What is Active Directory?

Active Directory (AD) is Microsoft's directory service: a central database of users, computers, and groups that decides who is allowed to access which resource on a Windows network. Domain Controllers (DCs) hold that database and answer every authentication request using the Kerberos and NTLM protocols. Because a single account, Domain Admin, can control the entire estate, attackers do not look for one broken server. They look for a path of small misconfigurations that chains an ordinary user up to full domain control.

HOW IT WORKS

01 How logon works: Kerberos and NTLM

AD authenticates with two protocols, and both are attacker targets.

- Kerberos is the modern default. When you log in, the DC (acting as the Key Distribution Center, or KDC) issues you a Ticket Granting Ticket (TGT). To reach a service, you exchange the TGT for a Service Ticket (TGS) for that specific service. Tickets, not passwords, are sent around the network.
- NTLM is the older challenge-response protocol. It is still enabled almost everywhere for backward compatibility, and its reliance on the password hash rather than the password itself is what makes attacks like Pass-the-Hash possible.

The practical takeaway: on a Windows network, a stolen ticket or a stolen hash is as good as a password.

02 Why attackers go after AD first

Active Directory is a single point of total control. The Domain Admins group, and a handful of equivalent groups and accounts, can run code on every domain-joined machine. Reach that level and ransomware can be pushed to thousands of endpoints in minutes.

Attackers rarely get there in one step. The real attack is a chain: phish one user, find that user can read a service account password, that service account can reset another account, that account has rights over a Domain Controller. Each link is a small misconfiguration that looked harmless on its own.

SOURCES

[1] Microsoft: Kerberos Authentication Overview

[2] MITRE ATT&CK Enterprise Matrix

[3] NIST SP 800-115 Technical Guide to Security Testing

03 The objects and stores worth knowing

A few names come up in almost every AD attack:

- SPN (Service Principal Name): a label that ties a service to the account running it. SPNs make Kerberoasting possible.
- SYSVOL: a file share on every DC that all users can read. Legacy scripts and the old Group Policy Preferences (GPP) feature sometimes left passwords here.
- NTDS.dit: the database file on the Domain Controller that holds every account's password hash. Stealing it is "game over" for the domain.
- LSASS: the process in memory on each Windows host that caches credentials of logged-in users. Dumping it is how attackers harvest hashes and tickets.

04 How a pentest approaches Active Directory

A penetration test of AD starts from a realistic position, usually a single standard user account or a foothold on one workstation, and tries to reach Domain Admin the way a real intruder would. The tester maps the environment, finds the weak links, and walks each chain to the end with reproducible evidence.

The deliverable is not a list of theoretical risks. It is the exact path from "ordinary employee" to "full domain control," with the specific accounts, permissions, and misconfigurations that made it possible and the fix for each one.

> THE MENTAL MODEL
>
> *Do not think of AD security as patching servers. Think of it as closing attack paths. One unpatched link in a chain of ten is enough, which is why mapping the whole graph beats hardening boxes one at a time.*

Test your Active Directory before an attacker does.
securelayer7.net/learn/active-directory/what-is-active-directory

Open online