GIAC Certified Incident Handler (GCIH) Commands Sheet

Practical commands for triage, DNS checks, packet review, log investigation, and response 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. Host and network triage

ipconfig /all / ifconfig / ip a	Check addressing, DNS, and interface state.
ping	Test reachability quickly.
tracert / traceroute	Map the path to a destination.
arp -a	Inspect local ARP cache.
netstat -ano / ss	See listeners, sockets, and sessions.

2. DNS and service investigation

nslookup / dig	Inspect DNS records and resolution behavior.
whois	Get infrastructure ownership context.
curl -I URL	Quickly inspect web headers and responses.
openssl s_client	Validate TLS handshake and certificate details.
nmap -sV	Identify exposed services and versions.

3. Packet and evidence review

tcpdump	Capture packets on Unix-like systems.
Wireshark filters	Isolate suspicious protocols, hosts, and flows.
grep / findstr	Search output, logs, and extracted artifacts.
journalctl	Review Linux logs.
Get-WinEvent	Query Windows event logs.

4. Process and response checks

tasklist / ps	List running processes.
taskkill / kill	Terminate a process if containment requires it.
hash utilities	Verify integrity or compare artifacts.

EDR console actions	Host isolate, kill process, collect triage package where supported.
show logging	Useful on network gear during incident scoping.

5. Practical reminders

Correlate before concluding	Use host, network, and auth evidence together.
Preserve timeline	Timestamps and order of events matter.
Check scope after first hit	One compromised host may be the tip of the problem.
Tie evidence to action	Every response step should link back to validated findings.