The Attacks that can Target your Windows Active Directory

Originalartikel

Backup

<html> Active Directory is at the center of many attacks as it is still the predominant source of identity and access management in the enterprise. Hackers commonly target Active Directory with various attack techniques spanning many attack vectors. Let's consider a few of these attacks and what organizations can do to protect themselves. <h2>Modern Active Directory attacks used by threat actors</h2> Many different attacks targeting Active Directory Domain Services (AD DS) can compromise the environment. Note the following modern attacks used against AD DS. DCSync
DCShadow
Password spray
Pass-the-Hash
Pass-the-Ticket
Golden ticket
Service Principal name
AdminCount
adminSDHolder
<h3>1. DCSync</h3> Domain controllers hosting Active Directory Domain Services use a type of replication to synchronize changes. An experienced attacker can mimic the legitimate replication activity of a domain controller and use the GetNCChanges request to request credential hashes from the primary domain controller. There are free and open-source tools, like Mimikatz, available to make this type of attack extremely easy. Protecting against DCSync attacks: Implement good security practices for domain controllers, protecting privileged accounts with strong passwords
Remove unnecessary accounts from Active Directory, including service accounts
Monitor changes to domain groups and other activity
<h3>2. DCShadow</h3> The DCShadow attack is very similar to the DCSync attack since it takes advantage of legitimate Active Directory communications traffic between domain controllers. In addition, the DCShadow attack uses the DCShadow command as part of the Mimikatz lsadump module. It uses instructions in the Microsoft Directory Replication Service Remote protocol. It allows attackers to register a rogue domain controller in the environment and replicate changes from it to other domain controllers in the background. It may include adding hacker-controlled accounts to the domain admins group. Protecting against DCShadow attacks: Protect your environment from privilege escalation attacks
Use strong passwords on all protected accounts and service accounts
Don't use domain administrator credentials to log in to client PCs
<h3>3. Password spray</h3> Password spraying is a password attack targeting weak account passwords in Active Directory Domain Services. With password spraying, attackers use a single common or weak password and try this same password against multiple Active Directory accounts. It offers advantages over the classic brute force attack since it doesn't trigger account lockouts, as the attacker only tries the password once per account. In this way, attackers can find weak passwords in the environment across multiple users. Protecting against Password spray attacks: Enforce strong passwords using good password policies
Prevent the use of incremental passwords or breach passwords
Prevent account password reuse
Encourage the use of passphrases for passwords
<h3>4. Pass-the-hash</h3> Like other password databases, Active Directory hashes the passwords stored in the database. A hash is simply a mathematical representation of a clear-text password that hides the password from plain sight. A pass-the-hash attack allows the attacker to access the hashed form of the user password and uses it to create a new session on the same network to access resources. With this attack, the attacker does not have to know or crack the password, only possess the password hash. Protecting against Pass-the-hash attacks: Limit

the number of users with admin rights
Use hardened workstations as admin jump boxes
Implement the Microsoft Local Administrator Password Solution (LAPS) for local accounts
<h3>5. Pass-the-ticket</h3> Modern Active Directory environments use Kerberos authentication, a ticket-based authentication protocol. Pass-the-ticket attacks use stolen Kerberos tickets to authenticate resources in the environment. Attackers can exploit authentication using this attack to move through an Active Directory environment, authenticate resources as needed, and for privilege escalation. Protecting against Pass-the-ticket attacks: Use strong passwords, especially for admin and service accounts
Eliminate breached passwords in the environment
Increase your overall security posture by following best practices in the environment
<h3>6. Golden ticket</h3> The Golden Ticket attack is a cyber-attack where an attacker steals the NTLM hash of the Active Directory key Distribution Service Account (KRBTGT). They can get this hash using other types of attacks. Once they have the password for the KRBTGT, they can grant themselves and others the ability to create tickets. Detecting this type of attack is difficult and can lead to long-term compromise. Protecting against Golden ticket attacks: Change the KRBTGT password regularly, at least every 180 days
Enforce least privilege in your Active Directory environment
Use strong passwords
<h3>7. Service Principal Name</h3> A Service Principal Name (SPN) is a special identifier for a service instance in Active Directory. Kerberos uses the SPN to associate a service instance, like Microsoft SQL Server, with an Active Directory account. Kerberoasting attacks attempt to crack the password of the service account used for the SPN. First, they capture the TGS ticket issued by their malicious request for a Kerberos service ticket. Then, they take the captured ticket offline to use tools like Hashcat to crack the service account's password in plain text. Protecting against Kerberoasting attacks: Monitor for suspicious activity, such as unnecessary Kerberos ticket requests
Use extremely strong passwords on service accounts and rotate these
Monitor service account use and other privileged accounts
<h3>8. Admin count</h3> Attackers generally perform surveillance of an environment once they have low-level access to a network. One of the first additional tasks an attacker seeks is elevating their privileges. To elevate privileges, they need to know which accounts are privileged accounts. An Active Directory attribute, called the AdminCount attribute, identifies users who have been added to protected groups, like Domain Admins. An attacker can effectively identify objects with administrative privileges by monitoring this attribute. Protecting against adminCount attacks: Monitor the adminSDHolder ACL regularly for rogue users or groups
Monitor accounts with the adminCount attribute set to „1“
Use strong passwords across the board
<h3>9. adminSDHolder</h3> Another common Active Directory attack vector is abusing the Security Descriptor Propagation (SDProp) process to gain privileged access. What is SDProp? It is an automated process in Active Directory where every 60 minutes, the SDProp process runs and copies the ACL from the adminSDHolder object to every user and group with an adminCount attribute set to „1“. Attackers can potentially add a rogue user or group to the adminSDHolder ACL. The SDProp process will then adjust the rogue user permissions to match the adminSDHolder ACL, thus elevating their privileges. Protecting against adminSDHolder attacks: Monitor the adminSDHolder ACL regularly for rogue users or groups
Monitor accounts with the adminCount attribute set to „1“
Use strong passwords across the board
<h2>Bolster Active Directory Security with Specops Password Policy (SPP)</h2> Active Directory is a prime target of attackers looking for easy ways to compromise business-critical data. Weak, breached, incremental, and other password types often make it easy to compromise accounts. Unfortunately, Active Directory does not contain native tools to enable modern password policies or protect against breached passwords. <a href=„https://specopssoft.com/product/specops-password-policy/?utm_source=bleepingcomputer&am

p;utm_medium=referral&utm_campaign=na_2023_bleepingcomputer&utm_content=guest-post“ target=„_blank“ rel=„nofollow noopener“>Specops Password Policy helps organizations protect passwords against various types of Active Directory attacks and provides a natural extension of the existing Group Policies. With Specops Password Policy, organizations can: <ul class=„c2“>
Create custom dictionary lists to block words common to your organization
Find and prevent the use of over 3 billion compromised passwords with Breached Password Protection which includes passwords found on known breached lists as well as passwords being used in attacks happening right now
Provide real-time dynamic feedback to end-users at password change with the Specops Authentication client
Block usernames, display names, specific words, consecutive characters, incremental passwords, and reuse a part of the current password
Target any GPO level, computer, user, or group population
Specops offers powerful breached password protection <figure class=„image c3“><figcaption>Specops Password Policy</figcaption></figure> <h2>Wrapping up</h2> Protecting your Active Directory infrastructure from attack is crucial to your overall cybersecurity posture. Cybercriminals commonly attack Active Directory accounts using many different attack vectors, including the ones we have listed. Increasing the overall password security in the environment, enforcing good password hygiene, and eliminating breached, incremental, and otherwise weak passwords help to bolster the security of your Active Directory environment and privileged accounts. Specops Password Policy with Breach Password Protection helps organizations achieve this goal effectively and easily. Sponsored and written by Specops Software
</html>