CompTIA CySA+ (CS0-003) Ports Sheet

High-yield ports and services for analyst workflows, log review, detection, and investigation 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; often appears in insecure service comparisons
22	TCP	SSH / SFTP	Secure remote access and transfer
23	TCP	Telnet	Plaintext admin access
25	TCP	SMTP	Mail transfer
49	TCP	TACACS+	Admin AAA
53	TCP/UDP	DNS	Resolution, tunneling, and exfil scenarios
67/68	UDP	DHCP	Address assignment
69	UDP	TFTP	Simple transfer, risky in hardened environments
80	TCP	HTTP	Plain web traffic
88	TCP/UDP	Kerberos	Authentication
110	TCP	POP3	Mail retrieval
123	UDP	NTP	Time synchronization
143	TCP	IMAP	Mail access
161/162	UDP	SNMP	Monitoring and traps
389	TCP/UDP	LDAP	Directory queries
443	TCP	HTTPS	Encrypted web/API traffic
445	TCP	SMB	Windows sharing and lateral movement context
514	UDP	Syslog	Log forwarding
636	TCP	LDAPS	Secure LDAP
1812/1813	UDP	RADIUS	AAA for network access
3389	TCP	RDP	Remote desktop

Exam traps

53 TCP/UDP	DNS is not just 'a port to memorize' — it appears in tunneling, exfiltration, and resolution failure questions.
445 TCP	SMB often matters in lateral movement and Windows admin context.
161/162 UDP	SNMP polling and traps serve different monitoring roles.
22 vs 23	SSH is secure; Telnet is plaintext and usually the wrong admin choice.