


# 4 Active Directory Attacks and How to Protect Against Them

---

 [blog.netwrix.com/2022/10/25/active-directory-attacks](https://blog.netwrix.com/2022/10/25/active-directory-attacks)

I was speaking with an Active Directory security engineer at a global pharmaceutical company recently, and I asked him the most classic question in the product management handbook: “What keeps you up at night?” So cliché (I know), but sometimes instead of an eye roll, you get a real gem, which is exactly what happened.

He said, “We’ve got a lot of good protections in place and run a pretty tight ship, but the worst thing that I think could happen is someone stealing our dit file.” I’d heard about this before. If an attacker can get a copy of the domain controller’s NTDS.dit file (essentially the Active Directory database), they could take it offline, crack every user’s password and log in using valid user credentials without anyone being the wiser. But how could an attacker actually steal this file? It’s locked because it’s always in use! You’d have to take the domain controller down, which someone would obviously notice. The questions started to pile up...

Long story short, the conversation got me going down a very interesting path. The more I learned about the NTDS.dit mystery, the more I came across other clever and crafty ways attackers are compromising AD. It makes sense; after all, Active Directory is a prime target in virtually any attack because adversaries know just how crucial it is in their quest to find and steal what they’re looking for.

Handpicked related content:

[Active Directory Security Best Practices](#)

In this blogpost, I’m not just going to list four Active Directory attacks you need to know about. I’m also going to explain how they work, the techniques and tools real attackers use to perpetrate these attacks, and how you can defend against them. Here’s the lineup:

## Attack #1. LDAP Reconnaissance

---

When an attacker uses LDAP queries to gather information about an Active Directory environment, they are performing LDAP reconnaissance. Using this method, the attacker may discover users, groups and computers, which can help them locate targets and plan future stages of their attack. Since this technique is used by attackers who have already infiltrated a company, it is an internal (rather than external) reconnaissance technique.

### How to protect against it?

---

Trust me, it is very difficult to prevent domain reconnaissance. Most of the information in Active Directory is available to all domain user accounts by default, so any compromised account can be used to perform this type of snooping. Monitoring LDAP traffic and

detecting abnormal queries is the most proactive approach to dealing with domain reconnaissance. The best way to mitigate your risk is to make sure that whatever is discovered cannot be used against you.

## **Attack #2. Local Admin Mapping using BloodHound**

---

BloodHound is a web application that identifies and visualizes attack paths in Active Directory environments. It identifies the fastest series of steps from any AD account or machine to a desired target, such as membership in the Domain Admins group. Regularly checking your AD using BloodHound can be an effective defense mechanism that helps you ensure that compromising an account or machine doesn't enable an attacker to compromise your domain.

Using two tools, PowerSploit and Invoke-UserHunter, BloodHound first constructs a map of which computers are accessible to which users, focusing on the Local Administrators group (Local Admin Mapping). Next, it enumerates a list of active sessions and logged-in users across domain-joined machines.

This data provides the building blocks for an attack plan. The adversary now knows who has access to what machines, and what user credentials can be stolen from memory. From there, it's just a matter of asking the right question and visualizing the attack path.

### **How to protect against it?**

---

The simplest method to prevent these types of attacks is to set controls on how servers are accessed. Microsoft best practices recommend using a tiered administrative model for Active Directory to strictly control access rights, which can minimize attack paths in Active Directory. In addition, keeping an eye out for anomalous authentication and login activity can help uncover attempts to exploit attack paths.

## **Attack #3. Pass the Hash with Mimikatz**

---

Once an attacker has established a presence in the network, their goal is to compromise additional systems and gain the privileges they need to accomplish their mission. Pass the Hash is a credential theft and lateral movement technique in which an attacker abuses the NTLM authentication protocol to impersonate a user — without ever obtaining the account's plaintext password. Mimikatz is a tool that makes performing Pass the Hash attacks much easier.

### **How to protect against it?**

---

You should use logon restrictions to ensure that your privileged account hashes are never stored in a place where they can be extracted. In addition, considering enabling LSA Protection, leveraging the Protected Users security group and using Restricted Admin mode for Remote Desktop.

## **Attack #4. NTDS.dit Extraction**

---

All Active Directory data is stored in the file [ntds.dit](#) (“the dit”) on each domain controller (by default, in C:\Windows\NTDS). To access the ntds.dit file on a domain controller, an adversary must first gain administrator access to Active Directory. Alternatively, the adversary can copy ntds.dit from a backup by compromising the organization’s backup solution.

## How to protect against it?

---

To reduce the risk of adversaries extracting your ntds.dit file, follow these best practices:

- Clean up Active Directory, including [Group Policy](#).
- Minimize the number of accounts that can log on to domain controllers.
- Follow the [clean source principle](#) for domain controllers: All infrastructure (for example, ESX and connected storage) and applications (for example, backup programs) that service domain controllers must be at the same security level as the domain controllers themselves.
- Maintain physical security for domain controller machines. If it can’t be ensured, consider running read-only domain controllers.
- Do not allow users to possess administrative privilege across security boundaries.

## How can Netwrix help?

---

Secure your Active Directory from end to end with the [Netwrix Active Directory security solution](#). It will enable you to:

- Uncover security risks in Active Directory and prioritize your mitigation efforts.
- Harden security configurations across your IT infrastructure.
- Promptly detect and contain even advanced threats, such as [DCSync](#) , [NTDS.dit extraction](#) and [Golden Ticket attacks](#).
- Respond to known threats instantly with automated response options.
- Minimize business disruptions with fast Active Directory recovery.

## FAQ

---

### What are common methods to attack Active Directory?

Most attackers gain access to Active Directory by compromising user credentials and then use [privilege escalation](#) techniques to gain further access. Common attacks include:

Read more about AD attacks in the [Netwrix Attack Catalog](#).

### Which tools can be used to compromise AD?

The most popular tools include:

- [Mimikatz](#)
- [PowerSploit](#)

- Bloodhound
- Death Star

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.

