CrackMapExec (CME) - Ethical Hacking Notes + Hacker Mindset

What is CrackMapExec?

- A post-exploitation tool for red teamers and pentesters.
- Commonly used in Windows/Active Directory environments.

Main Capabilities:

- Enumerate SMB shares and domain info.
- Test credentials against multiple hosts.
- Execute commands remotely.
- Dump password hashes and pivot through networks.

Sample Command:

```
crackmapexec smb 192.168.56.11 -u victimuser -p 1234 --exec-method smbexec -x "netsh advfirewall set al
```

Hacker Mindset Breakdown:

1. crackmapexec smb

- Targeting the SMB protocol (TCP port 445).
- Used to scan, enumerate, and execute commands.

2. 192.168.56.11

- The victim's IP address inside a local or lab network.
- Previously identified as live and reachable.

3. -u victimuser -p 1234

- Using known or guessed credentials.
- May have been found via previous attack or password spraying.

4. --exec-method smbexec

- Method for executing commands over SMB without touching disk.
- Avoids AV/EDR by being 'fileless' in many cases.

5. -x "netsh advfirewall set allprofiles state off"

- The actual payload: disables all Windows firewalls.
- Clears the way for reverse shells or pivoting tools.

Post-Command Hacker Goals:

- Drop payloads (e.g., PowerShell reverse shells).
- Add persistence (e.g., create user, backdoor).
- Explore network (map targets, scan, dump hashes).

Legal Reminder:

- ■ Use only in test labs or with written authorization.
- ■ Unauthorized use is illegal and unethical.