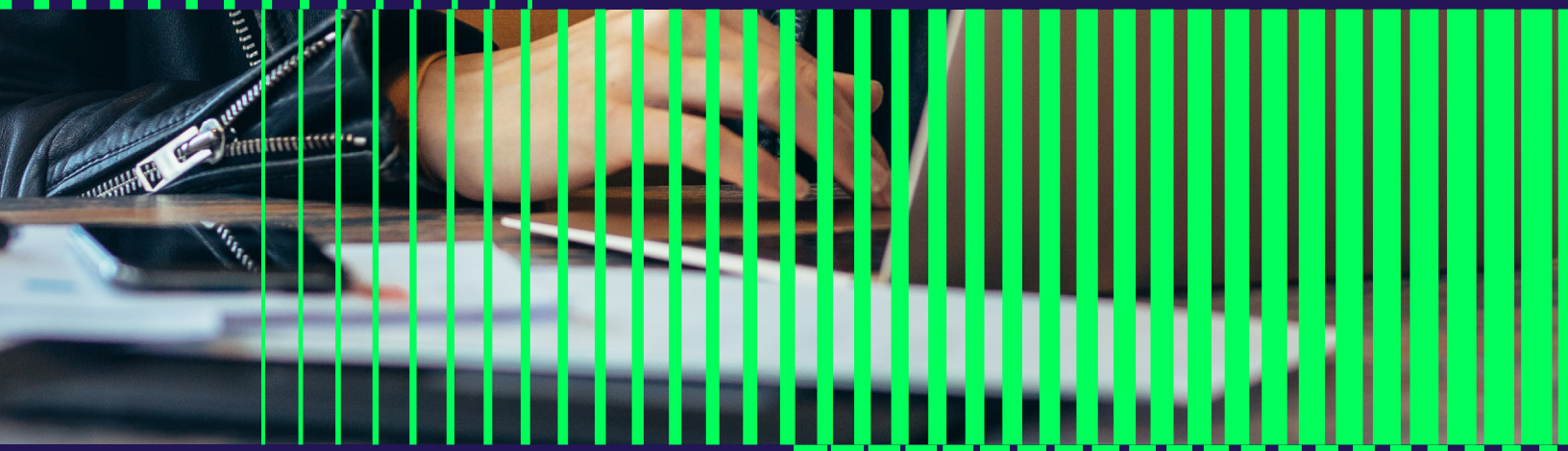
Delinea

Active Directory Security and Hardening

An ethical hacker's guide to reducing AD risks



WHITEPAPER

Delinea

Active Directory Security and Hardening:

An ethical hacker's guide to reducing AD risks

In this post, we're going to focus on common cyberattacks that target Active Directory (AD). Active Directory is deployed across many organizations around the world to deliver networking services so that users and computers can easily authenticate and be authorized to access network resources or log on to windows systems. AD also enables system administrators and infrastructure teams to manage corporate computer networks.

We'll cover common AD hacking techniques such as RDP brute force, LLMNR (Link-Local Multicast Name Resolution) using responder, mimikatz and Kerberoasting. The goal is to educate organizations on hacker techniques that put them at risk, and recommend actions to help reduce those risks.

Many organizations are under cyberattack every day; they're subjected to all kinds of security incidents. Some of the most damaging, such as ransomware, can bring a business to a complete halt. Below are several types of security incidents that keep security leaders awake at night. Which ones concern you most?

Before we get into the common hacking techniques let's do a recap on Active Directory components.

> Understanding hacker techniques and processes is the best way to defend against cyberattacks, and focusing on business risks is the best way to get security budget."

What keeps security leaders up at night?

- Malware
- Financial fraud
- Ransomware
- Compliance failure
- Data breach
- Data poisoning
- Insider threats
- Service/application downtime
- Revenue/brand Loss

Active Directory overview

Active Directory (AD) is a directory service that helps manage, network, authenticate, group, organize, and secure corporate domain networks. It enables users and computers to access different network resources such as log on to a windows system, print to a network printer, access a network file share, access cloud resources via single sign-on, or send a simple email.

Most users are usually provided with a **simple username and password** that is linked to their AD Account Object, wherein the background, AD uses LDAP (Lightweight Directory Access Protocol) to verify that the password is correct and whether the user is indeed authorized as part of a group or policy. Standard users will usually be part of a Domain Users group and have access to any object where Domain Users are authorized. An AD Administrator will be part of a group called Domain Admins which is a highly privileged group that can literally do anything within the network—the domain admin is sometimes referred to as having the "Keys to the Kingdom."

AD has numerous groups that allow various roles and authorizations, and which, for all organizations, must be well managed and secured to reduce the risk of malicious attackers gaining access via simple Active Directory misconfigurations.

Name	Type	Description
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords re...
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish cert...
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers ...
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords...
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic ...
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative ...
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Cont...
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for ...
HelpLibraryUpdaters	Security Group - Domain Local	
Key Admins	Security Group - Global	Members of this group can perform administrative ...
Protected Users	Security Group - Global	Members of this group are afforded additional prot...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access prop...
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Cont...
Schema Admins	Security Group - Universal	Designated administrators of the schema
SQLServer2005SQLBrowserUser$WIN-01S0KHJ45UC	Security Group - Domain Local	Members in the group have the required access and...

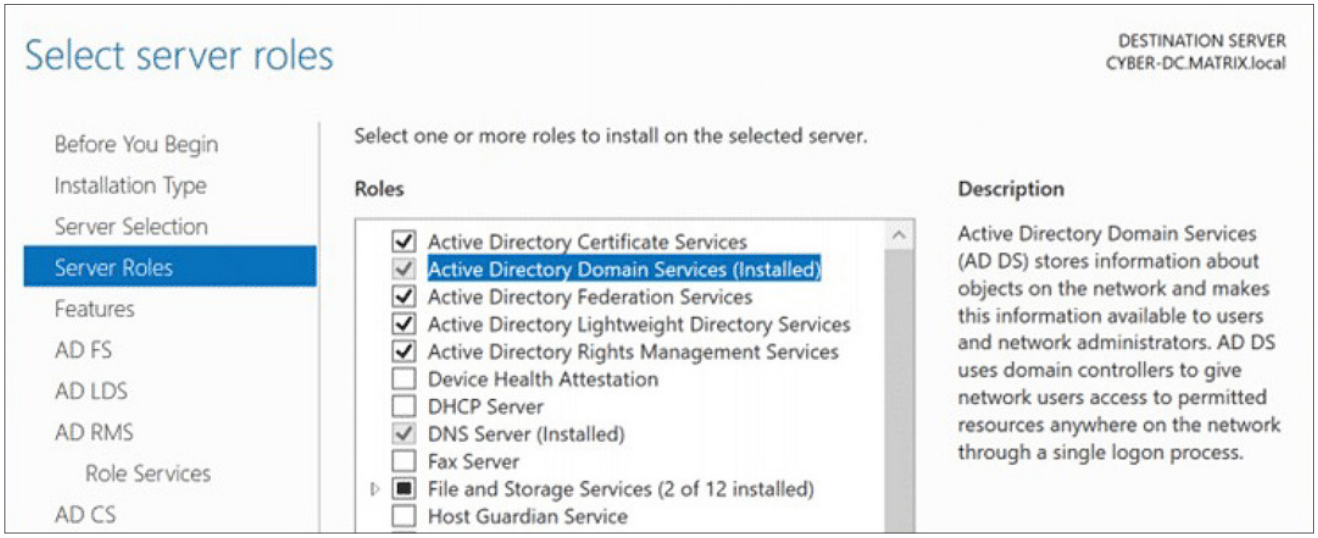
Common Groups within Active Directory

Active Directory is a hierarchy typically called a tree (Single Domain) or a forest (Multiple Domains) that stores information called objects. At the top of the domain is a domain controller (DC) which is used to host a copy of the Active Directory Domain Services (AD DS) — this is a schema on all the objects AD stores or delivers authentication and authorization services for. In large domains or global organizations, AD DS includes the ability to replicate changes to domain controllers within a single domain or forest. The domain controller also enables Domain Admins to manage all objects within, such as user accounts and network resources.

Active Directory Domain Services includes the following:

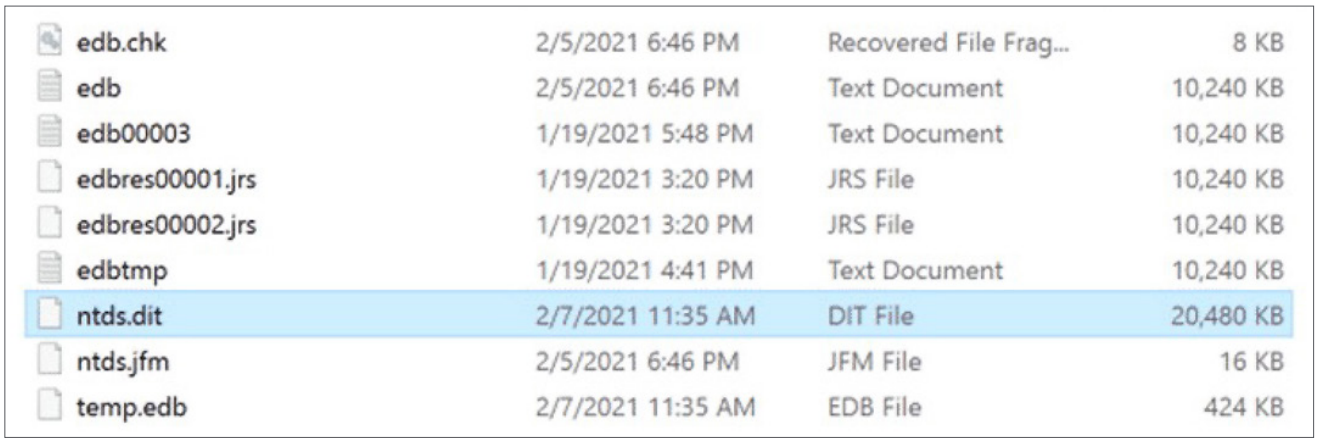
Most users are usually provided with a simple username and password that is linked to their AD Account Object, wherein the background, AD uses LDAP (Lightweight Directory Access Protocol) to verify that the password is correct and whether the user is indeed authorized as part of a group or policy. Standard users will usually be part of a Domain Users group and have access to any object where Domain Users are authorized. An AD Administrator will be part of a group called Domain Admins which is a highly privileged group that can literally do anything within the network — the domain admin is sometimes referred to as having the "Keys to the Kingdom."

AD has numerous groups that allow various roles and authorizations, and which, for all organizations, must be well managed and secured to reduce the risk of malicious attackers gaining access via simple Active Directory misconfigurations.



AD Server Roles

The AD DS data store is a vital component of Active Directory which is a database that stores and processes all the information for users, services, and applications. The AD DS store is typically named ntds.dit and located in the %systemroot%\NTDS folder located on the domain controller.

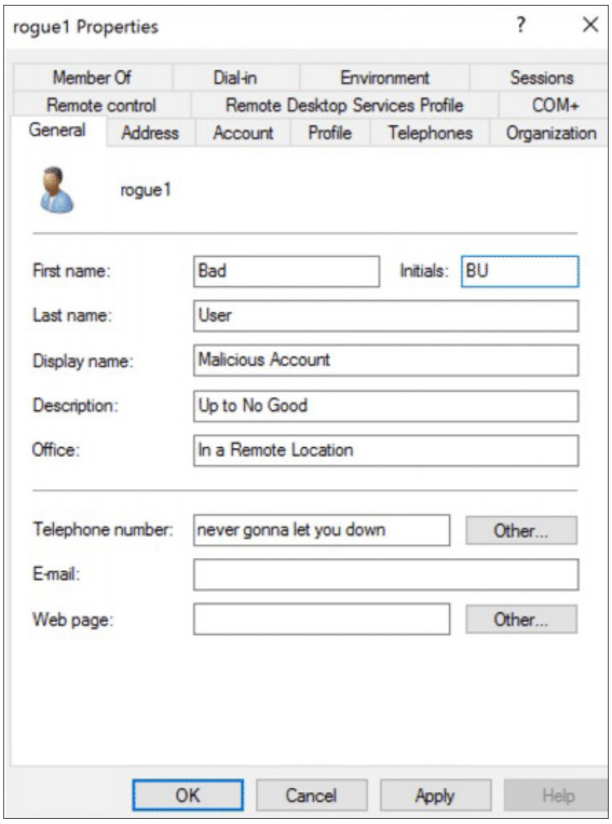


ntds.dit located in %systemroot%

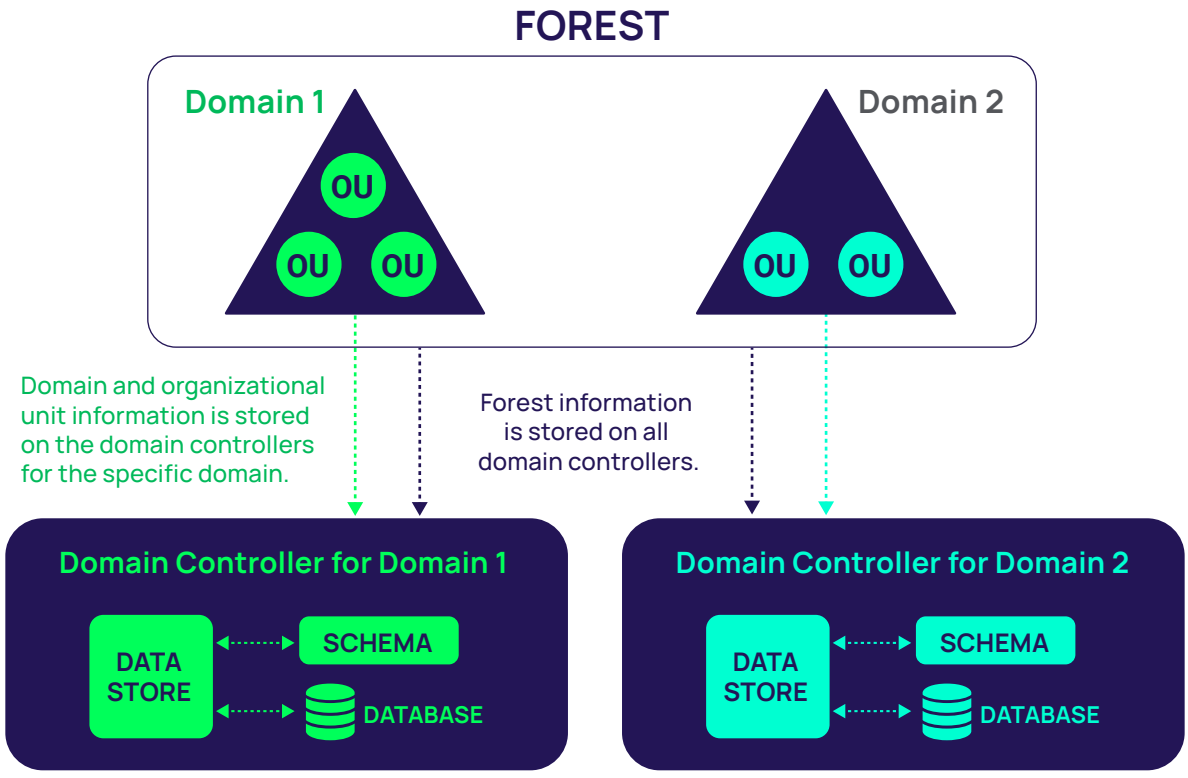
The Active Directory Domain Services schema is the definition of all the objects stored in the directory and enforces rules on the new objects created and object updates. These are separated into object types such as classes for examples, users and computers, or attributes, which is the information contained within the object such as first and last name.

Domains are typically used to group and manage the objects within the organization, such as applying rules and policies on how the objects should be used and adding the ability for role and scope policies on who has access to what, or who can make changes or updates to the Active Directory. As mentioned previously, domains can also be grouped into a tree with subdomains that share the same namespace as the parent; they're referred to as child domains.

For example, a top domain could be iamthetop.com and a subdomain could be child1.iamthetop.com and child2. iamthetop.com. A two-way transitive trust is created between the domains.



ntds.dit located in %systemroot%



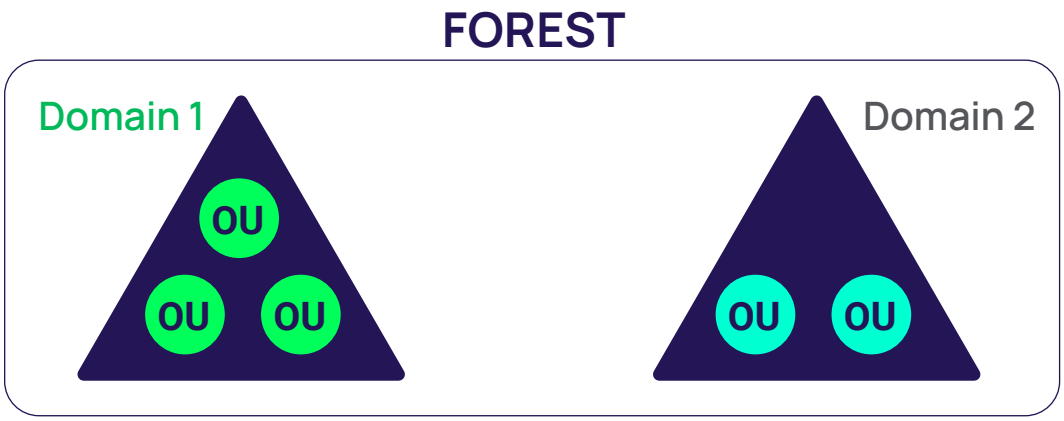
AD Structure - Source Microsoft.com Docs

Domains' trees and forests create partitions between the domains which enable more granular control over how data is replicated between each domain. This is typical for more complex organizations that have several business units or geographical locations and want to limit access and ensure policies adhere to, for example, local requirements. The forests can share a common schema and configuration. A global catalog that can be searched or queried across the domains permits the ability to establish different levels of trust between the domains and forest.

Active Directory also provides the ability to group objects into containers, or, as I tend to call them given my background in systems management—collections. These containers are called Organizational Units (OUs) and are used to structure the business and provide easier management. This allows for a role and scope approach. For example, you might have a domain admin who is responsible for North America and another domain admin who is responsible for EMEA. This approach enables you to limit the scope of their privileges and delegate administrator rights to only those objects within their region. It also provides the ability to apply various policies throughout the domains.

Active Directory provides two types of trust to establish the level of trust between domains. One is directional trust, which is one-way trust between domains; the other is transitive trust, a two-way domain trust that includes subdomains.

Further Microsoft Resources: Active Directory Structure and Storage Technologies



Azure Active Directory (Azure AD) is a cloud-based identity service that can synchronize your Active Directory Data Store and extend the capabilities to enable additional cloud services, such as Single Sign-On and Multi-Factor Authentication. Microsoft Azure can be used to connect and authenticate across many SaaS-based applications including Microsoft 365.

A serious security incident recently exposed a major risk. Attackers leveraged SolarWinds Orion product to deploy a backdoor to the networks of many organizations. They used on-premise domain administrator privileges to gain access and forged SAML tokens. This enabled them to move laterally from the victim's on-premise environment to their cloud environments.

Learn more about the SolarWinds Sunburst Incident in the blog:

SolarWinds Sunburst: One of the biggest cyberattacks targeting the software industry supply chain in history

So, as you can see, Active Directory plays a vital role in access and security within many organizations, both on-premise and in the cloud. Poor management and misconfiguration of Active Directory can enable a criminal attacker to gain access to these organizations' critical systems and deploy malicious payloads, like ransomware, which can bring business to an abrupt halt. This may result in huge financial losses and the public disclosure of sensitive company and employee data. For many businesses, this could be catastrophic and may come with massive financial costs in restoration, or compliance failure.

It's important to make Active Directory privileged access and security a top priority. If an attacker gains access to your Domain Admin accounts, it's basically game over for you.

To gain access to victims, attackers use a variety of hacking techniques that take advantage of poor access management, misconfigurations, and unpatched systems. Create a good security strategy based on a solid business risk assessment, and prioritize business cyber resilience.

Below are some of the most common causes of security incidents. As you can tell from this, a good security strategy is one that covers all the basics—and much more.

A fully compromised Domain Admin Account is a true security incident; response likely means rebuilding your Active Directory Domain."

→ Joseph Carson

Common breach causes

- Poor access management
- Insecure applications and APIs
- Misconfigured cloud storage
- Distributed Denial of Service (DDOS) attacks
- Overprivileged users
- Shared credentials
- Password only security controls
- Securing third-party access and remote employees
- Shadow IT

An ethical hacker's guide to reducing active directory risks

Below are seven of the most common Active Directory misconfigurations that attackers will quickly discover and abuse.

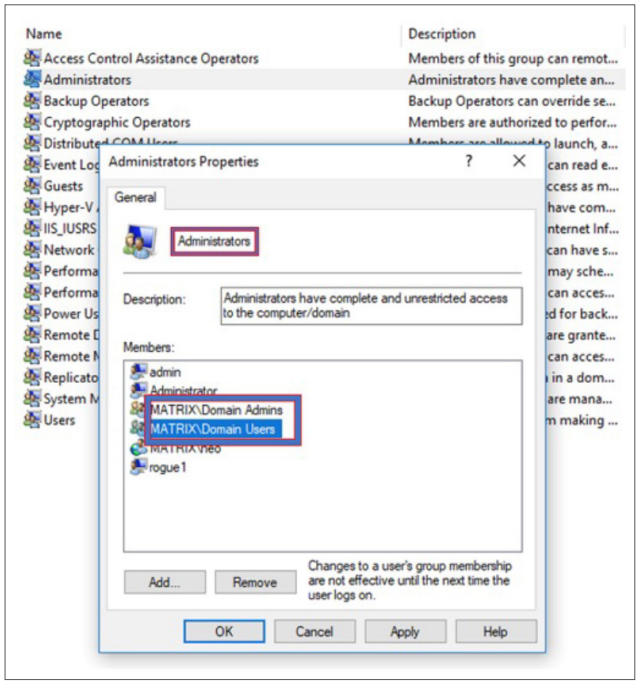
When an attacker gains a foothold in your network (most likely by using one of the techniques that I covered in A Hackers Guide to Protecting Endpoints,) the attacker will do an extensive enumeration on the compromised systems to create a digital blueprint of your Active Directory and the structure of your network, including high-value potential targets. Attackers will build this blueprint from network communications, protocols discovered, ports opened, network scans, and yes, even the names of the servers that we tend to name based on the service each is providing, such as SQL Server, ERP DB, etc.

1 Domain users with local administrator privileges

Adding Domain Users into the Local Administrator group is a common mistake. While the attacker might not have local admin rights on the system that provided the initial foothold, they will quickly try to discover misconfigurations and identify any networked systems that have included Domain Users within the Local Administrator Group. This misconfiguration allows the attacker to move laterally around the network and elevate from Domain User credentials to a Local Administrator.

This misconfiguration is a huge risk. If an attacker is able to log on to a windows endpoint as a local administrator they can leverage that compromised system and account as a staging system that can then be used to make network changes, elevate privileges to full domain admin, and disable any security settings.

RECOMMENDATION: Never add Domain Users into the Local Administrator Group. Make sure you continuously discover for this critical misconfiguration. If you need a Domain User to temporarily require local administrator privileges, apply the principle of least privilege by using an endpoint privilege security solution that can elevate privileges on demand without ever needing the user to be a local administrator. You could also add the user explicitly to the local admin group; however, this should be temporarily and never persistent.



Domain Users in Local Administrator Group

2 Weak and reused passwords: the attacker's favorite target

This is one of the most common causes of attackers gaining access to Active Directory networked systems to establish their initial foothold and set up the staging area. In the past year, thousands of organizations have enabled Remote Access to numerous business applications and systems so that employees can work from home and still access critical business applications. However, sometimes this means taking serious risks to ensure continuous business operations.

For many of these organizations, passwords are the only security control protecting access to the infrastructure. All too often, these passwords are weak or have been reused. Some of the methods attackers use to abuse these passwords are mentioned below.

RECOMMENDATION: Always use strong passwords. Use a privileged access management solution to create strong passphrases so employees don't have to.

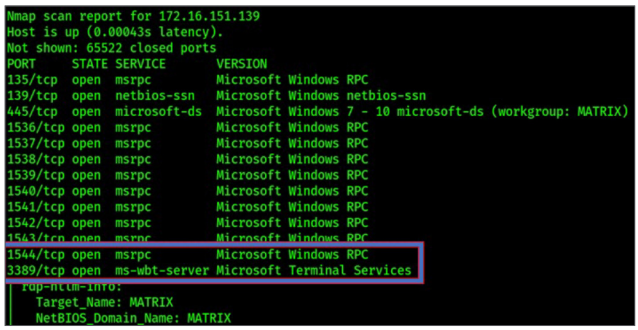
3 Brute forcing remote desktop protocol

Attackers consistently scan for endpoints with Remote Desktop Protocol Enabled. They use various scanning tools such as Massscan or Nmap to discover systems with port 3389 open.

Using tools such as crowbar, attackers will attempt to brute-force weak credentials. Once the brute-force is successful the attackers have remote access to a compromised system. This is a common issue when users reuse passwords for their company Active Directory account that they have also used in common internet services. A data breach may have exposed those credentials, adding them to the list of billions of known compromised passwords. Reusing compromised credentials means it's a matter of when, not if, an attacker will abuse them and gain access.

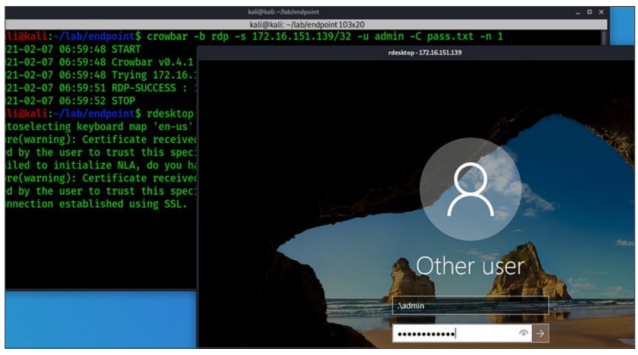
The attacker will then be able to use the compromised credentials to gain remote access to the victim's system and establish a foothold in their environment which can then be used for staging a lateral move or elevating privileges.

RECOMMENDATION: Never leave RDP directly exposed to the public internet without additional security controls such as multi-factor authentication and privileged access security. Audit for continuous brute-force attempts and scanning attacks.



NMAP Scan

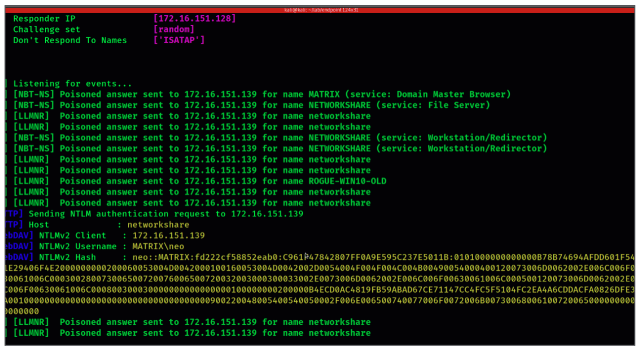
Using crowbar to brute force RDP



Remote Desktop

4 Netbios and LLMNR name poisoning using responder

Netbios and LLMNR (Link-Local Multicast Name Resolution) are old techniques that still get effortlessly abused, enabling an attacker to obtain a victim's NTLMv1 or NTLMv2 network hash. Again, weak passwords make this attack possible. This is why attackers continue to successfully use tools such as Responder, which can be executed via email, by listening over unauthorized network access, or even by plugging a USB into an unattended laptop.



Using Responder to Capture NTLM Hash and Crack

It's because of poor password hygiene that this attack is almost 100% successful. Using Responder, it will answer to network queries for SMB shares via LLMNR or NBT-NS. An unsuspecting victim's system will happily share its NTLM hash. Once the attacker has the hash, it's only a matter of time before they'll be able to crack it using tools like hashcat. The longer and more complex the password, the less chance of the attacker successfully cracking the password.

RECOMMENDATION: Always use strong passwords. Use a password access management solution to create strong passphrases so employees don't need to.

5 Using Domain Admin accounts for almost everything

One thing I have found in many Active Directory environments is systems administrators using the domain admin accounts for everything. This could mean anything from service accounts to remote access into systems, or leaving automated scheduled tasks to run backups, and a variety of other types of network management. While this is the easiest method, it's also a major attack vector for malicious attackers. They want you to do this as it allows them to easily elevate from a local administrator to gaining FULL DOMAIN Admin rights. This is why it's important to practice the principle of least privilege. Minimize the need to use domain admin accounts where possible.

An attacker who has local admin privileges will use that system as a staging victim, making some small changes and waiting for the domain admin to make the typical mistake: log on to a system where the attacker has local admin rights.

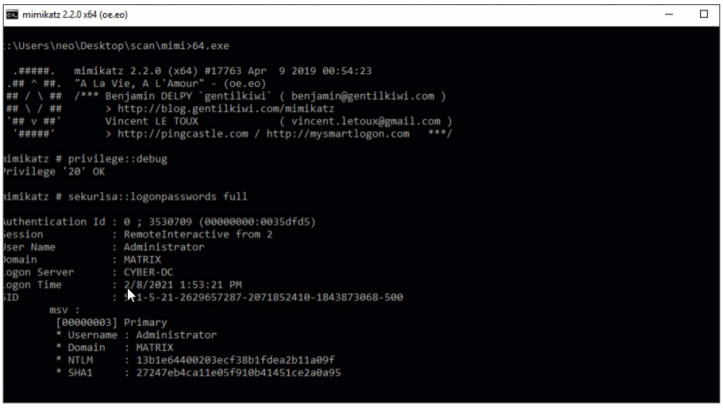
The attacker will modify the registry on a compromised system that will keep a cached credential in memory in cleartext. This change occurred in Windows 2012 where it was disabled by default, however, an attacker can easily add the following registry key to enable this.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest] "UseLogonCredential"=dword:00000001
```

The attacker will wait and every now and then they'll remote access onto the staging system to check if the domain admin left a footprint of the password that could be extracted in cleartext.

Since the attacker has local admin rights, they will disable security on the attacker staging system, run mimikatz as a privileged user, and be able to extract the domain admin password in cleartext. The attacker will continue this step until a domain admin makes this unfortunate mistake.

RECOMMENDATION: Prevent overprivileged users from having local administrator privileges on all systems. Ensure that endpoint application control is being used to prevent unauthorized applications such as mimikatz from running even if the attacker gains local admin privileges. Audit the environment for the registry settings that allow an attacker to extract passwords in cleartext.



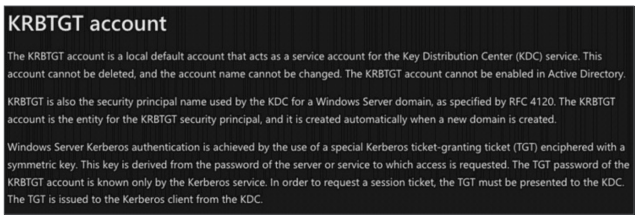
Using mimikatz to extract Domain Admin cleartext password

Limit using the Domain Administrator, but if you must, then use a privileged access security solution so that Domain Administrators passwords are rotated after each use. This way, even if the attackers can perform this malicious activity, the password should no longer be valid.

6 Overprivileged and unmanaged service accounts

Attackers will target privileged accounts within your network. Your service accounts are one of their top targets. Many organizations typically create and configure service accounts with elevated domain privileges so they can access the needed network resources.

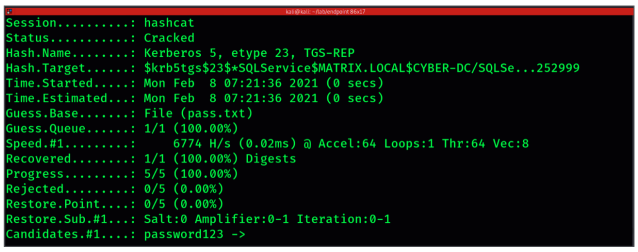
This is a technique used when service accounts are configured to use the SPN (Service Principal Name) so that when a user or system needs to access that service, they will get a Kerberos ticket signed with the NTLM hash of the account.



Source: Microsoft

Kerberoasting

Kerberoasting is a common hacking technique used by attackers and red teams to elevate privileges and gain privileged access to Active Directory. The technique is successful due mostly to the common practice of using weak service account credentials. The attacker uses a standard domain user to request the SPN which is signed by the NTLM hash of the service account, and when poor



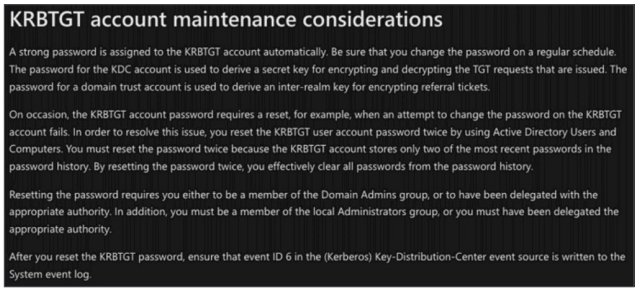
Using Impacket GetUserSPN.py to request Service SPN

passwords have been used, it's only a matter of time before a cracking machine can crack the hash revealing the plain text password and allowing the attacker to abuse the service account (which is typically a high-privileged user.)

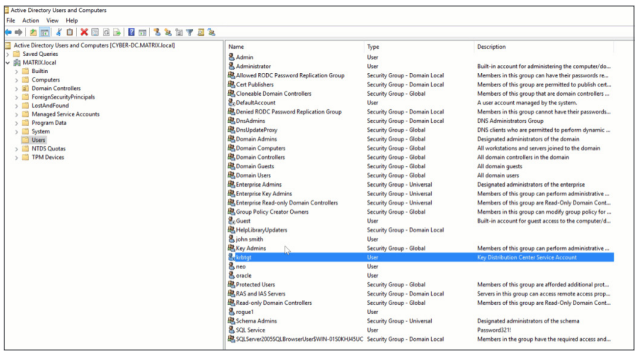
The example shows using GetUserSPN.py from Impacket. This requires having an authenticated compromised Domain credential to request the Service SPN. Once requested you will get a copy of the NTLM hash, and if a weak credential is used, an attacker can then use a password recovery and audit tool like hashcat.

RECOMMENDATION: Prevent Kerberoasting by using strong Service Account passwords and periodic resetting of Kerberos KDC Service Account. It is recommended that you reset the Kerberos KDC Service Account twice when doing this as the DC will maintain a password history of two. Use a Privileged Access Management solution to help discover, manage and secure service accounts.

Here is how you reset the Kerberos KDC Service account which can be found under View › Advanced Features › Select Users object in the Domain. You will find the krbtgt where you can now select and reset password.

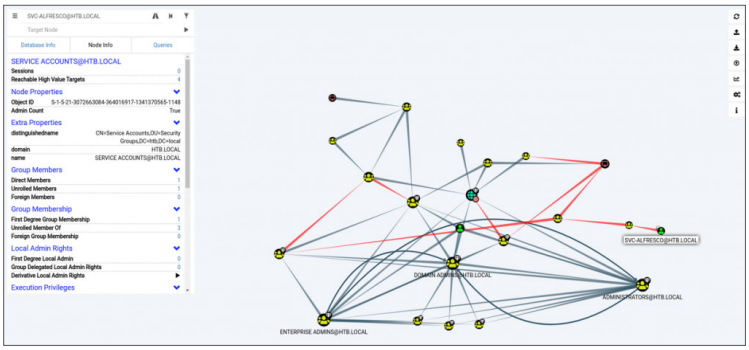


Source: Microsoft



7 Using BloodHound to discover privileged accounts

BloodHound is a single-page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a C# data collector.



Bloodhound Example from Hackthebox

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment.

RECOMMENDATION: Use Bloodhound to help you discover privileged accounts and relationships in your environment. Use a Privileged Access Management solution to discover and secure privileged access.

Active Directory security and hardening summary

As you can see, Active Directory is a top target for attackers and they'll use the techniques described above to abuse misconfigurations, weak security, and unmanaged accounts, enabling them to move around and elevate to highly privileged domain accounts.

Other techniques commonly used by attackers:

- SMB Relay
- Old and Unmanaged AD Accounts
- Legacy Systems that require backwards compatibility
- Eternal Exploits and unpatched systems such as CVE-2017-0144
- Mitm6

> A strong Active Directory starts with securing and managing privileged access."

About Joseph Carson:

- Chief Security Scientist at Delinea
- Over 25 years' experience in enterprise security
- Author of "Privileged Access Management for Dummies" and "Cybersecurity for Dummies"
- Cybersecurity advisor to several governments, critical infrastructure, financial and transportation industries
- Speaker at conferences globally

Some awesome resources:

- Sean Metcalf is a top expert in Active Directory Security – https://adsecurity.org/ is the go-to site for everything related to AD security. I highly recommend following Sean @PyroTek3
- Microsoft Active Direction Accounts Docs
- Heath Adams has some awesome practical pentesting courses if you are looking for something more practical

Let's not make it easy for attackers to abuse these common techniques. Put strong Active Directory security in place.

Make Active Directory privileged access and security your top security priority, as it should be. Remember, if an attacker gains access to your domain admin accounts, it's game over.

Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**