GIAC Penetration Tester (GPEN) Ports Sheet

High-yield ports and services for enterprise penetration testing, recon, auth testing, and lateral movement context.

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 transfer and insecure comparison point
22	TCP	SSH / SFTP	Secure shell and file transfer
23	TCP	Telnet	Plaintext remote access
25	TCP	SMTP	Mail flow and phishing context
53	TCP/UDP	DNS	Resolution, zone transfer, and recon value
67/68	UDP	DHCP	Address assignment
69	UDP	TFTP	Simple transfer
80	TCP	HTTP	Web apps and cleartext traffic
88	TCP/UDP	Kerberos	Authentication and abuse scenarios
110	TCP	POP3	Mail retrieval
123	UDP	NTP	Time sync
139/445	TCP	NetBIOS/SMB	Windows sharing and lateral movement context
143	TCP	IMAP	Mail access
161/162	UDP	SNMP	Monitoring and recon value
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
5985/5986	TCP	WinRM	Windows remote management

Exam traps

53 TCP/UDP	DNS is not just resolution; think recon, trust mapping, and zone transfer possibilities.
139/445 TCP	Windows sharing ports often matter in lateral movement chains.
22 vs 23	SSH is secure access; Telnet is plaintext and usually a weak-control sign.
5985/5986	WinRM can matter in enterprise admin paths and abuse scenarios.