VARONIS

Active Directory
Security Audit Checklist

Active Directory touches nearly every part of a modern organizations network infrastructure. Its complexity and reach provide a large surface area for attackers to find vulnerabilities and misconfigurations that can wreak havoc on your infrastructure.

The following checklist is a guide to locking down your Active Directory so you can feel more confident in your overall security posture.

While this guide is non-vendor specific, many of the gaps we highlight are substantially easier to detect and fix with Varonis. Please refer to 7 Key Risk Indicators in the Varonis Active Directory Dashboard for specifics of how Varonis can help detect advanced Active Directory attacks and proactively secure your environment.

Domain Actions

1 Rotate Kerberos domain account passwords every 40 days

If an attacker is able to compromise a domain controller, they may be able to steal the password hash of the KRBTGT account. This account can then be used to generate arbitrary (but valid) Kerberos tickets. A compromised KRBTGT account gives an attacker unrestricted access in the domain.

The KRBTGT account is a service account not typically accessed by users. It is used for Kerberos authentication on the KDC and its password derives the key for encrypting a TGT.

2 Track native Administrator account access attempts

Using the native Administrator account can make management easier for system admins. It is also challenging to break old practices.

The native admin account has a well-known name and SID, and also doesn't lockout by default. Attackers can compromise accounts by dumping Kerberos tickets and password hashes off of machines (or brute force). If an attacker were to compromise the native Administrator account, they would have highly privileged access throughout the domain.

Organizations should only use the native administrator account for initial build activities, and possibly, disaster-recovery scenarios.

Using a product like Varonis, you can easily configure alerts to detect when the native Administrator account is being used.

3 Remove permanent members of the Schema Admins group

Attackers can compromise an account that is a member of the Schema Admins group and have access to modify the full Active Directory schema.

Often organizations allow permanent access to the Schema Admins group for ease of maintenance.

Organizations should establish a policy of only granting temporary inclusion in the Schema Admins group, access should be monitored and members should be removed at the earliest opportunity.

4 Deploy Local Administrator Password Solution (LAPS)

An attacker can steal the password hash of a local computer account and use it to attempt pass-the-hash attacks (or other similar attacks). Typically the local admin password is the same across all PCs, so if it is compromised then all computers are compromised.

LAPS is a Group Policy Object client-side extension available from Microsoft that improves the controls available for the management of local administrator passwords. Most crucially it stores local admin account passwords in Active Directory so they can be managed across your organization instead of on a per machine basis.

> You should push LAPS to all of your managed machines as part of your local administrator account management.

5 Add all admin, service and other high-value accounts to the Protected Users Group

Members of the Protected Users group automatically implement basic security controls that greatly reduce the default memory footprint of credentials used in the sign in process.

User Account Actions

6 Remove all SID History Entries from the current domain users

SID history is used in migrations, but a user should not have the SID history of another user in the same domain. Attackers can use SID histories to escalate the privileges of a normal user to those of a privileged user in the domain.

7 Identify accounts with passwords that never expire

Attackers can compromise an active account and use its permissions to navigate the domain. Without a password expiration, there is no automatic mechanism to ensure that the credentials are reset.

Once identified, apply password expiration policies to the accounts.

8 Remove users in atypical Primary Groups

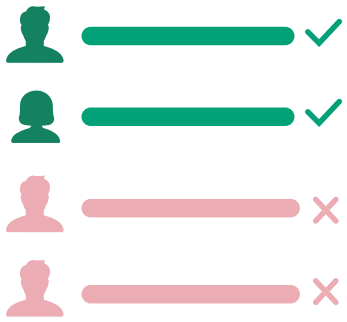
The Primary Group attribute of an object acts similarly to being a member of a group. Attackers can escalate the permissions of an account by switching the Primary Group to that of Domain Admins. Primary Group IDs are only for domain groups.

9 Limit the number of admin accounts with Service Principal Names (SPN)

Service Principal Names (SPN) uniquely identify each individual service instance on your network. A SPN is registered to a specific account within your larger Active Directory setup which then allows the service account to perform operations on your network with the privileges of that account.

Attackers target Service accounts as they often have admin privileges, are overprivileged and infrequently change passwords.

SPN service tickets are frequently the target of privilege escalation attacks as they can request a service ticket from Domain Controller Service Principal Names which may contain crackable hashes.



You should maintain minimal permissions on the accounts registered for SPN use, force AES cryptographic libraries in Kerberos (to make cracking more difficult) and enforce password length and complexity requirements on accounts.

10 Limit the number of users that do not require Kerberos pre-authentication

Old clients may not support Kerberos pre-authentication. These clients are extremely vulnerable to attack as they use a lower encryption level (RC4) which can be brute forced offline. (Kerberoasting).

11 Disable unconstrained delegation for Kerberos

Attackers can compromise an account that is trusted for Kerberos Delegation and use it to impersonate other user accounts. Kerberos delegation should only match specific service accounts to clients.

12 Limit accounts that do not require authorization data

Accounts for non-Windows machines on a domain that does not support Privilege Attribute Certificate (PAC) data to be sent to Kerberos can be compromised by falsely requesting tickets and cracking them offline.

13 Identify users with no password requirement

Accounts with no password requirements on length or complexity can easily be identified by attackers via querying for users with the “PASSWD_NOTREQD” flag via LDAP.

For high-value accounts, we recommend complex passwords of greater than 30 characters.

14 Limit the number of accounts that use Constrained Delegation

While less dangerous than Unconstrained Delegation, attackers can use constrained delegation to impersonate other users on the network to gain access to network resources. They can also use this technique to obfuscate their actions. Multi-tiered applications often use this right to connect to multiple servers while maintaining the authentication credentials of the original client.

Computer account actions

15 Disable weak Kerberos encryption types

Attackers can capture Kerberos tickets with weak encryption methods and attempt to crack account passwords. RC4 and other encryption methods other than AES are considered “weak encryption types” and should be disabled.

16 Don’t allow computer accounts that are also admin accounts

The SYSTEM account for that computer will have the set permissions on the network. This can be used for applications or scripts where the SYSTEM account will access network resources (such as a file server).

If an attacker were able to gain access to that computer and elevate to system rights, they would have privileged access on the domain.

17 Remove risky operating systems from your network

Older operations systems like Windows 7 and Windows Server 2008 R2 do not support the AES cryptographic suite. They rely on the outdated and significantly easier to crack RC4 or DES suites.

These limitations prevent you from implementing policies forcing the use of AES for all token encryption. It's important to consider that legacy clients put more than their just their own data at risk, but potentially all the data in your organization.

Privileged Account Actions

18 Restrict and monitor service accounts

Service accounts are used to automatically run processes and are often granted permissions beyond that for ordinary accounts. This and their lack of monitoring make them a frequent target of attacks.

19 Restrict and monitor service accounts

Executives in your organization have high visibility and are more prone to targeted attacks (spear-phishing, etc.). Attackers have taken over executive accounts and done things like initiate fraudulent wire transfers, request sensitive data or other nefarious actions.

Because of their valuable nature, more control needs to be given to make sure that they are acting in a normal and secure manner.

VARONIS

20 Monitor administrator account actions and behaviors

If compromised, Administrator accounts allow for havoc to unfold on your network. Attackers can not only launch attacks with elevated privileges but alter other accounts to grant themselves future backdoor access, delete logs that might detail their actions and exfiltrate data with impunity.

Why These Steps Are Not Enough

All an attacker needs is time and motivation to infiltrate your network. It's your job to make their efforts to break in and remain undetected as difficult as possible.

While you can start working through the above tasks right away, securing Active Directory is a substantial undertaking. To accomplish many of the items requires a mix of internal configuration investigation, monitoring and careful deliberate changes to confirmations.

During a cyber attack, it's a race between the attacker and defenders to see if the attacker can steal data before the defenders can close down the attacker's access to the network.

Beyond patching vulnerabilities and improving configurations you need to be able to do things like correlate data access and exfiltration with Active Directory account actions, catch attacks like Kerberoasting, Golden Ticket and Silver Ticket on the fly and pull back access across the board to the minimum needed.

You need to be able to:

- Monitor AD logins to detect encryption downgrade attacks
- Flag potential network reconnaissance from attackers using an account to access multiple servers in an unusually short time frame
- Detect pass-the-ticket attacks that bypass standard Kerberos processes
- Alert you to changes in admin groups, or unusual access patterns from privileged account groups