What is a Domain Controller?

A Domain Controller (DC) is a Windows server running Active Directory Domain Services. It stores the directory database (NTDS.dit), authenticates every logon using Kerberos and NTLM, and enforces security policy across the domain. Because it holds the password hash of every account, including Domain Admins and KRBTGT, compromising a Domain Controller is equivalent to compromising the entire domain, which is why DCs are the top-priority Tier 0 asset to protect.

HOW IT WORKS

01 Why it is the prize

Reaching a Domain Controller, or Domain Admin rights over it, is the goal of nearly every Active Directory attack:

- It enables DCSync to pull every hash including KRBTGT (`secretsdump.py -just-dc ...`).
- It exposes NTDS.dit for a full credential dump.
- It allows pushing code, including ransomware, to every domain-joined machine.

The whole attack chain in this section, enumeration, Kerberoasting, relay, ACL and AD CS abuse, exists to reach this single class of server.

> TIER 0
>
> *Domain Controllers, plus the accounts and systems that can control them, are Tier 0. They should be administered only from equally trusted systems, never from an ordinary workstation.*

HOW TO DEFEND

- Apply tiered administration. Only Tier 0 admins touch DCs, and only from clean, trusted systems.
- Keep Domain Admin credentials off lower-tier machines so attackers cannot pivot up.
- Patch DCs promptly and minimise installed roles and software on them.
- Monitor for DCSync replication from non-DC sources and for shadow-copy or backup access.
- Protect DC backups, which contain NTDS.dit.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos Authentication Overview

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

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-a-domain-controller

Open online