Checklist

10 Steps for Controlling who has Privileged Access to Active Directory

This checklist is adapted from the white paper, ***Top 10 Ways to Identify and Detect Privileged Users*** by Randy Franklin Smith**.**

Overview

Almost all cyber attackers are after the same two things: credentials and data. Attackers utilize tactics like malware and phishing scams to gain access to an organization's network. Once inside, they perform reconnaissance using tools like PowerShell to escalate their privileges—with the goal of gaining privileged access to Active Directory (AD). After they get ahold of these privileged accounts, they can access every system, application, and data resource connected to AD.

> **"Organizations without the tools to automate the monitoring and reporting of privileged access within their AD-centric environments always end up having embarrassing numbers of people with unsanctioned authority. STEALTHbits' AD solutions automate the laborious tasks associated with constantly ensuring AD security."**
>
> **Randy Franklin Smith,**
> **Microsoft Security MVP**

This checklist outlines 10 ways attackers try to gain privileged access to AD. Organizations can use this list to:

- Identify who has privileged access
- Determine where security risks lie
- Detect new privileged access grants

1. Built-in privileged groups such as Domain Admins

Check who is in built-in privileged AD groups like Domain, Enterprise, and Schema Administrators, as well as who is in the Local Administrators group with privileged access on endpoints. Also, monitor and get alerted when someone is added to one of these privileged groups to prevent unauthorized access.

2. Nested groups within privileged groups

Identify every member of groups that are nested within privileged groups. Track changes in the membership of these nested groups to ensure attackers do not gain privileged access. Use insight into group nesting to simply access rights and move to a more secure model.

3. Organizational unit permissions

Catalog all privileged organizational unit (OU) permissions, including permissions to the objects within an OU. Since OU permissions reviews are time- and labor-intensive, the best way to stay up-to-date is to automate the assessment of AD permissions as well as the tracking of permission changes.

4. Admin equivalent rights on domain controllers

Examine who can logon to a domain controller (DC) with administrator equivalent rights. The user rights can be found in group policy objects (GPOs) under user rights assignments. To gain visibility into the group membership and nesting details for these accounts, organizations need to use pre-built reports like those offered by STEALTHbits.

5. Users with password reset authority over other users

Determine who has the ability to reset other users' passwords, including rights assigned directly (object level) and though inheritance (OU level). Constantly monitor the state of password permissions and receive immediate notification of any changes in order to thwart attacks.

6. Users with knowledge of any privileged service accounts

Locate all privileged service accounts across domains and verify whether they are being used properly by analyzing the logon type. There should be only service startups, not interactive logons at a DCs' console, which may indicate malicious use of the service account.

7. Users with write access to GPOs that are applied to DCs or servers running applications with domain privileged access

Evaluate everyone with Write access to any group policy applied to DCs or servers running applications that have domain privileged access. Start by reviewing users and groups with permissions on GPOs linked to the Domain root or Domain Controllers OU. Then, review the permissions on any policies linked to the parent OU of servers that can run applications with privileged domain access. This dual approach gives you a full view of every user who can change these policies.

8. User accounts with access to any AD management solutions

Inventory all third-party applications running on DCs or servers that help manage Active Directory. Then, identify any service or proxy accounts with privileged access to AD that are being used to assist these applications. Checking these accounts, along with any account with permissions within the applications themselves, helps organizations identify risks and monitor accounts to ensure appropriate use.

9. Virtualization infrastructure admins

If an organization is running DCs or servers within a virtual infrastructure, it needs to identify which accounts have privileged access to its virtual environment. Do this by cataloging local Admin groups on a given DC or server and/or by finding privileged access within the virtual environment itself. This analysis is critical because service or proxy accounts with privileged access to AD can also be exploited within a virtual infrastructure.

> **"Assessing and detecting of privileged users is an obvious avenue for a third-party solution that automates some or all tasks. Without one, it's safe to say that no organization can stay on top of every method of privileged access."**
>
> **Randy Franklin Smith,**
> **Microsoft Security MVP**

10. Credential artifacts

Find where privileged users are logging onto DCs and servers. Ensure WDigest settings do not allow cleartext passwords to be stored memory. Not storing credential artifacts on servers and workstations makes it harder for attackers to gain access. To further strengthen security posture, establish multiple levels of privileged accounts so Domain Admin privileges are restricted to a few authorized administrators and local Admin privileges are used to address specific workstation issues.

Conclusion

To maintain a secure Active Directory, organizations need to regularly assess permissions and monitor them for changes that could signal malicious use. Staying on top of all privileged AD users is challenging without help from a third-party solution. STEALTHbits in-depth, automated permissions analysis and reporting helps you easily determine effective permissions associated with AD domains, OUs, and objects, as well as detect new privileged access grants.

For more information and to download our free trial, please click here.

About STEALTHbits Technologies

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.

Identify threats. Secure data. Reduce risk.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com