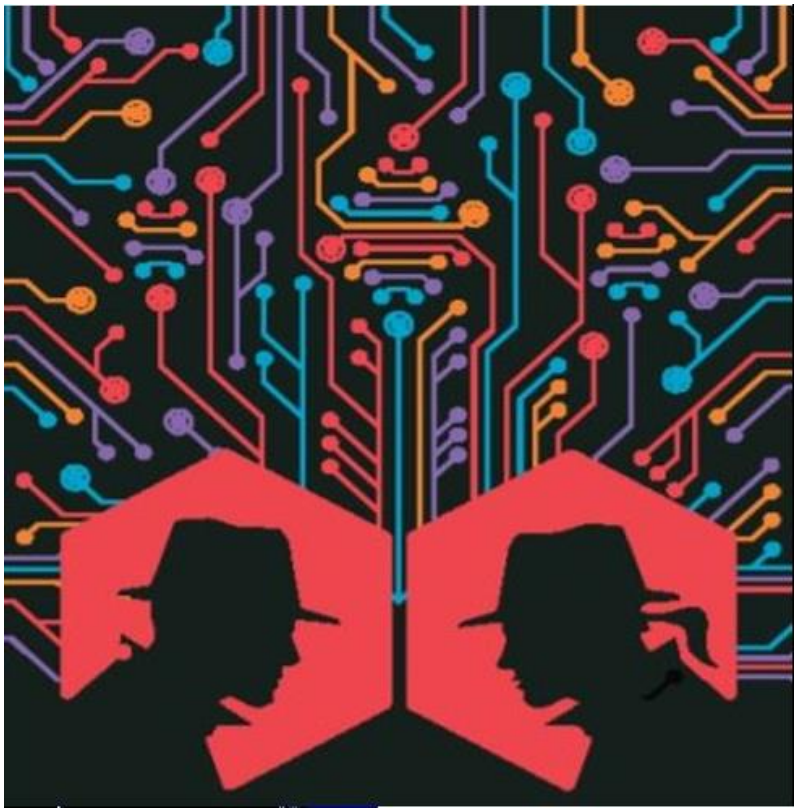


THE INCIDENT RESPONSE FIELD MANUAL

A consolidated guide for the Incident Responder

By Sampson T. Chandler

Senior Analyst at RSA

TABLE OF CONTENTS

INTRODUCTION

One of the most important (if not the most important) factors in keeping your company secure is providing and encouraging education/training.

"One of the best IDS/IPS is well trained users." – Aaron Scantlin

Some skills that are essential:

- Note taking / Organization
  - This will help in creating and making reports better.
  - Can be used as training materials for other employees
  - Accessing information in time sensitive situations
- Interpersonal Skills
  - Effective communication – Between teams and customers
- Public Speaking and Presentation Skills
  - Creating better presentations
  - Assists with training groups
  - Presenting ideas internally or externally
  - Reporting to executives or customers in general

The following is a condensed guide for Incident response to be referenced in assisting with developing, implementing, and improving, your incident response plan.

Other Resources:
Books

- DFIR intro - By Scott J. Roberts.
- The Practice of Network Security Monitoring: Understanding Incident Detection and Response - Richard Bejtlich's book on IR.

Communities

- augmentd - Community driven site provididing a list of searches that can be implemented in and executed with a variety of common security tools.
- Sans DFIR mailing list - Mailing list by SANS for DFIR.
- Slack DFIR channel - Slack DFIR Communitiy channel - Signup here.

Playbooks

- Demisto Playbooks Collection - Playbooks collection.
- IRM - Incident Response Methodologies by CERT Societe Generale.
- IR Workflow Gallery - Different generic incident response workflows, e.g. for malware outbreak, data theft, unauthorized access,... Every workflow constists of seven steps: prepare, detect, analyze, contain, eradicate, recover, post-incident handling. The workflows are online available or for download.

- PagerDuty Incident Response Documentation - Documents that describe parts of the PagerDuty Incident Response process. It provides information not only on preparing for an incident, but also what to do during and after. Source is available on GitHub.

Videos

- Demisto IR video resources - Video Resources for Incident Response and Forensics Tools.
- The Future of Incident Response - Presented by Bruce Schneier at OWASP AppSecUSA 2015.

Acknowledgements:

To the people who have helped and inspired me, thank you.

- Eric Guillen – My mentor – Lead Information Security Engineer at CenturyLink
- Brian Griffiths – VP of Operations at 2 Point Technology
- Lauren Proehl – Lead Information Security Engineer at CenturyLink
- Tim Dillman – Project Manager, PTC Security at KC Southern Railway Company
- Cory Kennedy – Adversary Researcher at CenturyLink
- Britney Hommertzheim – Director of Information Security at AMC
- Aaron Scantlin – Security Analyst at University of Missouri
- Alex Lauerman – Founder of TrustFoundry
- Nathan Kettlewell – Manager, Offensive Security Services
- Nathan Maxwell – Infosec and Network Administrator at CCI
- Justin Ferguson – Senior Application Security Engineer at New Context
- Bill Swearingen - Sr. Director Global Cyber Defense and Security Technology Innovation at CenturyLink
- Bryan Geraghty – Security Consultant at Security PS
- Julie Fugett – CISO at The University of Kansas
- Paul Rixon
- Noah Fugate – This kid is going places
- Carl Fugate – Chief Architect of Network Infrastructure at Gapgemini
- Kevin Bennett – Communications and Collaborations at Epiq
- Michael Ginsberg
- Caleb Christopher
- Mike Wyatt
- Eric Foster

And everyone else at SecKC

PREPARATION

Incident Questionnaire Checklist

This cheat sheet offers tips for assisting incident handlers in assessing the situation when responding to a qualified incident by asking the right questions.

(From Lenny Zeltser - https://zeltser.com/security-incident-questionnaire-cheat-sheet)

Understand the Incident's Background

- What is the nature of the problem, as it has been observed so far?
- How was the problem initially detected? When was it detected and by whom?
- What security infrastructure components exist in the affected environment? (e.g., firewall, anti-virus, etc.)
- What is the security posture of the affected IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?
    - What groups or organizations were affected by the incident? Are they aware of the incident?
    - Were other security incidents observed on the affected environment or the organization recently?
- Define Communication Parameters
    - Which individuals are aware of the incident? What are their names and group or company affiliations?
    - Who is designated as the primary incident response coordinator?
    - Who is authorized to make business decisions regarding the affected operations? (This is often an executive.)
    - What mechanisms will the team to communicate when handling the incident? (e.g., email, phone conference, etc.) What encryption capabilities should be used?
    - What is the schedule of internal regular progress updates? Who is responsible for them?
    - What is the schedule of external regular progress updates? Who is responsible for leading them?
    - Who will conduct "in the field" examination of the affected IT infrastructure? Note their name, title, phone (mobile and office), and email details.
    - Who will interface with legal, executive, public relations, and other relevant internal teams?
- Assess the Incident's Scope
    - What IT infrastructure components (servers, websites, networks, etc.) are directly affected by the incident?
    - What applications and data processes make use of the affected IT infrastructure components?
    - Are we aware of compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)
    - What are the possible ingress and egress points for the affected environment?

    - What theories exist for how the initial compromise occurred?
    - Does the affected IT infrastructure pose any risk to other organizations?
- Review the Initial Incident Survey's Results
    - What analysis actions were taken to during the initial survey when qualifying the incident?
    - What commands or tools were executed on the affected systems as part of the initial survey?
    - What measures were taken to contain the scope of the incident? (e.g., disconnected from the network)
    - What alerts were generated by the existing security infrastructure components? (e.g., IDS, anti-virus, etc.)
    - If logs were reviewed, what suspicious entries were found? What additional suspicious events or state information, was observed?
- Prepare for Next Incident Response Steps
    - Does the affected group or organization have specific incident response instructions or guidelines?
    - Does the affected group or organization wish to proceed with live analysis, or does it wish to start formal forensic examination?
    - What tools are available to us for monitoring network or host-based activities in the affected environment?
    - What mechanisms exist to transfer files to and from the affected IT infrastructure components during the analysis? (e.g., network, USB, CD-ROM, etc.)
    - Where are the affected IT infrastructure components physically located?
    - What backup-restore capabilities are in place to assist in recovering from the incident?
    - What are the next steps for responding to this incident? (Who will do what and when?)

Key Incident Response Steps

1) Preparation: Gather and learn the necessary tools, become familiar with your environment.
2) Identification: Detect the incident, determine its scope, and involve the appropriate parties.
3) Containment: Contain the incident to minimize its effect on neighboring IT resources.
4) Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.
5) Recovery: Restore the system to normal operations, possibly via reinstall or backup.
6) Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.

Link to Table of Contents

DEVELOPING A SUCCESSFUL INCIDENT RESPONSE PLAN

"Visibility and business context are core requirements for a successful incident response plan. Know the key resources needed for your business's success, and in the event of an incident, you'll be prepared to protect your organizations critical assets." – Gary Hayslip of Webroot.

The biggest challenge is getting the IR plan aligned with the actual capabilities and resources of the organization. The gold-standard IR plan assumes a gold-standard detection and response capability something that doesn't exist in most organizations.

A strategically implemented incident response plan must align with the company culture, business goals and technical capabilities of the organization to be successful in the long term

There is no "one size fits all" incident response plan for every business, but here are some things to consider in building one to make sure your company, or customer's, can handle an incident quickly, efficiently, and with minimal damage.

A strategically implemented incident response plan must align with the company culture, business goals and technical capabilities of the organization to be successful in the long term.

Crisis situations demand calm leadership. Executive-level tabletop exercises are also a proven approach to ensure the executive team is prepared to manage a large-scale breach scenario, including how to answer tough questions and make business-appropriate decisions under pressure.

- **Prepare**
    - Make Incident Response Plan dual purpose
        - Focused log data can benefit IT operations tremendously. Develop quarterly reports that show how central logging help security and operations
        - Integrate Incident Response into Project Management
    - Build Issue Focused Plans – Not a single plan for everything
        - Create a base template that can be modified for specific issues, or given information systems
        - Focus on most sensitive data and build our plan from there.
    - What defines an incident?
    - Create a severity chart and severity definitions
- **Build a team**
    - Compose internally, externally, or both.
- **Outline requirements and response times**
    - Create quick response guides that address specific scenarios or systems.
        - Should be most likely to happen scenarios
    - Ownership

        - The incident response plan and company policies must include business process owners, control owners, and data owners, to ensure the organizations objectives are met.
    - Develop communication plans and escalation matrix
- **Establish a disaster recovery strategy**
    - Partner with Diester Recovery and Business Continuity planning for cross pollination and building relationships.
- **Involve any relevant departments**
- **Train, Practice, and Repeat**
    - Education
        - Across all levels.
        - Offerings designed to meet people on their terms
        - Weekly security awareness email, posters on best practices, developing award system for people constantly showing they are following best practices.
    - After Action Review
        - Simulate test runs
        - Make a list of what went well, what didn't, and what could be improved on.
            8 Send list to everyone involved
        - Make changes based on findings and then repeat to verify changes work best

Keep a hard copy of your plan where it is easily accessible.

If you are storing your plan on the network, you may not be able to access it. Keep it on a external drive not connected to the network.

Link to Table of Contents

INCIDENT RESPONSE POLICY

An incident response policy, especially if drafted comprehensively and tested in advance, is an organization's most important shield against cyber-attacks. Organizations that rely a great extent on the Internet, computer networks, and deal with a vast amount of personal data can benefit a lot from investing in well-drafted incident response policies. This article discussed the key recommendations for drafting such policies

An incident response policy should be drafted carefully and include the following main components:

1. Identification of an incident response team

Incident response teams can be categorized into two groups, namely, centralized incident response teams and distributed incident response teams. Small organizations usually use the first category, whereas large organizations rely mainly on the second category because it allows them to effectively coordinate members located in culturally, linguistically, and legally diverse environments.

Irrespective of their type, incident response teams may comprise either organization's employees only or be outsourced partially or fully. The team description should include names, contact information, roles, and responsibilities of team members. For the sake of clarity, it is important to define and describe in detail the roles which each of the members will play in a case of an incident. Furthermore, it is essential for the organization to ensure that the members are not only mentioned in the document but also properly trained to perform their roles and responsibilities effectively. Therefore, the incident response policy should also indicate the number of trainings undertaken by each member of the response team.

The responsibilities of an incident handler (i.e., a person who serves as a security contact, has admin credentials and technical knowledge about information security incidents) and a resource manager (i.e., an individual who serves as a local authority and assesses the business impact of system's unavailability) should be distinguished separately.

2. Information about the system

The policy should include system details, such as network and data flow diagrams, hardware inventory, and logging data.

3. Incident handling and reporting procedures

Another crucial chapter of the policy should describe in detail the procedures for handling and reporting an incident (suspected or occurred). Next to guidelines on how to describe the incident (e.g., the timeline of the incident, the list of corrupted or unavailable files, mitigating mechanisms in place) as well as containment and eradication guidelines, such procedures should define what incidents will trigger response measures. By way of illustration, the procedures should answer the question of whether the organization is going to respond to a potential attack or the attack must be successful to trigger response measures.

The chapter governing incident handling and reporting procedures should include requirements for completing an incident intake report. The intake report needs to contain information about a contact person, the IP address and the physical location of the breached system, types of affected data, and a detailed description of compromised files containing personal or sensitive information. The actions being taken on the breached system should be documented in the intake report to serve for forensic analysis. Such documentation needs to take into consideration the following factors: the status of the incident, the summary of the incident, actions taken, chain of custody, impact assessments, contact information of the involved parties, a list of gathered evidence, and next steps to be taken.

4. "Lessons Learned"

An important aspect that is often omitted in an incident response policy is the "Lessons Learned" section. Using a meeting and a discussion among all parties involved, such "Lessons Learned" initiative may serve as a helpful tool in improving security measures in the organization and the incident handling process itself. Questions, such as "How well and adequately did staff and management perform when dealing with the incident?" "What information was needed sooner?", moreover, "What corrective actions can prevent similar incidents in the future?", may be a starting point to such a discussion.

5. Reporting to outside parties

An incident response policy may include timeframes and guidelines for reporting to third parties, e.g., reporting to IT personnel, security analysts, data protection or law enforcement authorities, media, affected external parties, and software, vendors. Depending on a jurisdiction, incident reporting may be required by law.

TIPS on Creating an Incident Response Policy:

1. Make it flexible

An incident response policy should be revised regularly to ensure that the document is up to date, includes relevant employees and outside parties, and responds to the newest trends in cybersecurity. Also, the definitions in the document should be broad enough to encompass all incident situations. Thus, if the document needs to be revised to address new security challenges, it will not be necessary to revise the definitions.

2. Ensure cooperation between organization's departments and staff

Successful drafting and implementation of an incident response policy requires close inter-organizational collaboration, especially in larger organizations. For example, handling a breach that has resulted in a loss of credit card data may require involvement not only of security experts for addressing software issues, but also PR specialists for drafting a public disclosure of the incident and customer support staff for discussing the breach with customers. Such an involvement should be initiated during the phase of policy planning, and not only during its implementation. Stakeholders that should be

engaged in the planning process may include internal and external IT, management, legal, and public relations teams.

3. Assess performance

The effectiveness of incident response procedures can be evaluated by using both quantitative and qualitative performance indicators. The time required for detecting, handling, investigating, and reporting an incident can be used as a quantitative indicator. The feedback provided by the members of the response team can serve as a qualitative indicator.

4. Do not forget testing

Simulating a breach may not only test the efficiency of an incident response policy but also contribute to identifying parts of the policy which need to be updated.

To summarize, incident response policies should address the following aspects of detecting an incident and responding to it: (1) appointing an incident response team comprised of internal and external stakeholders and their precise roles in handling of an incident; (2) technical information about the pre-incident status of organization's informational infrastructure; (3) definition and classification (ranking) of information security incidents within the organization; (4) detailed incident handling and responding procedures; (6) organizing a "Lessons learned" session; and (7) reporting to outside parties.

Irrespective of how well-written an incident response policy is, organizations should remain aware that, in the field of cyber-security, the strongest weapon remains prevention, which includes initial risk assessment, host and network security, malware prevention, and user awareness training.

Information Security Policies:

A high-grade ISP can make the difference between growing business and successful one. Improved efficiency, increased productivity, clarity of the objectives each entity has, understanding what IT and data should be secured and why, identifying the type and levels of security required and defining the applicable information security best practices are enough reasons to back up this statement. To put a period to this topic in simple terms, let's say that if you want to lead a prosperous company in today's digital era, you certainly need to have a good information security policy.

Link to Table of Contents

TOOLS

Adversary Emulation

- APTSimulator - Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised.
- Atomic Red Team (ART) - Small and highly portable detection tests mapped to the Mitre ATT&CK Framework.
- AutoTTP - Automated Tactics Techniques & Procedures. Re-running complex sequences manually for regression tests, product evaluations, generate data for researchers.
- Blue Team Training Toolkit (BT3) - Software for defensive security training, which will bring your network analysis training sessions, incident response drills and red team engagements to a new level.
- Caldera - Automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. It generates plans during operation using a planning system and a pre-configured adversary model based on the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™) project.
- DumpsterFire - Modular, menu-driven, cross-platform tool for building repeatable, time-delayed, distributed security events. Easily create custom event chains for Blue Team drills and sensor / alert mapping. Red Teams can create decoy incidents, distractions, and lures to support and scale their operations.
- Metta - Information security preparedness tool to do adversarial simulation.
- Network Flight Simulator - Lightweight utility used to generate malicious network traffic and help security teams to evaluate security controls and network visibility.
- Red Team Automation (RTA) - RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK.
- RedHunt-OS - Virtual machine for adversary emulation and threat hunting.

All in one Tools

- Belkasoft Evidence Center - The toolkit will quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps.
- CimSweep - Suite of CIM/WMI-based tools that enable the ability to perform incident response and hunting operations remotely across all versions of Windows.
- CIRTkit - CIRTKit is not just a collection of tools, but also a framework to aid in the ongoing unification of Incident Response and Forensics investigation processes.

- Cyber Triage - Cyber Triage remotely collects and analyzes endpoint data to help determine if it is compromised. It's agentless approach and focus on ease of use and automation allows companies to respond without major infrastructure changes and without a team of forensics experts. Its results are used to decide if the system should be erased or investigated further.
- Digital Forensics Framework - Open Source computer forensics platform built on top of a dedicated Application Programming Interface (API). DFF proposes an alternative to the aging digital forensics solutions used today. Designed for simple use and automation, the DFF interface guides the user through the main steps of a digital investigation so it can be used by both professional and non-expert to quickly and easily conduct a digital investigations and perform incident response.
- Doorman - osquery fleet manager that allows remote management of osquery configurations retrieved by nodes. It takes advantage of osquery's TLS configuration, logger, and distributed read/write endpoints, to give administrators visibility across a fleet of devices with minimal overhead and intrusiveness.
- Envdb - Envdb turns your production, dev, cloud, etc environments into a database cluster you can search using osquery as the foundation. It wraps the osquery process with a (cluster) node agent that can communicate back to a central location.
- Falcon Orchestrator - Extendable Windows-based application that provides workflow automation, case management and security response functionality.
- GRR Rapid Response - Incident response framework focused on remote live forensics. It consists of a python agent (client) that is installed on target systems, and a python server infrastructure that can manage and talk to the agent.
- Kolide Fleet - State of the art host monitoring platform tailored for security experts. Leveraging Facebook's battle-tested osquery project, Kolide delivers fast answers to big questions.
- Limacharlie - Endpoint security platform composed of a collection of small projects all working together that gives you a cross-platform (Windows, OSX, Linux, Android and iOS) low-level environment for managing and pushing additional modules into memory to extend its functionality.
- Mozilla Investigator (MIG) - Platform to perform investigative surgery on remote endpoints. It enables investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security.
- MozDef - Automates the security incident handling process and facilitate the real-time activities of incident handlers.
- nightHawk - Application built for asynchronus forensic data presentation using ElasticSearch as the backend. It's designed to ingest Redline collections.
- Open Computer Forensics Architecture - Another popular distributed open-source computer forensics framework. This framework was built on Linux platform and uses postgreSQL database for storing data.

- osquery - Easily ask questions about your Linux and macOS infrastructure using a SQL-like query language; the provided *incident-response pack* helps you detect and respond to breaches.
- Redline - Provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis, and the development of a threat assessment profile.
- The Sleuth Kit & Autopsy - Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things.
- TheHive - Scalable 3-in-1 open source and free solution designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.
- X-Ways Forensics - Forensics tool for Disk cloning and imaging. It can be used to find deleted files and disk analysis.
- Zentral - Combines osquery's powerful endpoint inventory features with a flexible notification and action framework. This enables one to identify and react to changes on OS X and Linux clients.

Disk Image Creation Tools

- AccessData FTK Imager - Forensics tool whose main purpose is to preview recoverable data from a disk of any kind. FTK Imager can also acquire live memory and paging file on 32bit and 64bit systems.
- Bitscout - Bitscout by Vitaly Kamluk helps you build your fully-trusted customizable LiveCD/LiveUSB image to be used for remote digital forensics (or perhaps any other task of your choice). It is meant to be transparent and monitorable by the owner of the system, forensically sound, customizable and compact.
- GetData Forensic Imager - Windows based program that will acquire, convert, or verify a forensic image in one of the following common forensic file formats.
- Guymager - Free forensic imager for media acquisition on Linux.
- Magnet ACQUIRE - ACQUIRE by Magnet Forensics allows various types of disk acquisitions to be performed on Windows, Linux, and OS X as well as mobile operating systems.

Evidence Collection

- bulk_extractor - Computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. Because of ignoring the file system structure, the program distinguishes itself in terms of speed and thoroughness.

- Cold Disk Quick Response - Streamlined list of parsers to quickly analyze a forensic image file (`dd`, E01, `.vmdk`, etc) and output nine reports.
- ir-rescue - Windows Batch script and a Unix Bash script to comprehensively collect host forensic data during incident response.
- Live Response Collection - Automated tool that collects volatile data from Windows, OSX, and *nix based operating systems.
- Margarita Shotgun - Command line utility (that works with or without Amazon EC2 instances) to parallelize remote memory acquisition.

Incident Management

- CyberCPR - Community and commercial incident management tool with Need-to-Know built in to support GDPR compliance while handling sensitive incidents.
- Cyphon - Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.
- Demisto - Demisto community edition(free) offers full Incident lifecycle management, Incident Closure Reports, team assignments and collaboration, and many integrations to enhance automations (like Active Directory, PagerDuty, Jira and much more).
- Fast Incident Response (FIR) - Cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents and is useful for CSIRTs, CERTs and SOCs alike.
- RTIR - Request Tracker for Incident Response (RTIR) is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports. RTIR builds on all the features of Request Tracker.
- Sandia Cyber Omni Tracker (SCOT) - Incident Response collaboration and knowledge capture tool focused on flexibility and ease of use. Our goal is to add value to the incident response process without burdening the user.
- threat_note - Lightweight investigation notebook that allows security researchers the ability to register and retrieve indicators related to their research.

Linux Distributions

- The Appliance for Digital Investigation and Analysis (ADIA) - VMware-based appliance used for digital investigation and acquisition and is built entirely from public domain software. Among the tools contained in ADIA are Autopsy, the Sleuth Kit, the Digital Forensics Framework, log2timeline, Xplico, and Wireshark. Most of the system maintenance uses Webmin. It is designed for small-to-medium sized digital

investigations and acquisitions. The appliance runs under Linux, Windows, and Mac OS. Both i386 (32-bit) and x86_64 (64-bit) versions are available.

- Computer Aided Investigative Environment (CAINE) - Contains numerous tools that help investigators during their analysis, including forensic evidence collection.
- CCF-VM - CyLR CDQR Forensics Virtual Machine (CCF-VM): An all-in-one solution to parsing collected data, making it easily searchable with built-in common searches, enable searching of single and multiple hosts simultaneously.
- Digital Evidence & Forensics Toolkit (DEFT) - Linux distribution made for computer forensic evidence collection. It comes bundled with the Digital Advanced Response Toolkit (DART) for Windows. A light version of DEFT, called DEFT Zero, is also available, which is focused primarily on forensically sound evidence collection.
- NST - Network Security Toolkit - Linux distribution that includes a vast collection of best-of-breed open source network security applications useful to the network security professional.
- PALADIN - Modified Linux distribution to perform various forenics task in a forensically sound manner. It comes with many open source forensics tools included.
- Security Onion - Special Linux distro aimed at network security monitoring featuring advanced analysis tools.
- SANS Investigative Forensic Toolkit (SIFT) Workstation - Demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Linux Evidence Collection

- FastIR Collector Linux - FastIR for Linux collects different artefacts on live Linux and records the results in csv files.

Log Analysis Tools

- Lorg - Tool for advanced HTTPD logfile security analysis and forensics.
- Logdissect - CLI utility and Python API for analyzing log files and other data.
- StreamAlert - Serverless, real-time log data analysis framework, capable of ingesting custom data sources and triggering alerts using user-defined logic.
- SysmonSearch - SysmonSearch makes Windows event log analysis more effective and less time consuming by aggregation of event logs.

Memory Analysis Tools

- Evolve - Web interface for the Volatility Memory Forensics Framework.

- inVtero.net - Advanced memory analysis for Windows x64 with nested hypervisor support.
- KnTList - Computer memory analysis tools.
- LiME - Loadable Kernel Module (LKM), which allows the acquisition of volatile memory from Linux and Linux-based devices, formerly called DMD.
- Memoryze - Free memory forensic software that helps incident responders find evil in live memory. Memoryze can acquire and/or analyze memory images, and on live systems, can include the paging file in its analysis.
- Memoryze for Mac - Memoryze for Mac is Memoryze but then for Macs. A lower number of features, however.
- Rekall - Open source tool (and library) for the extraction of digital artifacts from volatile memory (RAM) samples.
- Responder PRO - Responder PRO is the industry standard physical memory and automated malware analysis solution.
- Volatility - Advanced memory forensics framework.
- VolatilityBot - Automation tool for researchers cuts all the guesswork and manual tasks out of the binary extraction phase, or to help the investigator in the first steps of performing a memory analysis investigation.
- VolDiff - Malware Memory Footprint Analysis based on Volatility.
- WindowsSCOPE - Memory forensics and reverse engineering tool used for analyzing volatile memory offering the capability of analyzing the Windows kernel, drivers, DLLs, and virtual and physical memory.

Memory Imaging Tools

- Belkasoft Live RAM Capturer - Tiny free forensic tool to reliably extract the entire content of the computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system.
- Linux Memory Grabber - Script for dumping Linux memory and creating Volatility profiles.
- Magnet RAM Capture - Free imaging tool designed to capture the physical memory of a suspect's computer. Supports recent versions of Windows.
- OSForensics - Tool to acquire live memory on 32bit and 64bit systems. A dump of an individual process's memory space or physical memory dump can be done.

OSX Evidence Collection

- Knockknock - Displays persistent items(scripts, commands, binaries, etc.) that are set to execute automatically on OSX.

- macOS Artifact Parsing Tool (mac_apt) - Plugin based forensics framework for quick mac triage that works on live machines, disk images or individual artifact files.
- OSX Auditor - Free Mac OS X computer forensics tool.
- OSX Collector - OSX Auditor offshoot for live response.

Other Lists

- List of various Security APIs - Collective list of public JSON APIs for use in security.

Other Tools

- Cortex - Cortex allows you to analyze observables such as IP and email addresses, URLs, domain names, files or hashes one by one or in bulk mode using a Web interface. Analysts can also automate these operations using its REST API.
- Crits - Web-based tool which combines an analytic engine with a cyber threat database.
- Diffy - DFIR tool developed by Netflix's SIRT that allows an investigator to quickly scope a compromise across cloud instances (Linux instances on AWS, currently) during an incident and efficiently triaging those instances for followup actions by showing differences against a baseline.
- domfind - Python DNS crawler for finding identical domain names under different TLDs.
- Fenrir - Simple IOC scanner. It allows scanning any Linux/Unix/OSX system for IOCs in plain bash. Created by the creators of THOR and LOKI.
- Fileintel - Pull intelligence per file hash.
- HELK - Threat Hunting platform.
- Hindsight - Internet history forensics for Google Chrome/Chromium.
- Hostintel - Pull intelligence per host.
- imagemounter - Command line utility and Python package to ease the (un)mounting of forensic disk images.
- Kansa - Modular incident response framework in Powershell.
- PyaraScanner - Very simple multithreaded many-rules to many-files YARA scanning Python script for malware zoos and IR.
- rastrea2r - Allows one to scan disks and memory for IOCs using YARA on Windows, Linux and OS X.
- RaQet - Unconventional remote acquisition and triaging tool that allows triage a disk of a remote computer (client) that is restarted with a purposely built forensic operating system.
- Stalk - Collect forensic data about MySQL when problems occur.
- Scout2 - Security tool that lets Amazon Web Services administrators assess their environment's security posture.

- SearchGiant - Command-line utility to acquire forensic data from cloud services.
- Stenographer - Packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets. It stores as much history as it possible, managing disk usage, and deleting when disk limits are hit. It's ideal for capturing the traffic just before and during an incident, without the need explicit need to store all of the network traffic.
- sqhunter - Threat hunter based on osquery and Salt Open (SaltStack) that can issue ad-hoc or distributed queries without the need for osquery's tls plugin. sqhunter allows you to query open network sockets and check them against threat intelligence sources.
- traceroute-circl - Extended traceroute to support the activities of CSIRT (or CERT) operators. Usually CSIRT team have to handle incidents based on IP addresses received. Created by Computer Emergency Responce Center Luxembourg.
- X-Ray 2.0 - Windows utility (poorly maintained or no longer maintained) to submit virus samples to AV vendors.

Process Dump Tools

- Microsoft User Mode Process Dumper - Dumps any running Win32 processes memory image on the fly.
- PMDump - Tool that lets you dump the memory contents of a process to a file without stopping the process.

Sandboxing/reversing tools

- Cuckoo - Open Source Highly configurable sandboxing tool.
- Cuckoo-modified - Heavily modified Cuckoo fork developed by community.
- Cuckoo-modified-api - Python library to control a cuckoo-modified sandbox.
- Hybrid-Analysis - Free powerful online sandbox by Payload Security.
- Malwr - Free online malware analysis service and community, which is powered by the Cuckoo Sandbox.
- Mastiff - Static analysis framework that automates the process of extracting key characteristics from a number of different file formats.
- Metadefender Cloud - Free threat intelligence platform providing multiscanning, data sanitization and vulnerability assesment of files.
- Viper - Python based binary analysis and management framework, that works well with Cuckoo and YARA.
- Virustotal - Free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners.

- Visualize_Logs - Open source visualization library and command line tools for logs (Cuckoo, Procmon, more to come).

Timeline tools

- Highlighter - Free Tool available from Fire/Mandiant that will depict log/text file that can highlight areas on the graphic, that corresponded to a key word or phrase. Good for time lining an infection and what was done post compromise.
- Morgue - PHP Web app by Etsy for managing postmortems.
- Plaso - a Python-based backend engine for the tool log2timeline.
- Timesketch - Open source tool for collaborative forensic timeline analysis.

Windows Evidence Collection

- AChoir - Framework/scripting tool to standardize and simplify the process of scripting live acquisition utilities for Windows.
- Binaryforay - List of free tools for win forensics (http://binaryforay.blogspot.co.il/).
- Crowd Response - Lightweight Windows console application designed to aid in the gathering of system information for incident response and security engagements. It features numerous modules and output formats.
- FastIR Collector - Tool that collects different artefacts on live Windows systems and records the results in csv files. With the analyses of these artefacts, an early compromise can be detected.
- Fast Evidence Collector Toolkit (FECT) - Light incident response toolkit to collect evidences on a suspicious Windows computer. Basically it is intended to be used by non-tech savvy people working with a journeyman Incident Handler.
- Fibratus - Tool for exploration and tracing of the Windows kernel.
- IREC - All-in-one IR Evidence Collector which captures RAM Image, $MFT, EventLogs, WMI Scripts, Registry Hives, System Restore Points and much more. It is FREE, lightning fast and easy to use.
- IOC Finder - Free tool from Mandiant for collecting host system data and reporting the presence of Indicators of Compromise (IOCs). Support for Windows only.
- Fidelis ThreatScanner - Free tool from Fidelis Cybersecurity that uses OpenIOC and YARA rules to report on the state of an endpoint. The user provides OpenIOC and YARA rules and executes the tool. ThreatScanner measures the state of the system and, when the run is complete, a report for any matching rules is generated. Windows Only.
- LOKI - Free IR scanner for scanning endpoint with yara rules and other indicators(IOCs).
- Panorama - Fast incident overview on live Windows systems.
- PowerForensics - Live disk forensics platform, using PowerShell.

- PSRecon - PSRecon gathers data from a remote Windows host using PowerShell (v2 or later), organizes the data into folders, hashes all extracted data, hashes PowerShell and various system properties, and sends the data off to the security team. The data can be pushed to a share, sent over email, or retained locally.
- RegRipper - Open source tool, written in Perl, for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis.
- TRIAGE-IR - IR collector for Windows.

Link to Table of Contents

Six Stages to Incident Response

1. Preparation

a. Policy
    i. Organizations rules
b. Response Plan/Strategy
    i. Determining Impact
    ii. Prioritization
c. Communication
    i. Who gets contacted and when
        1. Example: (During eradication phase) We have identified cause of incident, contained it, and are working on the eradication of incident now. Our current findings have been shared with the following departments:
            a. Legal –
                i. To verify we are following all laws and regulations.
                ii. To see if criminal charges can be filed.
            b. Media – In case a message to the public/investors/whoever needs to be crafted before report is completed.
            c. End Users – They have already been notified of incident during identification/detection phase after verifying incident
            d. Managers – Have been notified of what containment procedures have taken place.
                i. What systems have been taken off line
                ii. An estimated time on the completion of eradication phase
                iii. Estimated time to bring systems back online
                iv. Possible issues we could run into
    ii. When to include law enforcement
d. Documentation
    i. Everything CIRT does needs to be documented
    ii. Who, What, When, Where, Why
    iii. Include Legal in the discussion incase criminal charges are filed
    iv. List dates, times, notes, and any other pertinent information
        1. Enable NTP (Network Time Protocol) on all devices that you can
    v. Document service or system account management
        1. Make sur IR can access these accounts if necessary
        2. Document who has knowledge of these accounts
e. Access Control
    i. CIRT team needs proper permissions during incident
f. Establish central logging capability
g. Change Management details determined
h. Asset Inventory
i. Out of band notifications.

2. Identification / Detection and Analysis -

(This phase is focused on validating that an event is, or is not, genuine incident. Time is of the essence during this phase as the more time spent determining if it is a genuine incident then the more time for the attack to do more damage which means more loss for the company)

a. Determine if actual incident
    i. Perform event intake
    ii. Assignment
    iii. Survey identification point
    iv. Identify potential limitations
b. Communication established between IR handlers and management – VERY IMPORTANT
c. Start documenting everything
    i. Who reported incident
    ii. How was it discovered
    iii. What is business impact
d. Run through system checklists
e. Perform network activity consistency check – Both internal and external
f. Log files
g. Error messages
h. Look at IDS and Firewalls
i. Gather any other data possible
j. Set logging levels to highest possible levels
k. Have sources of incident been identified.

3. Containment

a. Characterize the incident to drive following activity – DoS/DDos, Virus, Data loss, ransomware, internal employee, etc.
b. Notify internal parties based on incident
    i. Management
    ii. Legal
    iii. Media
    iv. Law enforcement
    v. ***follow “need to know” policy and use out of band communications***
c. Short term
    i. Isolate workstation
    ii. Can it be isolated?
    iii. Are infected systems isolated from non-infected?
    iv. If it can’t be isolated then discuss with managers about bringing systems down
d. Get forensic images
e. Long term
    i. Wipe and reinstall
    ii. Remove anything
    iii. Install patches

4. Eradication

a. Can system be reimaged and hardened with patches and/or countermeasures
b. Have artifacts from attack been removed and systems hardened?

c. Root cause identification

5. Recovery

a. Determine how to test to monitor systems are not susceptible to another attack or same attack
b. How long should monitor last
c. Look at prior baselines/benchmarks to compare
d. Continue to keep logging at highest levels until incident has been closed
e. Identify systemic issues
f. Develop mitigations

6. After Action Review

a. Complete all necessary documentation if not already done
b. Who? What? When? Where? Why? – All of these should be answered
c. What went well? What didn't? How can we improve?
d. Schedule meeting to discuss with any involved teams to see what can be improved

Jump Bag Recommendations:

- Journal for note keeping
- Contact list of CIRT members
- USB Drives
- A bootable USB drive or Live CD with up-to-date anti-malware and other software tools that can read and/or write to file systems of the computing environment that the incident response is to be performed in.
- A laptop with forensic software, anti-malware utilities, and internet access (if necessary for researching solutions or downloading tools).
- Computer and network tools kits
- Hard duplicators with write-block capabilities to create forensically sound copies of hard drive images

Link to Table of Contents


Update Incident Response Plan
Preperation, Establish Accountability
Detection and Analysis
Containment, Removal, & Recovery
Post-Incident Review

RESPONDING TO AN INCIDENT

Five things you need to do

1. Out of Bound Communication

- When handling an incident, communication is important; however, it needs to be done out of bounds. It is important to remember the attacker might still have access to your systems. Therefore, you should avoid communicating over:
    - Instant messenger
    - Email
    - Speaker phones
    - Where possible, all communication should take place face to face.

2. Reset Credentials

- Make sure that all passwords that have been compromised during the incident are reset. Remember that it is most likely that an attacker will strike more than once.

3. Coordinate System Shutdown

- If a compromised server is not shut down, it alerts the attacker that something is taking place within the environment they are attempting to infiltrate. This will lead them to install another set of tools and malware which then creates additional problems.

4. Stay Calm

- It is important that you remain calm during incident response, so you can follow protocol, and handle it effectively.

5. Report the Attack

- This should be common sense, but many cyberattacks go unreported. Regardless of whether your organization has their own incident response team or not, it is essential that law enforcement is contacted so that they can attempt to catch the perpetrator.

Five Things You Need to Avoid When Responding to a Security Incident

1. Communicating Too Quickly or Too Slowly

- If the security incident has an effect on your customers or partners, it's essential to have a full understanding about the breach. This will help you come up with an effective strategy. Understandably, upper management wants to put their partners and customers at ease. However, putting out a message and then having to retract it with conflicting information won't look good and will cause additional worry.
- Companies are often so overwhelmed after a breach has taken place that they fail to communicate effectively with relevant stakeholders. When communication is too slow, you are

in danger of losing stakeholder trust in your ability to handle security incidents in a timely manner.

- The same threats are also present when information is provided too quickly. If a company communicates too early, they run the risk of providing inaccurate, inconsistent or incomplete information, which can cause confusion and lead people to lose trust in the company.

2. Not Apologizing

- There is no such thing as a company that is completely safe from security breaches. Although companies and customers are aware that cyber-attacks are always going to be an issue, companies are still not customer focused enough when it comes to making a formal apology to their customers for putting them at risk. A data breach is unexpected, worrisome and traumatic for customers, and not acknowledging this and avoiding an apology can have terrible consequences.

3. Failure to Have a Breach Response Plan

- A breach response plan is a strategy to limit the risk of unauthorized access to systems and data. A properly outlined breach response plan plays a critical role in reducing the negative impact that a security breach can have. It also enhances the organization's ability to navigate through a crisis with relative ease.

4. Not Getting Timely Legal Advice

- There are severe legal implications associated with data breaches — you want to avoid these as much as possible. It is critical that you get the right legal advice early so that you can quickly recover from a security incident. What you don't want is to have to deal with a class action lawsuit because of a data breach.

5. Making the Same Mistakes Twice

- Even the most sophisticated companies will have to deal with a data breach. However, one of the most important aspects of dealing with a data breach is learning from your mistakes. The incident handling process consists of six phases:
    - Preparation
    - Identification
    - Containment
    - Eradication
    - Recovery

Review (lessons learned)

- It is recommended that after a major security incident has taken place, an organization should hold a meeting to discuss the lessons learned. During the meeting, you will need to identify your mistakes and evaluate them. Take inventory of what exactly happened and analyze how your team has dealt with reducing the impact of a data breach. The lessons learned phase should be the most important part of your post-breach activities. By implementing this strategy, not only will you improve the performance of your team and create benchmarks for potential future breaches, but you will also provide helpful reference and training materials.

It is important to mention that during the lessons learned phase you will uncover a number of issues that need improving or changing. You might also find there are some things you will need to get rid of entirely and others that you need to implement in order to improve your level of security.

Whatever you gain from your evaluation, make sure they are taken seriously and that you hire help from capable experts to assist in better protecting your business against data breaches.

It is virtually inevitable that your organization will become a victim of some type of security breach. As companies and businesses are enhancing their levels of security, cybercriminals continue to find ways to manipulate the system. The most important thing is that you take the necessary precautions to protect yourself against a security breach and that you are fully prepared for a breach when it happens. After the breach, make sure that you conduct a lesson learned meeting and that you implement any new ideas, suggestions and recommendations to protect your company against future attacks.

Link to Table of Contents

ASSESSING IMPACT OF CYBER ATTACKS

Assessing the impact of an incident can be very hard to determine. Researchers use a variety of financial models, damage quantifications, and business and asset valuation techniques to arrive at their estimates. There can be both short term and long-term impacts. There are a ton of articles, blogs, papers, and research on assessing/determining impact of attacks/incidents. A whole book could be written on this topic but like with most things it depends on the environment, corporation, and other factors. We recommend reading up on the subject and then determine best way to calculate impact based on the variables you are given.

Scott Musman from the MITRE Corporation has published a great paper on this subject.

https://www.mitre.org/sites/default/files/pdf/09_4577.pdf

Another example

Deloitte published a great article explain this more in-depth:
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

Link to Table of Contents

EFFECTIVE COMMUNICATION TECHNIQUES

Effective communication is extremely important during an incident. The old saying of "time equals money" is very true in this regard. Keep everyone updated as you progress through the incident response life cycle. People will be worried about their jobs, want answers immediately, and will be talking while you are working. You do not want to be wasting time responding to email after email. This should be done in the preparation phase though but if you receive an email asking for an update, you may want to start providing more.

- Create multiple email templates for various stages, that provide meaningful updates.
    - Example: (During eradication phase) Notify whoever necessary that you have successfully eradicated exploit, removed any other files left by attacker, and are patching the system. Estimated time till patch is installed is 10 minutes. Next update will be after verification that the patch prevents attacker from using exploit again and systems can be brought back online.
- **Be clear:**
    - Identify if you will need anything from anyone else
        - Logs, access, etc..
    - Possible issues you may encounter
    - Estimated time till next update, or completion of phase
        - Under promise but over deliver – not by too much though. Be careful with this.
- **Be compassionate**
    - This is a VERY stressful situation for everyone. Do not take things personally.
- **Display confidence**
- **Delegate other tasks.**
    - If you are busy and need to provide an update see if someone else can do it or can pause their work. As my old drill sergeant use to say, "team work makes the dream work".
- **Make a phone call** – Can't write an email for whatever reason? See about making a phone call.
    - Give an update and state you will be sending an email as well with an update when you can.
    - Sometimes a phone call is more personal and can be appreciated more

Link to Table of Contents

COMMUNICATION & SHARING INFORMATION

A well-defined communication protocol is the perfect tool to manage affected departments and stakeholders in a time of crisis. As any part of the IR plan, the communication plan must be documented, tested and validated regularly to ensure it meets the company's requirements.

Even the most advanced technologies become useless without proper planning, staff training and regular upkeep. Attack simulations and tabletop exercises as a viable alternative to traditional methods of disseminating the IR plan among other employees. Such methods provide excellent illustrative examples and require active participation from all people involved. Following this approach, the two-dimensional text in the IR plan becomes three-dimensional, because participants apply the procedure in practice.

Communication of the incident response plan involves several working groups. The first is the executive leadership team who must ensure everyone in the organization is aware of the importance of the incident response plan and must champion any required changes in the organization.

Attack simulations and tabletop exercises are also very effective ways to help your team understand what actions will be required of them during an incident.

Tabletop exercises should be conducted at the executive and technical level. The executive leadership team needs to understand critical decisions are made during an incident and their impact can potentially extend far beyond the impact of the actual incident. Tabletop exercises geared towards technical teams and subject matter experts are also very effective in identifying gaps in security tools, processes and training. These technical exercises are objective based, requiring the response team to prove the accuracy of tools, effectiveness of containment steps and execution of remediation processes.

For communication TLP, or Traffic Light Protocol, can be used. TLP refers to the traffic light signals and who you can share information with.

TLP categories:

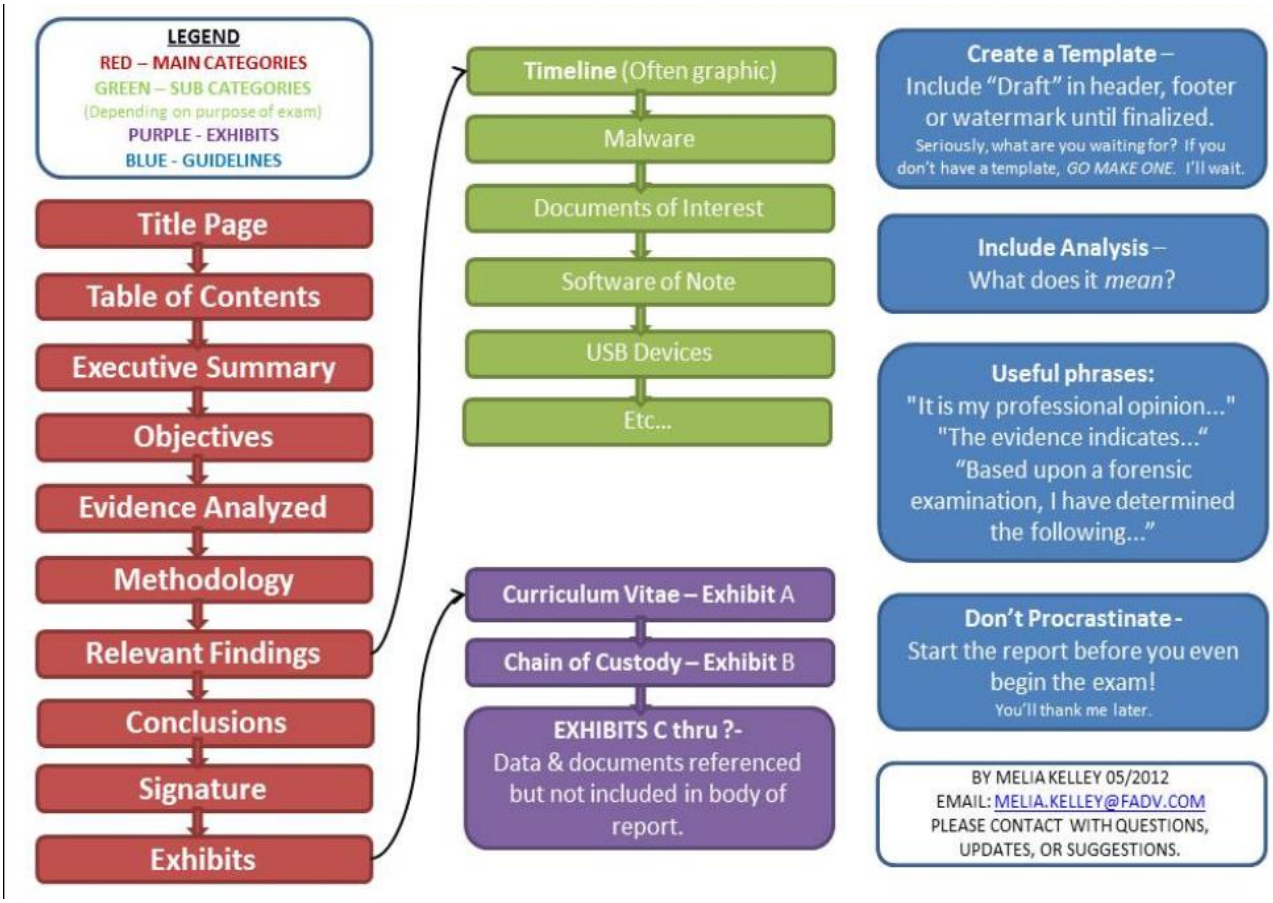
TLP-RED - "For your eyes only". Only to be used by you and not to be spread to other people, even within your own organization.

TLP-AMBER - To be used and shared with co-workers within your organization on a need-to-know basis and with clients or customers who need to know this information to protect themselves or prevent further damage.

TLP-GREEN - Used for information that is not very sensitive and can be shared with partners and peers, but not via publicly accessible channels (e.g. websites).

TLP-WHITE - Public information that can be shared freely, taking into account standard copyright rules.

REPORTING:



The executive summary serves as a high-level view of both risk and business impact in plain English. The purpose is to be concise and clear. It should be something that non-technical readers can review and gain insight into the incident and remediation/mitigation plans highlighted in the report.

Be SMART – Specific, Measurable, Actionable, Realistic (or Relevant)

While IT staffers may need all the technical details, executives don't need to understand *the technology*. They need to understand business risk, something a good executive summary will effectively communicate. It is imperative that business leaders grasp what's at stake to make informed decisions for their companies, and the executive summary is essential to delivering that understanding.

Visual communication can also be helpful in getting complex points across clearly. Look for graphs, charts, and similar visuals in communicating the summary data provided here.

The most valuable reports are those that speak to all audience members in the language they understand – especially those in leadership positions. Tailoring the report to compliance initiatives, particular security controls, and sensitive data specific to the organization, may improve the report's overall impact.

Remediation Tip - Remediation guides often fall short when it comes to the unique context of the client's needs. If a client has a vulnerable service running on a webserver that they depend on, the remediation should offer more than telling them to simply disable the service altogether.

Example Report:

http://www.adfmedia.org/files/CoalfireCMPvideosReport.pdf

Link to Table of Contents

PRESENTING TO EXECUTIVES:

Be SMART – Specific, Measurable, Actionable, Realistic (or Relevant)

- **Set expectations / Start Strong**
    - Start by outlining your presentation. This will allow you to get through it without them wanting to ask questions (they will still ask but not as much) and knowing that you've set aside time to properly discuss anything they want to.
        - If you have 30 minutes:
        - I will spend the first 15 minutes presenting our report on the incident
        - The next 15 minutes will be left open for discussion
- **KEEP IT SHORT & SIMPLE**
    - I can't say this enough and it will be hard to do. Realize they will ask questions if they want more details.
    - Lead with summary. Pretend your 100-page report had to be condensed into one slide. What do you say on it?
        - We detected an incident
        - Based on previously agreed upon documented procedures, and discussions during incident, we had to bring down the production environment to contain it
        - Estimated cost of production being down, and other variables, looks to be around x amount of dollars
        - To prevent this in the future we recommend doing this (provide cost if necessary).
    - Let them drive the conversation.
        - The questions they ask will tell you what they care about and what you should explain in detail more.
- **Have supporting documentation**
    - Senior executives will want you to be able to back up anything you say and will try to find holes in your logic.
    - The Boy Scout motto is "Be Prepared". So be prepared on any parts of your presentation that could be viewed as counter-intuitive, unexpected, challenging to current opinion or practices, or result in significant changes. You may need to have additional data at your fingertips, including back-up slides in an appendix section or a spreadsheet ready to go.
        - If they want more details on how you came up with the cost of something be able to show that. "On page/appendix x you will see a breakdown of how we got to that number"
        - Also realize they will try to tear apart anything when it comes down to cost and return. So again, be prepared.

- Try creating a “message map” of sorts
    - A message map is a framework used to create compelling, relevant messages for various audience segments. It also serves as an organizational alignment tool to ensure message consistency.
- **Know your audience.**
    - **This is the toughest one and will come with experience**.
    - What are their business goals and how will this affect them?
    - Usually they only care about cost, return, and trade-offs
    - Realize your findings may threaten one of their jobs so be prepared
        - An incident could end up being blamed on a CISO/CTO for not being properly prepared by not providing necessary training to end users.
        - Emails that involve important decisions, executives, policy or procedure changes, or anything going against your recommendations.
            8. If it was discussed over the phone, then also ask for it in writing **every** time. Do not do it until it is writing, and you have a copy.
- **Practice, practice, practice.**
    - Then practice some more.
    - Do your presentation out loud exactly as you plan to give it.
    - You might have questions that derail your presentation. How do you prepare for that?
    - During your presentation an executive may say something like “Got it next slide”. Move on, don’t take offense, don’t let it stop you.
- **Review**
    - Have people review your slides, graphs, data, etc.
        - Is it simple?
        - Easy to understand the points you are trying to make?
        - What do they recommend for improvement?

Link to Table of Contents

INDICATORS OF COMPROMISE (IOCS)

IOCs are information that can help with identifying specific malicious behavior on a system or within a network. There are standards where the definition differs or has a different name. IOCs are usually an IP address or domain name.

It is important to provide as much contextual information as possible for IOCs. Include the standard who, what, when, where, why? Always obtain as much contextual information as possible.

IOCs usually include IP address for command and control, file hashes, memory structure manipulation, process names, service names, network ports, and drivers

Individual elements of an Indicators of Compromise may include one or more of the following elements:

- IP Address
- TCP or UDP Ports
- Site Name
- URL
- Random text based DNS name
- File hash, creation time, modification times
- Service name
- Registry key, path, and value
- Directory path
- Virus signature
- Process name, DLL hooks
- A “string” analysis of a file may find IOC string patterns such as a malware authors handle
- Specific account names that appear on a system
- On *nix systems, configuration file references to files in /etc may also be included

Often there are systems within an organization that can help in the search for hits on IoCs.

Places to look at in general:

- **Proxy servers** register the websites that users visit intentionally or unintentionally. Domain names and URLs can be found in the logs of these systems.
- **DNS servers** answer DNS requests that systems within the organization perform. Logging on DNS servers is essential when looking for malicious IP addresses, domain names and DNS servers.
- **Mail servers** are used for receiving or sending email messages. You can use logging on your mail servers to see if your organization received specific malicious email messages by searching for specific subjects, attachments or senders.

- **Firewalls** monitor all kinds of network flows within the network and can allow or block traffic based on rules. Advanced firewalls also look at other traffic characteristics besides IP addresses and port numbers. Logging of firewalls can therefore be of excellent value.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)** are meant to detect or block attacks on a network. It is useful to see if an IDS or IPS has seen an IoC before. If not, it is wise to add detection rules to these systems so that this IoC will be detected or blocked in the future.
- **Antivirus software** is aimed at the individual systems within an organization. Such software monitors files and processes on a system. By supplying antivirus software with information on malicious files and processes, it is possible to detect the presence of such files and processes on the various systems within an organization.
- **Security Information and Event Management (SIEM)** is a solution that is especially suited for this task because as a central system, it contains logging from a variety of systems and applications.

Start with IoCs that can be deployed on systems where information on (parts of) the internal network passes through or is stored. Examples are SIEM solutions, mail servers or proxy servers. This way, an IoC can be deployed quickly to monitor for many different systems within the network. Sometimes, the only available IoCs are those with which individual systems can be investigated. In these cases, you can often use contextual information of the IoCs to deduct for which type of system thi IoC can be used (workstations, mail server, web server, etc). This often narrows the search space significantly.

Received an IoC hit now what:

Some types of IoC are more sensitive to false positives than others. A good example is an IP address. Sometimes an IP address is used exclusively for malicious activities, but other times an IP address is used for shared webhosting. In the latter case, it is possible that a single IP address houses multiple websites where only one website is malicious. When you see a hit on this IP address, it does not automatically mean that malicious activities took place. It can also be a connection to one of the non-malicious websites on this IP address. On the other hand, a hit on a hash value of a malicious file has a much lower chance of being a false positive. For this reason, it might be necessary to obtain additional contextual information, for example by obtaining information from the DNS servers indicating which domain name was queried that lead to a hit on an IoC of an IP address. If you encounter a hit on an IoC, find out which system within the network generated this hit. Where you will have to search depends on the type of IoC that generated a hit. As soon as you know which system within the network generated the hit, you can take action, such as isolating the system from the network. You can also consider taking additional actions, such as forensic investigation. The actions will differ per organization and per case. For example, an infection of a visitor's system that is connected to the public Wi-Fi network will be of less importance than an infection on the internal mail server, and therefore will most likely call for different actions to be taken.

Some general key indicators:

1. Unusual Outbound Network Traffic
Perhaps one of the biggest telltale signs that something is amiss is when IT spots unusual traffic patterns leaving the network.

A common misperception is that traffic inside the network is. Look for suspicious traffic leaving the network. It's not just about what comes into your network; it's about outbound traffic as well

Considering that the chances of keeping an attacker out of a network are difficult in the face of modern attacks, outbound indicators may be much easier to monitor.

Compromised systems will often call home to command-and-control servers, and this traffic may be visible before any real damage is done.

2. Anomalies In Privileged User Account Activity
The name of the game for a well-orchestrated attack is for attackers to either escalate privileges of accounts they've already compromised or to use that compromise to leapfrog into other accounts with higher privileges. Keeping tabs on unusual account behavior from privileged accounts not only watches out for insider attacks, but also account takeover.

Watching for changes -- such as time of activity, systems accessed, type or volume of information accessed -- will provide early indication of a breach.

3. Geographical Irregularities
Traffic between countries that a company doesn't do business with offers reason for pause.

When one account logs in within a brief period of time from different IPs around the world, that's a good indication of trouble.

As to data-breach clues, one of the most useful bits I've found is logs showing an account logging in from multiple IPs in a brief period of time, particularly when paired with geolocation tagging. Often, this is a symptom of an attacker using a compromised set of credentials to log into confidential systems.

4. Other Log-In Red Flags
Log-in irregularities and failures can provide excellent clues of network and system probing by attackers.

Check for failed logins using user accounts that don't exist

Similarly, attempted and successful log-in activity after hours can provide clues that it isn't really an employee who is accessing data.

5. Swells in Database Read Volume
Signs that someone has been mucking about data stores - one of them is a spike in database read volume

When the attacker attempts to extract the full credit card database, it will generate an enormous amount of read volume, which will be way higher than you would normally see for reads on the credit card tables

6. HTML Response Sizes
If attackers use SQL injection to extract data through a Web application, the requests issued by them will usually have a larger HTML response size than a normal request.

7. Large Numbers of Requests for The Same File
It takes a lot of trial and error to compromise a site. Attackers have to keep trying different exploits to find ones that stick. And when they find signs that an exploit might be successful, they'll frequently use different permutations to launch it.

So while the URL they are attacking will change on each request, the actual filename portion will probably stay the same. You might see a single user or IP making 500 requests for 'join.php,' when normally a single IP or user would only request that page a few times max.

8. Mismatched Port-Application Traffic
Attackers often take advantage of obscure ports to get around more simple Web filtering techniques. So if an application is using an unusual port, it could be sign of command-and-control traffic masquerading as "normal" application behavior.

9. Suspicious Registry or System File Changes
One of the ways malware writers establish persistence within an infected host is through registry changes.

Creating a baseline is the most important part when dealing with registry-based IOCs. Defining what a clean registry is supposed to contain essentially creates the filter against which you will compare your hosts. Monitoring and alerting on changes that deviate outside the bounds of the clean 'template' can drastically increase security team response time.

Similarly, many attackers will leave behind signs that they've tampered with a host in system files and configurations.

10. DNS Request Anomalies
One of the most effective red flags an organization can look for are telltale patterns left by malicious DNS queries.

Command-and-control traffic is often the most important traffic to an attacker because it allows them ongoing management of the attack and it needs to be secure so that security professionals can't easily take it over. The unique patterns of this traffic can be recognized and is a very standard approach to identifying a compromise.

Seeing a large spike in DNS requests from a specific host can serve as a good indicator of potentially suspect activity. Watching for patterns of DNS requests to external hosts, compared against geo IP and reputation data, and implementing appropriate filtering can help mitigate command and control over DNS.

Link to Table of Contents

NETWORK BASED ANALYSIS

Any inbound connection should point to an easily identifiable, authorized target on the DMZ or an internal asset.

If the information you have is network-based, obtain unique characteristics of the malicious network traffic. For example, you can search through the logs of the proxy server or DNS server for traces of malicious activities. You can also execute the malware in a controlled environment to monitor network traffic. This might result in sufficient information from which to create IoCs. At the network-level, there are several characteristics that you can use and share as an IoC.

Domain names, **IP addresses** or **URLs** to where the malware connects, or from where the malware is downloaded.

The User Agent HTTP header that is used by some types of malware when making an HTTP request. Attackers do this to pretend to be a browser to try to prevent standing out from the legitimate network traffic within an organization. Sometimes, this User Agent header is so unique that it differs from the User Agent header that legitimate browsers use. This can be a good IoC to monitor within the organization.

Distinctive patterns in network traffic. Just like files, network traffic can also contain patterns that can be used to create a good IoC. Many malware families communicate in such a unique manner with their Command & Control servers that this is an excellent way to monitor for malicious activities within the network. To do this, specific tooling with the accompanying rulesets is required, such as Snort7, uricata8 or Bro9 .

https://www.dfir.training/resources/downloads/cheatsheets-infographics/239-network-forensics-sans/file

Techniques:

- **Connections: Find Syn and Syn/Ack Packets**
    - It is very useful to see who initiated and responded to a connection request.
    - If there are more Syn's than Syn/Acks, it usually indicates scan or network problems
    - Show syn packets only
        - Tcpdump -n -r pcap tcp[13] = 0x02
    - Show Syn/Ack
        - Tcmpdump -r PCAP 'tcp[13=18' | wc -l
    - Find the count of SYN/ACK packets and source port number (warning slow)
        - Tcp -n -r pcap '(tcp[13] & 0x12 == 0x12)' | awk '{print #3}' | sed 's/.*\.//' | sort -u -n
        - Wireshark -> tcp.flags == 0x12
- **Port/Pair Combinations**
    - Find the unique source/port combination, then the port numbers (type of conversations). The goal being to identify communication patterns and perform data reduction

        - First generate the syn_ack.txt file:
            - Tcpdump -n -r.pcap '(tcp[13] & 0x12 == 0x12)' > syn_ack.txt
        - Get the unique sources and source ports:
            - Cat syn_ack.txt | cut -f 3 -d ' ' | sort | uniq -c
        - Get the unique source ports:
            - Cat syn_ack.txt | cut -f 3 -d ' ' | cut -f 5 -d '.' | sort | uniq -c
- **Application Specific Analysis Techniques**
    - **HTTP GET Requests**
        - In Wireshark use display filter"http.request". It can be worth looking through a URL list for things like "login.php" and trying to determine if they are obfuscated
        - Then limit the view in Wireshark and run "follow tcp stream" to analyze the data exchange
    - **Finding HTTP redirection with Wireshark**
        - Add these columns to show the following values:
            - Tcp.stream, http.location, and http.request.full_url
        - Then search through data, find a packet, look in the protocol details, rick click and "apply as column'. Apply the following display filter:
            - http.response.code == 302 or http.response.code == 301 or http.request
    - **HTTP GET and RESPONSE**
        - In Wireshark use filters http.request or http.response
        - The User-Agent string will identify the source browser and os
        - The Server string will identify the web server, which will hint at the underlying OS
    - **DNS Traffic**
        - Should be investigated for manipulation
        - You want to detect DNS name and IP address changes and short TTL values
            - Tcpdump -n -r pcap 'udp port 53' | grep -I CNAME (or grep A for A records, or...)
    - **Clear Text Credentials**
        - Dsniff tool can be used to retrieve usernames and passwords from pcap data. This is used to check credentials are passed in cleartext
            - Dsniff -p pcap
        - Network grep, or ngrep, can also be used. Below the option are quiet, case insensitive, and input file of PCAP_FILE
            - Ngrep -q -I password -I PCAP_FILE
    - **Traffic Volume**
        - Find traffic by volume to a host. This example is for a web server where 'pcap' is a packet capture using HTTP, port 80. For HTTPS, port 443, change the 'dst port' frm 80 to 443
            - Tcpdump -ntr pcap 'tcp[13] & 0x12 and dst port 80' | awk '{print $4}' | tr . ' ' | awk '{print $1"."$2"."$3"."$4"}' | sort | uniq -c | awk ' { print $2 "\t" $1 }'
    - **SMB Find file sharing**

        - You can use the Wireshark filter 'smb' to see if there is a Server Message Block traffic, and then 'smb.cmd == 0x73' to find a session request in the "Native OS' string.
        - To search for EXE's in pacap file within Wireshark use the display filter:
            - Smb.file contains "exe"
    - **Timeframe Analysis**
        - Full date + time output
            - Tcpdump -tttt -r pcap
        - Pcap span in days, returns count + date
            - Tcpdump -tttt -r pcap | cut -f 1 -d ' ' | sort | uniq -c
- **Identifying MAC Address Manipulation**
  There are several highly usesful techniques to detect MAC layer manipulation, but they require a visual check through the data. This method preserves DNS names at the end of the list and only gets IP packets.
    - MAC + IP + Source Port relationships analysis
        - Tcpdump -e -n -r pcap 'ip' | cut -f 2,14 -d ' ' | sort | uniq -c
    - To get the unique list and count of MAC addresses from a pcap trace
        - Tcpdump -e -r pcap | cut -f 2 -d ' ' | sort | uniq -c
    - To find MAC address in Wiresharek – look for ARP replies
        - Arp.opcode == 0x2
    - To review ARP traffic
        - Tcpdump -e -t -nn -r pcap 'arp' | sort -u
    - **Look for spoofed traffic**
        - The following will give MAC + IP + TTL + flags
        - You will need to remove duplicates or use conditional formatting
            - "C:\program files\Wireshark|tshark" -n -r trace.cap -T fields -e eth.addr -e ip.src -e ip.ttl -e tcp.flags
        - Look for fragmentation which is uncommon on a corporate network
        - Fragmentation is a technique used to foil IPS systems
            - **Fragmentation Checks**
            - Tcpdump
                - Tcmpdump -nn -r pcap "ip[6] & 0x20 != 0 or ip[6:2] & 0x1fff != 0'
            - Wireshark
                - Ip.flags.mf == 1
                - Ip.frag_offset >= 0x001
- **Top Talkers**
    - By IP, high to low:
        - Tcpdump -tnn -r pcap 'ip' | awl -F "." '{print $1"."$2"."$3"."$4}' | sort | uniq -c | sort -nr
    - **Determine which systems are generating ICMP errors**
        - Tcpdump -X -n -r pcap icmp
        - Look through data output
    - **Finding conversation with Wireshark**
        - Statistics -> Endpoints -> IPv4 tab

        - Statistics -> Conversations -> IPv4 tab
        - Statistics -> Protocol hierarch
- **Finding Gateway Addresses (multiple methods to do this)**
  Look for an IP sending ICMP Dest Unreachable messages. In wireshark use 'icmp' as a filter then look through the list, or tcpdump -r pcap 'icmp[0] = 3'
    - **Finding scanners**
        - Look for ICMP traffic
            - Tcpdump -r pcap 'icmp'
        - Look for TCP resets
            - Tcpdump -r pcap 'tcp[13} & 4!=0'
- **Reputation Risk Concepts**
  Reputation Risk is a measurement of how trustworth/untrustworthy a site is. Common cluse:
    - Site names registered within the last 10 days
    - Lite din threat sources like Robtex, malwaredomain, etc.
    - No reverse lookup value
    - Short /low ttl – 1 day for example
    - Site's whose IP addresses change frequently
    - Site names which are not humanly readable and just make no sense.

Suspicious Traffic Patterns

- **The real key to identifying suspicious traffic patterns is to have a good baseline for comparison.**
- **Unused Internal Address Activity**
    - Unused address spaes on the network, such as darknets, are often search by malware or intruders looking for soft targets.
    - One method to create an alarm for this is to assign a VLAN for each internal dark net, place those VLANS on a single switch, and on that switch stand up a linux box running detection mechanism which centrally logs.
- **Self-Signed Certificates**
    - Sites using self-signed certificates may be suspicious. The Bro IDS can be configured to extract SSL certification information. Output logs can then be reviewed for self-signed certificate usage.
- **Uncommon apps and port numbers**
    - Most normal internet traffic pattern is high client to low server with high ports.
    - It is uncommon to see high to high or low to low aside from well-known services.
    - The server side should be well known and identifiable with a client port greater than 1-2
    - If not this is suspicious
    - **Suspicious TCP Patterns**
        - Excessive SYN's are scanners.
    - **Suspicious Traffic Volume**
        - Fixed bandwidth patterns that can't easily be explained
        - Continual traffic patterns in every hour of the day to non-Web destinations.
        - File transfers from user workstations outside of normal hours
    - **Suspicious Broadcast Traffic**

        - Large broadcasts per second
        - Constant broadcasts
        - Gratuitous ARP traffic
    - **MAC / ARP Attacks**
        - Masive ARP Broadcast
        - Identical MAC with different IP addresses
        - ARP Who Has messages in rapid succession for different (often incremental) IP addresses
        - There is no NAC solution in place
    - **Suspicious ICMP**
        - ICMP packets greater than 10 bytes in size because ICMP can be sued as a covert channel with the attacker's data carried in the data segment using nonstandard type/codes
        - ICMP packets for non-defined type/codes
        - Excessive ICMP traffic

Using the Snort IDS

During an Incident – Use Snort's three Modes of Operation Sniffer Mode

- **Sniffer mode:**
    - Sniffs all packets and dumpt them to stdout
    - -v verbose
    - -d dumps packets payload
    - -x dumps entire packet in hex
    - -e display link layer data
- **Packet Logger Mode**
    - This mode is used to output file to a log file. You could use this to provide high resolution packet capture.
- **Test Mode**
    - This mode processes the config fiel and applies Snort rules to the collected traffic.

For Cisco Routers:

- Running config should match saved config
- Egress filtering should be in place
    - RFC 1918 private address should be block both outbound and inbound
    - External IP addresses specified as source IP should not be permitted outbound
- NAT translations
    - Only known internet facing services.
        - No RDP for SMB
- Limit inbound connectivity and NAT translation only protocols
- Tunnels
    - Investigate tunnel source and tunnel destination
- Router's web server should be disabled

- Null routing could be used to disrupt communications
- Syslog going into an interior server
    - Look for “logging on” and “logging ip-addresses”

Perimeter Firewall Intrusion Signs

- The firewall should only be managed from an interior IP address
- Logging is enabled and functioning
    - *If the firewall doesn’t log for a particular port, then ensure that downstream application servers are configure for logging, and that logging is enabled on the downstream system.*
- Valid NAT and service translations
    - No changes to what should be defined on the perimeter router. They should agree.
- Object definition agrees with an existing service on an authorized host
    - Many firewalls use object definitions. These often point to similar services, like “Valid DNS Servers” which are permitted 53 UDP traffic. When analyzing a firewall, dig beneath this level to make sure that the object definition actualy agrees with an existing service on an authorized host
- Firewall rule ordering
    - It is not hard to create a more “open” rule and then specific rules which should be reversed.
- There should be a “deny any” catch all rule at the end of the firewall chain
- Pay close attention to the phrase “any any”.
    - If any source address is allowed to initiate communication to any port or destination on an “inbound” basis, then there is an incident waiting to happen.
    - Example – from any any to server 3389

IDS/IPS Logs:

- IDS and IPS detect malicious behavior based on signatures, heuristics, or established network behavior baseline violations. For IR you want to retrieve as much historical data for the suspect IPs as possible. During incident keep a very close eye on the IDS and IPS and add instrumentation as the incident progresses.
    - Example – If you suspect an external IP address then a simple IDS/IPS rule to generate an alert when any system connects to that IP can be valuable.
- Use IDS/IPS source and destination to pull firewall log data as that will provide additional clarity on the communication patterns.

Perimeter VPN Concentrators:

- Frequently VPN's defer to the primary directory for user account validation through RADIUS or TACACS. Investigae any unusual user account activity such as repeat failed logon attempts.
-

Screen Services (DMZ) Network:

- Confirm that all communication patterns between the service/DMZ and the Commodity Internet network are known/validated.
- Verify Server inventory on the DMZ
- Check switch port activity to determine if certain ports are excessively listening

Interior Switch Devices:

- MAC address manipulation would manifest as
  - multiple MAC addresses assigned to a single port
  - MAC address changing over time
  - MAC addresses frequently disappearing
- Excessive inbound packets which are higher than average packet received counts may indicate a sniffer
- There should be a high percentage of observed MAC address with the MAC addresses in the CMBD, server asset management tool, or desktop management tool

Common TCP/IP Protocols and Ports

Protocol	TCP/UDP	Port Number	Description
File Transfer Protocol (FTP) (RFC 959)	TCP	20/21	FTP is one of the most commonly used file transfer protocols on the Internet and within private networks. An FTP server can easily be set up with little networking knowledge and provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.
Secure Shell (SSH) (RFC 4250-4256)	TCP	22	SSH is the primary method used to manage network devices securely at the command level. It is typically used as a secure alternative to Telnet which does not support secure connections.
Telnet (RFC 854)	TCP	23	Telnet is the primary method used to manage network devices at the command level. Unlike SSH which provides a secure connection, Telnet does not, it simply provides a basic unsecured connection. Many lower level network devices support Telnet and not SSH as it required some additional processing. Caution should be used when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear.

Simple Mail Transfer Protocol (SMTP) (RFC 5321)	TCP	25	SMTP is used for two primary functions, it is used to transfer mail (email) from source to destination between mail servers and it is used by end users to send email to a mail system.
Domain Name System (DNS) (RFC 1034-1035)	TCP/UDP	53	The DNS is used widely on the public internet and on private networks to translate domain names into IP addresses, typically for network routing. DNS is hieratical with main root servers that contain databases that list the managers of high level Top Level Domains (TLD) (such as .com). These different TLD managers then contain information for the second level domains that are typically used by individual users (for example, cisco.com). A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system.
Dynamic Host Configuration Protocol (DHCP) (RFC 2131)	UDP	67/68	DHCP is used on networks that do not use static IP address assignment (almost all of them). A DHCP server can be set up by an administrator or engineer with a poll of addresses that are available for assignment. When a client device is turned on it can request an IP address from the local DHCP server, if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the poll for assignment.
Trivial File Transfer Protocol (TFTP) (RFC 1350)	UDP	69	TFTP offers a method of file transfer without the session establishment requirements that FTP uses. Because TFTP uses UDP instead of TCP it has no way of ensuring the file has been properly transferred, the end device must be able to check the file to ensure proper transfer. TFTP is typically used by devices to upgrade software and firmware; this includes Cisco and other network vendors' equipment.
Hypertext Transfer Protocol (HTTP) (RFC 2616)	TCP	80	HTTP is one of the most commonly used protocols on most networks. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers.
Post Office Protocol (POP) version 3 (RFC 1939)	TCP	110	POP version 3 is one of the two main protocols used to retrieve mail from a server. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server.
Network Time Protocol (NTP) (RFC 5905)	UDP	123	One of the most overlooked protocols is NTP. NTP is used to synchronize the devices on the Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate.
NetBIOS (RFC 1001-1002)	TCP/UDP	137/138/139	NetBIOS itself is not a protocol but is typically used in combination with IP with the NetBIOS over TCP/IP (NBT) protocol. NBT has long been the central protocol used to interconnect Microsoft Windows machines.
Internet Message Access Protocol (IMAP) (RFC 3501)	TCP	143	IMAP version3 is the second of the main protocols used to retrieve mail from a server. While POP has wider support, IMAP supports a wider array of remote mailbox operations which can be helpful to users.

Simple Network Management Protocol (SNMP) (RFC 1901-1908, 3411-3418)	TCP/UDP	161/162	SNMP is used by network administrators as a method of network management. SNMP has a number of different abilities including the ability to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific actions are occurring. Typically, these are configured to be used when an alerting condition is happening. In this situation, the device will send a trap to network management stating that an event has occurred and that the device should be looked at further for a source to the event.
Border Gateway Protocol (BGP) (RFC 4271)	TCP	179	BGP version 4 is widely used on the public internet and by Internet Service Providers (ISP) to maintain very large routing tables and traffic processing. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet.
Lightweight Directory Access Protocol (LDAP) (RFC 4510)	TCP/UDP	389	LDAP provides a mechanism of accessing and maintaining distributed directory information. LDAP is based on the ITU-T X.500 standard but has been simplified and altered to work over TCP/IP networks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS) (RFC 2818)	TCP	443	HTTPS is used in conjunction with HTTP to provide the same services but doing it using a secure connection which is provided by either SSL or TLS.
Lightweight Directory Access Protocol over TLS/SSL (LDAPS) (RFC 4513)	TCP/UDP	636	Just like HTTPS, LDAPS provides the same function as LDAP but over a secure connection which is provided by either SSL or TLS.
FTP over TLS/SSL (RFC 4217)	TCP	989/990	Again, just like the previous two entries, FTP over TLS/SSL uses the FTP protocol which is then secured using either SSL or TLS.

From <http://www.pearsonitcertification.com/articles/article.aspx?p=1868080>

Link to Table of Contents

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation needed and DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect datagram for the Network
	1	Redirect datagram for the host
	2	Redirect datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem	0	Pointer indicates error
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

Link to Table of Contents

HOST BASED ANALYSIS

Windows Checklists for Anomalous Behavior:

To look for unusual processes and services use the following commands:

- taskmgr.exe – it displays running processes and services.
- In command prompt use these three commands:
    - tasklist – it displays a list of running services along with their corresponding PID (process ID), session name, session number, and memory usage. Getting a PID can be useful for using the taskkill command to end the questionable process.
    - wmic process list full – is a windows management interface control that will display all processes, along with detailed information such as their executable path and much more.
    - tasklist /svc – will display a list of all processes along with their corresponding PID, and services that are tied to them
- To look for unusual files and registry keys use the Windows search feature and look for files larger than 10MB, and use regedit to look for unusual entries in the following areas:
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
    - HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
      Generally those three registry entries will contain startup configurations for specific programs, including malware.
- To look for unusual network usage the following Windows commands in the command line interface (cmd) provides an excellent view of network activity on a particular system:
    - net view \\127.0.0.1 (or localhost) – displays shared folders that are on the system. If there are shared folders that are not supposed to be there that can be a significant red flag.
    - net session – displays open sessions with other systems on the network. This is useful for detecting communications with other systems on the network and determines whether the connections are legitimate. A good example: is a https connection to a rogue server on the internet and heavy bandwidth usage from the compromised computer in question with that rogue server.
    - nbstat –S will display NetBIOS activity over TCP/IP on the various network interfaces that a machine in question may have.
    - netstat and its various flags (e.g. netstat –na, netstat –nao, etc) provides a tremendous amount of information between listening and established TCP/IP connections, along with their ports and whether the protocol used is TCP or UDP. This is useful for determining unusual traffic patterns on the computer in question.
- To look for unusual start up (or scheduled) tasks, use the following commands:
    - msconfig –displays all startup configurations from services to files in the startup folder, etc. This is also useful for disabling anything trying startup during Windows login or boot-up, and to troubleshoot problems that are caused by nefarious or poorly written programs.

    - schtasks – displays tasks schedule to run at specific times. This is useful for not only troubleshooting problems, but also looking for would be logic bombs.
    - wmic startup list full – displays all of the services and programs that startup when Windows boots and/or upon Windows login.
- To look for unusual accounts use the following three commands:
    - lusrmgr.msc – this command is only useful for looking for local accounts on a machine. Two account types to specifically look for are Administrator accounts that are not supposed to be on the machine and active Guest accounts, as those can lead to serious security compromises.
    - net user (in command prompt) – displays all user accounts on a local machine.
    - net localgroup administrators – display all local administrator user accounts. This is useful for finding administrator accounts that do not belong on a particular machine.
- The final and most crucial area to look for unusual behavior is within event viewer. It displays all of the event log content that Windows actively records. The command for it to type in the run command box is eventvwr.msc.
    - Look for warnings, errors, and other events (e.g. system reboots during usual times, etc).
    - If the log files are missing, it is a reliable indicator that the machine has been or is compromised and the intruder is trying to hide his\her tracks.

Unix Checklists for Anomalous Behavior:

- To look for unusual processes and services use the following commands:
    - ps -aux – displays running processes along with their process-id (PID), associated user-ids (UID #), name, and other pertinent information. Pay particular attention to any process that is using the UID 0 user-id, because those processes are running with root permissions.
    - ps –ef – displays the full listing of all processes and can be useful for finding undesirable processes that are running.
    - lsof –p (PID) – displays a specific process in more detail, by displaying the files and ports associated with that process. This is appropriate for examining any Trojan, worms, and other network based malware on a UNIX system.
    - lsof +L1 – displays processes running from or accessing files that have been unlinked; basically it will show one to figure out if the attacker is hiding data or running a backdoor.
- To look for unusual files the “find” command along with its various flags allows one to search a UNIX system for malware. A few examples are listed below:
    - find / -uid 0 -perm -4000 –print – searches for files that have root permissions.
    - find / -size +50000k –print – searches for files of a specified or greater size. This is particularly useful for searching for files that may not belong on the system, like movies, games, et al.

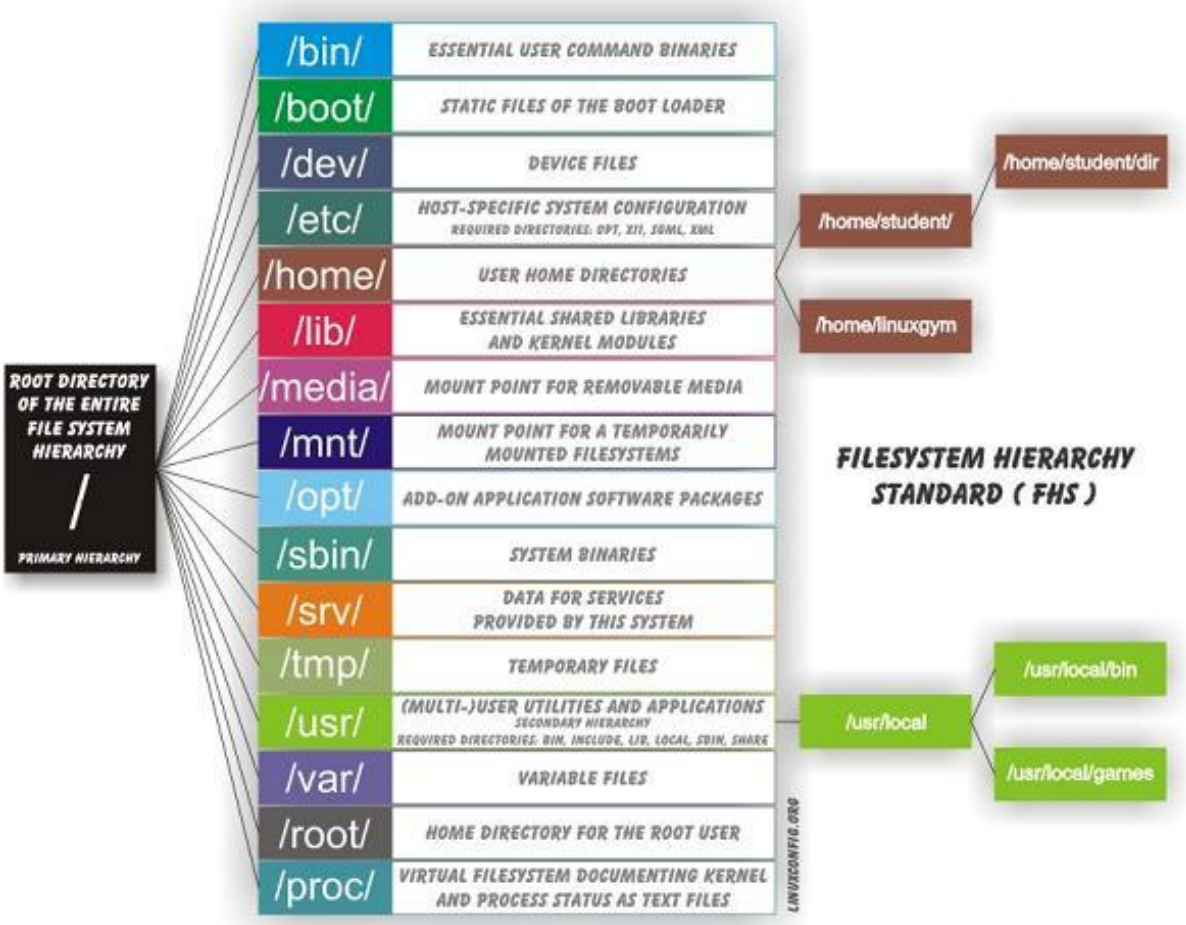
- To look for unusual network usage coming from a system's network interface type in the following command: ip link | grep PROMISC – this command will display any network interfaces that are running in promiscuous mode, which can be a clear indication of an attacker running a packet sniffer.
- Other useful commands to observe unusual network behavior are:
    - netstat –nap – this displays listening ports and in turn can be useful for finding backdoors.
    - arp –a – displays all MAC to IP address mappings of the system and can be useful for finding addresses of systems that are not part of the network (e.g. a rouge wireless access point that allows one to gain access into the internal network from the outside).
    - To look for scheduled jobs (i.e. tasks) by root or any other user, type in the following command: contrab –u root –l – this is useful for detecting logic bombs, scheduled connections to unknown hosts, and other potentially nefarious issues.
    - Two additional commands to display system-wide cron jobs are:
        - cat /etc/crontab – displays all jobs scheduled within the cron table.
        - ls etc/cron.* - lists files within the cron subdirectories.
        - To look for unusual accounts use the following commands to check the following files: i. sort –nk3 –t: /etc/paswd | less – displays all accounts sorted by UID (e.g. UID0, etc), this is useful for finding accounts with root permissions or accounts that do not belong on the system.
        - egrep ':0:' /etc/passwd – displays only accounts with root permissions.
        - getent passwd | grep ':0:' – same as above, except for systems with multiple authentication mechanisms. iv. find / -nouser –print – searches the entire system for orphaned files that may have been deleted by an attacker's temporary account.

- The best place to check for unusual system activity is the log files, especially in UNIX. Most log files are located in /var/log (or var/logs), or var/messages.
    - A good command to use for viewing log files is: more –f /var/log/messages – this allows a page by page review of all logged events. Pay particular attention to user authentication logins and any unusual patterns such as missing entries and times that may indicate an intruder is trying to hide his/her tracks.
- Other commands to check for possible clues are:
    - uptime – displays how long a system has been up and running. If the system's uptime is shorter or longer than it should be, then it could be a clear indication that something has changed and therefore may need further review. ii. free – is useful for checking how much ram is used. This is useful for detecting processes that are using a lot of memory (e.g. an attacker searching or modifying a database, etc). iii. df – is useful for checking available disk space. This can provide a reliable indication as to whether an attacker is installing malware or removing files from a system.

BASH:

Show everything modified between two dates =

$ find / -type f -newermt 20xx-xx-01 ! -newermt 20xx-xx-02 -ls 2>/dev/null



This image is copied from here: http://askubuntu.com/questions/138547/how-to-understand-the-ubuntu-file-system-layout/138551#138551

Get handy in using Linux. If you are new to Linux, refer the Linux command guide http://linuxcommand.org. Practice all the common commands and refer the ***man*** page for each of these commands.

Link to Table of Contents

FILE-BASED IOCS

If the information you have is file-based, obtain unique characteristics of these files that you can apply and share. When you encounter malicious files, you can verify this, for example, by letting your antivirus software scan the files. In most cases, the antivirus software will recognize the files as malicious. For files, there are several characteristics that you can use and share as an IoC.

The hash value of the file (MD5/SHA1/SHA-256). This hash value is characteristic for the file so that other parties can use this hash value to detect the same malicious file within their organization.

The location and name of the file. Often malware copies itself to a specific location on the system and renames the copy of itself, so it can start again when a restart of the system takes place.

Distinctive patterns within a malicious file. Often, different variants of the same malicious file are being used by attackers. These files are (in essence) all the same malware. Each file differs in small points from the other files. Attackers do this to prevent detection based, for example, on hash values of the files. These files often share the same patterns in their contents. With specific tooling, such as Yara6, it is possible to write rules to detect malicious files based on patterns in the contents of the files.

Specific registry keys that the malware creates or queries. Some Windows malware will want to make changes in the registry, for example, to change security settings on infected systems or to configure the system so that the malware is executed at every restart of the system. These registry keys can be unique enough to serve as a valid IoC.

Link to Table of Contents

SANS APT INCIDENT HANDLING CHECKLIST

(https://www.sans.org/score/checklists/apt-incident-handling)

The following outline is intended to be a checklist of actions appropriate to dealing with the threat and a compromise accomplished by this threat. Customized tailoring to each environment and situation is warranted and recommended. But this guide is a generalized set of actions appropriate to APT response.

- Preparation
  - Identify ownership and responsibility for all systems (including data) in the enterprise
  - Clear communication channels
  - Capabilities for encrypted email communication (potentially not using primary email server)
  - Capabilities for encrypted chat messaging (potentially not using primary chat server)
  - Telephone call list for coordination stored offline
  - Understanding which parties are to be notified
    - Develop contact list per system
    - System Owner
      - Possibly designated Point of Contact (POC), too
    - Technical POCs
      - Possible after hours / rotation / call list for response
  - Incident Response aware of and capable to address APT style attacks
  - Clear understanding of this threat's characteristics
    - Management has clear understanding of the threat
  - Authorized to respond on all systems in enterprise
  - Funded to perform extended investigations
    - If Incident handling isn't currently 24x7, what resources are available to continue IR work throughout sustained response
  - In house capability or contracts with business partner for
  - Incident Response
  - Forensic Investigation
  - Malware Reverse engineering
  - Containment Strategy for APT
  - Two basic strategies:
    - Watch and Learn
    - Disconnect
  - Define the Standard Operating Procedures (SOP) for when each scenario is used
  - Define a methodology for an incident responder to deviate from SOP as needed
    - This methodology should be part of SOP
    - Include steps for notification and justification of planned deviation
  - Press Team
  - Legal Team
- Identification
  - Remote Access Trojan (RAT)
  - Command and Control (C+C)

    - Encrypted Communications discovered
    - Covert Channel discovered
    - Host based IDS/IPS alert of unexpected system call, data access, port open
    - Direct External Notification (Law Enforcement, Business Partner)
    - Indirect External Notification (Open Source Intelligence of behavior, search in your environment)
    - Data discovered outside of organization (pastebin, news)
    - Blackmail “offer”
    - Notification to internal staff must occur in a discrete fashion
    - Encrypted
    - Limited to only those with need to know
    - Authorization to add additional resources to response effort is limited to Incident Response Management, and/or Business Unit Management
    - Categorize known Severity and Impact
    - Provide updates as important new information comes to light
- Containment
    - Watch and Learn versus Disconnect
    - Have this plan in place in advance! (per Preparation phase)
    - Extract and identify characteristics of adversary
    - Identify other affected systems
    - Utilize updated Network Intrusion Detection System (NIDS) / Network Intrusion Prevention System (NIPS) / Host Intrusion Detection System HIDS / Host Intrusion Prevention System (HIPS) signatures to assess assets throughout environment.
        - Update NIDS/NIPS/HIDS/HIPS to search for characteristic:
        - Files
        - System calls
        - Processes
        - Network
            - Ports
            - IP addresses
            - Host names
        - Use Packet Capture (pcap) / network forensic devices to replay old traffic to identify additional infected systems
    - Identify what has been stolen
    - Full pcap (which retains a copy of all data from the wire) is invaluable in this regard
        - Even w/ full pcap, traffic may be encrypted
        - Must break encryption to fully assess damage
        - May need host based forensics in coordination with full pcap to complete this assessment
    - Intellectual Property
    - Resources
        - Bandwidth
    - Identify legal ramifications
    - PCI
    - HIPAA
    - California HR (SB 1386) notification requirements
    - European data breach requirements
    - Many possible other legal ramifications

    - Is it appropriate to remove entire segment from network (disconnect?)
    - May be easier to identify malicious network traffic if the environment is still online because the traffic is still flowing, but may have ongoing loss of data
    - Contact Law Enforcement (LE)?
    - FBI typically interested in this sort of attack
    - The decision to involve LE may affect the amount of and degree of public reporting
    - Public Reporting?
    - US-CERT
    - Industry requirements?
        - Defense Industrial Base (DIB)
        - Medical
        - Sarbanes-Oxley (SOX) / Gramm-Leach-Bliley (GLB)
    - Partner notification
    - Customer Notification
- Eradication
    - Imperative that all affected systems be collected, and full forensic images be made.
    - Memory Images very important for APT since some techniques do not write to hard drive
        - Also may assist in assessment of ex-filtrated data
        - If data ex-filtration uses symmetric cipher, then decryption key will be present in Random Access Memory (RAM)
    - Preferred method is to seize hard drives as evidence, replace those hard drives with new system image.
        - Preferred because this drive is the legal evidence of wrongdoing
        - Any pcap / network information that could be evidence must also be preserved
        - Have SOP showing handling of evidence for pcap
        - Associate with case, make MD5 and SHA256 hash of stored pcap
    - Secondary option is to make forensic image (for example, remotely via encase enterprise or another enterprise forensic solution, then wipe drives and re-image
    - Without this evidence, a thorough investigation cannot be completed
    - Close all network vectors of ex-filtration
    - HTTPS inspection via proxy and Secure Socket Layer (SSL) intercept
    - Prohibit outbound encrypted communication except for known, authorized peers
    - Techniques demonstrated during this APT incursion
    - Close all vectors of re-infection
    - Remove all RAT / C+C / Backdoors
- Recovery
    - Close future network vectors of ex-filtration
    - HTTPS inspection via proxy and SSL intercept
    - Prohibit outbound encrypted communication except for known, authorized peers
    - Re-engineer systems to prevent reinfection
    - Segment critical data to more restricted areas
    - Implement auditing for critical data access
    - Identify individuals within environment who purposefully or accidentally aided APT, for counseling / training / discipline
- Lessons Learned
    - Assess Executive posture toward Incident Handling and Information Assurance. Is this loss just a cost of doing business, or is it an opportunity for massive change?

- Develop Intelligence group for identification of APT attacks
- Characterize the adversary
  - Use “Kill Chain” model or other counter-intelligence strategies
  - Adversary has limited resources, as well. Will re-use assets.
  - Attribution is very difficult, but is the end goal for counter-intelligence activities.
- Campaign to assist business members of various sorts of threats
- Malware drive by download = smash and grab from car
- APT = home invasion / hostage situation
- Explain potential loss of long term competitive advantage of business due to loss of IP
- Re-catalog and re-value assets in light of APT strategies and targets
- Avoid Blame, use incident to enhance capabilities
- Enhance methods for APT response, including
- “Watch and learn” capabilities
- Honey tokens for Intellectual Property (IP)
- Active honey-nets
- Deception capabilities
- Aggregation of data from all sources
- Security Information and Event Management (SIEM) if possible
- Identify additional data sources
  - Firewalls
  - HIDS
  - Windows Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) / Authentication
  - Wireless infrastructure
  - Any system not currently providing data
  - Servers
    - Web servers
    - Data base servers
  - Workstations

Link to Table of Contents

LAW ENFORCEMENT/LEGAL

https://www.sans.org/score/law-enforcement-faq

It should be clearly defined who contacts law enforcement, when they should so, and what to provide. This should be discussed with your legal department. The Department of Homeland Security is very helpful with determining the following
Evidence – Handling, collecting, and storing
Chain of Custody policies, and best practices

In order to justify bringing in law enforcement agencies, it is necessary to have a Corpus Delicti - literally, "the body of a crime". Is there reasonable evidence of a crime? Or is there simply an event or an occurrence that can't be explained? It is crucial to rule out non-criminal causes for what has happened before calling in law enforcement. They want to investigate computer crimes, not accidents.
A preliminary inquiry should include:

- Ruling out a normal hardware or a software failure.
- Developing a chronology or timetable of what happened.
- Auditing for any unusual activity during that time frame.
- Identifying any users or processes involved.
- Evaluating the motives of any actors. For an external attack, this motive may involve using a known exploit, the signature of a hacker or script kiddie. In an internal attack, the question becomes: "Who would have gained from this event?"

Building Cooperative Relationships

Law enforcement may be reluctant to share information with you, an outsider. So, start building trust with them before you have a crisis. As suggested earlier in this article, work in conjunction with local police to develop incident response policies. Get to know the leadership of your local police department's computer crimes unit. If you belong to a local technology association or computer security organization, contact the public affairs office of the police, and arrange to have a speaker come to your group. Get involved in networking through your local chapter of ASIS (American Society for Industrial Security, http://www.asisonline.org/) and the HTCIA (High Technology Crime Investigation Association, http://htcia.org/). And, of course, attend conventions and seminars on computer security where you meet law enforcement and get to know them. But most important, if law enforcement calls for help on a case, try to give them a helping hand. Cooperation is always a two-way street.

https://www.dfir.training/policy/71-acpo-good-practice-guide-for-digital-evidence-v5/file

Link to Table of Contents

INTERVIEW QUESTIONS

What is MD5 checksum?

MD5 checksum is a 128 bit value that helps identify the uniqueness of a file. You can have two file names, but each will have a different checksum. You use these checksums to compare two different files to identify if they are the same.

Name some common encryption algorithms that are used to encrypt data

Some common ones include triple DES, RSA, Blowfish, Twofish and AES.

What is an .ISO file?

An ISO file contains an application or CD image of several files and executables. Most app software can be made into an ISO that you then mount as a virtual drive and can browse files within the ISO. New Windows versions come with internal ISO mounting capabilities.

What is a SAM file?

A SAM, or Security Accounts Manager, file is a file specifically used in Windows computers to store user passwords. It's used to authenticate both remote and local Windows users, and can be used to gain access to a user's computer.

What is data mining?

Data mining is the process of recording as much data as possible to create reports and analysis on user input. For instance, you can mine data from various websites and then log user interactions with this data to evaluate which areas of a website are accessed by users when they are logged in.

What is data carving?

Data carving is different than data mining in that data carving searches through raw data on a hard drive without using a file system. Data carving is essential for computer forensics investigators to find data when a hard drive's data is corrupted.

What operating systems do you use?

Most computer forensic experts know at least one operating system well. Be honest with this question, but you should know either Windows, Linux or Mac operating systems well. Your interviewer will probably go into more detailed questions based on your answer.

What type of email analysis experience do you have?

Computer forensics relies on email analysis. You should be experienced with email servers such as MS Exchange and free web-based platforms such as Gmail and Yahoo.

What is steganography?

Steganography conceals a message within a message. In other words, someone can send an email message with content that says one thing, but every third word comprises a second message that makes sense to a recipient.

What are some common port numbers?

TCP port numbers are the virtual connections created by computers and applications. Common port numbers are 21 for FTP, 80 for web services, 25 for SMTP and 53 for DNS.

Describe the SHA-1 hash

The secure hash algorithm 1 is a hash algorithm that creates a 160-bit or 20-byte message digest.

How would you handle retrieving data from an encrypted hard drive?

First determine the encryption method used. For simple encryption types, try finding the configuration file. Use tools such as EaseUS Data Recovery, Advanced EFS Data Recovery or Elcomsoft Forensic Disk Decryptor. You can also use brute force methods.

What port does DNS run over?

53

What are some security issues related to the Cloud?

The biggest issue is the increased potential for data breaches or exfiltration as well as the potential for account hijacking. The Man in Cloud Attack is a new threat specific to Cloud usage. It is similar to the MitM attack, where an attacker steals the user token which is used to verify devices without requiring additional logins. Cloud computing introduces insecure API usage, which is discussed on the OWASP Top 10 Vulnerabilities list.

Describe some of the vulnerabilities listed on the OWASP Top 10 Vulnerabilities list?

This list is updated yearly with the current top 10 application security risks. Cross-site scripting is one item that has been on the list year after year. But others on the most current list include injections such as SQL, OS and LDAP, security misconfigurations, sensitive data exposure and under-protected APIs.

What is an ACL?

An access control list. It is a list used to grant users and processes access to system resources.

How would you be able to tell at the hex level that a file has been deleted in FAT12?

Run fsstat against the FAT partition to gather details. Run fls to get information about the image files. This will return information about deleted files and the metatdata information.

What are some tools used to recover deleted files?

Recuva, Pandora Recovery, ADRC data recovery, FreeUndelete, Active UNDELETE, Active partition or File recovery and more.

What is a form of simple encryption often used by an intruder or criminal?

XOR (exclusive OR)

How do you stay up to date on current cybersecurity trends?

This is a personal question; make sure you can share newsletters and websites you visit often. These could include InfoSec Institute, Cyberwire, IT whitepapers, and podcasts or webinars given by companies like Nessus, Metasploit and SANS.

How do you handle conflicting direction from different stakeholders?

This question is to see how you handle conflict. The best way to answer is you would first consult your direct supervisor, explain the conflict and ask for guidance on how to proceed.

If you needed to encrypt and compress data for transmission, which would you do first and why?

Compress then encrypt. Because encryption takes up resources and can be cumbersome to perform, it makes sense to compress the data first.

What is the difference between threat, vulnerability and risk?

A threat is what a potential attacker poses, by potentially using a system vulnerability that was never identified as a risk. Using this answer provides context for the three terms together, but you can define them separately.

- A threat is the possibility of an attack.
- A vulnerability is a weakness in the system.
- Risks are items that may cause harm to the system or organization.

Link to Table of Contents

OTHER INTERVIEW QUESTIONS

ACCOMPLISHMENT QUESTIONS:

- Let's talk about a major accomplishment you're proud of in your current job (previous job, education).
- What was the Problem or challenge?
- What Action did you take?
- What was the Result?
- What did you Learn?
- How have you Applied it?
- Self-Appraisal What qualities did you use to accomplish that? Give me examples where you demonstrated those qualities.
- If I called (name of manager, peer, direct report, or client) how would he/she say you were able to . . ?

GENERAL CULTURAL QUESTIONS::

- How is your lab configured at home? If you do not have a lab, how would you setup one?
- Are there any blogs you follow?
- What motivates your interest in the cyber security field?
- What is a topic you are currently studying?

NETWORKING 101 QUESTIONS::

- What port does DNS operate on?
- If connectivity is lost on a workstation, what is the first think you should check?
- You are a network administrator who has been assigned a class C subnet and want to split that subnet in half, how would you configure the subnet mask?
- When a Ethernet frame passes through a router, what happens to the MAC address?
- What is Network Address Translation?
- What happens when you type 'http://www.google.com' into your web browser?

System Administration 101:

- How would you tell from the command line what the MAC address is of one of your network interfaces?
- What is the version number of Windows 7?
- Where would you go to view the installed device drivers on a system?
- What tool could you use to remotely administer a Windows host through the command line?
- What log would show login information on a Windows host?
- How would you setup a scheduled job on a GNU/Linux machine?

Cyber Security 101:

- Explain the difference between a firewall, intrusion prevention system, and a intrusion detection system?
- What is a disadvantage of signature based malware detection?
- What is a zero-day vulnerability?
- A user reports that they received a suspicious looking email. How do you proceed?

Programming 101:

- What is a function?
- What is the difference between an interpreted language and a compiled language? What are the advantages and disadvantages between the two?
- What is machine code?
- Do you have a programming language you prefer? Do you have any experience writing software?

Digital Forensics:

- What is timeline analysis? What is the pivot point in timeline analysis?
- What is a registry hive? What registry hive is only found in volatile memory?
- What is the difference between Modified time-stamp and Change time-stamp? What is the Birth time-stamp generated?
- An incident has been reported that an enterprise host was identified communicating with a known malicious external host. The incident responders have already blocked the communication and have requested the disk for forensic investigation. You are the forensic analyst on duty when the disk arrives. How will you begin the investigation?

Developing IOCs from Malware Samples (a.k.a. Malware Analysis for IR):

- What is static analysis?
- What is dynamic analysis?

- What type of items do you look for during static analysis?
- How does static analysis influence how dynamic analysis is performed?
- Why would you disassemble or debug an application?
- What is a Windows Portable Executable?
- How would a piece of malware maintain persistence?
- What is the ESP register used for in the Intel x86–32 architecture?
- During execution of a piece of malware in a segregated virtual lab environment, the sample was observed making an HTTP GET request for a text file. Because the lab is segregated from the Internet, the sample did not receive the text file. What would you do to move the investigation forward?

Link to Table of Contents

REFERENCES / RESOURCES

Bayuk J. (2009). *How to Write an Information Security Policy*. Retrieved on 04/06/2014 from http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html?page=2

Entrepreneur. *Information Technology Security Policy*. Retrieved on 04/06/2014 from http://www.entrepreneur.com/formnet/form/731

IG Toolkit (2007). *NHS CFH_Corporate InfoSec Policy Template 2007*. Retrieved on 04/06/2014 from https://www.google.bg/?gfe_rd=cr&ei=kNYlU52dLOPb8gf93oG4CQ#q=NHS+CFH_Corporate+InfoSec+Policy+Template+2007

Olson, I & Abrams, M. *Information Security Policy*. Retrieved on 04/06/2014 from http://www.acsac.org/secshelf/book001/07.pdf

Perkins, J. (2013). *Information Security Policy*. Retrieved on 04/06/2014 from http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/infSecStaIT.pdf

Techopedia. *Information Security Policy*. Retrieved on 04/06/2014 from http://www.techopedia.com/definition/24838/information-security-policy

Timms, N. (2014). *Secure Networks: How to Develop an Information Security Policy*. Retrieved on 04/06/2014 from http://www.networkcomputing.com/secure-networks-how-to-develop-an-information-security-policy/a/d-id/1234642?

The University of Illinois (2014). Information Security Policy – The University of Illinois. Retrieved on 04/06/2014 from http://www.obfs.uillinois.edu/cms/one.aspx?portalId=909965&pageId=914038

University of Oxford (2012). *Information Security Policy*. Retrieved on 04/06/2014 from http://www.it.ox.ac.uk/media/global/wwwitservicesoxacuk/sectionimages/security/Information_Security_Policy_2012_07.pdf

Drinkwater, D. (2017). *10 steps for a successful incident response plan*. https://www.csoonline.com/article/3203705/security/10-steps-for-a-successful-incident-response-plan.html (26/01/2018)

Kovacs, E. (2016). *Suffocating Volume of Security Alerts Challenge Incident Response*. http://www.securityweek.com/incident-response-becoming-more-difficult-survey (26/01/2018)

Seqrite (2017). *5 steps for a successful incident response plan*. http://blogs.seqrite.com/5-steps-for-a-successful-incident-response-plan/(26/01/2018)

https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

https://www.proofpoint.com/sites/default/files/incidentresponse.pdf

https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

https://digital-forensics.sans.org/blog/2017/09/13/malware-analysis-cheat-sheets

https://www.sans.org/reading-room/whitepapers/incident/practical-incident-response-network-based-attack-37920

EXAMPLE OF ENTERPRISE'S INCIDENT POLICY

An "incident" or "information security incident" can be thought of as a violation or imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices.

If you observe or suspect prohibited material or programs on (company) systems, or inappropriate use of (company) systems, report it immediately to: security@company.com or (phone number).
If you detect any unusual or suspicious activity on your computer, DO NOT turn off your computer. By turning off the computer, valuable evidence may be lost. For questions about (company)'s Incident Response Program, contact the (company) Incident Response (IR) Team at IR-email@company.com.

Reporting phishing emails

If you receive a phishing email, follow these steps to report to IT:

1. Do not click any links in the email. Do not delete it yet. You may mark it as spam.
2. Forward the email to IT-email@company.com. As long as you haven't clicked on link or downloaded the file, you may stop here.
3. After receiving your notification, IT will create a ticket and may contact you for more information. IT may need to access your computer to view the email.

Reporting phishing incidents

If you also clicked on a link in a phishing email, follow these steps to report to IR team:

1. If you haven't already, follow the steps above for reporting phishing emails, and then continue to the next step.
2. Forward the phishing email to (IT email) and (IR email) and attach the original text you downloaded. Please include *Security Incident* the subject line, along with a brief description of the issue (Ex. Clicked on link in phishing email).

Reporting other incidents

To report a security incident, follow *all* of the steps below:

1. Send an email to (relevant emails) within 1 hour of identifying an incident. Please include *Security Incident* in the subject line, along with a brief description of the incident. When emailing Incident Response (IR) team, please include as many details as possible, including relevant URLs, emails, screenshots, and anything else. It is critical that you notify IR within 1 hour of suspected incident and provide all available information to assist the response team with triage. If email is unavailable, call the (designated person(s)) at (phone number). If ***classified information*** is part of the incident, do not attach the information to your report. Wait for instructions from the Incident Response (IR) team. If you do not receive a timely acknowledgement of your report, you can phone the IR team via the numbers listed in (link to phone numbers).
2. Open an Incident from here (link) describing the incident in **as much detail as possible, excluding sensitive data**. Keep this issue up to date by adding comments with appropriately summarized actions or information from interactions with the IR team. IR must be emailed updates as incidents unfold. * **If you suspect sensitive data is part of the security incident that you're reporting please reach out to the Incident Response team immediately at (Phone number) for next steps**.
3. Do not delete any potential evidence or modify the evidence without instruction from the Incident Response team. Please leave the instance running and reconfigure the Security Group or route for that instance or app to be dismissive of all ingress and egress traffic until a forensics review can be performed. A significant set of data is lost and is unrecoverable when instances or containers are "stopped" or "terminated."
4. Following notification, the Incident Response team will contact you requesting more information.
5. If you cannot access email please call the IT Service Desk at (phone #) and ask them to forward the relevant information to the addresses above.

Please note that incidents need to be reported *within one hour* of being identified. This isn't "within an hour of happening", but "within one hour of you becoming aware of the incident". The idea is to make sure we're promptly looping in the right people. So, as soon as you're aware of a problem, follow the above steps.

What is an incident?

First, it's important to note: it's always OK to err on the side of reporting! IR teams are good at their job, and they are totally used to false alarms. You'll never get in trouble for pinging them about something that turns out not to be an issue! Indeed, *you'll never get in trouble for pinging IR at all*. The most effective security "early warning system" is attentive staff, so "report early, report often"!

On to the answer to "what is an incident?": in a nutshell, an incident is anything that compromises (or could compromise) our "CIA": **Confidentiality, Integrity, or Availability.**

- **Confidentiality** means: "secrets". So personal information (PII) — names, phone numbers, social security numbers, etc — is one very important secret, but so are your passwords, service credentials, internal non-public documents, etc. Any time you suspect that any confidential information may have been leaked outside (company), you should open an incident.

- **Integrity** means the soundness/fitness of purpose of our systems or information. So, if a backup was lost, or if a app stopped logging for a while, or if some documents got deleted — those are integrity issues. Sometimes these can indicate deeper incidents (like an attacker deleting logs to cover their tracks), so it's important to report these, as well.

- **Availability** means the availability of the services we provide. So, if an app goes down, if something we expect to be running stops running — those are availability issues.

Remember: it's totally OK — and encouraged — to fail towards the side of reporting something. Organizations with very healthy IR systems see a lot of false alarms, and a lot of very low severity reports. This is good, because it indicates that people feel comfortable reporting day-to-day issues. The more we do it, the better we'll get at it. And this is ultimately the goal, because then when something serious happens, we'll be well-practiced at handling it smoothly and efficiently.

NETWORKING 101

Different Types of Networks

- **Local-area network** (LAN): The computers are geographically close together (that is, in the same building).
- **Wide-area network** (WAN): The computers are farther apart and are connected by telephone lines or radio waves.
- **Metropolitan-area networ**k (MAN): A data network designed for a town or city.
- **Home-area network** (HAN): A network contained within a user's home that connects a person's digital devices.
- **Virtual private networ**k (VPN): A network that is constructed by using public wires — usually the Internet — to connect to a private network, such as a company's internal network.
- **Storage area network** (SAN): A high-speed network of storage devices that also connects those storage devices with servers.

Network Components, Devices and Functions

Networks share common devices and functions, such as servers, transmission media (the cabling used to connect the network) clients, shared data (e.g. files and email), network cards, printers and other peripheral devices.

The following is a brief introduction to common network components and devices. You can click any link below to read the full Webopedia definition:

Server: A computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks.

Client: A client is an application that runs on a personal computer or workstation and relies on a server to perform some operations.

Devices: Computer devices, such as a CD-ROM drive or printer, that is not part of the essential computer. Examples of devices include disk drives, printers, and modems.

Transmission Media: the type of physical system used to carry a communication signal from one system to another. Examples of transmission media include twisted-pair cable, coaxial cable, and fiber optic cable.

Network Operating System (NOS): A network operating system includes special functions for connecting computers and devices into a local-area network (LAN). The term network operating system is generally reserved for software that enhances a basic operating system by adding networking features.

Operating System: Operating systems provide a software platform on top of which other programs, called application programs, can run. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Network Interface Card (NIC): An expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

Hub: A common connection point for devices in a network. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Switch: A device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model.

Router: A router is a device that forwards data packets along networks. A router is connected to at least two networks and is located at gateways, the places where two or more networks connect.

Gateway: A node on a network that serves as an entrance to another network.

Bridge: A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol

Channel Service Unit/Digital Service Unit (CSU/DSU): The CSU is a device that connects a terminal to a digital line. Typically, the two devices are packaged as a single unit.

Terminal Adapter (ISDN Adapter): A device that connects a computer to an external digital communications line, such as an ISDN line. A terminal adapter is a bit like a modem but only needs to pass along digital signals.

Access Point: A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN.

Modem (modulator-demodulator): A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

MAC Address: A MAC (Media Access Control) address, sometimes referred to as a hardware address or physical address, is an ID code that's assigned to a network adapter or any device with built-in networking capability.

Link to Table of Contents

NETWORK MODELS

To simplify networks, everything is separated in layers and each layer handles specific tasks and is independent of all other layers. Control is passed from one layer to the next, starting at the top layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. Network models are used to define a set of network layers and how they interact. The two most widely recognized network models include the TCP/IP Model and the OSI Network Model.

The 7 Layers of the OSI Model

The Open System Interconnect (OSI) is an open standard for all communication systems.The OSI model defines a networking framework to implement protocols in seven layers.

Physical Layer

This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Examples include Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.

Data Link Layer

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. Examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.

Network Layer

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. Examples include AppleTalk DDP, IP, IPX.

Transport Layer

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.Examples include SPX, TCP, UDP.

Session Layer

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. Examples include NFS, NetBios names, RPC, SQL.

Presentation Layer

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. Examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

Application Layer

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP

The TCP/IP model

The TCP/IP network model is a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.

Application

Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. Protocol examples include HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP.

Transport

Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data. Protocol examples include TCP, UDP, RTP.

Internet

Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams. Protocol examples include IP, ICMP, ARP, RARP.

Network interface

Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire. Protocol examples include Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.

Each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model.

Link to Table of Contents

NETWORK TOPOLOGIES

Network topology refers to the shape or the arrangement of the different elements in a computer network (i.e. links and nodes). Network Topology defines how different nodes in a network are connected to each other and how they communicate is determined by the network's topology.

Topologies are either physical or logical. There are four principal topologies used in LANs.

Bus Topology

All devices are connected to a central cable, called the bus or backbone. Bus networks are relatively inexpensive and easy to install for small networks.

Ring Topology

All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it.

Star Topology

All devices are connected to a central hub. Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the hub.

Tree Topology

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.

These topologies can also be mixed. For example, a bus-star network consists of a high-bandwidth bus, called the backbone, which connects a collections of slower-bandwidth star segments.

From <https://www.webopedia.com/quick_ref/network-fundamentals-study-guide.html>

DNS TERMINOLOGY, COMPONENTS, AND CONCEPTS

Introduction

DNS, or the Domain Name System, is often a very difficult part of learning how to configure websites and servers. Understanding how DNS works will help you diagnose problems with configuring access to your websites and will allow you to broaden your understanding of what's going on behind the scenes.

Domain Terminology

We should start by defining our terms. While some of these topics are familiar from other contexts, there are many terms used when talking about domain names and DNS that aren't used too often in other areas of computing.

Let's start easy:

Domain Name System

The domain name system, more commonly known as "DNS" is the networking system in place that allows us to resolve human-friendly names to unique addresses.

Domain Name

A domain name is the human-friendly name that we are used to associating with an internet resource. For instance, "google.com" is a domain name. Some people will say that the "google" portion is the domain, but we can generally refer to the combined form as the domain name.

The URL "google.com" is associated with the servers owned by Google Inc. The domain name system allows us to reach the Google servers when we type "google.com" into our browsers.

IP Address

An IP address is what we call a network addressable location. Each IP address must be unique within its network. When we are talking about websites, this network is the entire internet.

IPv4, the most common form of addresses, are written as four sets of numbers, each set having up to three digits, with each set separated by a dot. For example, "111.222.111.222" could be a valid IPv4 IP address. With DNS, we map a name to that address so that you do

not have to remember a complicated set of numbers for each place you wish to visit on a network.

Top-Level Domain

A top-level domain, or TLD, is the most general part of the domain. The top-level domain is the furthest portion to the right (as separated by a dot). Common top-level domains are "com", "net", "org", "gov", "edu", and "io".

Top-level domains are at the top of the hierarchy in terms of domain names. Certain parties are given management control over top-level domains by ICANN (Internet Corporation for Assigned Names and Numbers). These parties can then distribute domain names under the TLD, usually through a domain registrar.

Hosts

Within a domain, the domain owner can define individual hosts, which refer to separate computers or services accessible through a domain. For instance, most domain owners make their web servers accessible through the bare domain (example.com) and also through the "host" definition "www" (www.example.com).

You can have other host definitions under the general domain. You could have API access through an "api" host (api.example.com) or you could have ftp access by defining a host called "ftp" or "files" (ftp.example.com or files.example.com). The host names can be arbitrary as long as they are unique for the domain.

SubDomain

A subject related to hosts are subdomains.

DNS works in a hierarchy. TLDs can have many domains under them. For instance, the "com" TLD has both "google.com" and "ubuntu.com" underneath it. A "subdomain" refers to any domain that is part of a larger domain. In this case, "ubuntu.com" can be said to be a subdomain of "com". This is typically just called the domain or the "ubuntu" portion is called a SLD, which means second level domain.

Likewise, each domain can control "subdomains" that are located under it. This is usually what we mean by subdomains. For instance you could have a subdomain for the history department of your school at "www.history.school.edu". The "history" portion is a subdomain.

The difference between a host name and a subdomain is that a host defines a computer or resource, while a subdomain extends the parent domain. It is a method of subdividing the domain itself.

Whether talking about subdomains or hosts, you can begin to see that the left-most portions of a domain are the most specific. This is how DNS works: from most to least specific as you read from left-to-right.

Fully Qualified Domain Name

A fully qualified domain name, often called FQDN, is what we call an absolute domain name. Domains in the DNS system can be given relative to one another, and as such, can be somewhat ambiguous. A FQDN is an absolute name that specifies its location in relation to the absolute root of the domain name system.

This means that it specifies each parent domain including the TLD. A proper FQDN ends with a dot, indicating the root of the DNS hierarchy. An example of a FQDN is "mail.google.com.". Sometimes software that calls for FQDN does not require the ending dot, but the trailing dot is required to conform to ICANN standards.

Name Server

A name server is a computer designated to translate domain names into IP addresses. These servers do most of the work in the DNS system. Since the total number of domain translations is too much for any one server, each server may redirect request to other name servers or delegate responsibility for a subset of subdomains they are responsible for.

Name servers can be "authoritative", meaning that they give answers to queries about domains under their control. Otherwise, they may point to other servers, or serve cached copies of other name servers' data.

Zone File

A zone file is a simple text file that contains the mappings between domain names and IP addresses. This is how the DNS system finally finds out which IP address should be contacted when a user requests a certain domain name.

Zone files reside in name servers and generally define the resources available under a specific domain, or the place that one can go to get that information.

Records

Within a zone file, records are kept. In its simplest form, a record is basically a single mapping between a resource and a name. These can map a domain name to an IP address, define the name servers for the domain, define the mail servers for the domain, etc.

Link to Table of Contents

HOW DNS WORKS

Now that you are familiar with some of the terminology involved with DNS, how does the system actually work?

The system is very simple at a high-level overview, but is very complex as you look at the details. Overall though, it is a very reliable infrastructure that has been essential to the adoption of the internet as we know it today.

Root Servers

As we said above, DNS is, at its core, a hierarchical system. At the top of this system is what are known as "root servers". These servers are controlled by various organizations and are delegated authority by ICANN (Internet Corporation for Assigned Names and Numbers).

There are currently 13 root servers in operation. However, as there are an incredible number of names to resolve every minute, each of these servers is actually mirrored. The interesting thing about this set up is that each of the mirrors for a single root server share the same IP address. When requests are made for a certain root server, the request will be routed to the nearest mirror of that root server.

What do these root servers do? Root servers handle requests for information about Top-level domains. So if a request comes in for something a lower-level name server cannot resolve, a query is made to the root server for the domain.

The root servers won't actually know where the domain is hosted. They will, however, be able to direct the requester to the name servers that handle the specifically requested top-level domain.

So if a request for "www.wikipedia.org" is made to the root server, the root server will not find the result in its records. It will check its zone files for a listing that matches "www.wikipedia.org". It will not find one.

It will instead find a record for the "org" TLD and give the requesting entity the address of the name server responsible for "org" addresses.

TLD Servers

The requester then sends a new request to the IP address (given to it by the root server) that is responsible for the top-level domain of the request.

So, to continue our example, it would send a request to the name server responsible for knowing about "org" domains to see if it knows where "www.wikipedia.org" is located.

Once again, the requester will look for "www.wikipdia.org" in its zone files. It will not find this record in its files.

However, it will find a record listing the IP address of the name server responsible for "wikipedia.org". This is getting much closer to the answer we want.

Domain-Level Name Servers

At this point, the requester has the IP address of the name server that is responsible for knowing the actual IP address of the resource. It sends a new request to the name server asking, once again, if it can resolve "www.wikipedia.org".

The name server checks its zone files and it finds that it has a zone file associated with "wikipedia.org". Inside of this file, there is a record for the "www" host. This record tells the IP address where this host is located. The name server returns the final answer to the requester.

What is a Resolving Name Server?

In the above scenario, we referred to a "requester". What is the requester in this situation?

In almost all cases, the requester will be what we call a "resolving name server" A resolving name server is one configured to ask other servers questions. It is basically an intermediary for a user which caches previous query results to improve speed and knows the addresses of the root servers to be able to "resolve" requests made for things it doesn't already know about.

Basically, a user will usually have a few resolving name servers configured on their computer system. The resolving name servers are usually provided by an ISP or other organizations. For instance Google provides resolving DNS servers that you can query. These can be either configured in your computer automatically or manually.

When you type a URL in the address bar of your browser, your computer first looks to see if it can find out locally where the resource is located. It checks the "hosts" file on the computer and a few other locations. It then sends the request to the resolving name server and waits back to receive the IP address of the resource.

The resolving name server then checks its cache for the answer. If it doesn't find it, it goes through the steps outlined above.

Resolving name servers basically compress the requesting process for the end user. The clients simply have to know to ask the resolving name servers where a resource is located and be confident that they will investigate and return the final answer.

Zone Files

We mentioned in the above process the idea of "zone files" and "records".

Zone files are the way that name servers store information about the domains they know about. Every domain that a name server knows about is stored in a zone file. Most requests coming to the average name server are not something that the server will have zone files for.

If it is configured to handle recursive queries, like a resolving name server, it will find out the answer and return it. Otherwise, it will tell the requesting party where to look next.

The more zone files that a name server has, the more requests it will be able to answer authoritatively.

A zone file describes a DNS "zone", which is basically a subset of the entire DNS naming system. It generally is used to configure just a single domain. It can contain a number of records which define where resources are for the domain in question.

The zone's $ORIGIN is a parameter equal to the zone's highest level of authority by default.

So if a zone file is used to configure the "example.com." domain, the $ORIGIN would be set to example.com..

This is either configured at the top of the zone file or it can be defined in the DNS server's configuration file that references the zone file. Either way, this parameter describes what the zone is going to be authoritative for.

Similarly, the $TTL configures the "time to live" of the information it provides. It is basically a timer. A caching name server can use previously queried results to answer questions until the TTL value runs out.

Link to Table of Contents

THE DIFFERENCE BETWEEN FIREWALLS, IDS, AND IPS

The line is definitely blurring somewhat as technological capacity increases, platforms are integrated, and the threat landscape shifts. At their core we have

- **Firewall** - A device or application that analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port. Packets that do not match policy are rejected.

- **Intrusion Detection System** - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.

- **Intrusion Prevention System** - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.

The functional difference between an IDS and an IPS is a subtle one and is often nothing more than a configuration setting change. For example, in a Juniper IDP module, changing from Detection to Prevention is as easy as changing a drop-down selection from LOG to LOG/DROP. At a technical level it can sometimes require redesign of your monitoring architecture.

Given the similarity between all three systems there has been some convergence over time. The Juniper IDP module mentioned above, for example, is effectively an add-on component to a firewall. From a network flow and administrative perspective, the firewall and IDP are functionally indistinguishable even if they are technically two separate devices.

ICMP is a control protocol, meaning that it designed to not carry application data, but rather information about the status of the network itself. The best-known example of ICMP in practice is the ping utility, that uses ICMP to probe remote hosts for responsiveness and overall round-trip time of the probe messages.

Both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are transportation protocols, they are used to pass the actual data. The main difference between TCP and UDP is that TCP is a connection-oriented protocol, it guarantees that all sent packets will reach the destination in the correct order.

UDP, on the other hand, is a connection-less protocol. Communication is datagram oriented, so the integrity is guaranteed only on the single datagram. Datagrams reach destination and can arrive out of order or don't arrive at all. It's generally used for real time communication, where a little percentage of packet loss rate is preferable to the overhead of a TCP connection.

APPENDIX

Understand the Incident's Background

- What is the nature of the problem, as it has been observed so far?

- How was the problem initially detected? When was it detected and by whom?

- What security infrastructure components exist in the affected environment? (e.g., firewall, anti-virus, etc.)

- What is the security posture of the affected IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?

    - What groups or organizations were affected by the incident? Are they aware of the incident?

    - Were other security incidents observed on the affected environment or the organization recently?

- Define Communication Parameters

    - Which individuals are aware of the incident? What are their names and group or company affiliations?

    - Who is designated as the primary incident response coordinator?

    - Who is authorized to make business decisions regarding the affected operations? (This is often an executive.)

    - What mechanisms will the team to communicate when handling the incident? (e.g., email, phone conference, etc.) What encryption capabilities should be used?

    - What is the schedule of internal regular progress updates? Who is responsible for them?

    - What is the schedule of external regular progress updates? Who is responsible for leading them?

    - Who will conduct “in the field” examination of the affected IT infrastructure? Note their name, title, phone (mobile and office), and email details.

- Who will interface with legal, executive, public relations, and other relevant internal teams?

- Assess the Incident's Scope
  - What IT infrastructure components (servers, websites, networks, etc.) are directly affected by the incident?

  - What applications and data processes make use of the affected IT infrastructure components?

  - Are we aware of compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)

  - What are the possible ingress and egress points for the affected environment?

  - What theories exist for how the initial compromise occurred?

  - Does the affected IT infrastructure pose any risk to other organizations?

- Review the Initial Incident Survey's Results
    - What analysis actions were taken to during the initial survey when qualifying the incident?

    - What commands or tools were executed on the affected systems as part of the initial survey?

    - What measures were taken to contain the scope of the incident? (e.g., disconnected from the network)

    - What alerts were generated by the existing security infrastructure components? (e.g., IDS, anti-virus, etc.)

    - If logs were reviewed, what suspicious entries were found? What additional suspicious events or state information, was observed?

- Prepare for Next Incident Response Steps
    - Does the affected group or organization have specific incident response instructions or guidelines?

    - Does the affected group or organization wish to proceed with live analysis, or does it wish to start formal forensic examination?

    - What tools are available to us for monitoring network or host-based activities in the affected environment?

    - What mechanisms exist to transfer files to and from the affected IT infrastructure components during the analysis? (e.g., network, USB, CD-ROM, etc.)

- Where are the affected IT infrastructure components physically located?

- What backup-restore capabilities are in place to assist in recovering from the incident?

- What are the next steps for responding to this incident? (Who will do what and when?)