Cyber Security Practical Exam – ALL 24 PRACTICALS (Kali Linux)

Ethical Declaration: All practicals are performed on DVWA / Metasploitable in a controlled lab for academic purposes only.

COMMON INITIAL STEPS (FOR EVERY PRACTICAL)

```
sudo service apache2 start → start web server
sudo service mysql start → start database
ifconfig → check IP address
firefox http://127.0.0.1 → open DVWA / local lab
```

1. Nmap – Network Mapper

```
nmap -sn 127.0.0.1 → host discovery
nmap -sS 127.0.0.1 → TCP SYN scan
nmap -sV 127.0.0.1 → service & version detection
nmap -O 127.0.0.1 → OS detection
nmap -sC 127.0.0.1 → default scripts
nmap -sU 127.0.0.1 → UDP scan
```

2. Wireshark – Packet Analysis

```
wireshark → start Wireshark
Capture Filter: icmp → capture ICMP packets
Display Filter: tcp.port==443 → HTTPS analysis
Display Filter: dns → DNS packet analysis
```

3. John the Ripper – Password Cracking

```
hashid hashes.txt → identify hash type
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
hashes.txt
john --show hashes.txt
```

4. Whois – Domain Lookup

```
whois google.com → registrar & registrant info
```

5. Dig – DNS Query

```
dig google.com → A record
dig google.com MX → mail servers
```

```
dig google.com NS → name servers
```

6. TheHarvester – OSINT

```
theHarvester -d example.com -b all
```

7. Sublist3r – Subdomain Enumeration

```
sublist3r -d example.com -o subdomains.txt
```

8. Dirbuster – Hidden Directories

GUI Tool → Target URL → Wordlist: /usr/share/wordlists/dirbuster/

9. Gobuster – Directory Brute Force

```
gobuster dir -u http://testphp.vulnweb.com -w
/usr/share/wordlists/dirb/common.txt
```

10. Hydra – Bruteforce (Metasploitable)

```
hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt
ssh://192.168.56.101
```

11. DNSenum – DNS Enumeration

```
dnsenum example.com → DNS records & enumeration
```

12. Shodan – Internet Device Search

Search examples:

port:22, http.title:"login", country:IN

13. Zphisher – Phishing Attack

Technique: Social Engineering (Phishing)

Impact: Credential theft

14. Burp Suite – Intruder

```
burpsuite → start Burp
```

Attack Type: Sniper

15. Metasploitable – Information Gathering

```
nmap -sV 192.168.56.101 → service detection
nmap -O 192.168.56.101 → OS detection
```

16. Metasploitable – Exploitation (SMB/FTP/SSH/Telnet)

Exploiting weak services discovered during scanning

17. DVWA – SQL Injection

Set DVWA Security: LOW

Improper input validation leads to database leakage

18. DVWA – Blind SQL Injection

Infer data using TRUE/FALSE response behavior

19. DVWA – Hash Cracking (Hashcat)

```
hashcat -m 0 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat --show hashes.txt
```

20. DVWA – File Upload Vulnerability

```
Payload test.php
```

21. DVWA – File Inclusion

Manipulate file parameter to include local files

22. DVWA – Command Injection

```
ls → list directories
pwd → present directory
whoami → current user
```

23. DVWA – XSS (Stored)

```
alert('XSS')
```

24. Burp Suite – DVWA Bruteforce Login

Proxy ON → Intercept → Intruder Sniper attack

UNIVERSAL REPORT FORMAT (USE FOR ALL PRACTICALS)

Title
Objective
Tools Used
Procedure
POC (Screenshots)
Impact
Prevention & Mitigation
Best Practices
Ethical Declaration