What is unconstrained delegation?

Unconstrained delegation is a Kerberos setting (the TRUSTED_FOR_DELEGATION flag) that lets a server capture the full TGT of any user who authenticates to it and reuse that ticket to impersonate them anywhere. If an attacker controls such a server, they can coerce a Domain Controller to authenticate to it, capture the DC's ticket, and take over the domain. It is the most dangerous delegation type, and it should exist on nothing but Domain Controllers.

HOW IT WORKS

01 The abuse and payload

The classic attack pairs unconstrained delegation with a coercion trick:

1. Compromise (or find attacker-controlled) a host trusted for unconstrained delegation. 2. Coerce a high-value target, ideally a Domain Controller, to authenticate to it: `printerbug.py corp.local/user@dc-ip <attacker-host>` or PetitPotam. 3. Capture the incoming TGT from memory: `Rubeus.exe monitor` or `sekurlsa::tickets`. 4. Reuse the DC's TGT (Pass-the-Ticket) to run DCSync and take the domain.

Documented techniques shown for defensive awareness.

> FIND IT AND KILL IT
>
> *Enumerate every computer with TRUSTED_FOR_DELEGATION (unconstrained). Outside Domain Controllers, there should be none. Each one is a credential trap.*

HOW TO DEFEND

- Remove unconstrained delegation from every server that is not a Domain Controller; use constrained or resource-based delegation if delegation is genuinely needed.
- Mark privileged accounts "sensitive and cannot be delegated" (or add them to Protected Users) so their TGT is never forwarded.
- Mitigate coercion vectors (PrinterBug, PetitPotam) and restrict who can reach delegation hosts.
- Monitor for coercion attempts and for TGTs being captured.
- Enumerate regularly with BloodHound, which flags unconstrained delegation.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Best Practices for Securing Active Directory

[3] Microsoft: Kerberos Authentication Overview

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-unconstrained-delegation

Open online