GIAC Penetration Tester (GPEN) Commands Sheet

Practical commands and tools for recon, web testing, host checks, packet review, and reporting support.

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 discovery

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

2. Web and auth testing

curl	Check methods, headers, and baseline responses.
gobuster / dirb	Enumerate directories and files.
nikto	Quick web server checks.
openssl s_client	Inspect TLS/certificate behavior.
proxy workflow	Intercept and manipulate requests during web testing.

3. Host and network checks

ipconfig / ifconfig / ip a	Review interfaces and addressing.
ping	Test reachability.
tracert / traceroute	Map network path.
arp -a	Inspect local ARP cache.
netstat -ano / ss	View open ports and sessions.

4. Packets and evidence

tcpdump	Capture packets on Unix-like systems.
Wireshark filters	Isolate useful traffic quickly.
grep / findstr	Search logs and command output.

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

5. Practical reminders

Validate before reporting	Do not ship raw scan output as final truth.
Minimize impact	Proof should confirm risk without unnecessary damage.
Keep notes live	Commands and outputs belong in the report trail.
Map evidence to fix	Every finding should lead to useful remediation.