CompTIA PenTest+ (PT0-002) Commands Sheet

Practical commands and tools for recon, web checks, host validation, packet review, and reporting support. Legacy PT0-002 set.

Best for	Focus	Use with
Command recall before drills	What each command/tool does and when to use it	Use with ports sheet and cheat sheet

1. Recon and enumeration

whois	Pull ownership and registration context.
nslookup / dig	Query DNS records and test resolution.
nmap -sV	Discover services and versions.
nmap -O	Attempt OS detection.
theHarvester / similar OSINT tools	Gather emails, domains, and public footprints.

2. Web and content checks

curl	Test endpoints, headers, methods, and basic responses.
nikto	Quick web server misconfiguration and finding checks.
gobuster / dirb	Enumerate directories and files.
openssl s_client	Inspect TLS handshakes and certificates.
Burp-style proxy workflow	Intercept and manipulate web traffic during testing.

3. Host and network checks

ipconfig / ifconfig / ip a	Check local addressing and interfaces.
ping	Test reachability.
tracert / traceroute	Map path to a target.
arp -a	Inspect local ARP cache.
netstat -ano / ss	View sockets, listeners, and sessions.

4. Packet and log visibility

tcpdump	Capture packets on Unix-like systems.
Wireshark filters	Isolate protocols, hosts, and suspicious flows.
grep / findstr	Search evidence in output or files.

journalctl / Get-WinEvent	Review logs on Linux or Windows.
smbclient / ftp / ssh	Interact with exposed services during validation.

5. Practical reminders

Validate before report	Do not report raw scanner output as finished truth.
Minimize impact	Proof should be enough to confirm risk, not enough to break the client.
Keep notes live	Commands, outputs, and timestamps should be captured during the engagement.
Tie evidence to remediation	Every finding should point to a useful fix.