1 ROLE RESPONSIBILITIES

Detect, find the user, find the hole, assess scope, on your assigned OS. Command detail lives in the Linux/Windows Hardening References; this is the hunting workflow.

2 ORDER OF OPERATIONS

Baseline, day one: User list, process list, listening ports, cron/scheduled tasks for your host.

Ongoing: Watch the SIEM. Manual spot-check pass on your host periodically.

On detection: Rule out a teammate's untracked change. Report host, time, symptom to Captain.

Find user, then hole, then scope: In that order. Hand off to the engineer once confirmed.

After eviction: Re-check your host for the same pattern before calling it closed.

3 FIND THE USER

- *Linux:* `w`, `who`, `last`. Compare vs. `/etc/passwd` baseline.
- *Windows:* `query user`, Event ID 4624/4625. Compare vs. `Get-LocalUser` baseline.
- Either OS: a low-privilege account suddenly in an admin/sudo group is a signal on its own.
- `lastlog` (Linux): last login time per account, even ones never logged into.

4 TRACE A PROCESS TO ITS OWNER

- *Linux:* `ps -o user,pid,ppid,cmd -p [PID]`. `lsof -p [PID]` for open files/sockets.
- *Windows:* `Get-CimInstance Win32_Process -Filter "ProcessId=[PID]"` for `ParentProcessId`. Sysmon Event ID 1 if installed, includes hash and full command line.
- A shell spawned from a web server or service process is not normal, either OS.

5 FIND THE HOLE

- Weak/reused password: auth logs, repeated failures then a success, or an unfamiliar source address.
- Exposed/unpatched service: an unexpected listening port, or a known vulnerable version.
- Leftover backdoor: cron job, scheduled task, a modified startup file (`.bashrc` is a known trick), or a WMI event subscription.
- Forgotten trust path: an unrecognized `authorized_keys` entry, or an over-privileged service account.
- `find / -newer /etc/passwd -type f 2>/dev/null`: files modified since a known-stable point.
- `find / -perm -4000 -type f 2>/dev/null`: SUID binaries; compare against a known-good list.

6 CROSS-REFERENCE THE TIMESTAMP

- *Linux:* `grep "Accepted" /var/log/auth.log`, filtered to the window from Find the User.
- *Windows:* `Get-WinEvent -LogName Security`, Event ID 4624/4625, same window.
- The login that started the session is in that window.
- `ausearch -ts recent`: pull recent audit events on Linux by time window directly.

7 ASSESS THE SCOPE

- Lateral movement: connections to hosts it does not normally talk to. `ss -tunp` (Linux) or `Get-NetTCPConnection` (Windows).
- Exfiltration: unusual volume, or an unfamiliar destination.
- Affected resources: which services, databases, or files it touches.
- Other hosts: hand this to the SIEM lead. They can check every host at once.

8 RED TEAM TOOLING SIGNATURES

- *Ansible artifacts, Linux:* a `.ansible/tmp` directory under a user's home or `/root`, holding short-lived Python scripts. Confirm with the team before treating it as hostile; it means automated push tooling, red or blue.
- *Impacket psexec/smbexec, Windows:* Event ID 7045, a newly installed service with a short random name, `cmd.exe` spawned from `services.exe`.
- *Impacket wmiexec, Windows:* `cmd.exe` spawned from `WmiPrvSE.exe`, an abnormal parent for an interactive shell.
- *Pass-the-hash (CrackMapExec, Impacket):* Event ID 4624 logon type 3 immediately followed by 4648, same source, same second.
- *LOLBins worth flagging:* `certutil.exe -urlcache` (download disguised as a cert op), `regsvr32.exe /i:http...` (Squiblydoo), `mshta.exe`, `bitsadmin.exe /transfer`. None normally reach the internet.
- A short-lived, random-named file in `C:\Windows\Temp` or `ADMIN$`: an automated exploitation framework, not a human operator.

9 LINUX EXTRAS

- `history` / `/.bash_history`: check for commands an attacker ran, but treat as untrusted if they had access to edit it.
- `rkhunter --check` or `chkrootkit`: quick rootkit sanity check.
- `systemctl list-timers`: systemd timers are a cron alternative attackers also use for persistence.
- `diff` a fresh `ps -ef` / `ls` against a saved baseline for a fast anomaly spot.

10 WINDOWS EXTRAS

- PowerShell script block logging (Event ID 4104): catches obfuscated PowerShell commands in full.
- `Get-WmiObject -Namespace root\subscription -Class __EventFilter`: check for WMI-based persistence.
- Amcache/Shimcache: evidence a binary executed even if since deleted; worth knowing exist, dig deeper with Sysinternals if needed.
- `Get-Process | Select ProcessName,Path`: flag anything running from Temp or a user profile path.

11 LINUX FORENSICS

- `file [path]`: confirm a binary actually is what its name claims.
- `strings [binary] | less`: quick look for suspicious hardcoded strings (IPs, URLs, credentials).
- Check `/tmp`, `/dev/shm`, and `/var/tmp` for dropped binaries; world-writable and often ignored.
- `ldd [binary]`: confirm linked libraries look normal; a hijacked shared library is a quiet persistence method.
- `lsattr [file]`: check for a suspicious immutable flag an attacker set to protect their own foothold.

12 WINDOWS FORENSICS

- PowerShell history file, under `%APPDATA%` (`...\PSReadline\`): command history per user, even outside a logged session.
- Prefetch folder (`C:\Windows\Prefetch`): evidence a program ran, with a timestamp, even after deletion.
- Browser download history: a fast way to spot a tool an attacker pulled down through a GUI session.
- `Get-Item [file] | Select LastWriteTime, CreationTime`: timestamp comparison can reveal timestomping if creation postdates last-write oddly.

13 BUILDING YOUR OWN BASELINE

- Save output of `ps -ef`, `ss -tunp`, and the account list to a text file on day one.
- `diff` a fresh capture against that baseline any time something feels off; do not rely on memory of "what normal looks like."
- Re-save the baseline after any authorized change, or it will start reporting false positives on your own team's work.

14 TIMELINE RECONSTRUCTION

- Anchor on the one confirmed timestamp first (a login, a file write), then work outward from it in both directions.
- Cross-reference host-local logs against SIEM data for the same window; a gap between the two is itself informative.
- Write the timeline down as you build it. It is the artifact the engineer and Captain both need, not just your own mental model.

15 HANDOFF CHECKLIST

Before handing to the engineer: account name, process and parent process, entry timestamp, the specific hole, first-pass scope. Log all of it before eviction starts.

16 PATTERN LIBRARY

- A process with no parent, or a parent that already exited, is worth a second look on either OS.
- A user account logged in from two very different source addresses within minutes of each other.
- A service account with an interactive logon type; service accounts rarely need one.
- A scheduled task or cron entry with an oddly encoded or obfuscated command line.
- Traffic to an IP with no matching DNS lookup beforehand; real users resolve a name first.