PNNL's Pink Elephant Unicorn (PEU)

Cyber Security Capture-the-Flag (CTF) Competition

The PEU team would like to thank you in advance for any challenges that you volunteer to build. In the past 4 years, the largest criticism/suggestion was to reduce confusion/errors (have a standard format that all challenges followed) and to require thorough documentation so that the PEU team can properly troubleshoot and assist participants during the event. Also the need for thorough testing prior to the event, including making challenges more universal across operating system platforms.

As PEU is for Cyber Security education and training, here are our requirements for all submissions:

- **Solvable** – must have a solution that is repeatable
  - Must also have complete documentation - use the instructions in this guide and the template
- **Learning Objective** - think about the Cyber Security concept you are trying to teach
  - To learn or exercise a Cyber-related skill,
  - Use a tool commonly used by Cyber professionals,
  - Or to learn facts about Cyber Security, Critical Infrastructure, etc.
- If possible, worded with a generic **energy-related theme**. For example:
  - Someone must have played a prank on your house as all the lights keep flickering in this pattern. Does "01100110 01101100 01100001 01100111 01111011 01010000 01000101 01010101 01111101" mean something?
    - Answer: flag{PEU}
    - Learning objective: Number Conversion - binary to ASCII, which may help as a fundamental stepping-stone to more advanced number conversions, IPv4 addressing, etc.
- Do not reference any real names, places, etc.
  - Do not make claims or suggestions such as "how to compromise an energy facility"
- If you need help rewording your challenge to have a training-friendly theme or learning objective, please contact the PEU team for assistance.

We have enough space for 400 challenges (combined total, flags/bases/quizzes). However, the PEU team will review all submissions to determine the best fit for the competition. Checking that proper documentation is in place and will contact you if we have questions.

If you volunteer your time to make content and we include it, please do not disclose details and do not work on your own challenges if you attend the competition as a participant.

Contents

PEU Summary

- **Theme = Energy Grid.** If possible, try to make everything about your challenges Energy related in some way, even if just indirectly by spinning a written tale with your scenario. Such as Critical Infrastructure, Industrial Control System protocols, SCADA systems, etc. General Cyber Security and Computer Science themes are still acceptable.
- CTF framework. We are using the Facebook CTF framework (FBCTF) https://github.com/facebook/fbctf

Challenge Overview: https://github.com/facebook/fbctf/wiki/Challenge-Overview

Flag = Puzzle Zone, teams submit the answer flag to earn points ONCE

- Categories and some example ideas:
  - Cryptography – decode something to reveal a flag, such as number conversions, ciphers, and advanced algorithms
  - Reverse Engineering – Participants will be provided with a compiled program and use Strings, IDA Pro (free), Ollydbg, etc. to figure out how the program was built, in order to change/solve it to reveal the flag.
  - Digital Forensics – hunt through an OS for hidden files, flag hidden in slack space, steganography, etc.
  - Cyber Physical – puzzle is solved in the real world using Raspberry Pi, Arduino, or other Cyber Physical things
    - Such as CyPhy Town
  - Human – use of social engineering will reveal some secrets that help to unlock a flag
  - Network Defense – investigate a small PCAP file with WireShark to reveal a flag hidden in the network traffic
  - Scripting – participants write a script in any language of their choice that:
    - Solves a program that runs in command line too fast to humanly solve. When solved, the super-fast program displays the flag
    - Analyzes a huge file (or set of files) to extract the flag
  - Web – flag hidden in the Page Source or a common sub-page that is hidden (no link to it on the main page)
  - Based on Learning Objectives from CSEC or KSAs from NIST NICE Framework
- Upon solving or decoding your flag, it will be obvious because the participant will literally see a standard flag format
  - flag{some_text_here}
  - Participants would simply type their answer as "some_text_here"
- These answers ARE case sensitive

Quiz = Trivia, short answer questions or fill in the blank that can be solved through searching the Internet.

- No True/False or Multiple Choice questions
- Easy to type. The answer should be no longer than a short sentence. 2-3 words is ideal
- ONE unique answer. Double check by performing a Google search for your question. If multiple acceptable answers, either change or don't use your question.
  - If your answer is the first thing that appears or is easily searched, is worth few points
  - If hard to find, worth a lot of points. Should not be impossible to find.
- NOT case sensitive
- Avoid confusion - limit punctuation or don't use answers that are often spelled in a variety of ways, such as "Cyber Security", "cybersecurity", and "cyber-security".

Bases = For use by *Play Zone only*, King-of-the-Hill using a python script to track a flag file on vulnerable systems to know who currently "Pwns" that system. If you want to build something for the Play Zone, please contact PEU Play Zone admins first (contact Daniel.Sanner@pnnl.gov). NOTE: For PEUx5, currently investigating using a different AWS network design as well as new CTF framework as the FBCTF Bases functionality is not well documented and unable to implement at this time.

Hints = We highly recommend hints. If your hint gives a lot of help, consider making it cost points to purchase (cost is optional, but should cost less than the award for the challenge).

- Please *avoid causing extra confusion* with your hints
  - No extra riddles/puzzles in hints, just make hints clear (especially if you are making participants purchase it)
  - You could recommend a tool/skill/URL that could help solve the challenge

How to Create a Flag

Primarily known as the Puzzle Zone. Where participants solve challenges to decode or find a hidden 'flag' using Cyber Security knowledge or skills, which is submitted for points.

Overview:
The goal is to teach the basic concepts of Cyber Security, including Computer Science fundamentals. We are adding an Energy theme this year, so try to include references to the importance of security in critical infrastructure such as Energy. Generalize the references by simply using facts or artificial/fake simulations. *Avoid any statements where you claim to teach how to hack any realistic Energy target*. The goal of PEU is to teach about Cyber Security, **not** to teach people how to hack a real Energy Facility.

Requirements:

1. Send all submissions via e-mail to peu@pnnl.gov
    a. If too large for an e-mail, contact us and we'll figure out a way to get your submission
2. PDF, JPEG, and other common files for your challenge may be attached directly. Please zip any executable scripts or programs before sending (so they aren't blocked by e-mail filters). For large files, please contact a PEU Coordinator first.
    a. **NOTE**: If you are creating an executable program (Forensics, Reverse Engineering, Scripting challenges), please provide the raw/uncompiled code (please also include descriptive comments!) and what we need to compile it on our own. We will have our staff review and compile the code ourselves as an added security precaution.

Documentation is **required for all challenges**, please attach a file to your e-mail: [PuzzleTitle].[docx | txt]. Please fill out the template document that is attached.

- **Author's full name**
- **E-mail**
- **Category** (pick one or please ask if you need a new category)
    - Cryptography, Reverse Engineering, Digital Forensics, Cyber Physical, Human (aka Social Engineering), Network Defense, Scripting, Web, *Trivia*, *Play Zone*
- **Points** (how difficult do you think it is to solve, measured by time and skill required)
    - 100 - anyone can solve, maybe with a little online searching
    - 200 - anyone can solve, requires online searching or use of a simple tool
    - 300 - most can solve, but will take time to figure out. May require use of a skill or tool
    - 400 - difficult to solve even with online searches and the tools/skills needed may be difficult to learn
    - 500 - very difficult to solve, requires a lot of time, many steps, and not easy to look up
    - Other - if you need a higher value, please discuss with a PEU Coordinator
- **Title**
- **Learning Objective** – participants should already know or expected to learn something Cyber/Engery from this challenge
- **Question**
- **Hint** (recommended, but optional)
    - How many points does it cost to purchase your hint. The following is only a suggestion:
        - 0-10% - doesn't help very much, may just be giving away another part of the puzzle
        - 10-25% - references a tool that could help, but doesn't give away much
        - 25-50% - references a website with decent directions
        - 50-75% - is practically a step-by-step walk-through
- **Attachments** (if there are any)
- **How it was built** - just a high-level summary, including any references
- **How to solve** - just a high level summary. Doesn't need to be exact step-by-step instructions. Just explain the tool or skill used and roughly how it should be used to solve the challenge. Assume a PNNL Cyber professional (one of the PEU Coordinators) will be the one using this document to troubleshoot and help participants.
- **Answer** (flag)
    - Flags - must be in this format and is CASE sensitive: flag{some_text_here}
        - All Puzzles (with few exceptions) should reveal their plain text flag when solved
        - Some Play Zone systems will also have flag files (.txt or other) hidden inside files on target systems

Example Cryptography puzzle (documentation)

Name: Dan Sanner
E-mail: Daniel.sanner@pnnl.gov
Category: Cryptography
Points: 300 (only worth 200 points by difficulty, but an extra 100 for estimated time to solve)
Title: Cryptodoku
Learning Objective: Passwords, OTP, Hexadecimal-ASCII conversion
Question: Carly Cryptolady just read about One Time Pad (OTP) as being the most secure form of Cryptography. So she made her own and put it on a sticky note under her keyboard. She failed to understand how important it is to protect a OTP from being stolen. Can you decrypt her passphrase easily?
Hint Cost: 50 points
Hint: There are no zeroes in Sudoku, which should match up with one of the arrows in the message.
Attachment(s): Make a PDF or JPEG screenshot of the following…

Cipher Text message:

↓↓ ↓c ↓← ↓↗ ↗b →↔ ↗→ ↓↑ ↓f ↓b ↗→ ↖↕
↓9 ↗↔ ↖↕ ↓↓ ↗→ ↓e ↗d

Decryption Key:

↔	↙	←	9	↑	↓	7	→	2
9	4	↓	↖	→	↗	↔	↙	←
5	↗	↖	←	↔	8	↓	9	↑
↗	→	9	4	↓	2	↙	1	↔
←	↖	↙	5	7	3	↑	↓	9
↓	3	↑	8	←	9	→	↖	↗
↑	↓	→	3	9	←	↖	↗	↙
2	9	↔	↗	↙	→	←	↑	↓
↙	←	7	6	↖	↑	9	↔	5

Additional instructions to PEU team:

To avoid text formatting issues, save the Cipher Text and Key as a PDF for participants to download. This is probably a level 300 Cryptography due to the time needed to solve it.

How To Solve:

It's just a symbol-based Sudoku that is converted into a Hexadecimal message. Then into ASCII.

3		1	9		6	7		
	4						8	1
5				3	8			4
		9	4		2		1	
			5	7	3			
	3		8		9	5		
4			3	9				8
2	9						4	
		7	6		4	9		5

3	8	1	9	4	6	7	5	2
9	4	6	2	5	7	3	8	1
5	7	2	1	3	8	6	9	4
7	5	9	4	6	2	8	1	3
1	2	8	5	7	3	4	6	9
6	3	4	8	1	9	5	2	7
4	6	5	3	9	1	2	7	8
2	9	3	7	8	5	1	4	6
8	1	7	6	2	4	9	3	5

Original Sudoku puzzle from http://www.websudoku.com/?level=1&set_id=5493866252

Use symbols for a Sudoku that replace those numbers 1-9 (0 is not on the puzzle, 9 is a freebie)
Convert symbols to Base-9 [0,1,2,3,4,5,6,7,8]. Letters A through F are freebies, not a true conversion; just the rest of the 16-character alphabet is filled in.

↕ = 0	↓ = 6	A
← = 1	↗ = 7	B
↖ = 2	↙ = 8	C
↔ = 3	9 = 9	D
↑ = 4		E
→ = 5		F

Cipher Text message (original):
↓↓ ↓c ↓← ↓↗ ↗b →↔ ↗→ ↓↑ ↓f ↓b ↗→ ↖↕ ↓9 ↗↔ ↖↕ ↓↓ ↗→ ↓e ↗d

Convert code to Hexadecimal using simple translation:
66 6c 61 67 7b 53 75 64 6f 6b 75 20 69 73 20 66 75 6e 7d

Convert to ASCII for Plain Text:
flag{Sudoku is fun}

Only type "Sudoku is fun" as the answer.
Answer: Sudoku is fun