CrackMapExec (CME) - Ethical Hacking Notes

What is CrackMapExec?
- CrackMapExec is a post-exploitation tool used in ethical hacking.
- It's designed for assessing large Active Directory networks.
- Often called the 'Swiss Army Knife' for pentesters.

Key Features:
- SMB enumeration: List shares, users, sessions, etc.
- Credential validation: Test username/password combinations.
- Remote command execution: Run commands on remote Windows machines.
- Lateral movement: Pivot to other systems.
- Hash dumping: Extract NTLM hashes after gaining access.

Common Commands:
1. Basic SMB check:
   crackmapexec smb 192.168.56.11

2. Check shares:
   crackmapexec smb 192.168.56.11 --shares

3. Test credentials:
   crackmapexec smb 192.168.56.11 -u username -p password

4. Remote command execution:
   crackmapexec smb 192.168.56.11 -u username -p password --exec-method smbexec -x "whoami"

5. Disable firewall remotely:
   crackmapexec smb 192.168.56.11 -u username -p password --exec-method smbexec -x "netsh advfirewal

Legal Use:
- ■ OK in home labs and test environments
- ■ Illegal to use on unauthorized systems

Tip: Always use CME responsibly within ethical hacking boundaries.