

Commonly Attacked Network Ports - Ethical Hacking Study Guide

Port | Protocol | Service | Reason for Targeting

22	SSH	Remote shell access	Brute-force attacks, misconfigured auth
23	Telnet	Remote terminal access	Unencrypted, outdated, easy to exploit
21	FTP	File Transfer Protocol	Anonymous login, cleartext credentials
80	HTTP	Web traffic (insecure)	Vulnerable web apps, XSS, SQLi
443	HTTPS	Secure web traffic	Misconfigured certs, hidden pages
445	SMB	Windows file sharing	EternalBlue, WannaCry, RCE attacks
3389	RDP	Windows Remote Desktop	Brute-force, BlueKeep, weak creds
3306	MySQL	Database	Weak auth, data exfiltration
5900	VNC	Virtual Network Computing	No or weak authentication
25	SMTP	Mail server	Relay abuse, phishing spam campaigns

Note: Port scanning tools like Nmap are often used to detect these open ports.
Use firewalls, strong passwords, and patching to reduce risk.

Pro Tip: Obscure ports like 1337, 8080, or 8443 are also used for hidden services.

Legal Reminder:

- ■ Only scan and test on networks you own or have permission to test.
- ■ Unauthorized scanning or exploiting is illegal and unethical.