1 ORDER OF OPERATIONS

Enumerate: `systeminfo`, `Get-ComputerInfo`. Users: `Get-LocalUser`. Running: `Get-Process`, `Get-Service`. Ports: `netstat -ano`. Domain-joined? `Get-ComputerInfo | select CsPartOfDomain`.

Firewall: `Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True`. Allow only what is required, block the rest.

User Management: `Get-LocalUser`, `Get-LocalGroupMember Administrators`. Disable unneeded accounts. Reset passwords on anything real.

Verify & Update: `sfc /scannow`. Windows Update GUI or `Get-WindowsUpdate`. `DISM /Online /Cleanup-Image /RestoreHealth` if sfc reports damage.

Secure Services: `Get-Service | Where Status -eq Running`. Disable unnecessary: `Set-Service [name] -StartupType Disabled`.

Enable Auditing: Advanced Audit Policy Configuration, or `auditpol /set`. Install Sysmon if allowed. Watch Event Viewer.

Deny red team tooling: Disable unused WinRM/PSRemoting, restrict admin shares, kill PowerShell v2 (see below).

2 USERS & GROUPS

net user [name] /add: create account.
- `net user [name] [pass] /add`: with password set.

net user [user] [newpass]: change password.

Get-LocalUser — Set-LocalUser: PowerShell equivalent, scriptable.
- *Batch reset:* `Get-LocalUser | Set-LocalUser -Password (Read-Host -AsSecureString)` in a loop.

net localgroup [group] [user] /add: add to group.
- `net user [user] /active:no`: disable.
- `net user [user] /active:yes`: reactivate.

whoami /priv: current user's privileges.

whoami /groups: group memberships, including hidden ones.

net accounts: view/set password and lockout policy locally.

runas /user:[user] cmd: run as another user.

Get-ChildItem -Path C:\Users -Recurse -Filter authorized_keys: find SSH keys if OpenSSH is installed.

query user / quser: logged in users and session IDs.

logoff [session ID]: force a session closed.

3 NETWORKING

ipconfig /all: interfaces and addresses.

netstat -ano: connections/routing, with owning PID.
- `Get-NetTCPConnection`: filterable, scriptable equivalent.

Windows Defender Firewall:
- *Status:* `Get-NetFirewallProfile`
- *Allow port:* `New-NetFirewallRule -DisplayName X -Direction Inbound -LocalPort 443 -Protocol TCP -Action Allow`
- *Block outbound by default:* `Set-NetFirewallProfile -DefaultOutboundAction Block`
- *List rules:* `Get-NetFirewallRule | Where Enabled -eq True`
- *Legacy CLI:* `netsh advfirewall firewall add rule name="X" dir=in action=allow protocol=TCP localport=443`

nmap [host(s)]: same external tool as Linux.
- `nmap -A [host]`: OS, service version, script scan.
- `Test-NetConnection [host] -Port [n]`: native port check, no nmap needed.

arp -a: local ARP cache, spot unexpected hosts.

Get-DnsClientCache: local DNS resolver cache.

4 FILE PERMISSIONS

icacls [file]: view or change permissions.

icacls [file] /grant [user]:(R,W): grant read/write.

icacls [file] /remove [user]: remove explicit permissions.

icacls [file] /inheritance:r: strip inherited permissions.

Get-Acl / Set-Acl: PowerShell equivalent, scriptable.

takeown /f [file]: take ownership.

attrib +h +s [file]: hidden/system flags; attackers hide with these too, worth checking for.

5 IMPORTANT FILES & LOCATIONS

...\config\SAM: local account database.

HKLM/HKCU ...\Run & RunOnce: common persistence.

...\winevt\Logs: Event Viewer logs on disk.

...\drivers\etc\hosts: local DNS overrides, check for tampering.

Startup folder: `shell:startup`, per-user and all-users.

HKLM\...\Winlogon\Shell: another classic persistence key.

Scheduled task XML: `C:\Windows\System32\Tasks`.

WMI event subscriptions: fileless persistence, check with `Get-WmiObject -Namespace root\subscription -Class __EventFilter`.

Get-WinEvent -LogName [log] -MaxEvents [n]: tail-like read of a log.

6 EVENT VIEWER & AUDITING

Setup: Local Security Policy → Advanced Audit Policy Configuration; enable logon, account management, process creation. Install Sysmon if allowed.

Key Event IDs:
- `4624 / 4625`: successful / failed logon.
- `4634`: logoff.
- `4720`: user account created.
- `4732`: member added to a local group.
- `4728`: member added to a global group.
- `4688`: new process (needs Audit Process Creation on).
- `5140`: network share accessed.
- `1102`: audit log cleared. Rare, always investigate.

Get-WinEvent -FilterHashtable `@{LogName='Security';Id=4625}`: query by ID directly.

PowerShell script block logging: enables full command capture, huge for catching obfuscated PowerShell. Turn on via Group Policy → Windows Components → PowerShell.

7 SERVICES & SCHEDULED TASKS

Get-Service: list services and status.
- `Set-Service [name] -StartupType Disabled`: persistence/state.
- `Restart-Service [name]`: after a config change.

schtasks /query /fo LIST /v: all scheduled tasks, verbose.

Task Scheduler (taskschd.msc): check root and Microsoft → Windows folders; attackers often hide here.

Get-ScheduledTask — Where Author -notlike `"Microsoft*"`: filter to non-default tasks.

Get-CimInstance Win32_StartupCommand: another view of startup persistence.

8 MALWARE: DEFENDER & SYSINTERNALS

Windows Defender:
- `Get-MpComputerStatus`: confirm real-time protection on.
- `Update-MpSignature`: update signatures.
- `Start-MpScan -ScanType FullScan`: run a full scan.
- `Get-MpThreatDetection`: recent detections.

Sysinternals Suite (download ahead of time):
- *Autoruns / autorunsc.exe*: everything set to run at startup, CLI-friendly for scripting.
- *Process Explorer*: deeper than `tasklist`; parent/child, loaded DLLs.
- *TCPView*: GUI version of `netstat`.
- *Sigcheck*: verify a binary's digital signature before trusting it.

Yara on Windows: same rule syntax as Linux, works cross-platform.

9 PROCESSES & THREAT HUNTING

Get-Process: all running processes.

tasklist /svc: processes with hosted services.

taskkill /PID [pid] /F: kill a process.

taskkill /IM [name.exe] /F: kill all by image name.

Get-CimInstance Win32_Process -Filter

`"ProcessId=[pid]"`: includes `ParentProcessId`, the Windows equivalent of tracing `/proc/[pid]`.

- A shell (`cmd.exe`, `powershell.exe`) spawned from a service or web server process is not normal.

Sysmon Event ID 1: process creation with full command line and hash, if installed.
Get-Process — Select ProcessName,Path: flag processes running from unusual paths (Temp, user profile).

10 DENY RED TEAM: WINRM & LOLBINS

Confirm nothing legitimate depends on an item, then disable it and log the change.

- **WinRM/PSRemoting:** transport for Ansible's `winrm` connection and most PowerShell/Empire-style lateral movement. Disable if unused: `Disable-PSRemoting -Force`, block 5985/5986 at the host firewall.
- **Admin shares (`C$`, `ADMIN$`):** what psexec/wmiexec ride in on. Scope to your management host with a firewall rule instead of a blanket disable if your team relies on them.
- **PowerShell v2:** installable alongside v5+, lacks v5's logging; attackers downgrade to it on purpose. `Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2`.
- **LOLBins to watch/restrict via AppLocker:** `certutil.exe -urlcache` (download disguised as a cert op), `regsvr32.exe /i:http...` (Squiblydoo), `mshta.exe`, `bitsadmin.exe /transfer`. None normally reach the internet.
- **Compilers/scripting runtimes added for dev convenience (Python, Perl via Chocolatey):** remove if no scored service needs them; same Ansible/scripted-payload exposure as Linux.

11 ACTIVE DIRECTORY BASICS

Get-ADUser -Filter * -Properties *: every domain account.
Get-ADGroupMember "Domain Admins": who has full control.
dcdiag: domain controller health check.
repadmin /replsummary: replication status.
Get-GPO -All / **gpresult /r**: list GPOs, or confirm what applied.
nltest /domain_trusts: list domain trusts.
Common attack patterns:

- Kerberoasting: unusual TGS requests for service accounts (Event ID 4769).
- New accounts added directly to privileged groups.
- Unconstrained delegation with no real need.

12 RDP & REMOTE ACCESS

Enable/Disable RDP:

- `Set-ItemProperty -Name fDenyTSConnections -Value 0` on the Terminal Server key: enable.
- Value `1` disables it.

Require Network Level Authentication: via Group Policy, or `Set-ItemProperty` on `UserAuthentication`.
Restrict who can connect: add only required users to Remote Desktop Users, not Administrators broadly.
Local Security Policy (secpol.msc): password policy, lockout policy, user rights assignment.
AppLocker / Software Restriction Policies: block execution from Temp or Downloads.
PSRemoting security: prefer HTTPS listener over the HTTP default; use constrained endpoints where possible.