers.

Slide 39



The TCP/IP Stack

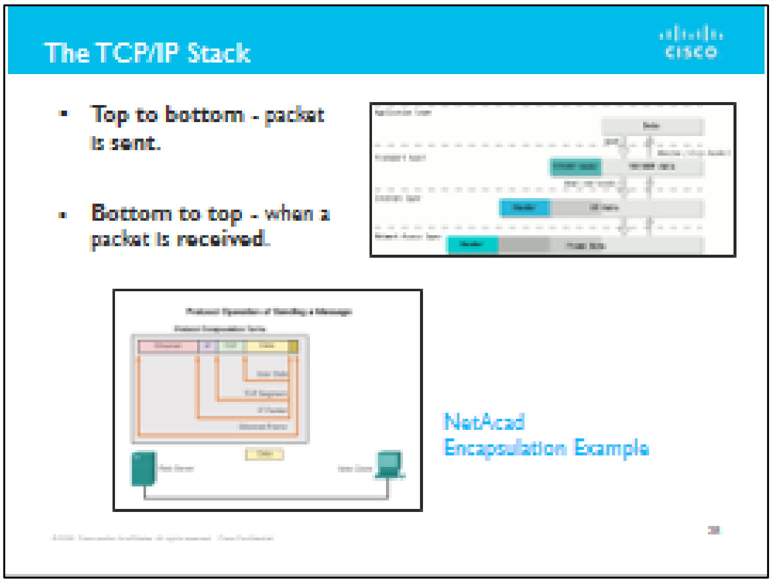
- Packets are different from packages.
- Packet opens when it reaches a new router (or "hop").
- New router opens ("decapsulates") the packet.

Removes the **link** layer to read the information inside the **Internet** layer.

- Adds **link** headers to the packet and sends it on its way.

- One way that packets are different from packages: whenever your packet reaches a new router (or "hop") on its journey, that router has to open up ("decapsulate") the packet.
- It needs to remove the **link** layer so that it can read the information inside the **Internet** layer. It then adds l**ink** headers to the packet again and sends it on its way.

Slide 40



The TCP/IP Stack

- Top to bottom - packet is sent.
- Bottom to top - when a packet is received.

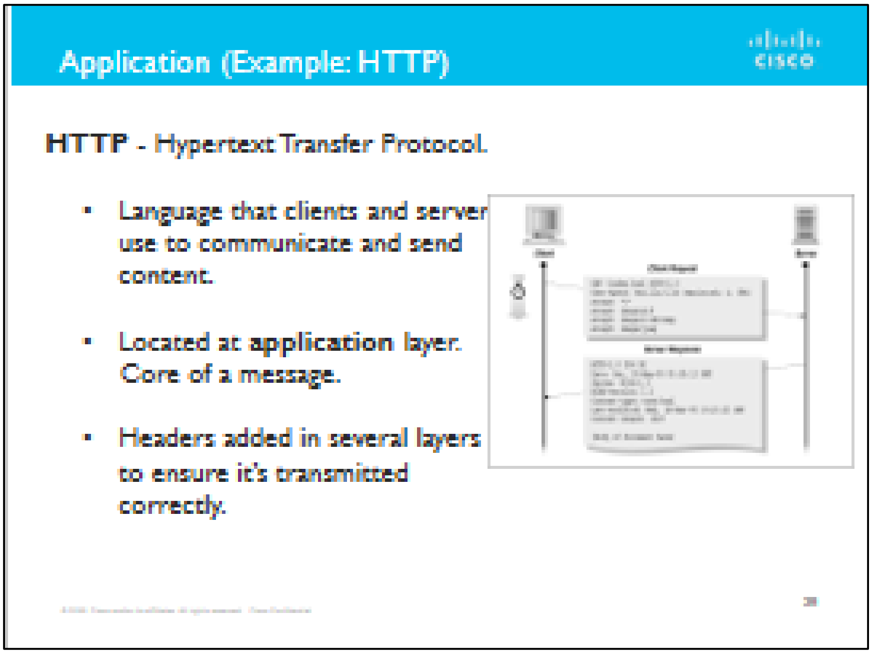
NetAcad Encapsulation Example

- Packets are different from packages: whenever your packet reaches a new router (or "hop") on its journey, that router has to open up ("decapsulate") the packet. It needs to remove the **link** layer so that it can read the information inside the **Internet** layer. It then adds **link** headers to the packet again and sends it on its way.

- From **top to bottom**, this diagram shows what it looks like when a packet is **sent**.
- From **bottom to top**, this diagram shows what it looks like when a packet is **received**.

Click on the bottom screenshot to launch the website directly or copy and paste: https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.1.3

Slide 41



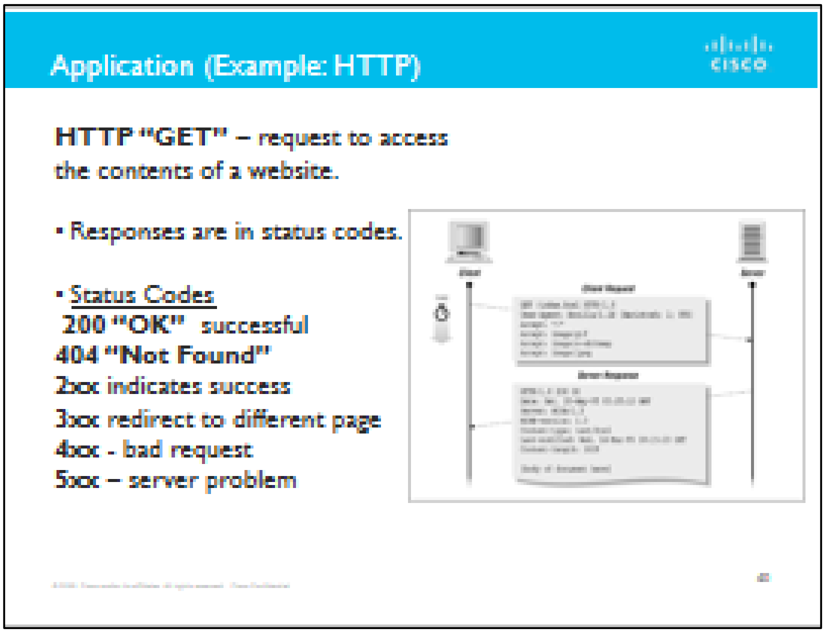
Application (Example: HTTP)

HTTP - Hypertext Transfer Protocol.

- Language that clients and server use to communicate and send content.
- Located at application layer. Core of a message.
- Headers added in several layers to ensure it's transmitted correctly.

- HTTP stands for Hypertext Transfer Protocol.
- HTTP is a sort of language that clients and servers can use to communicate with each other and to send content back and forth.
- HTTP communication is at the **Application** layer.
    - This is the core of a message sent over a network.
    - Headers will be added to it in several layers to ensure that it is transmitted correctly.

Slide 42



Application (Example: HTTP)

HTTP "GET" – request to access the contents of a website.

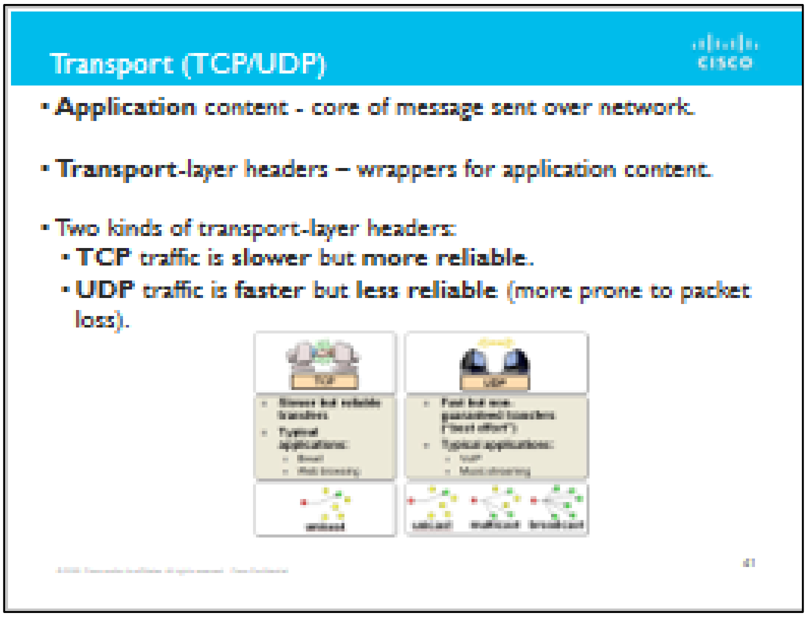
- Responses are in status codes.

- Status Codes

200 "OK" successful
404 "Not Found"
2xx indicates success
3xx redirect to different page
4xx - bad request
5xx – server problem

- To access the contents of a website, your computer sends an **HTTP "GET"** request.
- If the server has the web page the client is asking for, it sends back a status code of **200** "OK," along with the content of the web page.
- If the server doesn't have the page that the client is requesting, it can respond with a code of **404** "Not Found."
- There are other status codes too:
  - Codes starting with **2xx** indicate success.
  - **3xx** codes redirect the client to a different page.
  - **4xx** codes indicate that the client has sent a bad request of some kind.
  - **5xx** codes indicate a problem with the server.

Slide 43



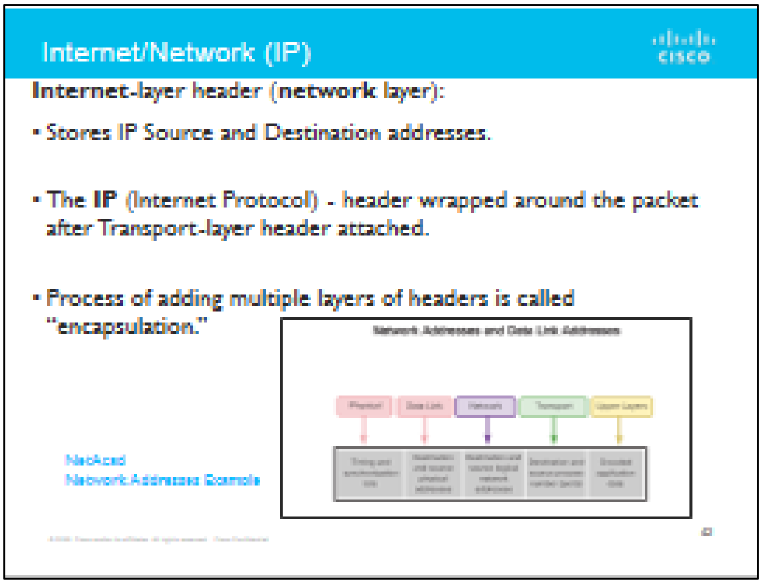
Transport (TCP/UDP)

- Application content - core of message sent over network.
- Transport-layer headers – wrappers for application content.
- Two kinds of transport-layer headers:
  - TCP traffic is slower but more reliable.
  - UDP traffic is faster but less reliable (more prone to packet loss).

TCP
Slower but reliable transfers
Typical applications:
Email
Web browsing
unicast
UDP
Fast but non-guaranteed transfers ("best effort")
Typical applications:
VoIP
Music streaming
unicast
multicast
broadcast
41

- The **application** content is the core of a message that gets sent over the network.
  - It is then wrapped in **transport**-layer headers.
- There are two main kinds of transport-layer headers for our purposes:
  - **TCP** traffic is **slower** but **more reliable**.
  - **UDP** traffic is **faster** but **less reliable** (more prone to packet loss).
- HTTP traffic uses TCP.
- VoIP phone calls and streaming videos use UDP.
  - Why do you think this is?
- For the sake of our example, we would wrap our HTTP GET message in a TCP header, because HTTP traffic uses TCP at the Transport layer.

Slide 44



Internet/Network (IP)

Internet-layer header (network layer):

- Stores IP Source and Destination addresses.
- The IP (Internet Protocol) - header wrapped around the packet after Transport-layer header attached.
- Process of adding multiple layers of headers is called "encapsulation."

NetAcad
Network Addresses Example

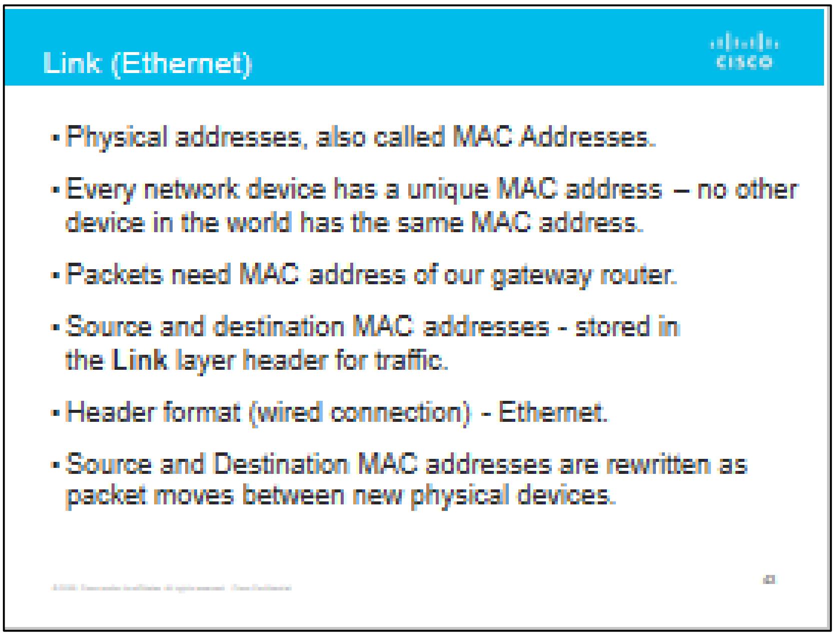
Network Addresses and Data Link Addresses
Physical
Data Link
Network
Transport
Upper Layers
Timing and synchronization bits
Destination and source physical addresses
Destination and source logical network addresses
Destination and source process number (ports)
Encoded application data

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.2.1

- IP Source and Destination addresses are stored in the **Internet**-layer header. This is also called the **network** layer.
- The **IP-header** (Internet Protocol) is wrapped around the packet after the transport-layer header is attached—the process of adding multiple layers of headers is called "encapsulation."
- For another visualization of how this works, check out this illustration!
- To follow along with the example, our Network-layer IP header for this packet would have our computer's IP address as the source address and the web server's IP address as the destination address.

Click on the bottom screenshot to launch the website directly or copy and paste: https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.2.1

Slide 45



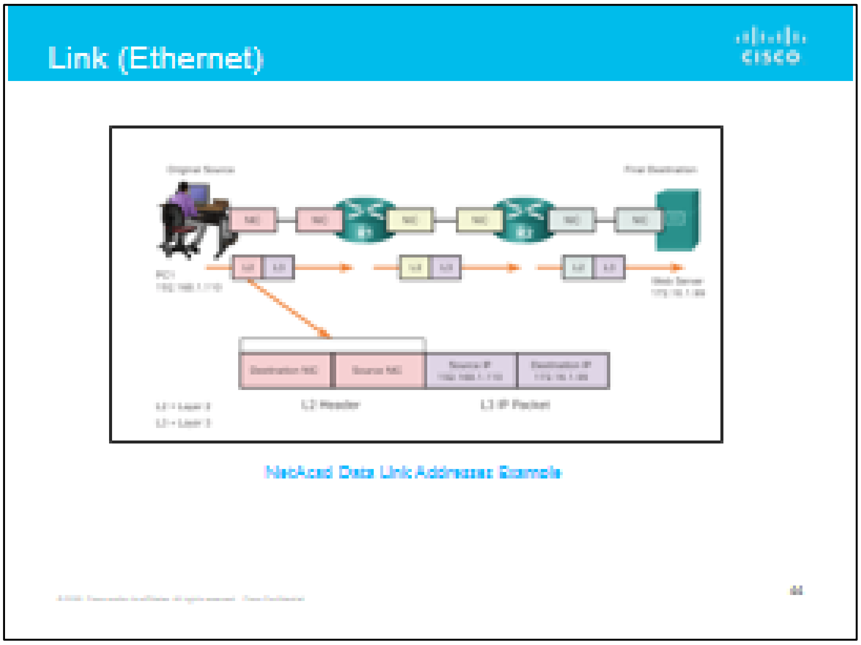
Link (Ethernet)

- Physical addresses, also called MAC Addresses.
- Every network device has a unique MAC address – no other device in the world has the same MAC address.
- Packets need MAC address of our gateway router.
- Source and destination MAC addresses - stored in the Link layer header for traffic.
- Header format (wired connection) - Ethernet.
- Source and Destination MAC addresses are rewritten as packet moves between new physical devices.

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.2.2

- How do we know what physical device “owns” the IP address of your computer? Of your router?
- Physical addresses are also called MAC Addresses.
- Every network device has a unique physical address, a MAC address that no other device in the world has.
- When we send a packet over a network connection, whether it is wireless or wired, we need to address that packet to the MAC address of our default gateway, the router.
- The source and destination MAC addresses for a packet are stored in the **link** layer header for traffic. The specific name for this header format is Ethernet (when we're using a wired connection).
    - Just like we use TCP or UDP at the transport layer, or IP at the Internet layer, we use Ethernet at the link layer.

Slide 46



Link (Ethernet)

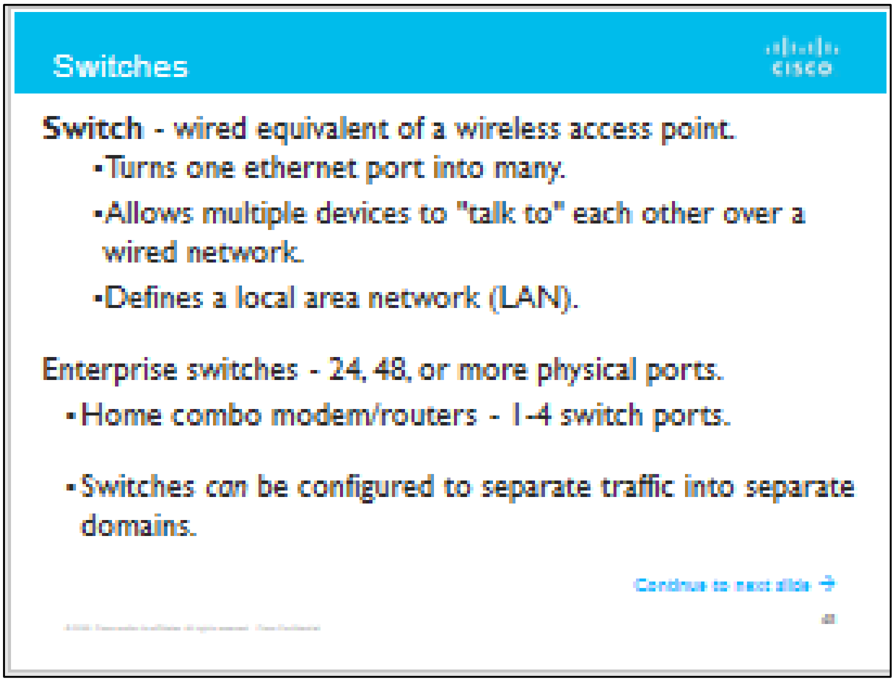
NetAcad Data Link Addresses Example

44

- Every time we transmit a packet across a network, we need to rewrite the source and destination MAC addresses, because the packet will be transiting between new physical devices.
- Click on the screenshot to launch the website directly or copy and paste for an illustration of how this works:

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.2.2

Slide 47



Switches

Switch - wired equivalent of a wireless access point.

- Turns one ethernet port into many.
- Allows multiple devices to "talk to" each other over a wired network.
- Defines a local area network (LAN).

Enterprise switches - 24, 48, or more physical ports.

- Home combo modem/routers - 1-4 switch ports.
- Switches can be configured to separate traffic into separate domains.

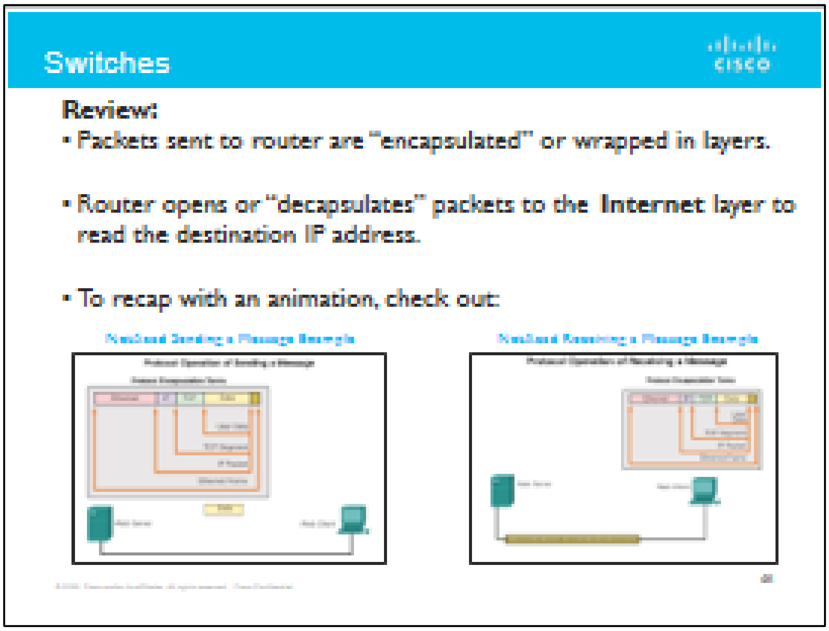
Continue to next slide →

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.1.3

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.1.4

- A switch is the wired equivalent of a wireless access point.
- You can think of a switch's job in the following ways:
  - It turns one Ethernet port into many.
  - It allows multiple devices to "talk to" each other over a wired network.
- A switch defines a local area network (LAN).
- Enterprise switches can have 24 ports, 48 ports, or even more ports.
  - Smaller switches exist too. Most home combo modem/routers have 1-4 switch ports available for wired clients.
- By default, hosts connected to the Ethernet ports on a switch can communicate with one another.
  - Switches *can* be configured to separate traffic into separate domains.
- How does this work? It involves MAC addresses (the address for the **link** layer on the TCP/IP stack).

Slide 48



Switches

Review:

- Packets sent to router are “encapsulated” or wrapped in layers.
- Router opens or “decapsulates” packets to the Internet layer to read the destination IP address.
- To recap with an animation, check out:

NetAcad Sending a Message Example
Protocol Operation of Sending a Message
NetAcad Receiving a Message Example
Protocol Operation of Receiving a Message
48

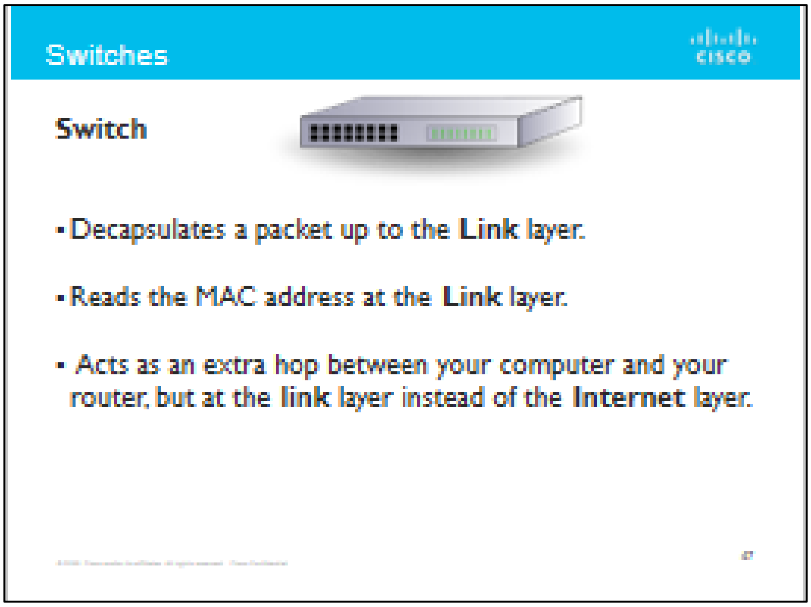
https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.1.3

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#3.3.1.4

Review:

- When you send a packet to your router, recall that you wrap it up (“encapsulate” it) in various layers to help it get where it needs to go.
- Your home router opens that packet up (i.e., “decapsulate” it) as far as the **Internet** layer on the TCP/IP stack so that it can read the destination IP address.
- To recap with an animation, check out these two slides: Click on the individual screen shots or click 3.3.1.3 (Links to an external site.) & 3.3.1.4 (Links to an external site.)
- A switch does something similar, but it only decapsulates a packet up to the **link** layer, that is, just enough to read the MAC address.
  - Recall how, with IP routing, several hops are necessary to get from a source to a destination.
  - A switch acts as an extra hop between your computer and your router, but at the **link** layer instead of the **Internet** layer.

Slide 49



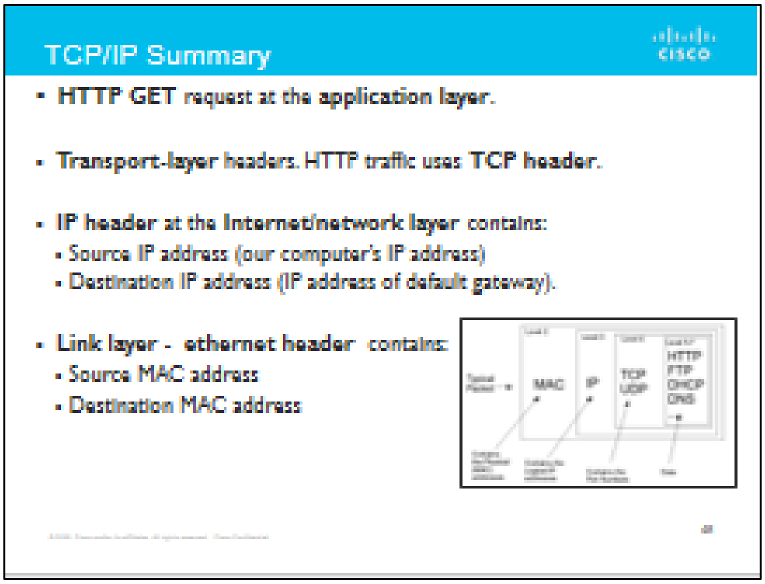
Switches

Switch

- Decapsulates a packet up to the **Link** layer.
- Reads the MAC address at the **Link** layer.
- Acts as an extra hop between your computer and your router, but at the **link** layer instead of the **Internet** layer.

- A switch does something similar to a router, but it only decapsulates a packet up to the **link** layer, that is, just enough to read the MAC address.
  - Recall how, with IP routing, several hops are necessary to get from a source to a destination.
  - A switch acts as an extra hop between your computer and your router, but at the **link** layer instead of the **Internet** layer.

Slide 50



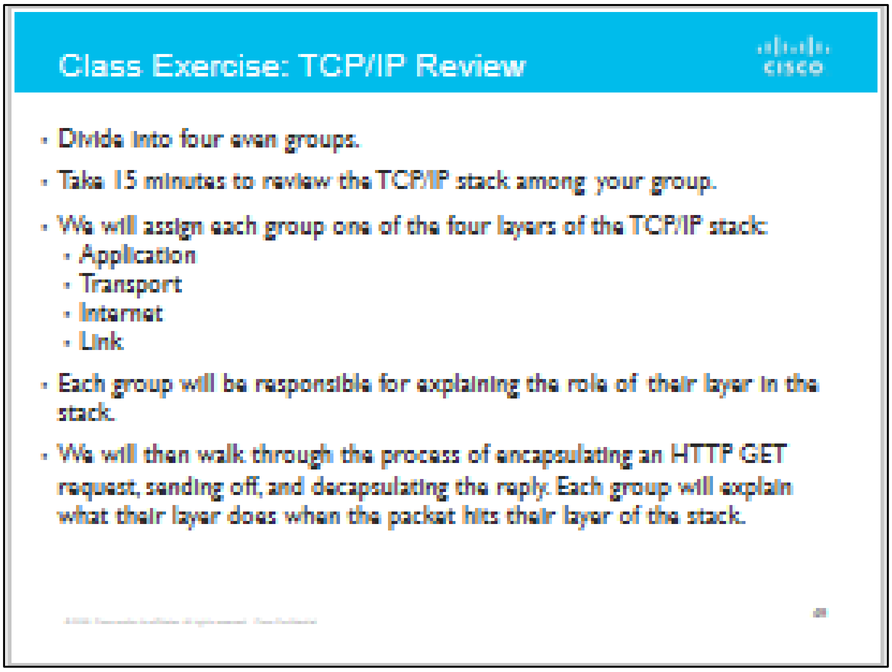
TCP/IP Summary

- HTTP GET request at the application layer.
- Transport-layer headers. HTTP traffic uses TCP header.
- IP header at the Internet/network layer contains:
  - Source IP address (our computer’s IP address)
  - Destination IP address (IP address of default gateway).
- Link layer - ethernet header contains:
  - Source MAC address
  - Destination MAC address

Typical Packet
MAC
IP
TCP
UDP
HTTP
FTP
DHCP
DNS
Data

- We start with the actual message we want to send to the web server. This is an **HTTP GET** request, and is at the a**pplication layer**.
- We then add **transport-layer** headers. For our HTTP traffic, we use a **TCP header**.
- Then, we wrap an **IP header** around that. This header has the Source IP address (our computer’s IP address), and the Destination IP address (the IP address of our default gateway). This is at the **Internet/network layer**.
- Finally, at the **link layer**, we wrap the packet in an **ethernet header** by encoding our Source MAC address (the physical address of our computer) and Destination MAC address (the physical address of our default gateway).

Slide 51

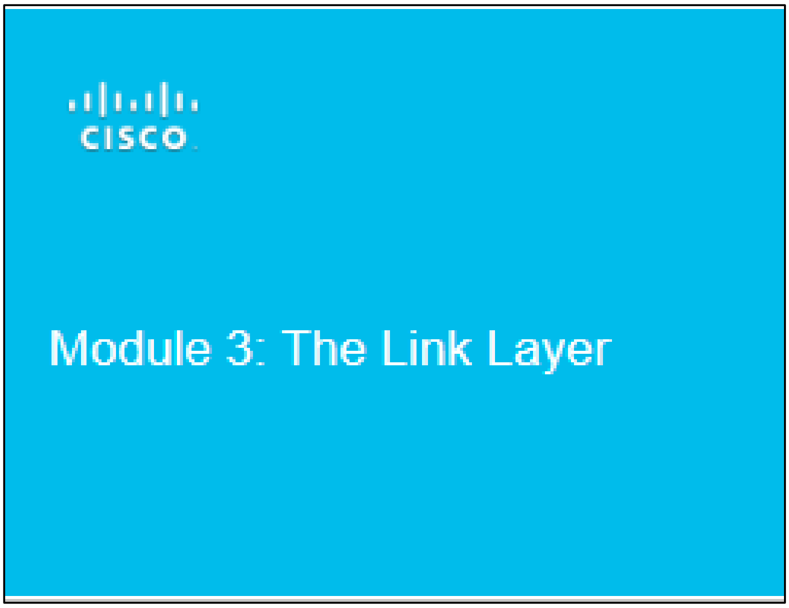


Class Exercise: TCP/IP Review

- Divide into four even groups.
- Take 15 minutes to review the TCP/IP stack among your group.
- We will assign each group one of the four layers of the TCP/IP stack:
  - Application
  - Transport
  - Internet
  - Link
- Each group will be responsible for explaining the role of their layer in the stack.
- We will then walk through the process of encapsulating an HTTP GET request, sending off, and decapsulating the reply. Each group will explain what their layer does when the packet hits their layer of the stack.

- Divide students into four even groups.
- Take 15 minutes to review the TCP/IP stack among each group.
- Assign one of the four layers of the TCP/IP stack to each group:
  - Application
  - Transport
  - Internet
  - Link
- Each group will be responsible for explaining the role of their layer in the stack.
- We will then walk through the process of encapsulating an HTTP GET request, sending it off, and decapsulating the reply. Each group will explain what their layer does when the packet hits their layer of the stack.

Slide 52


Module 3: The Link Layer

Module 3: The Link Layer

Slide 53

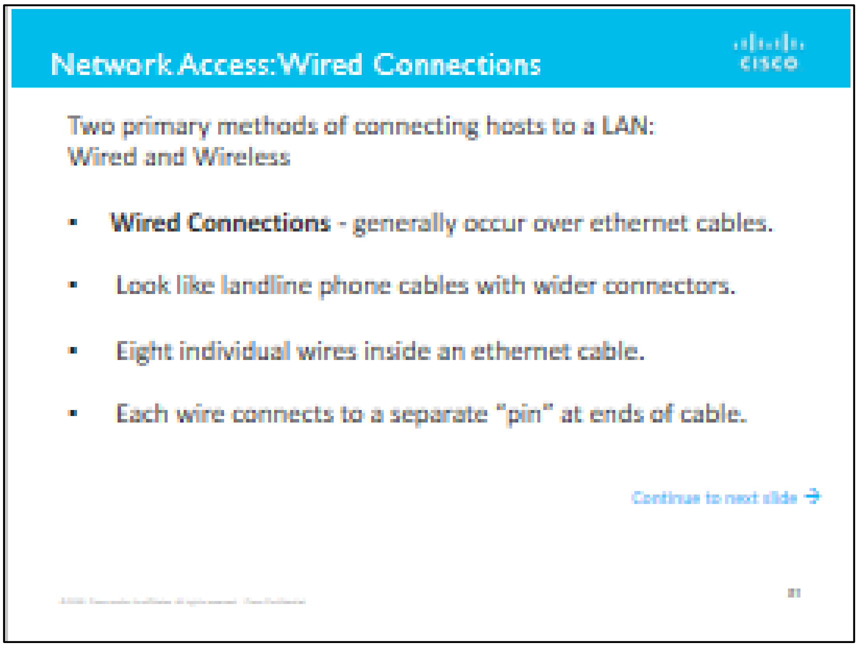
Modules 1 & 2 Kahoot! Review

https://play.kahoot.it/#/k/0ecf4263-b94e-47dc-9a80-521d8b2b4bc6

When you click on the logo a start screen will appear. Instructor will have the option to choose 1:1 play where students use their individual devices or shared devices for small groups.

For more information on how to play Kahoot! visit:
https://files.getkahoot.com/academy/Kahoot_Academy_Getting_Started_Guide_2nd_Ed_-_June_2016.pdf

Slide 54



Network Access:Wired Connections

Two primary methods of connecting hosts to a LAN:
Wired and Wireless

- **Wired Connections** - generally occur over ethernet cables.
- Look like landline phone cables with wider connectors.
- Eight individual wires inside an ethernet cable.
- Each wire connects to a separate "pin" at ends of cable.

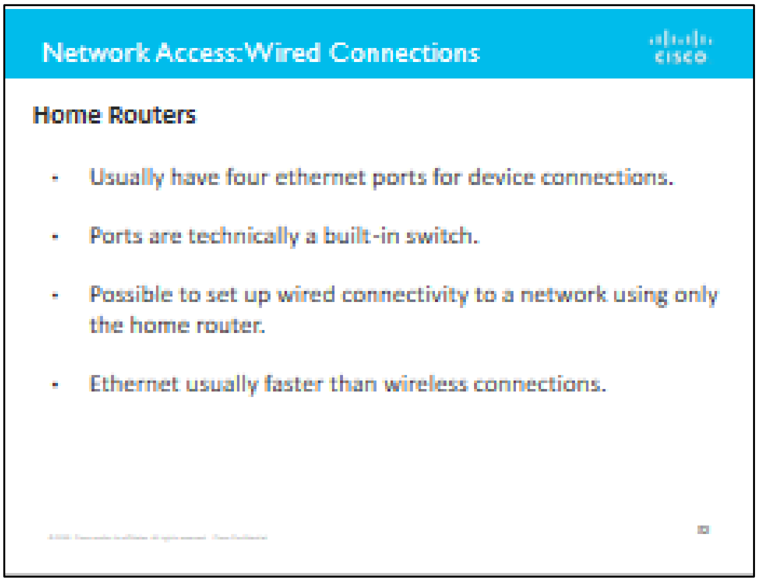
Continue to next slide →

- There are two primary methods of connecting hosts to a LAN: Wired and Wireless.

Wired Connections

- Wired connections generally occur over Ethernet cables.
- Ethernet cables look like landline phone cables, except the connector is wider.
- Inside an Ethernet cable, there are eight individual wires, each of which connects to a separate "pin" at both ends of the cable.

Slide 55



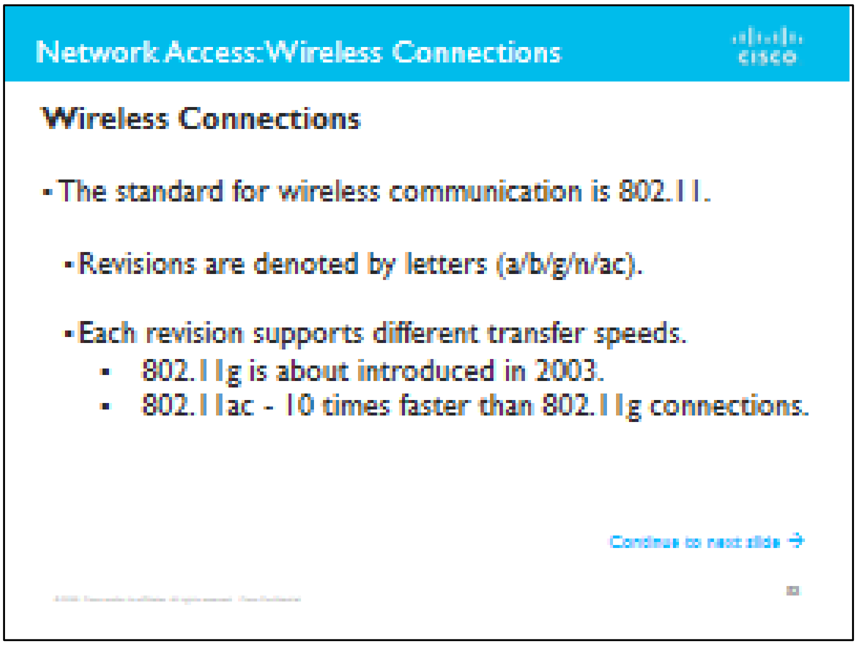
Network Access: Wired Connections

Home Routers

- Usually have four ethernet ports for device connections.
- Ports are technically a built-in switch.
- Possible to set up wired connectivity to a network using only the home router.
- Ethernet usually faster than wireless connections.

- Most home routers have about four Ethernet ports available for device connections.
  - These ports are technically a built-in switch.
  - It is generally possible to set up wired connectivity to a network using only the home router.
- Ethernet tends to be considerably faster than wireless connections.

Slide 56



Network Access: Wireless Connections

Wireless Connections

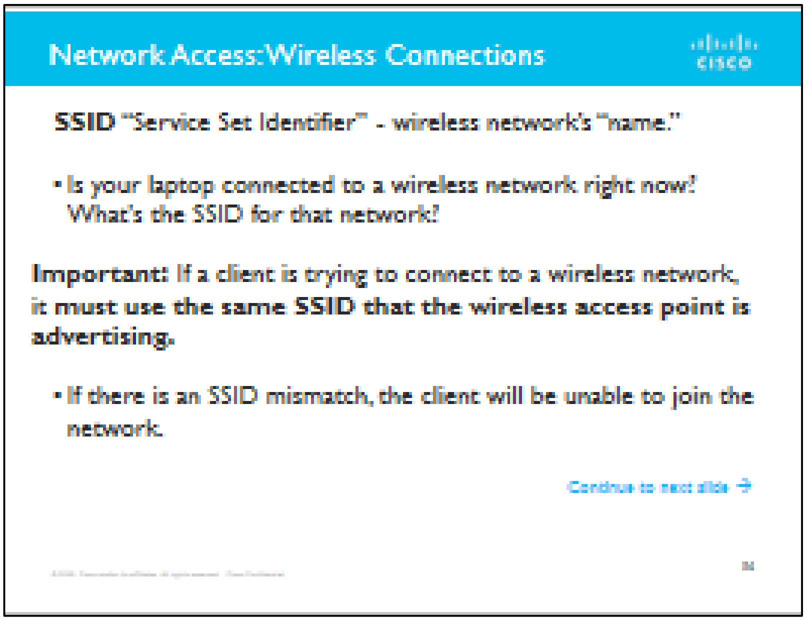
- The standard for wireless communication is 802.11.
  - Revisions are denoted by letters (a/b/g/n/ac).
  - Each revision supports different transfer speeds.
    - 802.11g is about introduced in 2003.
    - 802.11ac - 10 times faster than 802.11g connections.

Continue to next slide →

Wireless Connections

- Wireless connections occur over the air.
- The standard for wireless communication is 802.11, and there are several revisions to this standard.
- These revisions are denoted by letters (a/b/g/n/ac).
- Each revision supports different transfer speeds.
- 802.11g is about 14 years old (it was introduced in 2003).
- 802.11ac is relatively new.
- 802.11ac connections can be over 10 times faster than 802.11g connections.

Slide 57



Network Access: Wireless Connections

SSID "Service Set Identifier" - wireless network's "name."

- Is your laptop connected to a wireless network right now? What's the SSID for that network?

Important: If a client is trying to connect to a wireless network, **it must use the same SSID that the wireless access point is advertising.**

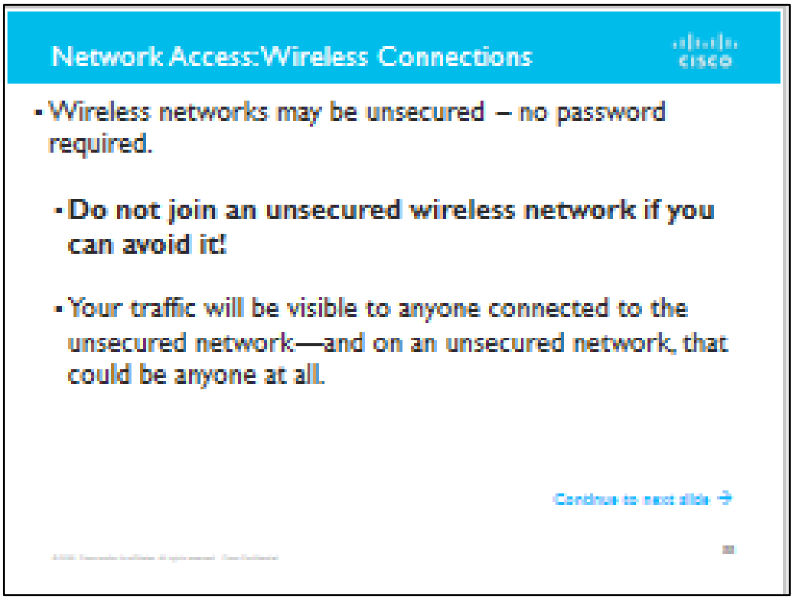
- If there is an SSID mismatch, the client will be unable to join the network.

Continue to next slide →

Wireless Connections

- A wireless network is identified by an **SSID**, "Service Set Identifier." You can think of this as being the wireless network's "name."
    - Is your laptop connected to a wireless network right now? What's the SSID for that network?
- **Important:** If a client is trying to connect to a wireless network, it must use the same SSID that the wireless access point is broadcasting.
    - If there is a mismatch, the client will be unable to join the network.
- Wireless networks may be unsecured. Any host can join an unsecured network.
    - If you can avoid it, do not join a wireless network which is not secured by a password!
    - Your traffic will be visible to anyone connected to the network—and on an unsecured network, that could be anyone at all.

Slide 58



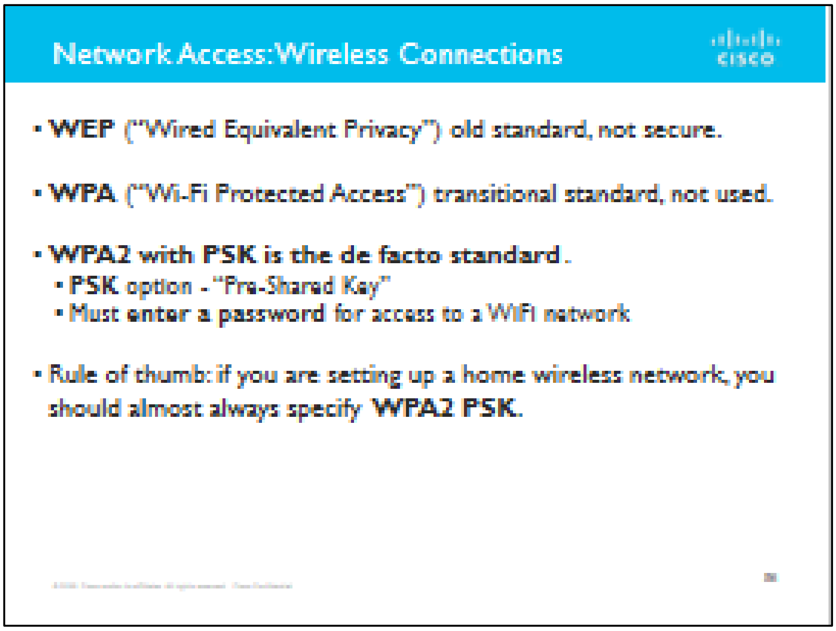
Network Access: Wireless Connections

- Wireless networks may be unsecured – no password required.
  - **Do not join an unsecured wireless network if you can avoid it!**
  - Your traffic will be visible to anyone connected to the unsecured network—and on an unsecured network, that could be anyone at all.

Continue to next slide →

- Wireless networks may be unsecured. Any host can join an unsecured network.
  - If you can avoid it, **do not join a wireless network which is not secured by a password!**
  - Your traffic will be visible to anyone connected to the network—and on an unsecured network, that could be anyone at all!
- Wireless networks may also be secured, and there are a few different types of security.

Slide 59

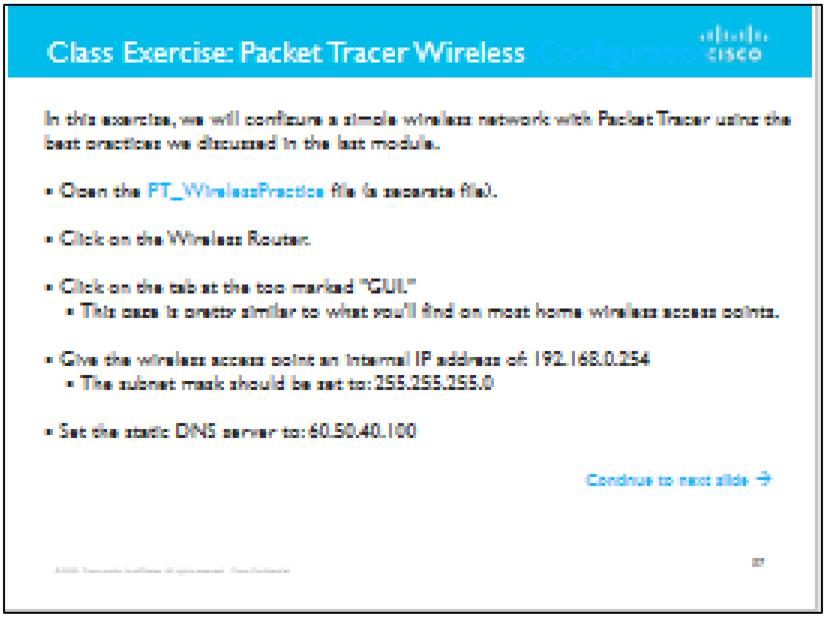


Network Access: Wireless Connections

- **WEP** ("Wired Equivalent Privacy") old standard, not secure.
- **WPA** ("Wi-Fi Protected Access") transitional standard, not used.
- **WPA2 with PSK is the de facto standard.**
  - PSK option - "Pre-Shared Key"
  - Must enter a password for access to a WiFi network
- Rule of thumb: if you are setting up a home wireless network, you should almost always specify **WPA2 PSK**.

- The **WEP** ("Wired Equivalent Privacy") standard was introduced about 20 years ago.
  - WEP is not considered secure anymore.
  - A WEP password can be broken by an attacker in less than three seconds.
- The replacement for WEP is called **WPA2**.
  - Why "2"?
  - **WPA** ("**WiFi Protected Access**") was introduced as a transitional standard, compatible with older hardware that had previously only been used for WEP. Once older hardware was transitioned out of the marketplace, WPA was replaced with WPA2.
- Today, **WPA2** is the de facto standard.
- **WPA2** is most often specified with the **PSK** option. PSK stands for "**Pre-Shared Key**," and this just means that you must enter a password for access to a Wi-Fi network secured in this way.
- Rule of thumb: if you are setting up a home wireless network, you should almost always specify **WPA2 PSK**.

Slide 60



Class Exercise: Packet Tracer Wireless Configuration

In this exercise, we will configure a simple wireless network with Packet Tracer using the best practices we discussed in the last module.

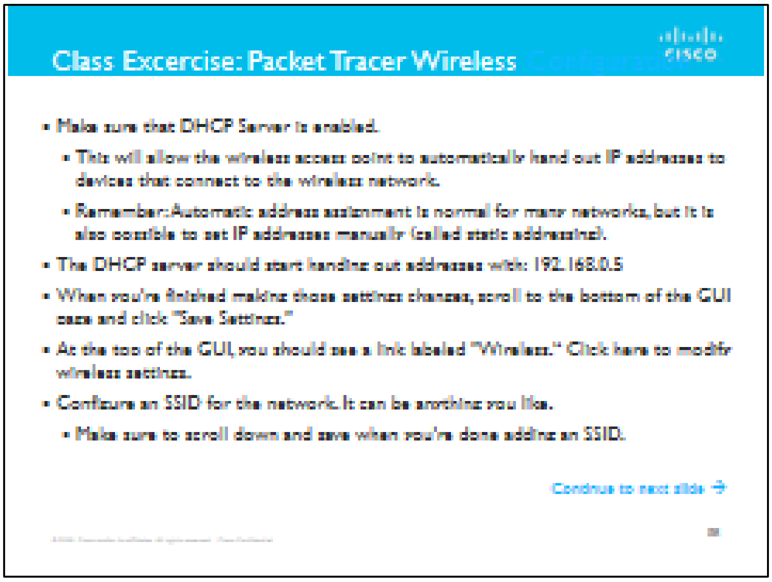
- Open the PT_WirelessPractice file (a separate file).
- Click on the Wireless Router.
- Click on the tab at the top marked "GUI."
  - This page is pretty similar to what you'll find on most home wireless access points.
- Give the wireless access point an internal IP address of: 192.168.0.254
  - The subnet mask should be set to: 255.255.255.0
- Set the static DNS server to: 60.50.40.100

Continue to next slide →

- In this exercise, we will configure a simple wireless network with Packet Tracer using the best practices we discussed in the last module.

- Open the PT_WirelessPractice file.
- Click on the Wireless Router.
- Click on the tab at the top marked "GUI."
  - This page is pretty similar to what you'll find on most home wireless access points.
- Give the wireless access point an internal IP address of: 192.168.0.254
  - The subnet mask should be set to: 255.255.255.0
- Set the static DNS server to: 60.50.40.100
- Make sure that DHCP Server is enabled.
  - This will allow the wireless access point to automatically hand out IP addresses to devices that connect to the wireless network.
  - Remember: Automatic address assignment is normal for many networks, but it is also possible to set IP addresses manually (called static addressing).
- The DHCP server should start handing out addresses with: 192.168.0.5
- When you're finished making those settings changes, scroll to the bottom of the GUI page and click "Save Settings."
- At the top of the GUI, you should see a link labeled "Wireless.“ Click here to modify wireless settings.
- Configure an SSID for the network. It can be anything you like.
  - Make sure to scroll down and save when you're done adding an SSID.

Slide 61



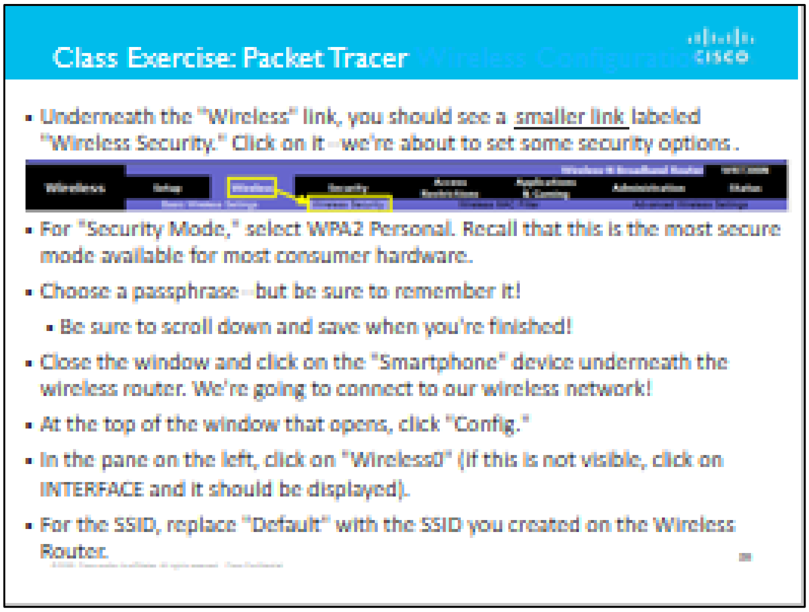
Class Excercise: Packet Tracer Wireless Configuration

- Make sure that DHCP Server is enabled.
  - This will allow the wireless access point to automatically hand out IP addresses to devices that connect to the wireless network.
  - Remember: Automatic address assignment is normal for many networks, but it is also possible to set IP addresses manually (called static addressing).
- The DHCP server should start handing out addresses with: 192.168.0.5
- When you're finished making those settings changes, scroll to the bottom of the GUI page and click "Save Settings."
- At the top of the GUI, you should see a link labeled "Wireless." Click here to modify wireless settings.
- Configure an SSID for the network. It can be anything you like.
  - Make sure to scroll down and save when you're done adding an SSID.

Continue to next slide →

- Make sure that DHCP Server is enabled.
  - This will allow the wireless access point to automatically hand out IP addresses to devices that connect to the wireless network.
  - Remember: Automatic address assignment is normal for many networks, but it is also possible to set IP addresses manually (and this is called static addressing).
- The DHCP server should start handing out addresses with 192.168.0.5.
- When you're finished making those settings changes, scroll to the bottom of the GUI page and click "Save Settings."
- At the top of the GUI, you should see a link labeled "Wireless". Click here to modify wireless settings.
- Configure an SSID for the network. It can be anything you like.
  - Make sure to scroll down and save when you're done adding an SSID.

Slide 62



Class Exercise: Packet Tracer Wireless Configuration

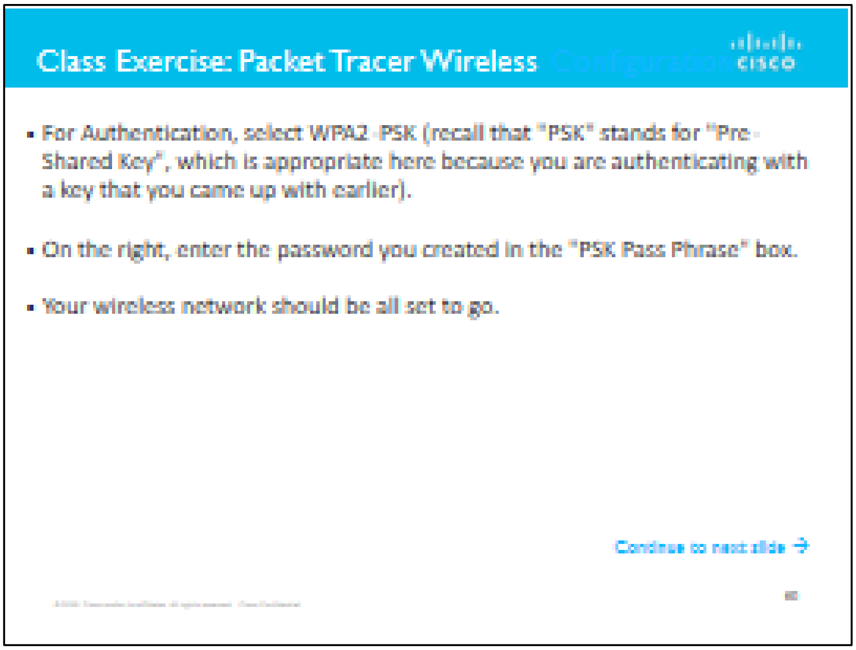
- Underneath the "Wireless" link, you should see a smaller link labeled "Wireless Security." Click on it--we're about to set some security options.

- For "Security Mode," select WPA2 Personal. Recall that this is the most secure mode available for most consumer hardware.
- Choose a passphrase--but be sure to remember it!
  - Be sure to scroll down and save when you're finished!
- Close the window and click on the "Smartphone" device underneath the wireless router. We're going to connect to our wireless network!
- At the top of the window that opens, click "Config."
- In the pane on the left, click on "Wireless0" (If this is not visible, click on INTERFACE and it should be displayed).
- For the SSID, replace "Default" with the SSID you created on the Wireless Router.

https://150566673.netacad.com/courses/487683/files/46796301/download?wrap=1

- Underneath the "Wireless" link, you should see a smaller link labeled "Wireless Security." Click on it--we're about to set some security options.
- For "Security Mode", select WPA2 Personal. Recall that this is the most secure mode available for most consumer hardware.
- Choose a passphrase--but be sure to remember it!
  - Be sure to scroll down and save when you're finished.
- Close the window and click on the "Smartphone" device underneath the wireless router. We're going to connect to our wireless network.
- At the top of the window that opens, click "Config."
- In the pane on the left, click on "Wireless0." If this is not visible, click on INTERFACE and it should be displayed.
- For the SSID, replace "Default" with the SSID you created on the Wireless Router.

Slide 63



Class Exercise: Packet Tracer Wireless Configuration

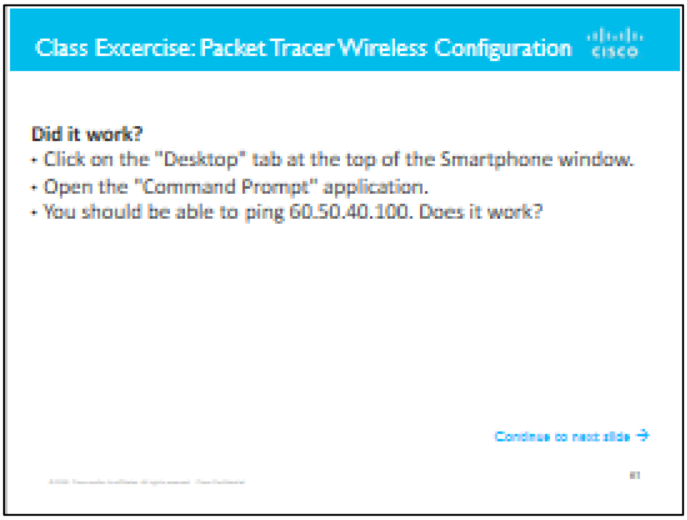
- For Authentication, select WPA2-PSK (recall that "PSK" stands for "Pre-Shared Key", which is appropriate here because you are authenticating with a key that you came up with earlier).
- On the right, enter the password you created in the "PSK Pass Phrase" box.
- Your wireless network should be all set to go.

Continue to next slide →

https://150566673.netacad.com/courses/487683/files/46796301/download?wrap=1

- For Authentication, select WPA2-PSK (recall that "PSK" stands for "Pre-Shared Key", which is appropriate here because you are authenticating with a key that you came up with earlier).
- On the right, enter the password you created in the "PSK Pass Phrase" box.
- Your wireless network should be all set to go.

Slide 64



Class Excercise: Packet Tracer Wireless Configuration

Did it work?

- Click on the "Desktop" tab at the top of the Smartphone window.
- Open the "Command Prompt" application.
- You should be able to ping 60.50.40.100. Does it work?

Continue to next slide →

https://150566673.netacad.com/courses/487683/files/46796301/download?wrap=1

- Click on the "Desktop" tab at the top of the Smartphone window.
- Open the "Command Prompt" application.
- You should be able to ping 60.50.40.100. Does it work?

PT_WirelessPractice.pkt

- Underneath the "Wireless" link, you should see a smaller link labeled "Wireless Security." Click on it--we're about to set some security options.
- For "Security Mode", select WPA2 Personal. Recall that this is the most secure mode available for most consumer hardware.
- Choose a passphrase--but be sure to remember it!
    - Be sure to scroll down and save when you're finished!
- Close the window and click on the "Smartphone" device underneath the wireless router. We're going to connect to our wireless network!
- At the top of the window that opens, click "Config".
- In the pane on the left, click on "Wireless0". (If this is not visible, click on INTERFACE and it should be displayed).
- For the SSID, replace "Default" with the SSID you created on the Wireless Router.
- For Authentication, select WPA2-PSK (recall that "PSK" stands for "Pre-Shared Key", which is appropriate here because you are authenticating with a key that you came up with earlier).
- On the right, enter the password you created in the "PSK Pass Phrase" box.
- Your wireless network should be all set to go!

Slide 65

Module 3 Packet Tracer Kahoot!

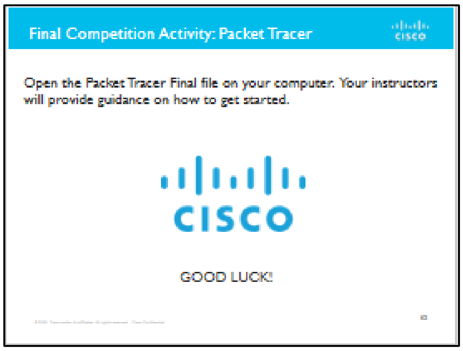
Https://play.kahoot.it/#/k/e781e168-5e89-42d0-939c-303dbdded245

When you click on the logo a Start screen will appear.

Instructor will have the option to choose 1:1 playing where students use their individual devices or Shared devices for small groups.

Need more information on how to play Kahoot? Visit: https://files.getkahoot.com/academy/Kahoot_Academy_Getting_Started_Guide_2nd_Ed_-_June_2016.pdf

Slide 66



Final Competition Activity: Packet Tracer

Open the Packet Tracer Final file on your computer. Your instructors will provide guidance on how to get started.

GOOD LUCK!

There are three pages dedicated to Cisco Slide 66

https://150566673.netacad.com/courses/487683/files/46885892/download?wrap=1

https://150566673.netacad.com/courses/487683/files/46676792/download

Open the Packet Tracer Final file on your computer and follow the on-screen instructions to proceed. The instructor will provide guidance on how to get started.

Read instructions and test software before the activity.

Overview: Instructors must download required software on to computers before activity. Ensure students have correct peer assignments with . Open the Packet Tracer server .pka software. Have students open client .pka files for their peer. When connected to the Packet Tracer server the Peer icon will turn blue. Start game on provided Packet Tracer server .pka file. Students begin the exercise. Stop game when the time is up. Check scores.

Note: To function correctly, the Packet Tracer server and clients must be on the same network. Because all networks are different, in some cases the scoring server could have issues connecting to the students’ clients and not show scores. If so, the instructors will check each student client for the individual scores.

Slide 66 Continued

Instructions for the Instructor:

Pre-work:

1- Download the latest version of Packet Tracer on each computer at https://www.netacad.com/group/offerings/packet-tracer

2- Assign each laptop a peer number e.g., peer 1, 2, 3, 4, 5,...29, etc.

3- Download the client .zip file below and put the client .pka file on the laptops, or make available for each team to download. There are 30 .pka files (0-29), one for each team. Each laptop needs to have a unique file (e.g. P1, P2, P3... P29) that aligns with the peer assignment give in the step above.

4- Load the server .pka file on the instructor's laptop (below).

Advanced Camp 2017 client v19 Clients.zip

Advanced Camp 2017 Server v2.pka

5- All laptops need to be on the same network.

https://www.netacad.com/group/offerings/packet-tracer/

Instructor launches the server on this computer.

Students launch client.

- Locate the cloud icon that reads "Peer followed by a number (e.g., Peer33 -- with NO space between Peer and number)" and double click on it.
- Connection Type: don't change, should be "Outgoing"
- Enter the IP address of the Packet Tracer server (on server host computer, type "ipconfig" to find IP address)
- Peer port number remains the same (38000)
- Enter in the Peer Network Name = the peer number you assigned to each laptop. "Peer1", "Peer2", "Peer3", etc, The peer number will also be the same as the peer cloud in the packet tracer when it is open as well as in the .pka file name (...P**1**.pka)
- Password = "cisco"
- Click "connect" The cloud will turn blue on both the client and the server. If the information is entered wrong, it will show as red. If red, check that all the above is correct.

Slide 66 Continued

Once all clients are connected (blue on the server), then click the "Start Game" button on the server (a separate little window that opens up).

The instructions will pop up on the client and the students and now click on the "Game" cloud to open the scenario.

NOTE: A timer is not built in. You can start a timer on your own, so the students know how long they have to complete the task. It is recommended you give at least 1 hour. You will be able to track the progress of the players.

Once the time has passed, click the "Stop Game" button.

During the competition, you will see progress bars for each user. It may not start at 0 and that is OK because everyone should start at the same place. Everyone can see each other students progress so keep in mind that scoring is not instantaneous.

The last task is to have each student save the file with a new name (File -->Save As -->name it with their name and peer number – no space.).

The winner is determined by who completed the most tasks in the time given. The scoreboard should give the percentage for each student, but it does take time for the scores to become available. The team with the highest percentage wins. If there is a scoring problem, you can open the Packet Tracer in question on the student's laptop (or copy the file to another laptop) and grade it manually.

If no scores show up on the scoreboard you will need to grade each Packet Tracer manually.

Extensions -->Activity Wizard --> password "Cyb3rCamp2017" --> check activity, check activity (again) -- > Check Results (on smaller window) -- > Assessment Items and Connectivity tests. This will tell you what the students did or did not get right based on the grading. Some of the activities they do will not be graded command-by-command but rather by a connectivity test.

NOTE: Chat is enabled. This allows players to chat with each other as well as the server. It is recommended that they do not use the chat.

Instructor Post-Survey

Dear Camp Coordinators & Instructors,

Thank you again for taking the time to give us your valuable feedback on our AFA CyberCamp program. The Camp Coordinator/Instructor Post-survey should take 5-10 minutes.

See you all next Summer!

2018 Instructor Post-Survey

https://www.surveymonkey.com/r/MZ7MBJH

SECURING NETWORKS, SECURING FUTURES

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM

For more information on how to participate in the CyberPatriot National Youth Cyber Defense Competition, visit www.uscyberpatriot.org or contact info@uscyberpatriot.org

Scan to join our mailing list.