Active Directory security, in plain terms.

Active Directory is the identity backbone of most Windows networks, and the path attackers take through it is well-worn: enumerate the directory, harvest or crack credentials, abuse over-broad permissions, and chain it all up to Domain Admin. This section breaks each step into a plain-language explainer with the real technical names a defender needs to recognise. Start with the foundations, then follow the attack chain.

HOW IT WORKS

01 Key terms explained

Plain-language definitions of the names that come up across these attacks. Each page covers what the term is, the attack it enables, and how to defend.

Kerberos and tickets

- What is a Kerberos ticket (TGT and TGS)?
- What is the KRBTGT account?
- What is a Service Principal Name (SPN)?
- What is a Golden Ticket?
- What is a Silver Ticket?
- What is Pass-the-Ticket?

Credentials and lateral movement

- What is LSASS?
- What is Mimikatz?
- What is Pass-the-Hash?
- What is NTDS.dit?
- What is DS-Replication-Get-Changes?

Recon, permissions and delegation

- What is BloodHound?
- What is a Domain Controller?
- What is RBCD?
- What is unconstrained delegation?
- What is SYSVOL and GPP passwords?

AD Certificate Services (ESC series)

- What is ESC1?
- What is ESC2?

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Best Practices for Securing Active Directory

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

- What is ESC3?
- What is ESC4?
- What is ESC5?
- What is ESC6?
- What is ESC7?
- What is ESC8?

Defenses

- What is a gMSA?
- What is LAPS?
- What is Credential Guard?
- What is the Protected Users group?

02 How to read this section

The articles are ordered the way a real attack unfolds.

- Foundations first: what AD is and how Kerberos and NTLM work.
- Reconnaissance next: enumeration and BloodHound, the map every attacker draws.
- Credential attacks: Kerberoasting, AS-REP Roasting, and the NTLM hash and relay attacks.
- Permission and trust abuse: ACL and delegation paths, and AD Certificate Services.
- The end-game: DCSync and ticket forgery, which mark full compromise.

Each explainer ends with how a penetration test surfaces that specific weakness in your own environment.

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

Open online