

# Exploiting Active Directory in Hybrid Environments

## Overview

Active Directory (AD) is an industry-standard identity and access management platform that provides a database for managing users, computers, and groups primarily in Microsoft environments. In recent years, the industry has shifted operations and infrastructure towards cloud environments (AWS, GCP, Azure); resulting in many organizations employing a hybrid environment. A hybrid environment generally contains on-premises infrastructure in combination with services and infrastructure running in the cloud. Hybrid environments tend to create particularly complex relationships within authentication protocols, accounts and related permissions, certificates, and cloud identities. From an offensive security perspective, these relationships provide more a widened attack surface from solely on-premises environments.

Active Directory is often a valuable target for attackers as it centralizes authentication for enterprise assets such as users, workstations, servers, and other resources. Mokhtar et al. (2022) describes Active Directory attacks as “multi-stage” including enumeration, credential access, privilege escalation, and lateral movement. Compromise of privileged or misconfigured identities provide additional attack paths as these can be further leveraged to obtain access in an environment as opposed to compromising a single endpoint.

Active Directory attacks often exploit core functionality of AD components rather than software vulnerabilities; for example Kerberos authentication, delegation, NTLM, and Active Directory Certificate Services (ADCS) all provide core functionality while providing additional attack vectors.

As these are core components of Active Directory, many of these underlying features and configurations are required for enterprise AD operations, but an insecure configuration can lead to these becoming attack vectors. This paper will examine several attack examples of Active Directory environments, with a focus on how these attacks are carried out in hybrid environments.

## Exploitation of Kerberos Authentication

Kerberos is the primary authentication protocol within modern Windows environments which replaces the deprecated predecessor NTLM. Microsoft documents Windows implementation of Kerberos to use a trusted

internal Key Distribution Center (KDC) which lives on domain controllers and uses AD as the account database (Microsoft, n.d.). Successful authentication results in receiving a ticket granting ticket (TGT), which allows users to request tickets for other resources within the domains environment. The overall ticket architecture reduces password transmission but is often a strong target as successful exploitation can be very valuable. Obtaining or crafting a trusted ticket, authentication can be completed without the need for a traditional password, MITRE documents these techniques under T1558, Steal or Forge Kerberos Tickets (MITRE ATT&CK, n.d.).

A common technique carried out by attackers is “Kerberoasting”, where an authenticated user can request a service ticket for an account associated with an SPN, the resulting ticket is partially encrypted using information derived from the account’s password, which allows for an attacker to take the ticket offline and attempt to crack it using common tools such as Hashcat or John the Ripper.

Kerberoasting is dangerous, and complex as simply requesting a ticket is legitimate Kerberos functionality, and not particularly malicious; the attacker does not need elevated privileges to obtain this ticket. The weakness is particularly exploitable when a service account uses a weak password, or one that may be listed in a breach. If the service account possess administrative privileges across the domain; cracking the password/ticket can allow for privilege escalation and lateral movement throughout the environment.

Additionally, rather than solely intercepting tickets, tickets can be forged as well through two techniques. A golden ticket can be created after obtaining the cryptographic secret associated with the domains KRBTGT account as this account protects TGTs, the compromise of the account can allow an attacker to generate fraudulent tickets that the domain views as legitimate. A silver ticket technique attack exists which involves forging a service ticket using the secret associated with a particular service account (MITRE ATT&CK, n.d.). These attacks demonstrate why Active Directory exploitation goes much deeper than stealing passwords. Authentication tickets, and the underlying cryptographic technology used to create them can be just as valuable as plaintext credentials.

## Resource Based Constrained Delegation

Kerberos delegation is another Active Directory attack surface, and it exists as delegation allows applications to access other resources while acting on behalf of an authenticated user. Delegation is often very complex in environments and can be easily misconfigured, opening a strong risk and attack vector to an environment. Microsoft identifies delegated authentication as one of the capabilities provided through Kerberos (Microsoft, n.d.).

Resource-based constrained delegation (RBCD) allows destination resources to determine which principals (source) may authenticate to it on behalf of users. RBCD uses the ‘msDS-AllowedToActOnBehalfOfOtherIdentity’

attribute on target objects to define the relationship (The Hacker Recipes, n.d).

From an offensive perspective, this is particularly useful and interesting as an account can modify the delegation configuration of other computers within the environment. For example, an attacker may not have domain administrator privileges within the current compromised account, lateral movement to an account delegated 'GenericWrite' against a computer object in ADUC can create a dangerous delegation relationship.

Established delegated relationships provide further Kerberos functionality such as S4U2Self and S4U2Proxy which have exploitation ability to obtain service tickets impersonating other identities in an environment (The Hacker Recipes, n.d.). Exploitation of these methods can be effective to convert control (delegation) of an AD object into impersonation of privileged accounts & target (destination) services.

RBCD research highlights the importance in secure configuration, as even limited permissions can result in a strong attack path. Security researchers recently examined the relationship between Active Directory permissions, RBCD exploitation, enumeration, and Microsoft patches (*Attacks on Active Directory*, 2025). RBCD highlights that security readiness in Active Directory cannot be examined solely by the amount or who/what has privileged access; it must take into account non-administrative accounts with write privileges to sensitive objects.

## Active Directory Certificate Services Exploitation

Active Directory Certificate Services (ADCS) is another attack surface, the functionality of ADCS allows organizations to deploy public key infrastructure (PKI) and issue certificates for authentication, encryption, and other enterprise functions without the need of a 3rd-party certificate authority, essentially allowing organizations to create and sign certificates themselves. The risk in this functionality is the concept of authentication through certificates.

Certified Pre-Owned research conducted by SpecterOps researchers documented various ways ADCS configurations can be abused for privilege escalation, credential theft, and establishing persistence (Schroeder & Schroeder, 2026). This research establishes the ESC(1-8) terminology commonly used to categorize ADCS escalation paths.

Certificate templates define requestors, expiration dates, use cases, required information, etc; they are important as insecure combination of certificates can create an escalation path. For example, a certificate template may permit low-privileged users to request certificates and the certificate template allows the requestor to specify who the certificate identifies, this misconfiguration could be a key attack point. The Hacker Recipes documents

multiple ADCS attack paths involving vulnerable certificate templates, certificate authority (CA) settings, enrollment permissions & endpoints (The Hacker Recipes, n.d.).

ADCS highlights why passwords are not the sole focus in environments, if certificates have the ability to authenticate to accounts in the environment, an attacker's objective may shift from obtaining credentials to obtaining a valid certificate.

## NTLM Relay Against ADCS

NTLM authentication is a legacy Microsoft Windows authentication protocol utilizing a challenge-response mechanism to verify identities without sending passwords. NTLM authentication can be relayed to vulnerable certificate enrollment services, creating a significant attack path. NTLM relay involves receiving authentication attempts from a victim account and forwarding the challenge-response exchange request to another service rather than cracking the victim account's password.

ADCS web enrollment services can be vulnerable in the case that they accept NTLM authentication without strong controls surrounding NTLM. The Hacker Recipes documented how HTTP-based certificate enrollment endpoints can be targeted with NTLM relay attacks, allowing the attacker to authenticate to the enrollment service using relayed credentials and potentially requesting a certificate representing the victim identity (The Hacker Recipes, n.d.).

The impact of NTLM relay is dependent upon the identity being relayed and whether the relayed account has administrative privileges within the environment; as this can allow for privilege escalation and lateral movement throughout the network.

Microsoft addressed NTLM relay risks in KB5005413, where they explain techniques like PetitPotam can be used as part of the NTLM relay attack against ADCS environment lacking the appropriate controls (Microsoft, n.d.). Microsoft has recommended protections including Extended Protection for Authentication and signing mechanism for services still accepting NTLM authentication. It is worth noting all versions of NTLM is considered to be deprecated as of June 2024 (Microsoft, n.d.).

NTLM relay attacks demonstrate the importance of analyzing a full attack chain rather than an individual vulnerability; when these techniques and vulnerabilities are chained together, it poses a strong weakness.

# Exploitation in Hybrid Environments

As mentioned, many organizations across the industry employ hybrid environments featuring a mix of on-premises infrastructure in combination with services and infrastructure hosted by cloud providers. Hybrid environments pose an additional attack surface as security must be configured appropriately in both environments. Organizations often sync Active Directory with Microsoft Entra ID, using storage within the cloud while supporting internal applications, file servers, CAs, and other domain assets on-premises.

With the idea of syncing Active Directory with Entra ID, synchronization and Entra-side permissions must be properly configured for user accounts.

Mokhtar et al. (2022) research suggested that Active Directory attacks often progress through stages; enumeration, credential access, privilege escalation, lateral movement. Hybrid environments naturally have a larger amount of identities and relationships to manage which leads to additional attack vectors.

## Chaining Active Directory Exploitation Techniques

This was briefly mentioned earlier, but the risk does not inherently lie in singular vulnerabilities, but rather chaining multiple vulnerabilities together to progress an attack on a target environment. For example, an initial access to low privileged domain account may have limited access to systems across an environment but it may possess the permissions to enumerate Active Directory allowing for further discovery and enumeration. The enumeration then identifies service accounts vulnerable to Kerberoasting, which can then be used to access additional resources/permissions within the environment. ADCS creates additional possibilities in attack stages as enumeration can identify an insecure certificate template or enrollment endpoint which an attacker can then leverage with NTLM relay techniques to authenticate.

Modern Active Directory exploitation often involves the use chaining vulnerabilities and weaknesses in configurations leading to elevated permissions and lateral movement within a network, very rarely does an attacker start an attack with administrative privileges in early stages of an attack.

## Conclusion

Research identified that Active Directory exploitation often involves the use legitimate components of Active

Directory, that become valuable in an offensive perspective when misconfigurations or insecure permissions are made available. Though these core components and functionality of Active Directory have legitimacy, it is essential to properly secure these components to avoid security gaps.

Kerberoasting shows how legitimate ticket requests can expose service accounts weak credentials which can be further leveraged to move laterally within an environment and elevate privileges.

Golden and silver ticket techniques show why it is essential to secure Kerberos authentication secrets. RBCD attacks can utilize AD permissions and convert them into impersonation capabilities, while ADCS exploitation shows that it is important to secure certificate and consider certificates as a form of authentication as opposed to solely password-based authentication. NTLM relay attacks against ADCS emphasizes the possibility of chaining multiple components of AD together to allow for a successful attack path.

Active Directory exploitation is complex, but the core functionality of Active Directory provides lots of potential for misconfigurations and insecure relationships that can be exploited. Attackers do not necessarily need to defeat authentication mechanisms natively as they can use their technology to manipulate relationships to further progress in an environment.

## References

*Attacks on active directory - resource-based constrained delegation and new patches.* (2025, February 2). IEEE Conference Publication | IEEE Xplore. <https://ieeexplore.ieee.org/abstract/document/10916465>

*Dirkjanm.io.* (2026, August 5). dirkjanm.io. <https://dirkjanm.io/>

Mokhtar, B., Jurcut, A., ElSayed, M., & Azer, M. (2022). Active Directory Attacks—Steps, Types, and Signatures. *Electronics*, 11(16), 2629. <https://doi.org/10.3390/electronics11162629>

Robinharwood. (n.d.). *Kerberos authentication overview in Windows Server.* Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview>

Schroeder, W., & Schroeder, W. (2026, January 28). *Certified Pre-Owned.* SpecterOps. <https://specterops.io/blog/2021/06/17/certified-pre-owned/>

Steal or forge Kerberos tickets, technique T1558 - Enterprise | MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/techniques/T1558/>

The Hacker Recipes | The Hacker Recipes. (n.d.). <https://www.thehacker.recipes/>

Windows-Release. (n.d.). KB5005413: Mitigating NTLM relay Attacks on Active Directory Certificate Services (AD CS) | Microsoft Support. <https://support.microsoft.com/en-us/servicing/os/windows-server/2021/07/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs>



**hunts.dev**

Originally published on hunts.dev

<https://hunts.dev/blog/exploiting-active-directory-in-hybrid-environments/>