1 ROLE RESPONSIBILITIES

Accounts, groups, GPOs, DNS on the domain controller. Any hole or foothold touching AD.

2 ORDER OF OPERATIONS

Baseline, day one: `Get-ADUser -Filter * -Properties *`, `Get-ADGroupMember "Domain Admins"`. Save the list.
Ongoing: Re-check privileged groups regularly. Watch for off-onboarding account creation.
On report: Confirm if AD is involved. If yes, run it, coordinating with the engineer.
Eviction: Disable/reset the account. Remove from any group it should not be in. Check for an unauthorized trust or delegation change.
Patch: Re-harden the account/group baseline. Confirm password/lockout GPOs still linked and applying.

3 ROUND-START CHECKS

- `dcdiag`: domain controller health.
- `repadmin /replsummary`: replication status.
- `repadmin /showrepl`: per-partner replication detail if summary looks off.
- `Get-GPO -All`: confirm expected GPOs linked.
- `gpresult /r` on a client: confirm policy applies.
- `Get-ADDomainController -Filter *`: confirm every expected DC is actually there.

4 ACCOUNTS & GROUPS

- `Get-ADUser -Filter {Enabled -eq $true}`: active accounts vs. baseline.
- `Get-ADGroupMember "Domain Admins"`: should be short, known.
- `Get-ADGroupMember "Enterprise Admins"`: check this too; often forgotten.
- `New-ADUser` / `Remove-ADUser`: create or remove.
- `Set-ADAccountPassword`: reset a compromised account.
- `Disable-ADAccount`: faster than deleting when unsure.
- `Get-ADUser -Filter * -Properties LastLogonDate | sort LastLogonDate`: find stale accounts.
- `Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects`: check the recycle bin.

5 COMMON ATTACK PATTERNS

- Kerberoasting: unusual TGS requests for service accounts. Event ID 4769. Check with `klist` on a suspect host for oddly-requested tickets.
- DCSync-style replication requests from a non-DC account: Event ID 4662 with replication GUIDs.
- Direct additions to Domain Admins or similar, outside a normal change. Event ID 4728/4732.
- Unconstrained delegation enabled with no real need: `Get-ADComputer -Filter {TrustedForDelegation -eq $true}`.
- A new account plus a privilege change together: one incident, not two.
- Golden/silver ticket suspicion: unusually long-lived Kerberos tickets, or tickets for accounts that no longer exist.

6 DNS ON THE DC

- `Get-DnsServerZone`: list zones.
- `Get-DnsServerResourceRecord -ZoneName [zone]`: list records, scan for anything unrecognized.
- SOA serial recent and increasing.
- Unexpected records, especially wildcards or off-subnet.
- Zone transfers restricted to actual secondaries: check `Get-DnsServerZoneTransferPolicy` or the zone's transfer tab.

7 GROUP POLICY

- `New-GPO -Name "X"` then `New-GPLink`: create and link.
- Highest value: password policy, lockout, software restriction, audit policy.
- `Get-GPOReport -All -ReportType HTML -Path report.html`: dump every GPO's settings for review.
- Check `gpresult /r` periodically. A GPO that stops applying looks identical to one never created.
- AppLocker or Software Restriction Policy can be pushed via GPO to block execution from Temp/Downloads domain-wide.

8 TRUSTS & REPLICATION

- `nltest /domain_trusts`: list trusts.
- `Test-ComputerSecureChannel`: confirm a machine's trust relationship with the domain is intact.
- `repadmin /replsummary`: look for consistently failing partners, not just one bad sync.

9 DENY RED TEAM: AD-SPECIFIC

- Restrict WinRM to a jump-host allowlist via GPO: the transport for Ansible's `winrm` connection and most PowerShell-based lateral movement.
- **Protected Users** group for privileged accounts: blocks NTLM auth and long-lived Kerberos ticket caching, blunting Mimikatz-style credential theft.
- Enforce SMB signing domain-wide: breaks NTLM-relay tooling (Responder, Impacket's `ntlmrelayx`).
- AppLocker via GPO, block execution from Temp/Downloads: removes the landing zone for a dropped implant.
- Rename or disable the built-in Administrator account domain-wide once a real admin path is confirmed working.

10 TOOLS

- *ADSI Edit*: raw view of AD objects and attributes, for when the normal consoles do not show enough.
- *BloodHound*: maps attack paths through group memberships and permissions; useful defensively to find your own risky paths before red team does.
- *dsquery / dsget*: quick command-line AD lookups without loading the full RSAT GUI.

11 ENUMERATION ONE-LINERS

- `Get-ADComputer -Filter * -Properties OperatingSystem`: inventory every domain-joined machine and its OS.
- `Get-ADOrganizationalUnit -Filter *`: confirm the OU structure matches what you expect.
- `Search-ADAccount -LockedOut`: accounts currently locked, worth knowing before assuming an account is simply gone.
- `Search-ADAccount -AccountDisabled`: cross-check against who should actually be disabled.
- `Get-ADFineGrainedPasswordPolicy -Filter *`: check for password policies that override the domain default for specific groups.
- `Get-ADUser -Filter {AdminCount -eq 1}`: users ever granted privileged group membership, even if since removed. A good source of forgotten accounts.

12 SYSVOL & NETLOGON

- `\\[domain]\SYSVOL`: replicated share holding GPO templates and logon scripts.
- Logon scripts here run on every login; a modified one is a very effective, very quiet backdoor.
- Compare script hashes against a known-good baseline if one exists.
- Confirm SYSVOL replication itself is healthy: `dfsrmig /getglobalstate` on newer domains, or check the File Replication Service event log on older ones.

13 CERTIFICATE SERVICES, IF PRESENT

- If AD CS is deployed, check for certificate templates that allow low-privileged users to enroll for templates granting elevated rights.
- `certutil -TCAInfo`: quick sanity check on the CA's own configuration.
- A rogue or unexpectedly issued certificate is a persistence mechanism that outlives a password reset.

14 LAPS (LOCAL ADMIN PASSWORD SOLUTION)

- If deployed, local administrator passwords rotate automatically and are stored in AD, readable only by authorized accounts.
- `Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd`: check whether LAPS is actually populating passwords, not just installed.
- Removes the single-shared-local-admin-password problem, a common and serious finding on its own.

15 HANDOFF TO ENGINEER

When AD is not the whole story, hand off clearly: account, group, GPO, what you already changed. Log it before moving on.

16 PATTERN LIBRARY

- An account created and added to a privileged group within the same short window: rarely legitimate.
- A computer object with unconstrained delegation that has no clear operational reason to need it.
- A GPO that exists but is not linked anywhere, or is linked somewhere unexpected.
- Replication errors that appear suddenly on a domain controller that was healthy an hour earlier.