CompTIA PenTest+ (PT0-002) Ports Sheet

High-yield ports and services for recon, enumeration, validation, and post-exploitation context. Legacy PT0-002 set.

Best for	Focus	Use with
Fast port memorization	Port / protocol / service / use case	Use with commands sheet and quick summary

Port	Protocol	Name	Use case
20/21	TCP	FTP	Legacy file transfer and common comparison point
22	TCP	SSH / SFTP	Secure shell and file transfer
23	TCP	Telnet	Plaintext remote access
25	TCP	SMTP	Mail transfer and phishing infrastructure context
53	TCP/UDP	DNS	Resolution, zone transfer, tunneling scenarios
67/68	UDP	DHCP	Address assignment
69	UDP	TFTP	Simple transfer, weak by design
80	TCP	HTTP	Web apps and cleartext traffic
88	TCP/UDP	Kerberos	Authentication
110	TCP	POP3	Mail retrieval
123	UDP	NTP	Time sync
139/445	TCP	NetBIOS/SMB	Windows file sharing and lateral movement context
143	TCP	IMAP	Mail access
161/162	UDP	SNMP	Monitoring and traps
389	TCP/UDP	LDAP	Directory services
443	TCP	HTTPS	Encrypted web/API traffic
514	UDP	Syslog	Log forwarding
587	TCP	SMTP TLS	Mail submission
636	TCP	LDAPS	Secure LDAP
3389	TCP	RDP	Remote desktop
5900	TCP	VNC	Remote control

Exam traps

53 TCP/UDP	DNS is not just for resolution; think zone transfer, tunneling, and recon value.
139/445 TCP	Windows sharing ports often matter in lateral movement chains.
22 vs 23	SSH is secure access; Telnet is plaintext and a weak-control indicator.
80 vs 443	Web testing logic changes when TLS and proxies are involved.