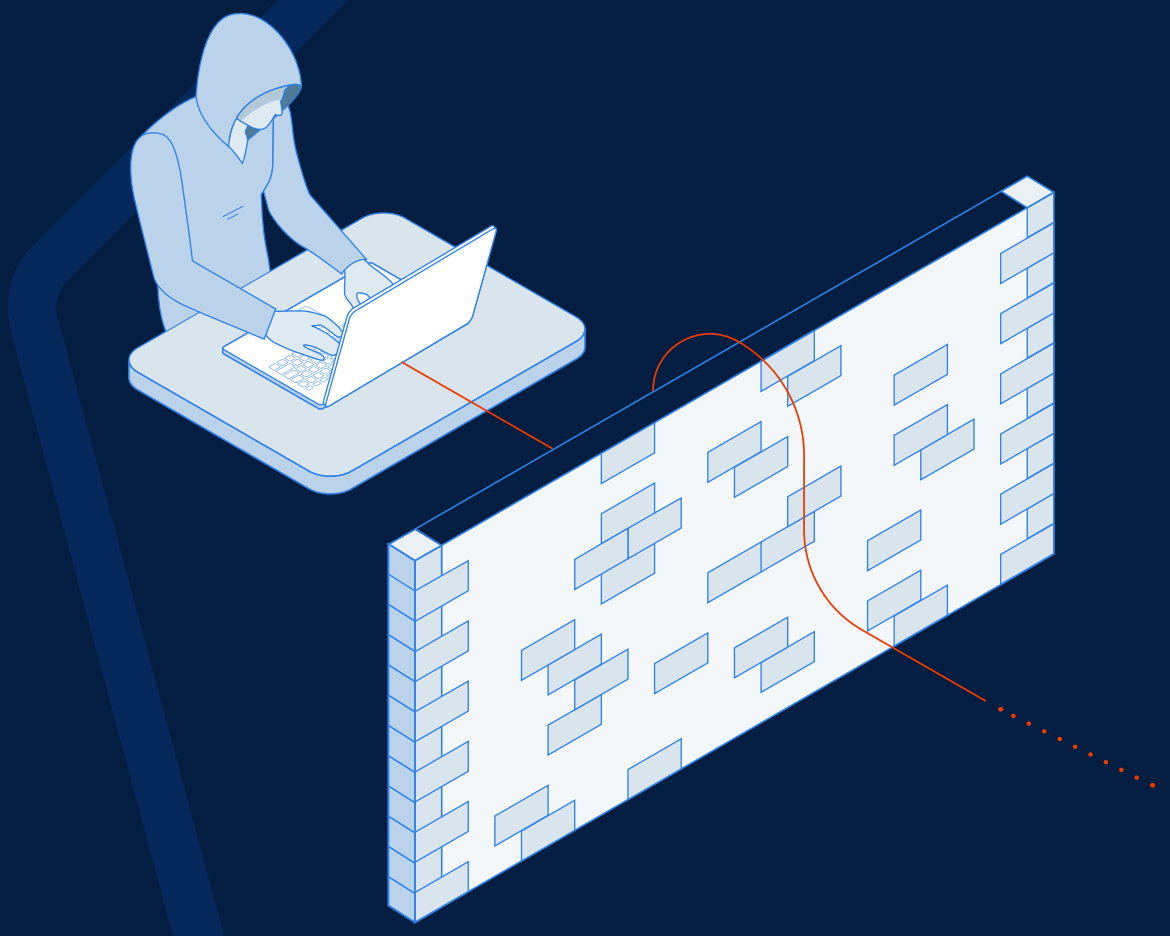
tenable.ad™

SECURING ACTIVE DIRECTORY:

HOW TO PROACTIVELY DETECT ATTACKS



Active Directory has been the main identity and access management solution for organizations over the past 21 years. That fact has not changed, and the technology from Microsoft hasn't changed much either. This stale IAM solution is known not only to admins but attackers.

Organizations need to take a different approach when it comes to protecting their AD infrastructure, as well as all the resources on the network where AD is controlling and protecting access. Attackers have taken a highly sophisticated approach to attacking AD, from external and internal positions alike. History has proven that traditional security tools and approaches have not been very effective due to the increased number of successful attacks and the continued attack paths into AD. A single solution is not available to solve the security issues of AD, but with the correct tools and approach, security can be strengthened and attacks can be reduced.

AD History and Exposure

To say that Active Directory has not changed much over the past two decades is an understatement. As Active Directory hits its 21st birthday, some things remain the same, notably the objects and attributes that are contained within the infrastructure.

What does all this mean? First, very little effort needs to go into Active Directory education, as it has not and will not change. Second and more importantly, attackers have been able to find hidden backdoors and develop sophisticated attacks to obtain domain dominance.

Each feeds the other. If organizations are not staying on top of Active Directory while attackers are constantly finding backdoors, the attacks will continue to escalate, and efforts to secure AD will continue to slide.

- Environment is based on domains and forests
- Users, groups, and computers are the core objects
- Each domain is broken down for management of objects using organizational units (OUs)
- Group Policy is the preferred method for controlling users and computers
- Required services such as DNS and DHCP remain consistent
- Kerberos and NTLMv2 remain the preferred authentication protocols
- Password policy controls remain unchanged and stagnant

AD Security Solutions

Over the years, Microsoft has developed a few security solutions for on-prem AD, but often they are short-lived, eventually lose support, or are replaced with different solutions. The one technology that has remained at the forefront of AD security is Group Policy. Group Policy did see enhancements over the years with the inclusion of many ADM/ADMX customizations, Group Policy Preferences, and Advanced Audit Policy. However, the core architecture of Group Policy has remained the same.

Other security solutions have been introduced over the years too:

- Auditing and Advanced Auditing
- Security Configuration Wizard (SCW)
- Security Compliance Manager (SCM)
- Desired State Configuration (DCM)
- Local Administrator Password Solution (LAPS)
- Protected Users group

The overall issue with each of these solutions is the inability to truly secure most of the environment. The solutions only affect some computers, some security settings, and some attacks. Often, even if the solution has merit, they are not well marketed and therefore are not adopted for all AD installs.

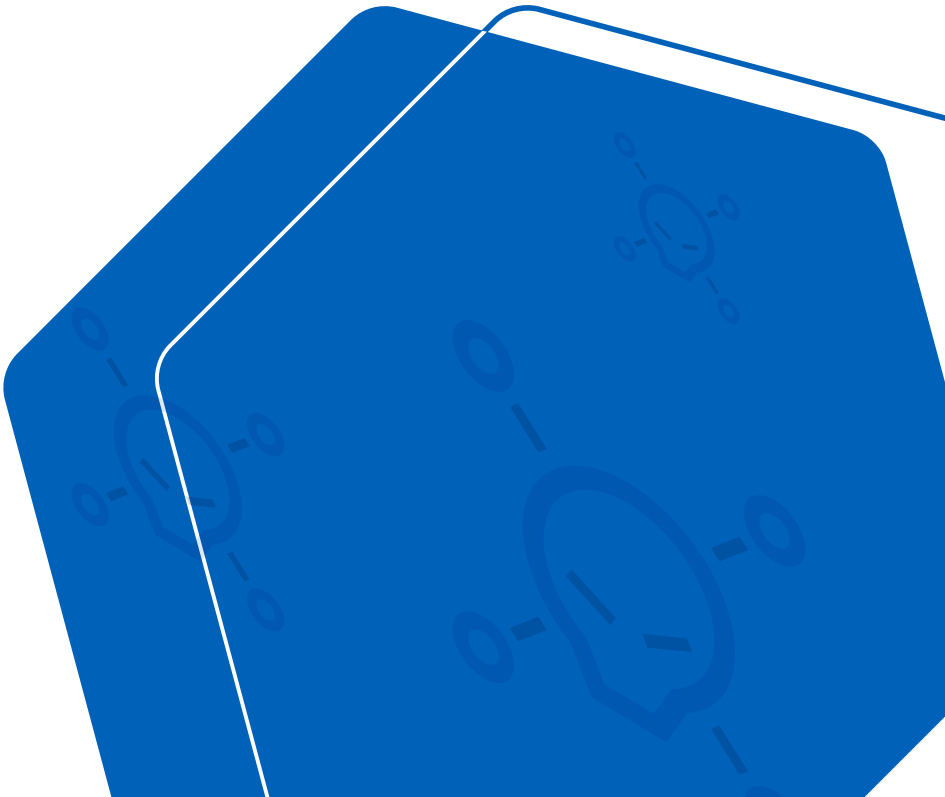
New Attacks Are Complex and Hidden

With static infrastructure and unstable security solutions, it is a feeding frenzy for hackers. Attacks on Active Directory have risen substantially, not to mention the depth of the attacks. Attackers for years have wanted to be able to attack the environment without generating any tracks or events. This is exactly what many of the new attacks allow.

The industry seems to blame Microsoft itself, as the foundation for Active Directory was not secure from the beginning. Without any enhancements, these core security holes and gaps remain.

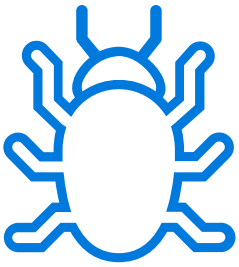
Regardless, these new attacks are making traditional monitoring solutions ineffective against detecting the attacks or any information related to the attacks. Attacks today are leveraging the foundational concepts on which AD and Microsoft are built, bypassing any event logging or change tracking that these AD monitoring solutions have been able to see for years. The attackers are leveraging lateral movement and privilege escalation to get to the domain domination phase in only a few hours or days. Here are some of the modern attacks/concepts that are plaguing AD today:

- DCSync
- DCShadow
- Password spray
- Pass-the-Hash
- Pass-the-Ticket
- Golden ticket
- Service Principal Name
- AdminCount and adminSDHolder



Detection Is Not Simple

As these attacks work their destruction behind the scenes of existing technologies required for Microsoft, Windows, and AD to run, they are nearly impossible to detect. The attackers have taken many different approaches to bypass monitoring systems and activity logs. Not all attacks, however, follow the same approach.



Slow Attacks

Some attacks are slow, meaning the activity looks like normal actions on the network. Meanwhile, they can provide highly insightful information to the attacker in a short amount of time. These attacks mostly go after the passwords of user accounts, so that no privileges are required. They only need access to the network to attempt to log on.

One such attack is a password spray attack. Users in any environment often use common passwords. So if the full list of user account names can be obtained, which is possible from Active Directory by any user, every username can be tested against a few common passwords. The key is to use fewer passwords than the account lockout policy limits, which is also readable by any user in the domain.

Attacks That Use Core Technology and Configurations

Consider that Microsoft Active Directory was created in 2000. Yahoo was a tech wunderkind and Bill Clinton was president. The technologies that Microsoft built in to ensure that communication was seamless are still built into the technology today. Over the years the technologies have been used against the environment, as information related to certain privileged accounts was discovered easily. Some of the common built-in technology being used against the AD environment includes:

- Service Principal Names
- Admincount and adminSDHolder SIDHistory
- User Primary Group ID

These essential aspects of the environment were designed to ensure security and consistency, but the attackers are now leveraging them to create backdoors and gain persistent access without being noticed. For example, the adminCount and adminSDHolder attack is quite simple in concept, and nearly impossible to stop without persistent attention to the details. In short, the attacker will alter the ACL held in the adminSDHolder object to include an account they control, giving the account Modify or Full control. When the background process runs to place the ACL on all objects that contain the adminCount attribute equal to 1, the attacker is given permissions over the privileged objects.

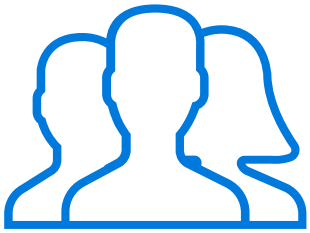
Attacks That Bypass Logging

New attacks have been devised that are quite sophisticated and ingenious. These attacks do require privileges in Active Directory, but with so many other attacks giving the attacker privileges, they are only used after those privileges are granted. The purpose of the privileged attack is to gain persistence without anyone noticing. The two attacks that fall under this category include:

- **DCSync**
- **DCShadow**

The overall purpose of DCSync is to get the password account data so that offline attacks can be made password hashes which are obtained by the attack. The DCShadow attack is a little different in that it creates a fake domain controller, which is used to inject attacks into the replication stream, altering objects and attributes without leaving a trace.

Both attacks bypass the logs. This is possible because they mimic a new domain controller, and the log of the fake domain controller never exists! This is an ideal attack for organizations that are relying on the security event log to see activity. AD monitoring, SIEM solutions, and even most agent-based solutions will fail to recognize these attacks.

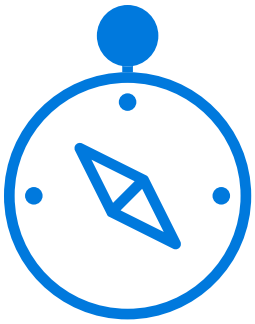


Attacks That Impersonate Other Users

Attacks that have been around for a while but continue to spawn new options include:

- Pass-the-Hash
- Pass-the-Ticket
- Silver Tickets
- Golden Tickets

These attacks are in some way using stolen credentials to impersonate the user. Of course, the stolen credentials are from a privileged user, so that the highest possible privileges can be used in the domain. Pass-the-Hash and Pass-the-Ticket use the raw hashed information to impersonate the user, while Silver and Golden Tickets take over part of the Kerberos authentication process which allows for access to services and all accounts in the enterprise.



Proactively Detect a Variety of Attacks

Consider that most AD environments were created years ago. When Active Directory was installed, today's security issues were not even known to be an issue. Every organization that runs Active Directory needs to be informed of their existing security issues that could lead to an attack against their infrastructure. Unfortunately, AD monitoring and SIEM solutions do not provide this service or feature.

Tenable.ad for AD does right out of the gate. When you install Tenable.ad for AD, the system will provide a list of existing issues and misconfigurations that need to be fixed immediately.

Not only does every organization need to clean up its current security posture for AD, but ongoing monitoring is needed to ensure that misconfigurations and attacks do not occur. So many organizations think that if only security hardening is required, the settings will not change. This is not the case in any production Active Directory environment. Settings change all the time due to error, installations, updates, and attacks.

Therefore, if any misconfiguration or attack initiates, time is of the essence to detect and alert the organization. Some attacks are slow, while other attacks can take only minutes. The faster the attack can be identified, the better the chance it can be negated.

AD monitoring and SIEM solutions rely on security logs for their knowledge of ongoing actions in and around Active Directory. Tenable.ad does not wait for the activity to be logged. Instead, Tenable.ad uses the raw AD replication stream to obtain information before the action is even performed. With every second making a difference, this could make or break the negation of the attack. (Of course, Tenable.ad can send the information it finds to a SIEM, which is why SIEMs are a vital component of the overall security of any organization.)

Summary

With Active Directory being so well known and stagnant, attackers have been able to find new and innovative backdoors into the infrastructure. These backdoors are clever, allowing for information to be gained with little to no privileges, which allows the attackers to be on the network without being noticed. There are some attacks which require privileges, but these attacks can bypass the security log, and thus AD monitoring and SIEM solutions. To detect all attacks being used today, a proactive approach like Tenable.ad is the best solution. Tenable.ad provides immediate information regarding misconfigurations, as well as real-time detection of any new misconfigurations or attacks. All with no agents and no privileges.

To see Tenable.ad work in your environment, contact us.

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com