THE 6 SILENT KILLERS IN YOUR ACTIVE DIRECTORY SETUP

(THAT ATTACKERS LOVE TO FIND)

AD DOES NOT NEED TO BE BROKEN TO BE VULNERABLE

Active Directory (AD) is one of the most critical and targeted components of any IT environment. It manages authentication, enforces access control, and defines the identity structure across your organization.

Despite its importance, AD is often quietly misconfigured. These issues do not break systems or trigger alerts, which is why they frequently go unnoticed for years. But behind the scenes, they create ideal conditions for attackers to gain credentials, escalate privileges, move laterally, cross trusts, and gain full forest control.

Most compromises do not rely on advanced exploits. Instead, attackers “live off the land,” taking advantage of misconfigurations, excessive permissions, poor password hygiene, and years of unchecked configuration drift, common issues in many environments.

Even when AD appears to be functioning normally, that stability can mask serious security gaps. These are the weaknesses that red teams target early, and that real attackers exploit to silently take over critical infrastructure.

Here are six of the most dangerous and commonly overlooked weaknesses that often live deep inside Active Directory environments.

01

Misconfigured Network Protcools

Before an attacker can escalate privileges or spread laterally, they must gain an unauthenticated foothold. From an internal perspective, one of the most common ways is through man-in-the-middle attacks using tools like Responder and mitm6.

NBT-NS, LLMNR, MDNS, DHCP WPAD, DNS Update Privileges, and DHCP6 settings all contribute to an internal network attacker's ability to attract or even coerce authentication attempts in an attempt to crack the Net-NTLM password hashes or better, relay them to vulnerable targets as we'll talk about next.

Why it matters: Tools like Responder and mitm6 are still some of the quickest ways to gain an authenticated foothold in Active Directory.

02

Relayable Window Targets

The ability for an attacker with a man-in-the-middle position to relay authentication attempts is key to escalating privileges and spreading laterally. The only way to stop this is air-tight Windows configurations.

Simple changes like enabling SMB signing, LDAP channel binding, LDAPS, HTTPS on certificate enrollment endpoints, EPA on MSSQL, and so forth can make a huge difference in an attacker's ability to relay authentication towards vulnerable targets.

Why it matters: Tools like ntlmrelayx are widely used to go from zero to domain admin due to relayable targets and Active Directory misconfigurations.

03

Misconfigured Certificate Services (ADCS)

Active Directory Certificate Services (ADCS) is a powerful feature and a dangerous one when misconfigured. Many organizations unknowingly allow low-privileged users to request certificates that grant them higher access.

Attackers use this to impersonate users, including Domain Admins, without ever needing a password. Known ESC# escalation paths are incredibly effective and shockingly common.

Why it matters: Combining tools like Certipy and Certify with weak ADCS enrollment templates is one of the fastest, quietest ways for an attacker to go from domain user, or even unauthenticated, to domain admin access.

04

Overprivileged Service Accounts

Service accounts are designed to run automated tasks, but they are often set up with broad, persistent permissions. In some cases, they are granted Domain Admin rights simply to “make things work.”

Worse, these accounts usually have passwords that never expire and are not monitored for unusual activity. Kerberoasting and ASRep roasting attacks are often used to retrieve TGS kerberos tickets for service accounts and crack them offline to obtain cleartext passwords.

Why it matters: Attackers use tools like GetUserSPNs and GetNPUsers to compromise service account credentials.

Once compromised, a service account with excessive privileges gives an attacker persistent, stealthy control across systems.

05

Generalized Excessive Privileges

Adhering to the least privilege principle is one thing to say and an entirely different thing to do at scale in the enterprise. Attackers continually take advantage of excessive privileges.

So many different breach contexts all boil down to excessive privileges. It could be a large group of accounts that are unnecessarily joined to the VPN access group. Executives could be exempt from MFA. A machine account could be unnecessarily configured for unconstrained delegation. Sometimes it’s a group added to local admins on several workstations or servers. Simple things like SMB shares with guest access enabled or sensitive shares granted to all domain users surface repeatedly during our engagements.

Why it matters: Excessive privileges are the most common way that attackers exploit and escalate their privileges within Active Directory.

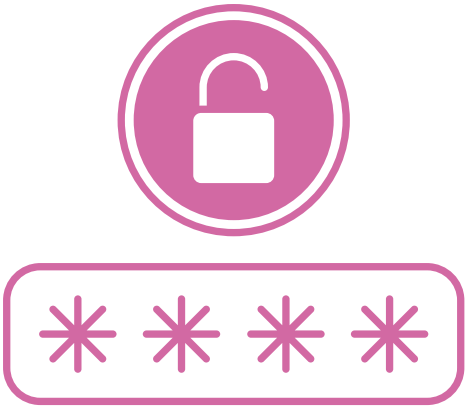
06

No Meaningful Audit/Monitoring Controls

Logging is often enabled by default, but logging alone does not provide security. Without structured audit policies, centralized log collection, or real-time alerts, attackers can operate invisibly.

Key activities, such as privilege changes, certificate requests, or group modifications, may go completely unnoticed.

Why it matters: If you are not watching critical changes, you are leaving the door open and never seeing who walks through it.



HOW IT ALL CONNECTS

These vulnerabilities rarely exist in isolation. More often, they form a clear and exploitable path, which red teams and attackers refer to as the “attack chain.” Here’s how that typically plays out:

THE AD ATTACK CHAIN

One Flaw Away from Domain Compromise

Initial Access
An attacker compromises a low-level user account using phishing or weak credentials.

↓

Privilege Escalation
They exploit misconfigured certificate services or overpowered service accounts to gain elevated access.

↓

Lateral Movement
With more access, the attacker moves across systems to find valuable data or users.

↓

Credential Harvesting
They collect passwords and hashes from memory, shares, or other exposed systems.

↓

Domain Admin Compromise
Finally, the attacker gains full control by accessing a Domain Admin account.

BREAKING THE CHAIN BEFORE IT STARTS

These issues are not theoretical. They are real, active attack paths we see in live environments all the time, often before the client has any idea.

That is why a thorough review of your Active Directory environment is critical, it can uncover and neutralize these threats before they are exploited. A hardened AD significantly reduces your risk surface and helps prevent a full-scale breach before it ever begins.

The Next Step:

Want help identifying silent misconfigurations in your AD? A structured review provides clear visibility and concrete steps to secure your environment. **Reach out to schedule an Active Directory Security Essentials Review with Depth Security today!**