GIAC Certified Incident Handler (GCIH) Ports Sheet

High-yield ports and services for incident response, lateral movement, detection, and containment workflows.

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 baseline comparison
22	TCP	SSH / SFTP	Secure admin and file transfer
23	TCP	Telnet	Plaintext remote access
25	TCP	SMTP	Mail flow and phishing context
49	TCP	TACACS+	Admin AAA
53	TCP/UDP	DNS	Resolution, tunneling, and C2 context
67/68	UDP	DHCP	Address assignment
69	UDP	TFTP	Simple transfer
80	TCP	HTTP	Plain web and beaconing context
88	TCP/UDP	Kerberos	Authentication and abuse scenarios
110	TCP	POP3	Mail retrieval
123	UDP	NTP	Time sync for logs
139/445	TCP	NetBIOS/SMB	Windows sharing and lateral movement
143	TCP	IMAP	Mail access
161/162	UDP	SNMP	Monitoring and traps
389	TCP/UDP	LDAP	Directory queries
443	TCP	HTTPS	Encrypted web/API/C2 context
514	UDP	Syslog	Log forwarding
636	TCP	LDAPS	Secure LDAP
1812/1813	UDP	RADIUS	Network access AAA
3389	TCP	RDP	Remote desktop and lateral movement

Exam traps

53 TCP/UDP	DNS is not just resolution; think tunneling and command channels too.
139/445 TCP	Windows sharing ports often matter in lateral movement investigations.
22 vs 23	SSH is secure access; Telnet is plaintext and usually a weak-control sign.
80 vs 443	Encrypted traffic changes what you can see and how you investigate it.