GIAC Security Essentials (GSEC) Commands Sheet

Practical commands for host checks, DNS, packet review, logs, and hands-on security validation.

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

1. Basic host checks

ipconfig /all	Check Windows addressing, gateway, DNS, and lease state.
ifconfig / ip a	Inspect interfaces on Unix-like systems.
ping	Test basic reachability and latency.
tracert / traceroute	Map the path to a target.
arp -a	View local ARP cache entries.

2. DNS and network checks

nslookup / dig	Query DNS records and resolution behavior.
netstat -ano / ss	View listeners, sockets, and sessions.
route print / ip route	Inspect routing decisions.
whois	Get domain and ownership context.
curl -I URL	Quick HTTP header and reachability check.

3. Packet and service visibility

tcpdump	Capture packets on Unix-like systems.
Wireshark filters	Narrow traffic by host, protocol, or field.
nmap -sV	Identify exposed services and versions.
openssl s_client	Inspect TLS handshakes and certificates.
grep / findstr	Search output and logs quickly.

4. Log and process review

journalctl	Review Linux logs.
Get-WinEvent	Query Windows event logs.
tasklist / ps	List running processes.

taskkill / kill	Terminate a process if needed during response.
show logging	On supported network devices, review recent events.

5. Practical reminders

Correlate sources	Do not rely on one log, one packet, or one command alone.
Time matters	Logs without time sync reduce investigation value.
Validate safely	Confirm issues without creating unnecessary impact.
Document findings	Good notes support both learning and real operations.