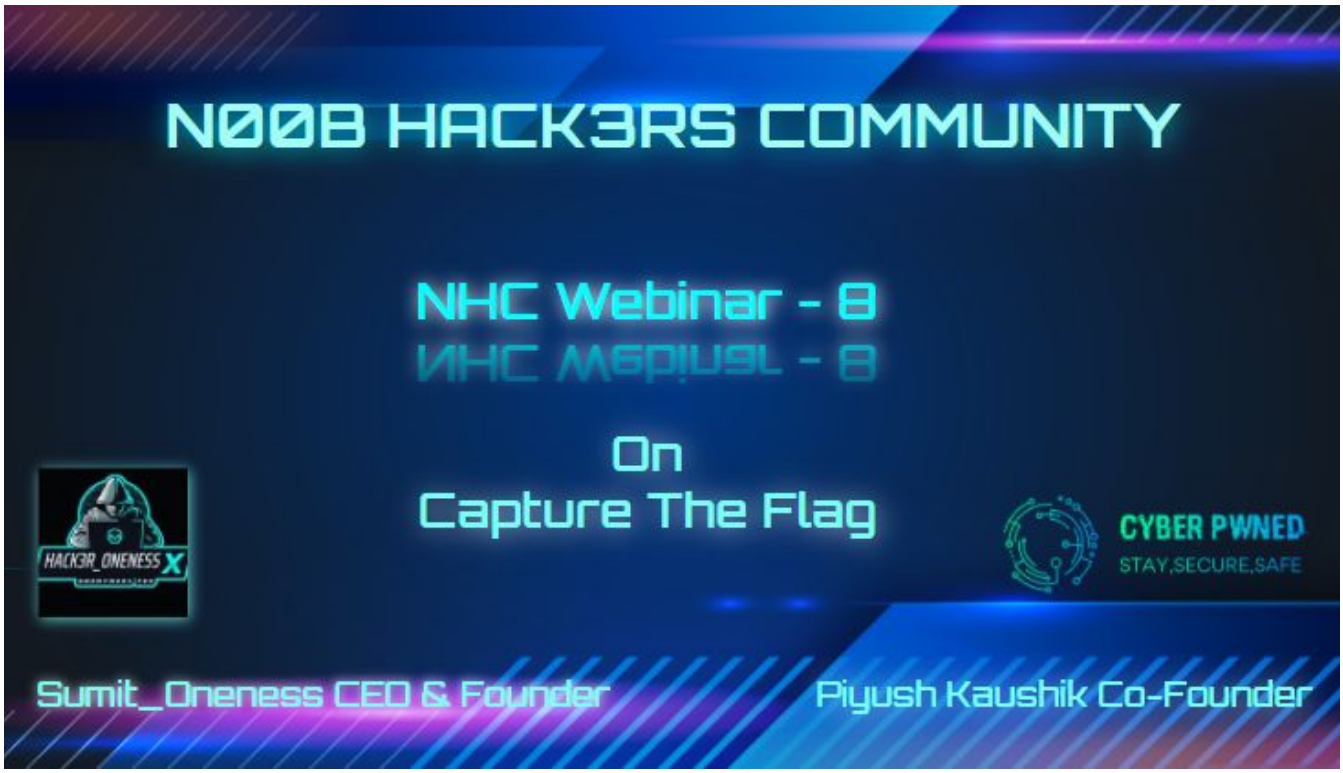


Webinar - 8

Topic : Introduction to Capture the Flag - CTF - Pre-Hacking Assessment

The contents in this pdf has proposed by "Sumit Oneness" in the behalf of NHC.

Note:
This content is prepared only for educational purposes, if somebody misuse it, then the team is not liable for it.

Capture the Flag? : Cisco Says !!

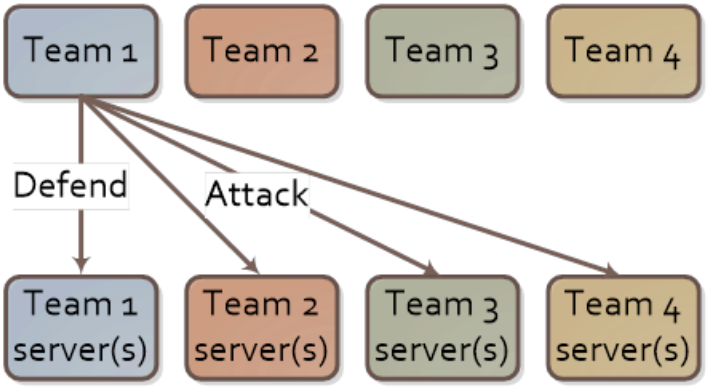
- Cyber security is a high priority of companies, small and big, as cyber attacks have been on the rise in recent years. In response to these attacks, security professionals and college students have been through rigorous training as to how hackers are able to get into the companies and how to defend against them. One way of cyber security training is through a cyber security capture the flag (CTF) event. A cyber security CTF is a competition between security professionals and/or students learning about cyber security. This competition is used as a learning tool for everyone that is interested in cyber security and it can help sharpen the tools they have learned during their training.

- **Origin of CTF :** The very first cyber security CTF developed and hosted was in **1996** at **DEFCON** in **Las Vegas, Nevada. DEFCON is the largest cyber security conference in the United States** and **it was officially started in 1993 by Jeff Moss.** DEFCON had become a platform for a skills competition and as the Internet grew, both DEFCON and the CTF competitions did as well. CTF competitions have become global as they do not have any borders and can be done via the Internet. International teams were competing for different types of prizes and bragging rights. **There are two formats of the cyber security CTF: attack-defend** and **Jeopardy-style.**

Types of CTF :

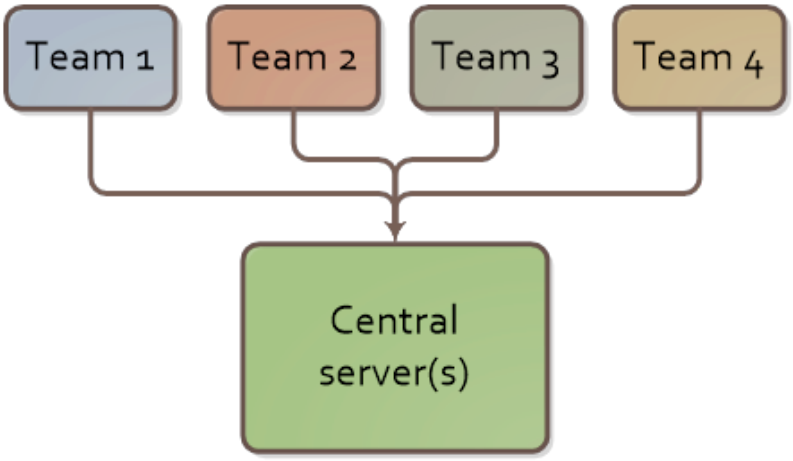
- **Attack & Defense**
- **King of the Hill (KOTH)**
- **Jeopardy (General Beginner)**
- **Linear CTF (Chain of CTF)**

Attack & Defense :



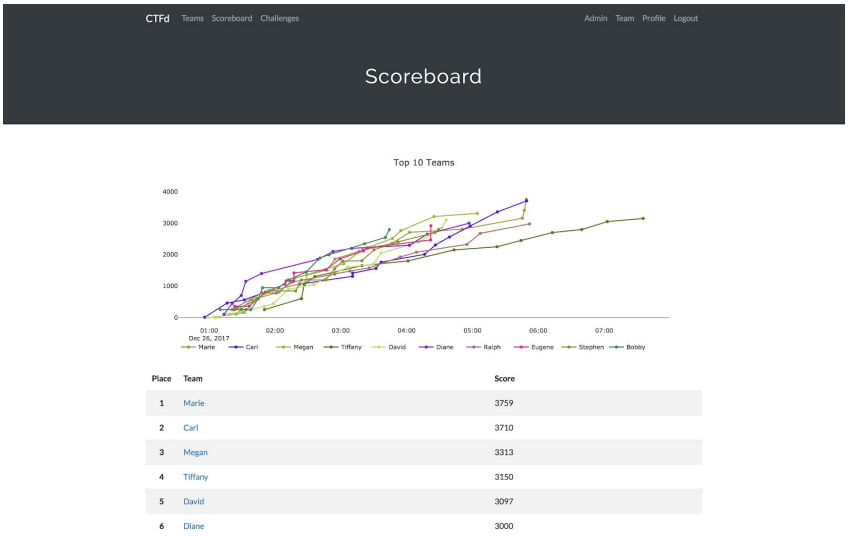
- **Attack and Defense** CTFs consist of a combination of hacking (attack) and securing (defense) systems. In general, each team has one or multiple servers they need to protect. This server can contain both known and unknown vulnerabilities which the teams will have to identify. After identifying a vulnerability, the team should patch this vulnerability in their own server(s) and at the same time exploit the vulnerability in the servers of the other teams. **(Contents took from **CTF.ZONE**)

King of the Hill (KOTH) :



- **King of the Hill CTFs** are CTFs where there is a central set of servers which can be attacked. The teams do not have their own set of servers as in the Attack & Defense CTFs. King of the Hill CTFs are quite often found using blackbox style challenges (without any inside information on the systems involved), where the players need to identify the vulnerability of the remote servers and find out how to exploit them. This can include using Metasploit or public exploits to exploit specific vulnerabilities. After hacking a system the team should try to secure the system to prevent other teams from hacking it as well and blocking them from scoring points. **(Contents took from **CTF.ZONE****)

Jeopardy style CTF :



Place	Team	Score
1	Marie	3759
2	Carl	3710
3	Megan	3313
4	Tiffany	3150
5	David	3097
6	Diane	3000

- Jeopardy style CTFs consist of multiple separate challenges which need to be solved to score points. The style is based on the old TV show Jeopardy because of the similar setup.
- The challenges in a Jeopardy style CTF are divided into specific categories and difficulty levels. In Jeopardy people can have the option to focus on the type of challenges they have experience or knowledge in by choosing which category they try to solve a challenge in.
- This combined with the multiple difficulty levels makes the Jeopardy style CTFs suitable for players with different backgrounds and skills.

Standard Jeopardy CTF Categories :

Network	Anything network related, such as analyzing packet captures (PCAPs) or network communication, port knocking etc.

Crypto	Crypto can be classic crypto algorithms such as substitution, Vigenere and Ceasar (rot13) ciphers. But also encodings like Morse, Braille, Base64 and XOR. More advanced crypto challenges include weaknesses in ECB mode, bit flipping, padding oracle attacks (CBC) and hash function length extension attacks.
Web	All kinds of challenges related to Web and HTTP. Including, but not limited to: SQL injection, Directory traversal, File inclusion, scripting language quirks, XSS, JavaScript decoding.
Forensics	Anything related to Forensics. Quite often also containing Steganography, which is regarded as non-forensics by regular CTF players. Challenges can include Windows, Linux, Android or Exotic platforms forensics.
Binary	Binary challenges are challenges where you get a binary which you need to reverse engineer. Binaries are usually Windows or Linux executables, but can also be from more exotic environments.
Pwnables	Pwnables are challenges where you need to exploit a specific local or remote vulnerability. These vulnerabilities van be hosted on Linux or Windows and can be Buffer overflows, Format strings or a different kind of vulnerability. The level of difficulty can be made harder with mitigations such as ASLR and NX. Pwnable challenges are sometimes also found in the Binary category.

Real Life	Onsite CTFs can also have Real Life challenges such as lock picking, alarm disabling, (fake) bomb defusing, dumpster diving, a laser room, AI or SCADA hacking.
Trivia / Recon	Trivia questions are any kind of knowledge question, answers are usually general knowledge in the security field or can be found by using search engines. Recon stands for reconnaissance and is information gathering by searching online using Google or other tools.

Challenges not fitting in the above categories are usually found in a Misc, Special or Bonus category.

In smaller CTFs the categories might be combined. The challenge categories can also be adjusted for specific themed CTFs.

In case of a specific Forensics CTF you could for example opt for: Malware, Memory forensics, System forensics & Log Files.

Linear CTF :

Linear CTFs are usually story based and consist of a set of CTF challenges which need to be solved in order to reach the final flag. Linear CTFs are mostly used for recruitment purposes where the player can show its skills by solving all challenges. A downside of linear CTFs is that the challenges all need to be solved and also need to be solved in order. Getting stuck on a single challenge means not being able to continue. Because players can only work on one challenge at the time this type of CTF is more suitable for individual players instead of teams.

Environment Setup for CTF :

Kali Linux :

- Kali Linux has a lot of useful tools for solving CTFs challenges.
- Click here for instructions on setting up Kali with VMware.

General Skills Required :

- Python
- Perl
- PHP
- JS
- Basics of HTML, JS & CSS

CTF Online Tools :

- Online Tools to crack CTF Contests🚩 | by Dhanu R
- Morse decoder : https://twsteg.devsec.fr/
- Baconian CTF : https://rumkim.com
- https://github.com/eugenekolo/sec-tools/tree
- Spectrograms : https://academo.org/demos/spectrum-analyzer
- Stegno : https://developertoolkits.com/ocr/image-to-text-converter
- Stegno : https://futureboy.us/stegano/decinput.html
- Crack the hash using John The Ripper :
- john --- wordlist =~/Documents/dictionary.txt hashes.hash (Command)
- Edit Hex Value : hexed.it
- steghide extract -sf file
- Jpeg : With diff:
- diff -a flag_img real_img | hexdump -C
- Pcap : https://pcap.honeynet.org : https://pcapng.com

- DNS Scanner : Dns dumpster
- Hash Analyzer : https://www.tunnelsup.com/hash-analyzer/
- BinWalk Tool Exfiltration
- Convert audio to text : https://speech-to-text-demo.ng.bluemix.net/
- Crypto Morse Decode :
- https://morsecode.world/international/decoder/audio-decoder-adaptive.html
- Guide to use Reverse search engine:
- https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations

Online Websites for Practices against CTF :

Pentest and CTF Labs :

- **HackTheBox : https://www.hackthebox.eu/**
- **Vulnhub : https://www.vulnhub.com/**
- **PracticalPentestLabs : https://practicalpentestlabs.com/**
- **Labs Wizard Security : https://labs.wizard-security.net/**
- **Pentest Lab : https://pentesterlab.com/**
- **Hackthis : https://www.hackthis.co.uk/**
- **Shellter : https://shellterlabs.com/pt/**
- **Root-Me : https://www.root-me.org/**
- **Zenk-Security : https://www.zenk-security.com/epreuves.php**
- **W3Challs : https://w3challs.com/**
- **NewbieContest : https://www.newbiecontest.org/**
- **The Cryptopals Crypto Challenges : https://cryptopals.com/**
- **PenetrationTestingPracticeLabs: http://www.amanhardikar.com/mindmaps/Practice.html**
- **alert(1) to win : https://alf.nu/alert1**
- **Hacksplaining : https://www.hacksplaining.com/exercises**

- **Hacker101 : https://ctf.hacker101.com/**
- **Academy Hackaflag : https://academy.hackaflag.com.br/**
- **PentestIT LAB : https://lab.pentestit.ru/**
- **Hacker Security : https://capturetheflag.com.br/**
- **PicoCTF : https://picoctf.com/**
- **Exploitation Education : https://exploit.education/**
- **Root in Jail : http://ctf.rootinjail.com/**
- **CMD Challenge : https://cmdchallenge.com/**
- **Try Hack Me : https://tryhackme.com/**
- **Hacking-Lab: https://www.hacking-lab.com/index.html**
- **PWNABLE : https://pwnable.kr/play.php**
- **WHO4REYOU : https://34.73.111.210/**
- **Google CTF : https://capturetheflag.withgoogle.com/**
- **ImmersiveLabs : https://immersivelabs.com/**
- **Attack-Defense : https://attackdefense.com/**
- **OverTheWire : http://overthewire.org/**
- **SANS Challenge : https://www.holidayhackchallenge.com/**
- **SmashTheStack : http://smashthestac.com/**

“NHC Learning Material! Please Read it carefully, also helpful for Quiz ASSIGNMENT”

Thanks & Regards

From,

N00B HACK3RS COMMUNITY], NHC

Founder : Sumit Oneness

Co-Founder : Piyush Kaushik

15-08-2020