Capture the Flag

Exercise Title: CTF – Capture the Flag
Exercise Duration: Custom
Prerequisites: Participants should have a knowledge base and some familiarity (in theory) with one to two of the concepts below. Beginners will practice the techniques associated with the theory and advanced players will demonstrate the Knowledge Skill or Ability to perform them in this cyber exercise challenge.

- Linux command line knowledge
- Windows and Linux service exploitation
- Port scanning, networking scanning, vulnerability scanning
- SQL injection
- PHP code exploitation
- PII discovery
- Privilege escalation
- Brute force
- Password hash cracking
- Forensics and reverse engineering
- Reconnaissance or Open Source Intelligence (OSINT) gathering
- Understanding of basic network functions, standards, and protocol
- Familiarity with a Scripting language–with a focus on Python and PowerShell
- Some knowledge of common Logical Security Controls

Target Market: All
Objective: Execute exploits to obtain firsthand knowledge of network vulnerabilities. Through the use of open source exploits, network defenders and Red Teamers will better understand the vulnerabilities in networks. The CTF is like no other environment commonly known and by enumerating and exploiting a living city, participants will gain hands-on, real world experience in a safe environment.
Instructor / Facilitator: Merit Network (Ann Arbor) and attend at your local Cyber Hub
Location: Live online remote (attend from work or home)
Technical Service Requirements: The CTF exercise utilizes VMWare View Client Horizon (free), internet, bring your own device (BYOD).

Who Should Attend?

Participants should have a baseline of security knowledge and familiarity of security concepts. Those new to security should first attain basic knowledge and some familiarity with common tools and techniques. While mastery is not required, understanding of common vulnerabilities and their remediation is recommended. Introductory challenges such as Linux and Python provide a great baseline for the beginner. For those with experience, the CTF provides a world class and challenging game for all levels of security practitioners. Players ranging from the most experienced red and blue teamers in the world to beginners, will stay engaged and challenged by this exercise.

Overview?

Capture the Flag is a gamified learning tool, developed by carving out core servers and network infrastructure from Alphaville. Participants traverse through

challenges in Alphaville to find flags and input them into the scoring system. As individual participants or in teams, they use penetration testing and forensic skills to gather clues and collect evidence. A self-paced exercise, the CTF is a means to assess individual skills across a broad range of systems and challenges. Individuals or small groups pursue threads of artifacts in a timed, scored environment. Each thread is built around a specific security skills set, such as web, SQL, and password security. Recovering artifacts gets harder as the player progresses along the thread, providing an active, adaptable challenge. Host a CTF at an organization, a tech conference, or anywhere else with an internet connection OR get long term access for a deep dive into the many challenges and obstacles. CTF is divided into over 19 tracks, all independent of each other. If a player progresses partially through one track and would like to play elsewhere, they can simply go back to the Challenge page and select a different track.

Capture the Flag is an excellent approach to learn deeply technical concepts in a non-traditional, gamified environment.

What is it? Gamified learning tool, developed by carving out core servers and network infrastructure inside Merit's virtual Cyber city, Alphaville. Participants traverse through challenges in Alphaville to find flags and input them into the scoring system. Flags have various points based on difficulty. The scoreboard tracks participant's progress throughout the day.

What does it include? Virtual access to a robust online cyber exercise. All participants are shown how to access and interact with the CTF environment through the in game tutorial. Inside the exercise, assistance in how to solve challenges is offered via hints for a reduction in points for any challenge. A top score announced at the end of the exercise.

Why take this class? The CTF is not a class, it is a self-paced progression through systems as they exist in the real world. It represents a means to assess individual skills across a broad range of systems and challenges. The CTF is also mapped to the NICE / NIST framework which gives participants an indication that they can perform the corresponding KSA-T.

What sets this Capture the Flag aside from all others?

- **Each player or team receives their own set of over 20 VMs.** Everyone has their own environment. Each player's instance is completely contained and unique to that individual. If one player accidentally "takes down" their School server with a Hail Mary Attack, it doesn't affect or impede the game for the rest of the players.
- **It can be accessed from anywhere in the world.** As long as your computer has an internet connection, you can connect to the CTF.
- **We aren't relying on brick and mortar machines for each CTF exercise.** They are all virtual machines. The Michigan Cyber Range virtual infrastructure can support up to 100+ simultaneous players, each with their own isolated virtual environment.
- **Capture the Flag has over 100 challenges!** Content in the CTF is the largest virtual collection known today and it mirrors almost every instance of web connectivity. It often

takes individuals over a year to progress through the entire game.
- **Dynamic and diverse content alleviates frustration and encourages learning.** Along with the challenges, there are nearly 200 trivia questions. Hints help track ability level by reducing scores but keep players engaged and learning.
- **CTF is updated frequently to keep pace with a fast changing landscape!**

Required Skills

CTF participants should have basic computer skills, familiarity with the command line, understanding of
IP addressing and DNS, familiarity with basic security concepts, problem solving skills, and Resourcefulness. Often participants will not know all the solutions to problems encountered in the CTF so some solutions will require research outside of the game. All participants must hold intermediate-to-advanced cybersecurity and programming skills to succeed in the exercise!

NOTE: Participants are shown how to access and interact with the CTF environment through the in game tutorial. Assistance in how to solve challenges is offered via hints for a reduction in points for that challenge.

Necessary Knowledge Base

Participants should have a knowledge base and some familiarity (in theory) with one to two of the concepts below. Beginners will learn the techniques associated with the theory and advanced players will demonstrate the Knowledge Skill or Ability to perform them.

- Linux command line knowledge
- Windows and Linux service exploitation
- Port scanning, networking scanning, vulnerability scanning
- SQL injection
- PHP code exploitation
- PII discovery
- Privilege escalation
- Brute force
- Password hash cracking
- Forensics and reverse engineering
- Reconnaissance or Open Source Intelligence (OSINT) gathering
- Understanding of basic network functions, standards, and protocol
- Familiarity with Scripting language – with a focus on Python and PowerShell
- Some knowledge of common Logical Security Controls

Why a CTF? Learning Objectives

Computer security represents a challenge to education due to its interdisciplinary nature. Topics in computer security are drawn from areas ranging from theoretical aspects of computer science to applied aspects of information technology management. This makes it difficult to encapsulate the spirit of what constitutes a computer security professional.

One approximation for this measure is the 'capture the flag' competition. Attack-oriented CTF competitions try to distill the essence of many aspects of professional computer security work into a single short or long term exercise that is objectively measurable. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploitation, creative thinking, toolkit

knowledge, and operational tradecraft.

Game Details

CTF is divided into 19 tracks, all independent of each other. If a player progresses partially through one track and would like to play elsewhere, they can simply go back to the Challenge page and select a different track.

1. Linux 100
   Basic Linux, functionality
   Basic Linux command line skills
   Networking
   OS fundamentals
   Basic built-in tools

2. Linux 101
   Basic Linux, functionality
   Basic Linux command line skills
   Networking
   OS fundamentals
   Basic built-in tools

3. Python 101
   Basic python syntax
   Logic problem solving
   Basic functions and command line operations

4. Find PII (Library)
   Online card catalog with public workstations
   Securing PII
   Service Discovery
   Database vulnerabilities

5. School Computer
   A high school with older than average OS versions in use
   Reverse Engineering
   Service Exploitation

6. Deface the Website (City Hall)
   Holds vital records and facilitates city services requests
   Coding Weaknesses

7. Are you SCADA the dark?
   City power grid, which includes a generator, substations, and smart meters
   Service Exploitation
   SCADA
8. Zenda is owned!
   Private business
   Incident Response & Forensics

9. Recon 101
   Reconnaissance or Open Source Intelligence (OSINT) gathering is an important first step in penetration testing. A pen-tester works on gathering as much intelligence on your organization and the potential targets for exploit. Reconnaissance denotes the work of information gathering before any real attacks are planned.

10. Networking 101
    A strong foundation of basic networking concepts is fundamental to a successful career in information technology. You will gain an understanding of basic network functions, standards, and protocols, to prepare you to tackle advanced networking skills.

11. PowerShell 101
    Learn to control Windows via the command line and gain power over this widespread operating system. Windows PowerShell is a task-based, command-line, automation platform and scripting language that allows you to simplify the management of your systems. Learn common logic.

12. PowerShell 102
    Learn to control Windows via the command line and gain power over this widespread operating system. Windows PowerShell is a task-based, command-line, automation platform and scripting language that allows you to simplify the management of your systems. Learn basic cmdlets and common logic.

13. Cryptography 101
    Cryptography is the reason we can transmit sensitive information over the internet and protect our privacy when storing data. Cryptography aims to protect data from viewing by third parties, and cryptanalysis is the study of cryptographic systems to find weaknesses. This track contains aspects of both cryptography and cryptanalysis.

    In this track, you will be challenged to analyze and break classical codes, find steganographic data hidden in files, and break weak forms of encryption. You will also demonstrate knowledge of how to use modern cryptography tools such as open ssl and gpg.

14. Binary Forensics (New)
    This module is for teaching basic analysis of malicious binary executables, and network protocols. In this module you learn how to get useful strings out of a binary using Nmap to gain insight into C2 (Command and Control) locations. You will also use NMap to gain insight into networked protocols, and content. This module also covers Network capture and
    Reverse Engineering.

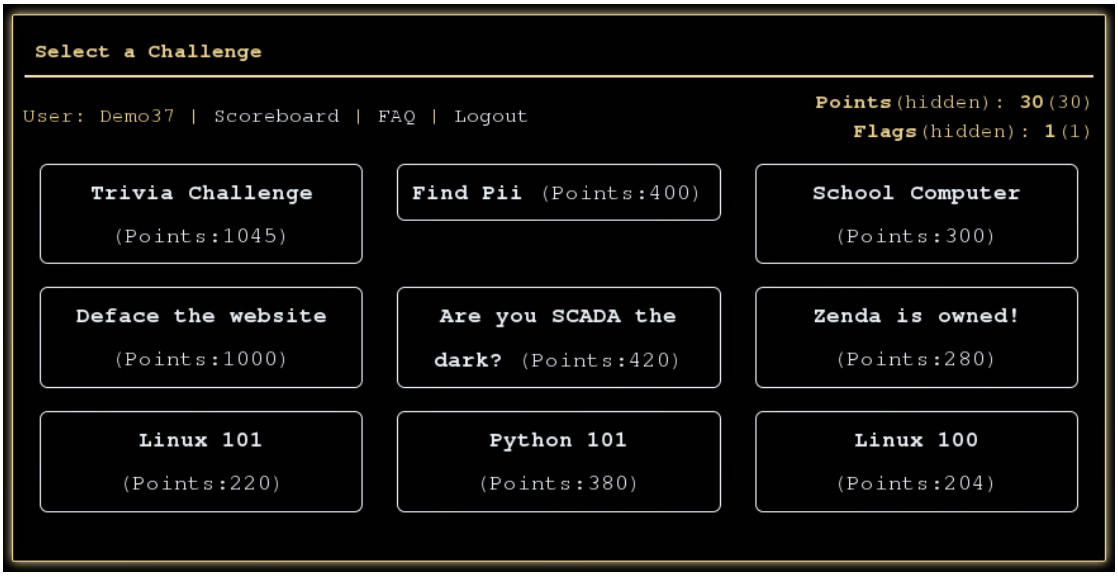
15. Network Forensics (New)
    Network Forensics explores the basics of analyzing and monitoring network traffic. This can be used to help monitor for anomalous traffic and identify intrusions.

16. Digital Forensics (New)
    The purpose of this challenge is to find evidence of data exfiltration from an MS Windows partition, from an employee who engaged in corporate espionage.

17. GIT 101 (New)
    The purpose of this challenge is to teach the users the fundamentals of a source control tool,

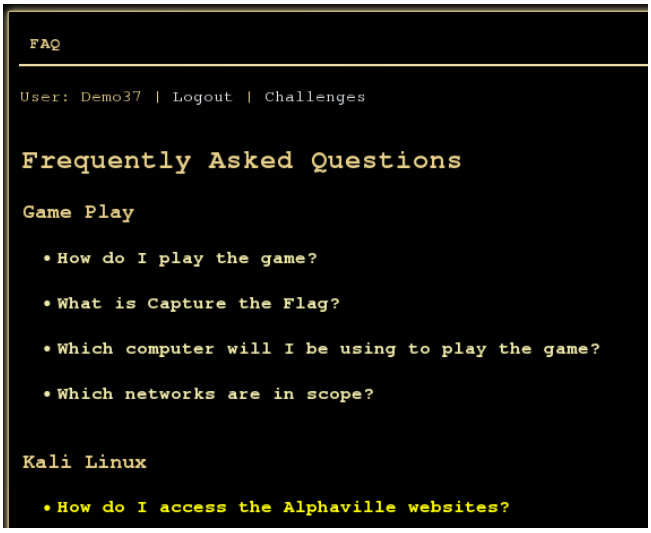
namely GIT.

18. Trivia Challenge (possibly no point value to winning flags dependent on event)
    Test your trivia knowledge in these categories: Windows, Security, Network, General, Linux, History, Forensics, and Movies.



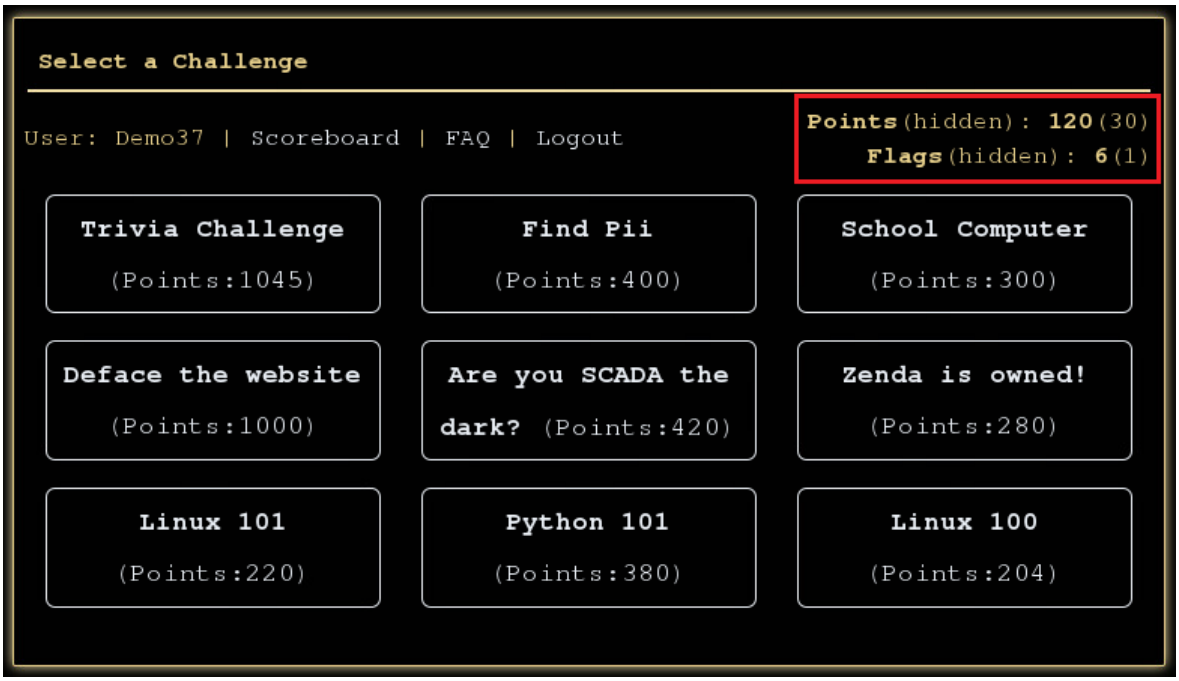
CTF FAQ

Capture the Flags starts players off in a FAQ where they can learn how gameplay works and answer any other general questions about the game.



Scoring Engine

The CTF scoring engine keeps track of player progress with a scoring engine that records both flags and hidden flags during game play and displays your score inside of the game at the top right.



As players find flags, different flag codes are entered into the scoring engine. If players get stuck, hints can be unlocked with penalty to help players progress through the game. Trivia Challenge has no point value to winning flags. It is used to test your trivia knowledge in these categories: Windows, Security, Network, General, Linux, History, Forensics, and Movies.

Scoreboard

The scoreboard gives information about the players in a CTF event:

- Combined player progress for the entire event except Trivia. (yellow progress bars)
- Current happenings in the game (information in middle circle)
- Top Challenge Rating (CR) – This rating is determined for dividing the score value by the flag number and gives us an idea about the difficulty level of the challenges the player has completed.
- Top Stats based on points.

Note: When the CTF teams play, CR and Top Stats reflect the teams' information.

Capture the Flags Event Types

- Single player game hosted by Cyber Range team member(s) or Cyber Hub administrator(s) – One or more (based on player count) of the MCR technical staff members are there to proctor the game and answer questions about game play. This does not include helping participants with challenges to get flags.

- Team Based Events – Same as single player events except flags are submitted for the team for scoring. Teams can consist of 2 or more players all sharing one Kali Linux VM.

Capture the Flag Durations

How long can a Capture the Flag exercise last? Due to the diverse and abundant amount of content in Capture the Flag, exercise or event durations can be scaled up or down depending on desired outcomes. A 4 to 8 hour event is very common. During this time frame a winner is determined by who can complete the most challenges in the allotted time. This same event could be extended for days if desired. Short term CTFs are usually proctored by a Cyber Hub or MCR technical administrator.

How long does it take to complete all of the challenges? Depending on the experience level, skill set and knowledge of a participant, a CTF can take anywhere from a few days to several months to finish. An expert may be able to finish the entire CTF in a solid day but keep in mind that completion is not always the goal, but to see how many challenges can be completed in an allotted time. Whether it is a single day event or long term access, players work at their own pace and benefits of gameplay only increase with their desire to learn.

For long term gameplay, extended access licenses can be acquired. In long term access cases, Capture the Flag is used as a training tool to sharpen a security team or it can be used for educational purposes to teach red team tactics to students in a classroom setting.

NIST Standards Correlation

The NICE Cybersecurity Workforce Framework (NCWF) is a national resource that categorizes and describes cybersecurity work. It provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work as well as a common set of tasks

and skills required to perform cybersecurity work. Through the process of identifying the cybersecurity workforce and using a standard set of terms we can work together to educate, recruit, train, develop, and retain a highly-qualified workforce. KSAs (Knowledge, Skills, and Abilities (and Tasks)) in this framework have been assigned to all challenges in Capture the Flag to better help qualify the educational and training received from participation.

- See http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-181 for a complete list of KSAs

Limitations

Internet Access

Although researching solutions to challenges during game play is encouraged, there is no internet access inside of the Capture the Flag environment. Internet searches, such as utilizing, "Google" must be done on your host machine or elsewhere.

VMware Horizon Client vs HTML Access

To access Capture the Flag, players connect to a VMware View Desktop, which is a Kali Linux virtual machine. Connecting to a View Desktop can be done via a client that is installed on the host machine or with View HTML Access via a web browser.

Which method should you use?

The VMware View Client requires administrator rights to install but allows the player to use the Kali Linux desktop with multiple monitors.

However, VMware HTML Access does not require the installation of software but only one active windows is available which mean if a player has 2 monitors, the Kali Linux desktop will only be displayed on one screen.

Max supported simultaneous CTF players

The Michigan Cyber Range can support up to 100 simultaneous Capture the Flag instances. This mean that 100 single players or 100 teams can play at once. The average attendance is 30 participants.