Attacking Constrained Delegation to Elevate Access

blog.netwrix.com/2023/04/21/attacking-constrained-delegation-to-elevate-access

This article rounds out a series of articles on Kerberos delegation. Before reading it, we suggest making sure you are familiar with both Active Directory delegation and Kerberos delegation, and have read the earlier posts in the series that provide an overview of how resource-based constrained delegation and unconstrained delegation are configured and how they can be abused.

Handpicked related content:

[Free Guide] Active Directory Delegation Best Practices

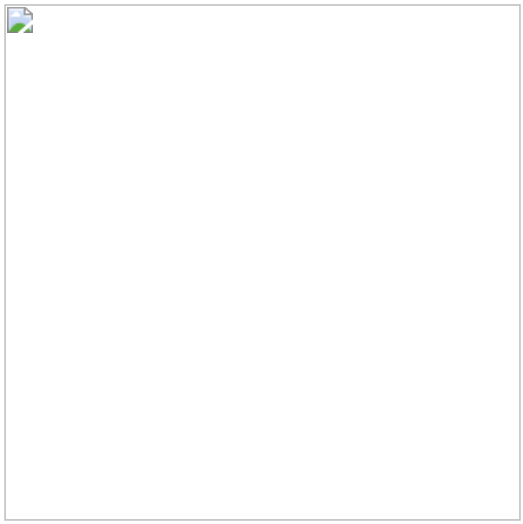
This article explains how a **constrained delegation** attack enables an adversary to gain elevated access to vital services.

Constrained Delegation

Constrained delegation enables administrators to configure which services an Active Directory user or computer account can delegate to and which authentication protocols can be used. It is configured on the Delegation tab for the AD object:

When constrained delegation is set on an account, two things happen under the covers:

- The userAccountControl attribute for the object is updated with the "TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION" flag.
- The msDS-AllowedToDelegateTo attribute is populated with the specified SPN.



Constrained Delegation Attack

In theory, constrained delegation limits the damage that could result if an AD account is compromised. But constrained delegation can be abused: An adversary who compromises the plaintext password or password hash of an account that is configured with constrained delegation to a service can then impersonate any user in the environment to access that service. For example, if constrained delegation is configured to a Microsoft SQL SPN, an attacker could get privileged access to that database.

How an Attack Unfolds

Let's assume the following:

- We have gained a foothold in an IT environment.
- We compromised an account with local administrator privileges on a workstation.
- We used Mimikatz to get a password hash left in memory after a logon, and the associated account (the 'notadmin' account) has constrained delegation configured.

Thus, all we have so far is access to the one machine we have landed on and the password hash of an account configured for constrained delegation.

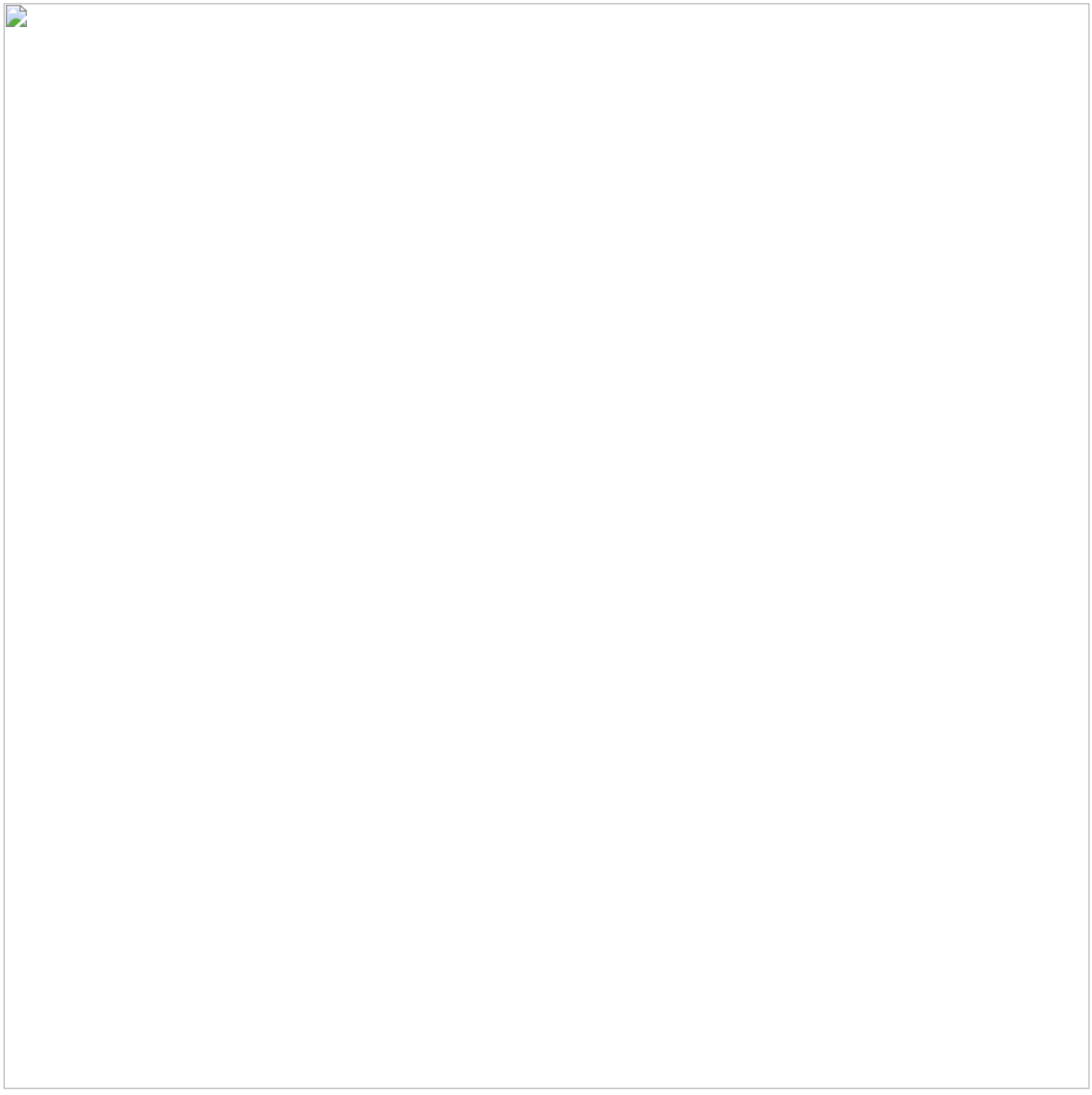
Step 1. Recon

To exploit constrained delegation, we need three key things:

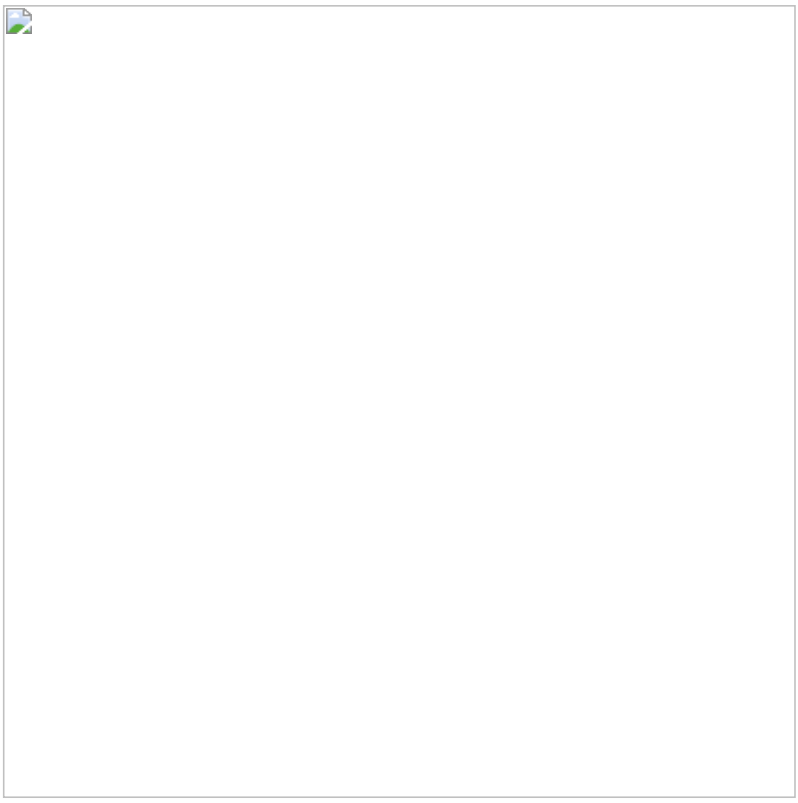
- A compromised account configured with constrained delegation
- A target privileged account to impersonate when requesting access to the service
- Information on the machine hosting the service we will be gaining access to

We have the first, so let's get the other two.

1.1: First, let's see what the constrained delegation of the 'notadmin' account is configured for:

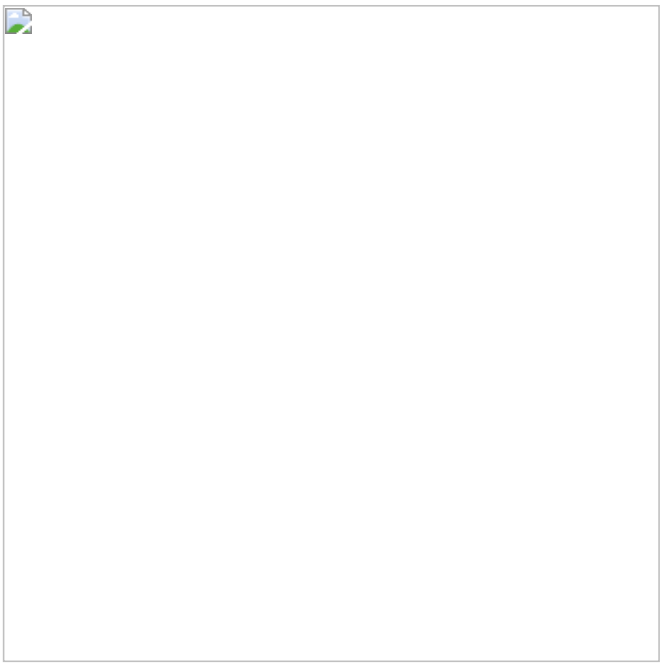


1.2: We now know that constrained delegation is configured for the CIFS and LDAP SPN on the SBPMLAB-DC2 host. So let's understand exactly what the SBPMLAB-DC2 host is (even though the name somewhat gives it away!). Maybe the group membership of the computer will tell us something.



1.3: We're in luck: The machine that this user is able to delegate access to is a domain controller (DC). Now let's find a good user to impersonate when accessing this service. The following PowerShell common will enumerate the members of the Domain Admins group:

Get-ADGroup 'Domain Admins' | Get-ADGroupMember

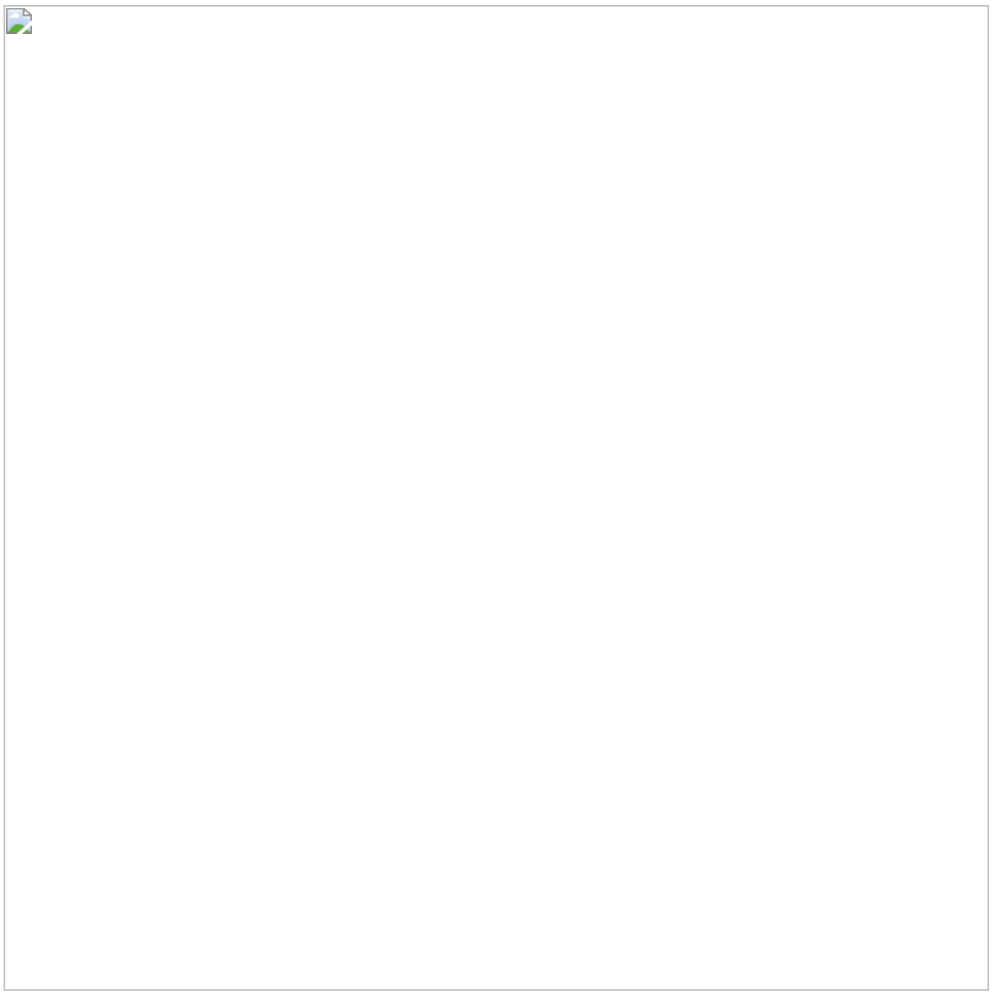


We can see that account 'KevinJ' is a member of Domain Admins, so now we have all the pieces we need to exploit constrained delegation.

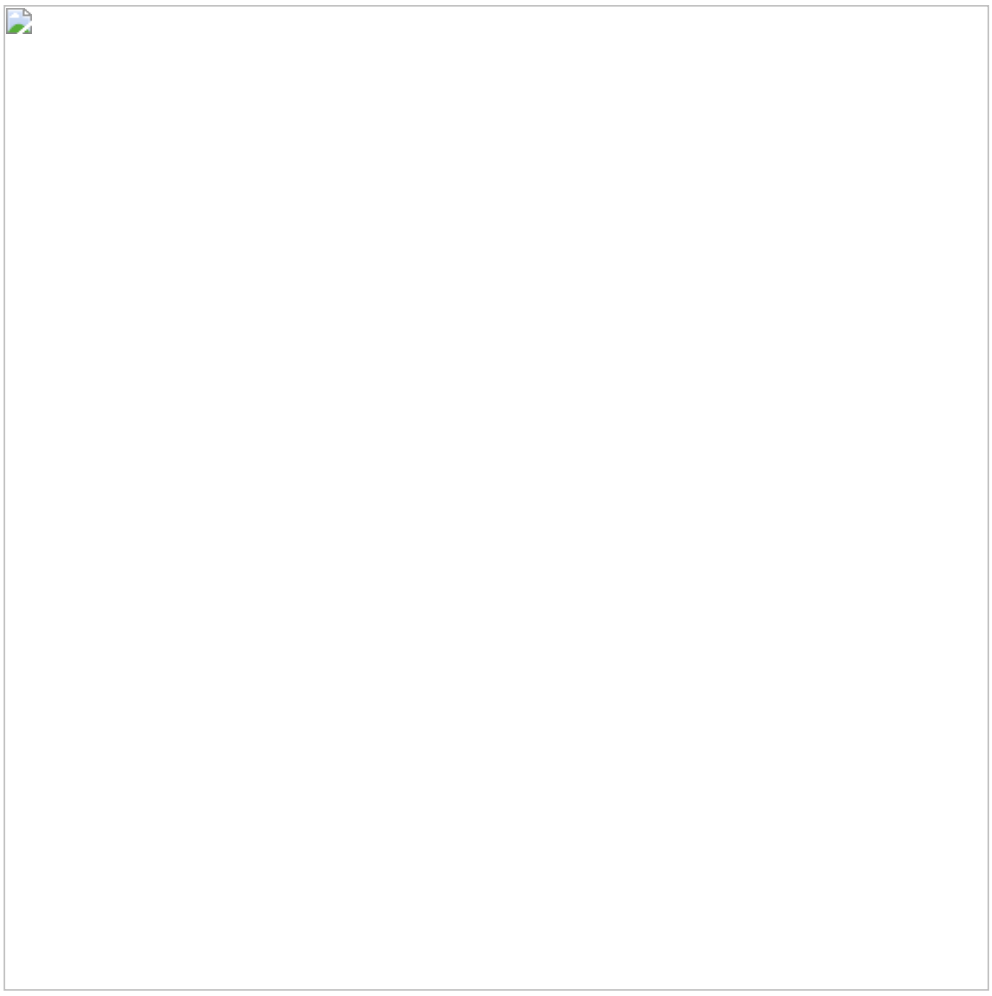
Step 2. Gaining Access

Using a tool like Kekeo, we can request the ticket granting ticket (TGT) for the account with constrained delegation configured, execute the ticket granting service request for the account we want to impersonate, and then access the target service.

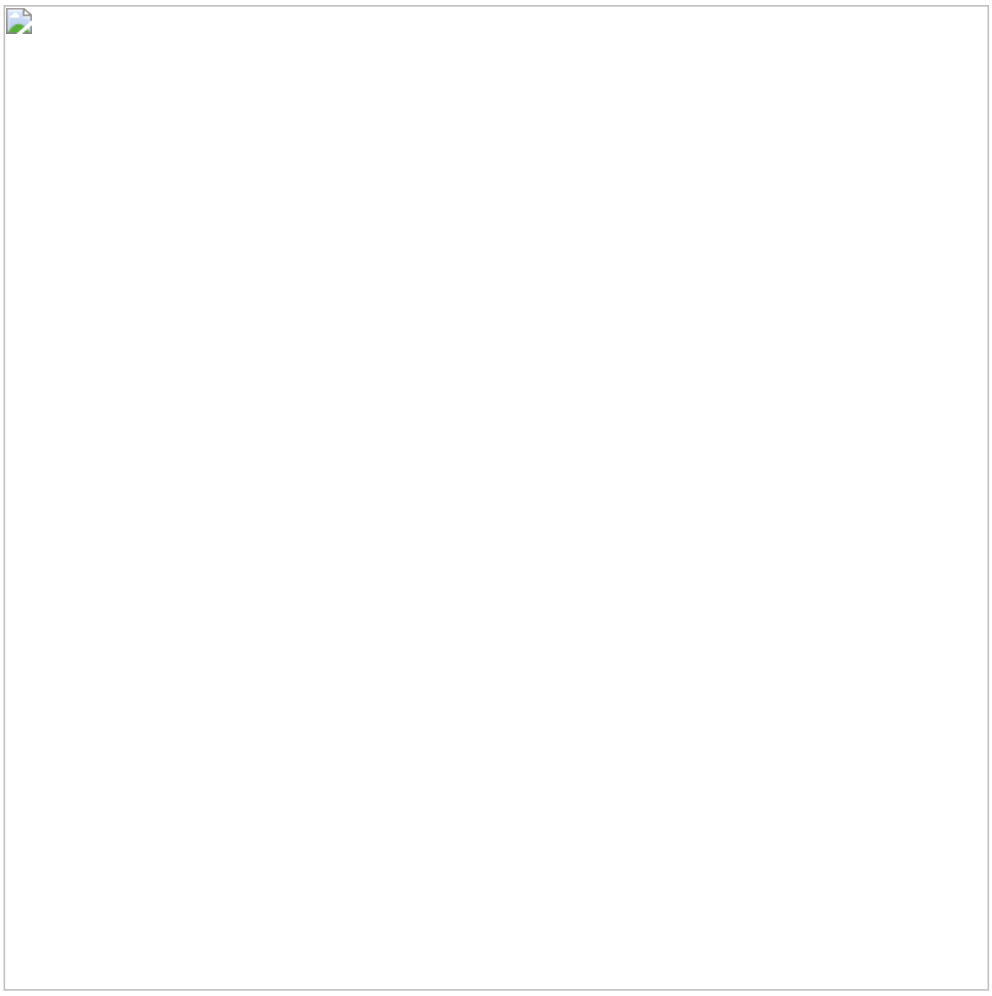
Keep in mind that we do not yet have access to the C$ admin share on the target host:



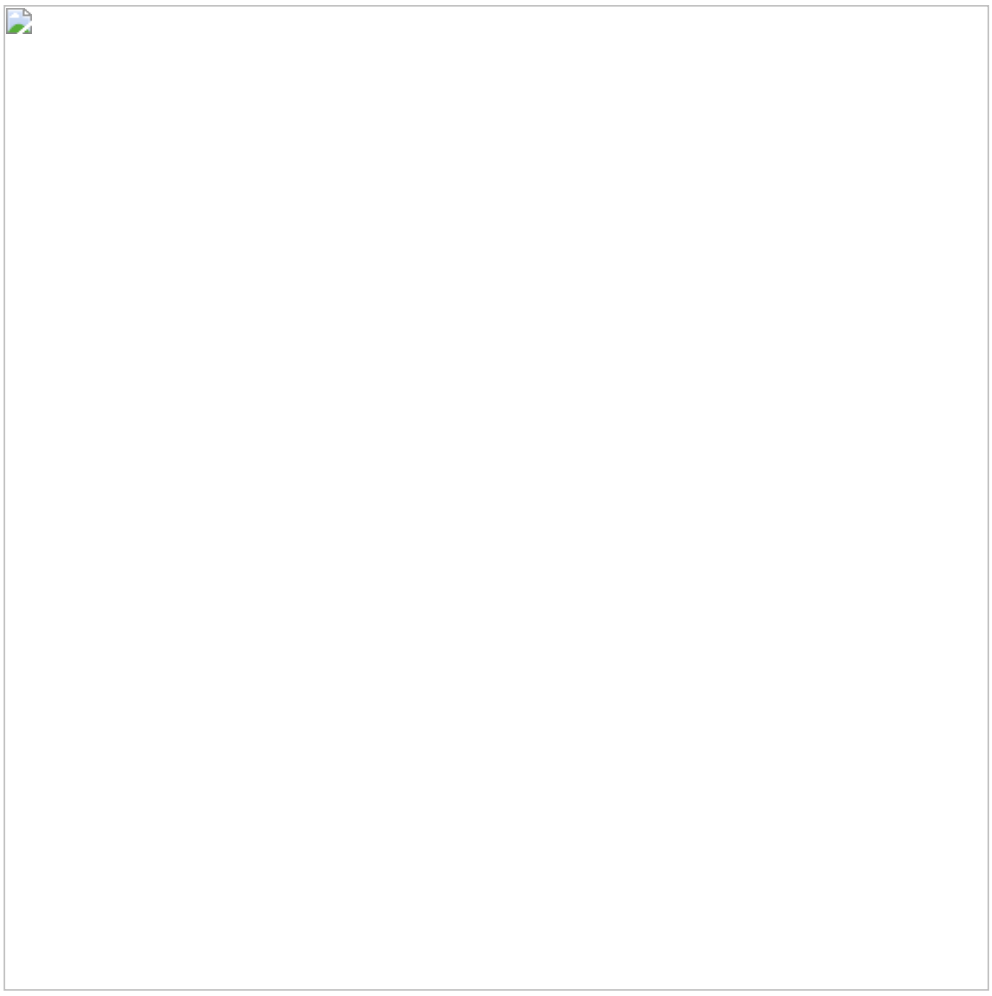
2.1. Using Kekeo, we request the TGT for the ‘notadmin’ account using its password hash:



2.2. Now that we have the TGT, we execute the TGS request for the account we want to impersonate for the target service that the ‘notadmin’ account is constrained to:



2.3. Switching back to Mimikatz, we are able to use Pass the Ticket to gain access to the CIFS service on the target host:

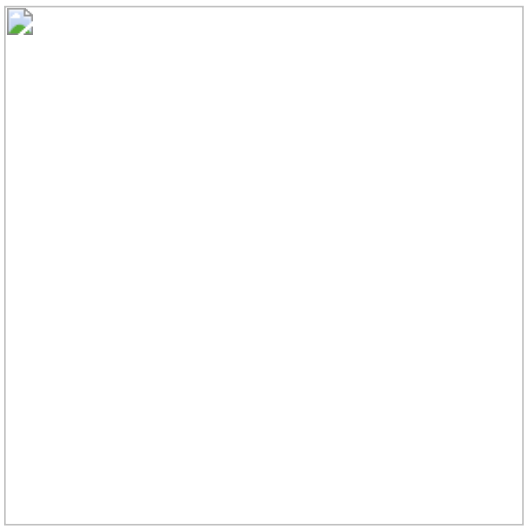


As you can see, after the ticket is imported, we can navigate to the C$ admin share on the domain controller. That means we could potentially steal a copy of the NTDS.dit file and try to crack user passwords offline.

Protecting against Delegation-based Attacks

A critical technique for defending against delegation-related attacks is to either put sensitive accounts that should not be delegated in the Protected Users group, or mark the 'Account is sensitive and cannot be delegated' checkbox in Active Directory Users and Computers on the Account tab:

For broader protection, consider the Netwrix Active Directory Security Solution. It provides comprehensive reports that provide clear insight into where unconstrained and constrained delegation are configured, as well as the specific service accounts that are constrained. Using this information, you can reduce risk and secure your environment more effectively. On top of this, you can easily detect and automate your response to sophisticated threats and mitigate their impact.



FAQ

What is a constrained delegation attack?

A constrained delegation attack is a type of cyberattack in which an adversary gains unauthorized access to a target system or service by exploiting the permissions granted to a service account. By compromising the service account or by intercepting and manipulating the Kerberos traffic between services, the attacker can impersonate a user and gain unauthorized access to other services that the service account is allowed to access. This type of attack can be more difficult to execute than an unconstrained delegation attack, but it is still a serious threat to network security.

What are constrained and unconstrained delegation?

Constrained delegation and unconstrained delegation are two ways that the Kerberos authentication protocol can be configured to enable a service to impersonate a user to access other services. Unconstrained delegation allows a service to impersonate a user to access any other service within an Active Directory domain. Constrained delegation, on the other hand, limits the scope of delegation by specifying which services a service can access on behalf of a user.

What does unconstrained delegation mean?

Unconstrained delegation is a Kerberos delegation configuration that allows a service to impersonate a user to access any other service within an Active Directory domain. This type of delegation can be exploited by attackers to move laterally within a network and gain access to sensitive data or systems.

Why is unconstrained delegation bad?

Unconstrained delegation is considered bad because it can enable attackers to move laterally within a network and gain access to sensitive data or systems. It is recommended to use constrained delegation instead, which limits the scope of delegation and reduces the risk of successful attacks.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.