

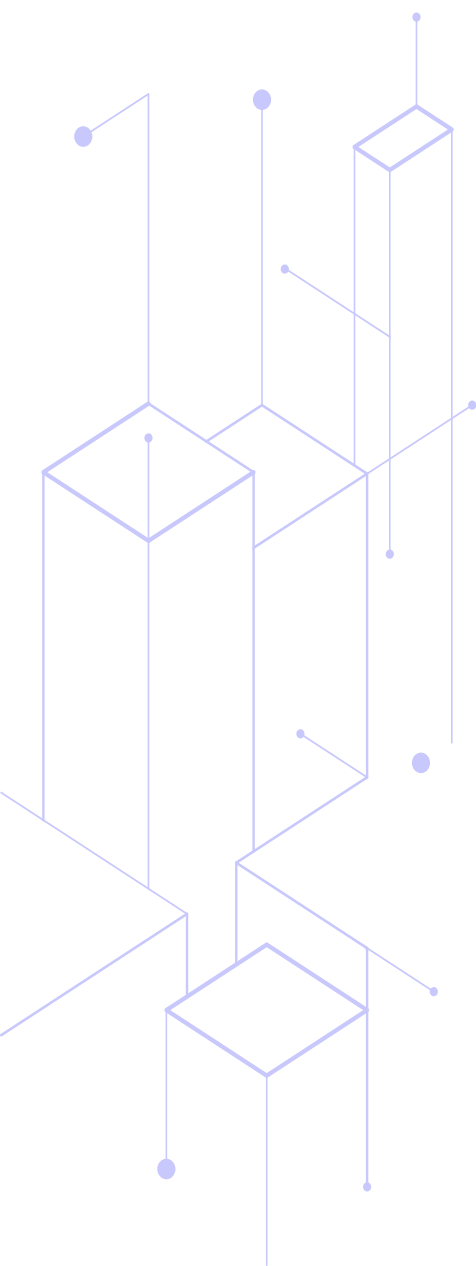
Securing privileged access in Active Directory

15 Windows event IDs to track and detect privilege escalation attacks



Table of contents

Introduction	1
What are privileged accounts and why are they important?	2
What are privilege escalation attacks?	3
Steps hackers take in a privilege escalation attack	4
Here's how the Universal Health Services (UHS) fell prey to a privilege escalation attack	8
How to audit privilege escalation attacks using the native tool	9
Important events to track using Event Viewer to detect privilege escalation attacks	10
Why is it challenging to detect privilege escalation attacks using native logs?	12
How to audit privilege escalation attacks with ADAudit Plus	12
Real-time change auditing	12
Spot behavioral anomalies with UBA	14
Real-time alerts on suspicious activities	15



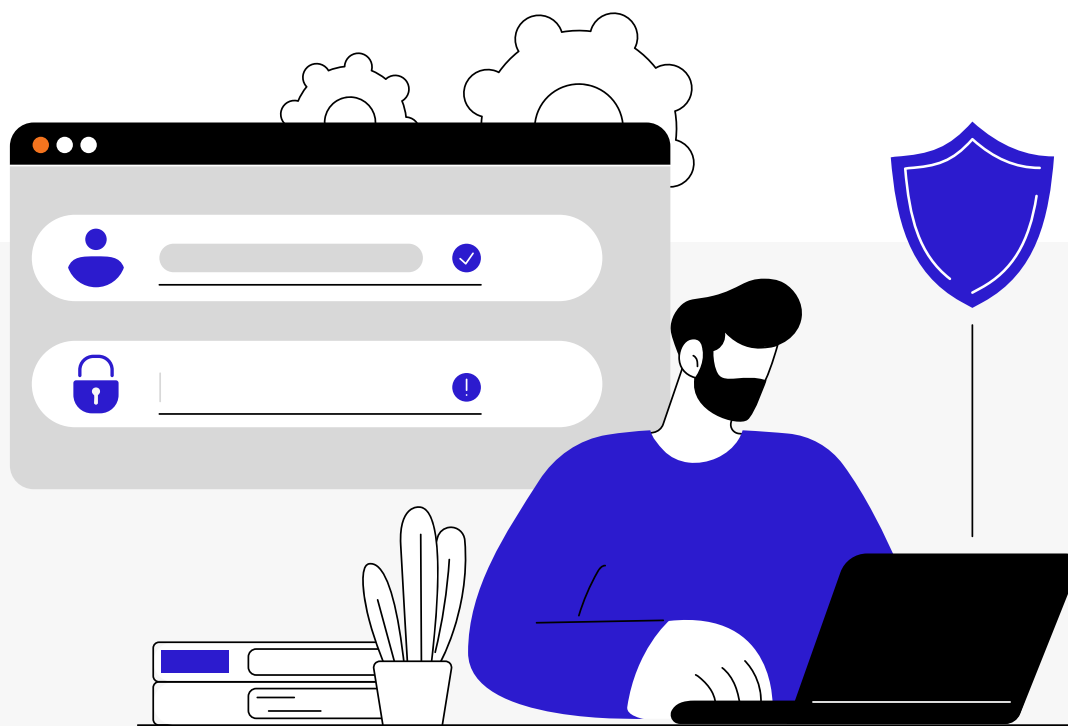
Introduction

AD is the central hub for the management of user accounts, resource allocation, and security protocols.

As the primary repository for critical information like credentials and user data within the network, ensuring the security of AD is crucial to prevent unauthorized access and data breaches.

A key component of AD is privileged accounts that provide elevated access and functionality beyond standard user accounts. Privileged accounts provide the user with multiple capabilities, including being able to perform software installations, manage system upgrades, and configure modifications. This functionality makes them susceptible to privilege escalation attacks. Threat actors often attempt to identify and exploit system vulnerabilities by elevating a standard user to a privileged account. This gives the hackers complete access to the system, allowing them to carry out malicious acts and create chaos by exploiting these enhanced capabilities.

Consequently, this situation leads to a harmful duality characterized by both intent and capability. This enables attackers to create chaos by taking advantage of their enhanced abilities.



What are privileged accounts and why are they important?

Privileged accounts confer more privileges than ordinary accounts. The accounts are associated with roles within an organization, such as help desks, security teams, IT admins, application owners, database administrators, and more. Privileged accounts can also be machine-to-machine or application-to-application accounts that perform autonomous functions without human intervention.

AD accounts with privileged group memberships possess critical rights, privileges, and authority, enabling comprehensive control over AD and domain-connected systems. These accounts wield significant power, allowing execution of various operations essential for system management and security.

These accounts are constantly targeted for cyberattacks globally. According to the [Microsoft Vulnerabilities Report 2023](#) a total of 1300 incidents were reported, the leading vulnerability category for the third consecutive year in 2022 was Elevation of Privilege. It comprises 55% (715) of the total Microsoft vulnerabilities for the year. This concern is heightened by a recent [Identity Defined Security Alliance study](#). The study found inadequately managed identities to be the second most common breach enabler in 2023. Of the surveyed organizations, 37% reported violations due to this discrepancy. In light of this alarming statistic, it is crucial that privileged identity security in AD is given high priority. This is to prevent far-fetched repercussions of compromised accounts.



What are privilege escalation attacks?

A privilege escalation attack involves gaining elevated rights, permissions, or privileges illegally. In this way, the scope of an identity, account, user, or machine is extended beyond what was originally assigned. Attackers seek to exploit security weaknesses within a system's security framework in order to breach their security perimeter.

It's not uncommon for threat actors to target privileged accounts. Most common privilege accounts that attackers target are:



Domain administrator account:

These accounts allow an attacker to manipulate the entire domain infrastructure, giving them unparalleled control over a network.



Domain service accounts:

These accounts enable cross-system services and can be exploited to conceal breaches.



Local administrator accounts:

When attackers infiltrate these accounts, they gain access over a single computer, which allows them to move laterally across multiple computers in the network.



Emergency accounts:

These accounts are utilized in contingency situations, but become avenues of exploitation when left unguarded.



Service accounts:

These accounts are used for running services and related operations in a Windows environment.

These privileged data accounts, including user accounts and application accounts, become attractive targets, as they might contain a treasure trove of sensitive information.

Steps hackers take in a privilege escalation attack

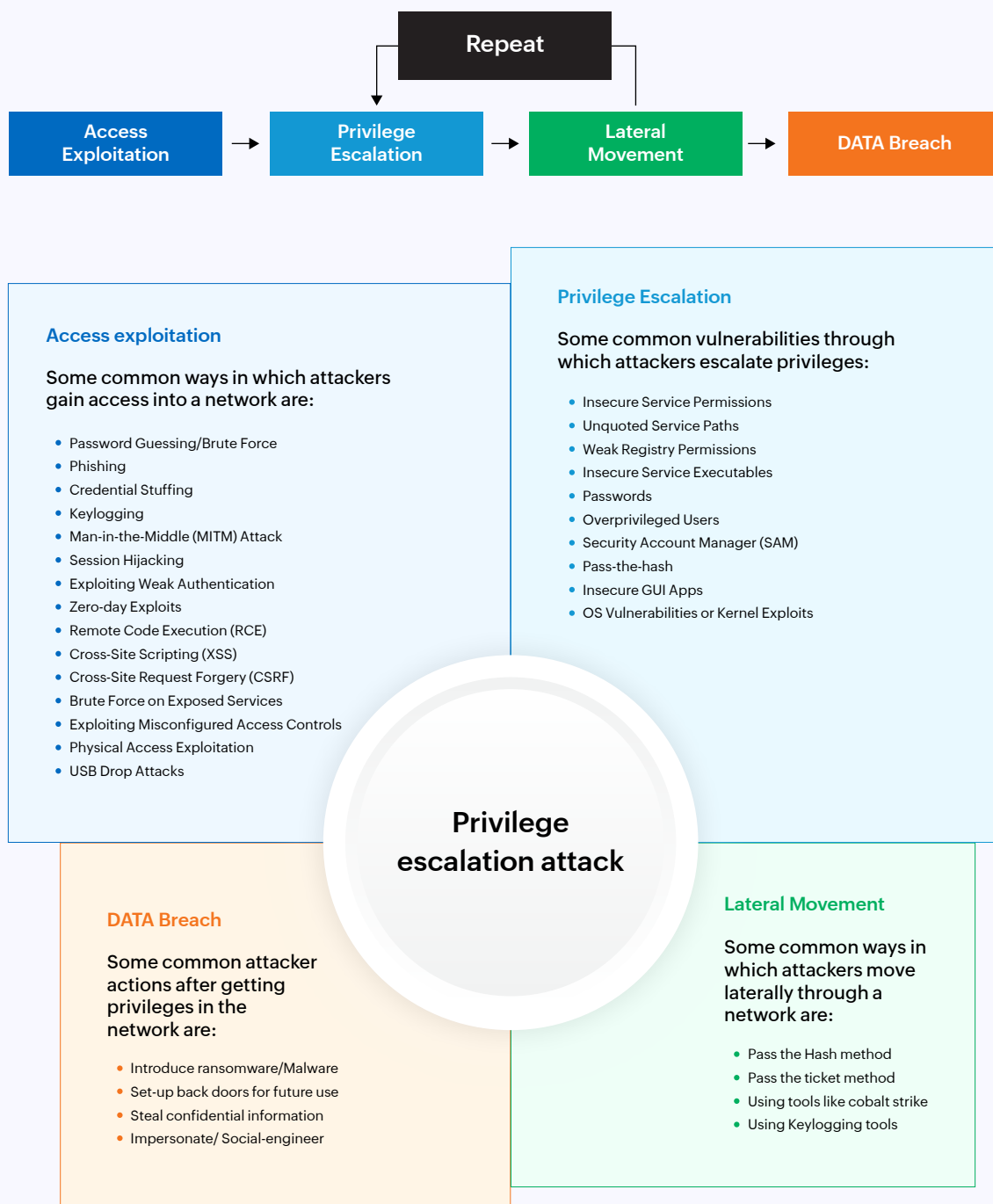


Figure 1: Privilege escalation attack steps

As part of a privilege escalation attack, there are typically several steps:

Reconnaissance

Attackers collect information about the AD structure, user accounts, group memberships, and system configurations. Potential targets and vulnerabilities may be identified through scanning the network.

The following tools are likely the most widely used for reconnaissance and detection purposes:

- ➔ **Nmap** is a versatile open-source network scanning tool for discovering devices, assessing security, and identifying vulnerabilities on a network.
- ➔ **Wireshark** is a popular open-source network analyzer used by administrators, security experts, and developers to examine and record network traffic, revealing insights into device communication on a network, aiding in issue resolution, behavior analysis, and security threat detection.
- ➔ **Metasploit** is a widely-used penetration testing framework that assists security professionals in identifying and exploiting vulnerabilities in computer systems, helping them assess and strengthen their cybersecurity defenses.
- ➔ **BeEF, the Browser Exploitation Framework**, empowers ethical hackers and security pros to assess and exploit web browser vulnerabilities, enabling remote control and demonstrating security weaknesses for enhanced web app security.
- ➔ **Cobalt Strike** is a commercial penetration testing tool that is often used by cybersecurity professionals and red teams to simulate advanced cyberattacks, test security defenses, and assess an organization's vulnerability to sophisticated threats. It provides a range of capabilities, including post-exploitation, command and control, and beaconing, making it a popular choice for offensive security assessments.

Access exploitation

Attackers employ a variety of methods to infiltrate networks, seeking vulnerabilities for unauthorized access. Here are a few of the methods they use:

- ➔ **Password guessing and brute-force attacks** are used by attackers to attempt all possible password combinations until they find the correct one. This method relies on automation and exploits weak passwords, compromising digital accounts, systems, or data.
- ➔ **Phishing** uses deceptive emails, messages, or fake websites to trick individuals into revealing sensitive information, like passwords or financial details.

- **Credential stuffing** uses stolen credentials from one breach to gain access to other accounts. Hackers depend on end users deploying the same password in more than one of their accounts, which a surprising number do.
- **Key logging attacks** capture keystrokes to extract sensitive information.
- **Man-in-the-middle attacks** occur when threat actors intercept and possibly alter communication between two parties without their knowledge. By positioning themselves between the sender and receiver, the attacker can eavesdrop, manipulate data, and potentially compromise the confidentiality and integrity of the communication.
- **Session hijacking** exploits vulnerabilities in communication channels or steals session identifiers, so the attacker can take over the user's session. This is accomplished by accessing sensitive data or performing actions on their behalf without consent.

Privilege escalation

Once attackers have gained access to the network, they attempt to gain more control by elevating their privileges. By exploiting AD vulnerabilities, they gain access to higher privileges than they were granted initially, such as misconfigured permissions and weakly secured service accounts.

Here are some common AD vulnerabilities:

- **Unpatched software** can be exploited on operating systems, applications, and components related to AD if not updated with the latest security patches.
- **Weak password policies** impact AD accounts by making them susceptible to brute-force attacks, where attackers guess passwords to gain unauthorized access.
- **Misconfigured permissions** are those that are incorrectly configured, which can lead to unauthorized access to sensitive data related to AD objects, such as user accounts, groups, or organizational units.
- **Overprivileged accounts** enable attackers to escalate their privileges within AD environments by exploiting accounts that are assigned more privileges than necessary.
- **Insecure service accounts** can be exploited by attackers to gain unauthorized access to the network.
- **Group policy misconfigurations** can lead to security vulnerabilities that can enable attackers to modify systems, impact user behavior, and compromise security settings.

Lateral movement

Attackers with elevated privileges can move laterally across a network and explore different systems and resources. An attacker typically attempts to escalate their privileges to that of a Domain Administrator. Using this enhanced privilege, they can then access and exfiltrate sensitive data, manipulate user accounts, alter security settings, and gather more information utilized in this or in a future attack. Here are some of the tactics attackers use to move laterally across the network:

- **Pass the Hash** exploits stolen password hashes to authenticate on other systems without providing the actual password.
- **Pass the Ticket** uses Kerberos tickets to move undetected between Windows systems, assuming the identity of a compromised account. Using this tactic, they gain unauthorized access and maneuverability without raising suspicions.
- **Cobalt Strike** simulates legitimate network activity while allowing remote access and lateral movement. It enables bad actors to establish a foothold in a single system and pivot through the network, mimicking common user behavior.
- **Key logging** tools record keystrokes, including passwords, entered by users. This provides the attacker with the necessary credentials to access other systems, further aiding lateral movement.

Data exfiltration

Attackers use various tactics to exfiltrate data after obtaining domain admin privileges. To infect the network, they first introduce malware or ransomware. The malicious programs then exploit vulnerabilities, spread across systems, and encrypt data, forcing victims to pay for its release. Simultaneously, attackers establish backdoors, that create hidden entry points for unauthorized access in the future. Backdoors are designed to evade detection, enabling attackers to return and manipulate the compromised network.

Here's how the Universal Health Services (UHS) fell prey to a privilege escalation attack

The UHS was victimized by an intricate Ryuk ransomware attack in September 2020 and had an estimated impact of \$67 million. Using social engineering, the attackers exploited human vulnerabilities in a multifaceted manner. Employees were manipulated to click on spam messages, a seemingly innocuous action that set off a chain of peril.

The attack was conducted by embedding a deceptively innocent link within an email. The recipients downloaded a seemingly innocuous Google document, containing an executable PowerShell script. Bazaarloader Trojan, a malicious piece of software, was introduced to the system via this script once it was executed.

Using this newly gained foothold, the attackers installed the Bazaar backdoor software via the Trojan. Through this backdoor, Bloodhound software was able to identify valuable target accounts and identify them. Using this information, the attackers manipulated Cobalt Strike to pivot between accounts, allowing Ryuk ransomware to spread rapidly.

The attackers also leveraged Mimikatz, a powerful tool that harvests and exploits authentication credentials, to extend their authority. They searched for stored passwords in the system's memory, gained access to privileged accounts and escalated their privileges, and spread Ryuk ransomware relentlessly. As a result, a large number of files were encrypted with the RUYK extension, rendering them unusable for the rightful owners.

In an unsettling ending, employees discovered their files were now locked. It was only possible to regain access by paying the attackers' ransom demands. This incident highlights the need for cybersecurity vigilance, employee education, and robust digital defense mechanisms to defend against disruptive cyberattacks.

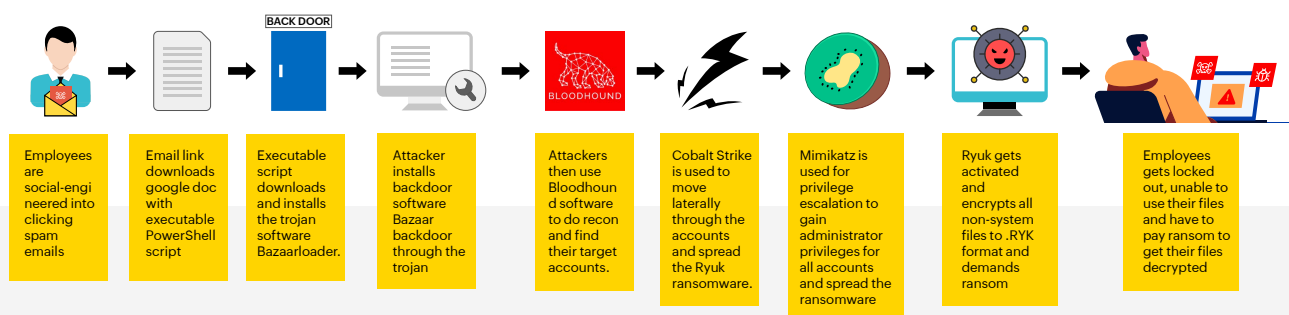


Figure 2: UHS RYUK attack steps

How to audit privilege escalation attacks using the native tool

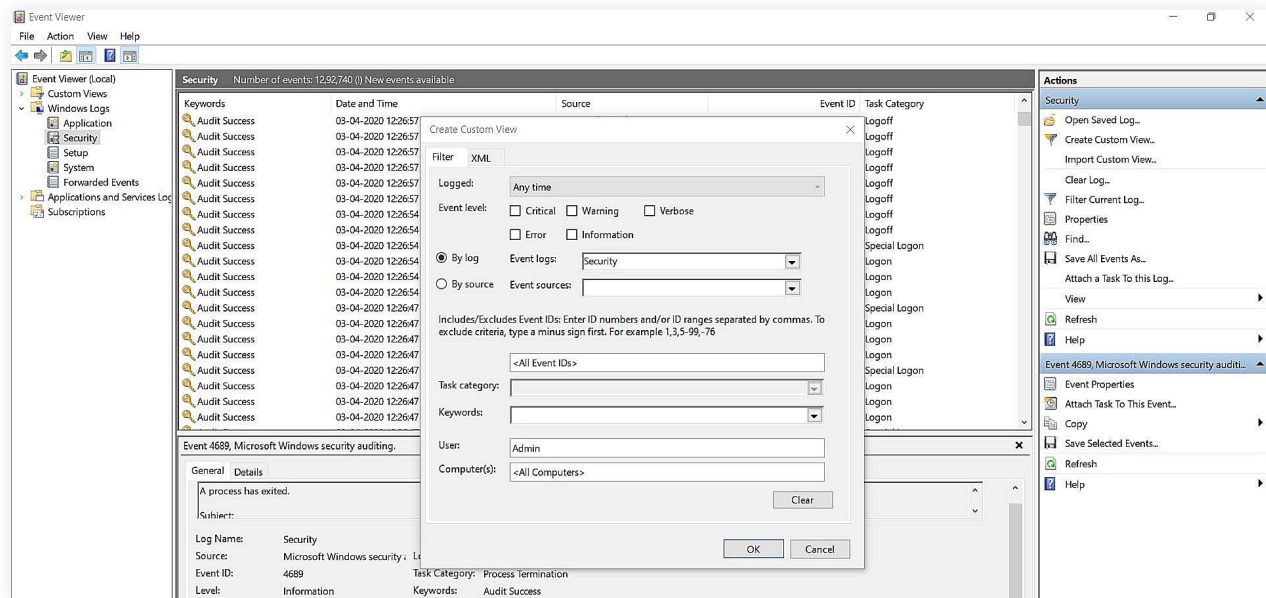


Figure 3: Windows Event Viewer

The use of a native tool can provide insights into privilege escalation attempts and identify potential vulnerabilities.

Windows Event Viewer provides a centralized location for viewing logs from a variety of sources, including security events. Privilege escalation attacks and attempts can be identified by tracking the following event IDs.

Important events to track using Event Viewer to detect privilege escalation attacks

Event ID	Description	How does it help?
4672	Special privileges assigned to new logon.	Collecting this log helps track instances of users logging in with special privileges, such as administrator accounts. It helps identify unusual or unauthorized administrative access, which could indicate privilege abuse or unauthorized system changes.
4673	A specified user has exercised the user right specified in the Privileges field	This log records attempts to call privileged services, providing insights into processes that might be trying to perform actions beyond regular user capabilities. Monitoring these logs can help identify potentially malicious processes attempting to exploit privileges.
4674	An operation was attempted on a privileged object.	This log records attempts to perform operations on privileged objects, which could include critical system files or sensitive resources. Collecting these logs helps detect unauthorized attempts to access or modify critical assets.
1102	The audit log was cleared.	This log indicates when the security audit log itself is cleared or tampered with. Monitoring this event is crucial for identifying potential cover-up attempts by attackers trying to erase their tracks.
4728	A user was added to a privileged global group.	Collecting this log helps in tracking changes to security groups, which could be indicative of privilege escalation. It aids in identifying unauthorized modifications to group memberships.
4732	A user was added to a privileged local group.	This event signifies the addition of a member (which could be a user or a group) to a security-enabled local group. It provides insight into changes made to group memberships, potentially affecting access to local resources and permissions.
4756	A user was added to a privileged universal group.	This log captures additions to universal security groups. Universal groups often have broader permissions, so tracking changes helps in identifying potential privilege abuse or unauthorized access.
4719	System audit policy was changed.	Collecting this log helps in tracking modifications to the system's audit policy. Unauthorized changes to audit settings could indicate attempts to cover up malicious activities.

4648	A logon was attempted using explicit credentials.	This log records logon attempts using explicit credentials, which could be indicative of attackers trying to bypass regular authentication methods. Monitoring this event helps in detecting unauthorized access attempts.
4735	A security-enabled local group was changed.	This log focuses on changes specifically in security-enabled global groups. Tracking these changes helps in identifying potential privilege escalation or unauthorized changes.
4740	A user account was locked out.	Collecting this log aids in tracking repeated failed login attempts. This event can indicate brute-force attacks or unauthorized access attempts, providing insights into potential ongoing attacks.
4663	An attempt was made to access an object.	This log records attempts to access objects like files, folders, or resources. Monitoring these logs helps in identifying unauthorized attempts to access sensitive data or systems.
4698	A scheduled task was created	This log records instances when a scheduled task is created on the system. Collecting these logs is important for monitoring the creation of tasks that might be used for malicious purposes, such as executing unauthorized scripts or programs, and helps in identifying potential security risks or ongoing attacks involving task scheduling.
4624 and 4625	An account was either successfully logged into, or a login attempt was made but it failed.	These log records successful logon events and failed login attempts. Collecting these logs is crucial for detecting unauthorized access attempts, password guessing, or brute-force attacks. Collecting these logs is essential for tracking legitimate user activity, as well as for identifying unusual logon patterns that might indicate unauthorized access or potential security breaches within the network.

Why is it challenging to detect privilege escalation attacks using native logs?

There are several inherent limitations to detecting privilege escalation attacks through native logs. Having no contextual information in these logs presents a major challenge. This makes it difficult to determine the true reason behind recorded actions. It can be difficult to differentiate legitimate activities from potential abuses without a thorough understanding of the circumstances.

Furthermore, native logs are limited in detail, and significant gaps in the data often exist. As a result, crucial events are left undocumented and comprehensive investigations cannot be conducted.

In addition, malicious actors have mastered the art of evasion, utilizing covert techniques to sidestep detection mechanisms. Conventional native log analysis cannot detect these techniques, which are hidden within the intricate web of log data. This necessitates the use of advanced detection methods.

How to audit privilege escalation attacks with ADAudit Plus

ManageEngine ADAudit Plus helps protect against privilege escalation attacks. It provides extensive monitoring and analysis of privileged activities within an organization's IT environment.

This real-time AD change notification, security and compliance auditing solution monitors user behavior, promptly detecting unauthorized actions and escalation attempts. Alerts and reports enable admins to respond swiftly to suspected activities, preventing privilege escalation before it occurs.

ADAudit Plus' capabilities for detecting anomalies play a vital role in preventing privilege escalation threats. This solution sets a baseline of normal user behavior and detects deviations from it which assists in preventing privilege escalation attacks by detecting unauthorized access attempts early.

Real-time change auditing

ADAudit Plus' real-time change auditing feature identifies suspicious activities indicative of privilege escalation attacks by monitoring and tracking changes made to user accounts, permissions, and system configurations. IT admins are notified instantly when user behavior patterns deviate from established patterns, such as sudden permission elevations or unauthorized role changes. In this way, the IT team can rapidly respond and mitigate threats.

Comprehensive audit trail:

AD Audit Plus generates an audit trail for every modification made in AD. This includes changes to user accounts, group memberships, permissions, and system settings. This data provides a comprehensive historical record of events, facilitating post-incident analysis and forensic investigation. By analyzing the sequence of events that lead up to privileged escalation attempts, security teams can identify the source of the attack and its impact.

USER NAME	CALLER USER NAME	DOMAIN CONTROLLER	MODIFIED TIME	REMARKS	EVENT CODE	CALLER USER DOMAIN	DOMAIN	EVENT NUMBER	USER DISPLAY NAME	DESCRIPTION
user99	admanager	admandemo.admanagerplus.com	Apr 04,2020 06:26:47 AM	A user account was unlocked.	8	ADMANAGERPLUS	ADMANAGERPLUS	4767	-	User account 'user99' was unlocked by 'ADMANAGERPLUS\admanager'.
user99	admanager	admandemo.admanagerplus.com	Apr 04,2020 06:26:47 AM	A user account was changed.	8	ADMANAGERPLUS	ADMANAGERPLUS	4738	-	User account 'user99' was changed by 'ADMANAGERPLUS\admanager'. Changed Attributes : 'User Account Control'
user99	admanager	admandemo.admanagerplus.com	Apr 04,2020 06:26:47 AM	A user account was changed.	8	ADMANAGERPLUS	ADMANAGERPLUS	4738	-	User account 'user99' was changed by 'ADMANAGERPLUS\admanager'. Changed Attributes : 'Display Name'

Figure 4: ADAudit Plus' audit trail

Threshold-based alerts:

AD Audit Plus enables IT admins to configure thresholds and policies according to the organization's security needs. It allows tailoring alert criteria according to the risk tolerance and compliance requirements of the organization. Admins can receive alerts when activities deviate from established norms by setting thresholds for changes and access attempts.

Name

Threshold based alerts - Logons

Description

Severity

☐ Attention
 ☒ Trouble
 ☐ Critical

Category

All GPO Printer

Report Profiles

Locked out Users

+

x

Alert Message

%ACCOUNT_NAME% has been locked out

[Add]

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Advanced Configuration

☒ Threshold Based Alerts

No of events

10

/occurring within

5

(mins) and has the same

Event Type

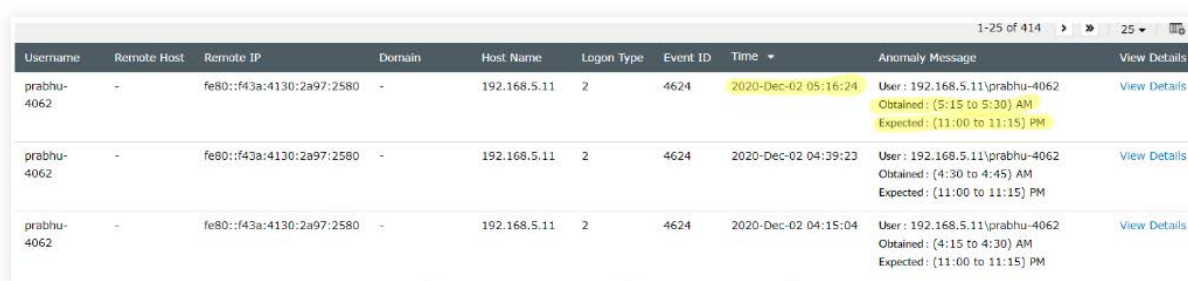
Figure 5: Threshold based Alert profile creation

Spot behavioral anomalies with UBA

AD Audit Plus' user behavior analytics (UBA) capability detects anomalies and patterns that indicate malicious intent or unauthorized access attempts. This system establishes a baseline of typical user behavior, including access patterns, activity frequencies, and resource interactions. Deviations from this norm are promptly identified, triggering alerts for suspicious activities, including privileged escalation attempts. UBA immediately recognizes abnormal behavior, such as a user account attempting to escalate privileges by modifying user roles or accessing sensitive systems.

AD Audit Plus' UBA can identify anomalous user behavior based on time, count, and abnormal patterns.

Time-based: Time-based anomaly detection identifies privilege escalation attacks by analyzing user behavior over time. If a user suddenly exhibits unusual actions, such as accessing privileged resources or escalating privileges outside their routine, the system triggers an alert.



Username	Remote Host	Remote IP	Domain	Host Name	Login Type	Event ID	Time	Anomaly Message	View Details
prabhu-4062	-	fe80::f43a:4130:2a97:2580	-	192.168.5.11	2	4624	2020-Dec-02 05:16:24	User: 192.168.5.11\prabhu-4062 Obtained: (5:15 to 5:30) AM Expected: (11:00 to 11:15) PM	View Details
prabhu-4062	-	fe80::f43a:4130:2a97:2580	-	192.168.5.11	2	4624	2020-Dec-02 04:39:23	User: 192.168.5.11\prabhu-4062 Obtained: (4:30 to 4:45) AM Expected: (11:00 to 11:15) PM	View Details
prabhu-4062	-	fe80::f43a:4130:2a97:2580	-	192.168.5.11	2	4624	2020-Dec-02 04:15:04	User: 192.168.5.11\prabhu-4062 Obtained: (4:15 to 4:30) AM Expected: (11:00 to 11:15) PM	View Details

Figure 6: Time-based anomalies for windows login

Pattern-based: With AD Audit Plus' UBA, privilege escalation attacks can be detected using a pattern-based anomaly detection approach. Sequences of events are analyzed to identify unexpected sequences where individual events appear normal but together deviate from expected patterns. This method helps uncover privilege escalation attempts that might not stand out in isolation.



Host Name	Object Name	Service Name	Vendor Name	Time	Anomaly Message	Report Name	View Details
192.168.6.1	-	Oracle VM VirtualBox 5.2.2	Oracle Corporation	2020-Jul-15 16:19:33	Pattern: HOSTNAME->USERNAME->TIME Obtained: 192.168.6.1->[ueba_user1] Expected: [ueba_user2]	Software Installed	View Details
192.168.5.1	-	Oracle VM VirtualBox 5.2.2	Oracle Corporation	2020-Jul-15 16:19:29	Pattern: HOSTNAME->USERNAME->TIME Obtained: 192.168.5.1->[ueba_user2] Expected: [ueba_user1]	Software Installed	View Details
192.168.6.1	-	Oracle VM VirtualBox 5.2.2	Oracle Corporation	2020-Jul-15 16:19:29	Pattern: HOSTNAME->USERNAME->TIME Obtained: 192.168.6.1->[ueba_user1] Expected: [ueba_user2]	Software Installed	View Details
192.168.5.1	-	Oracle VM VirtualBox 5.2.2	Oracle Corporation	2020-Jul-15 16:19:29	Pattern: HOSTNAME->USERNAME->TIME Obtained: 192.168.5.1->[ueba_user2] Expected: [ueba_user1]	Software Uninstalled	View Details

Figure 7: Pattern-based anomaly for software installation

Count-based: ADAudit Plus' UBA uses count-based anomaly detection to identify privilege escalation attacks. It raises an alert if a user's activity suddenly exhibits an unusually high frequency or magnitude of privilege-related actions, such as accessing sensitive resources or elevating permissions.

Host Name	Username	Domain	Object Name	File Type	Process Name	Time	Anomaly Message	View Details
192.168.6.1	ueba_user2	-	System32	-	C:\Windows\System32\mmc.exe	2020-Jul-15 16:28:59	User : 192.168.6.1\ueba_user2 Obtained : 399 events Threshold : 73 events	View Details
192.168.5.1	ueba_user1	-	System32	-	C:\Windows\System32\mmc.exe	2020-Jul-15 16:28:59	User : 192.168.5.1\ueba_user1 Obtained : 395 events Threshold : 73 events	View Details
192.168.5.1	ueba_user1	-	C:\Windows\System32\eventvwr.msc	-	C:\Windows\System32\mmc.exe	2020-Jul-15 10:28:59	User : 192.168.5.1\ueba_user1 Obtained : 200 events Threshold : 40 events	View Details
192.168.6.1	ueba_user2	-	System32	-	C:\Windows\System32\mmc.exe	2020-Jul-15 10:28:58	User : 192.168.6.1\ueba_user2 Obtained : 199 events Threshold : 41 events	View Details

Figure 8: Count-based anomaly for file modifications

ADAudit Plus provides various reports to monitor these anomalies. Reports such as user logon activity, unusual lockout activity time, unusual volume of file activity, and new process on the server help IT admins detect potential security breaches.

Real-time alerts on suspicious activities

Admins are promptly notified on suspicious activities conducted by privileged users. This includes access to sensitive files, modifications to privileged accounts, and configuration changes. An alert is triggered when suspicious behavior is detected.

ADAudit Plus' real-time alerts for privileged user management provide:

Immediate detection: ADAudit Plus continuously monitors user activities, and enables admins to detect suspicious actions in real-time. This ensures that any unauthorized or unexpected actions by privileged users are identified promptly, reducing the window of opportunity for potential security breaches.

Granular monitoring: The real-time alerts feature provides granular monitoring of privileged user activities. It tracks actions such as system configuration changes, file access, permission modifications, and user account manipulations. This level of detail helps admins pinpoint exactly what activity raised suspicion, aiding in rapid response and investigation.

Alert Profiles

Domain

admanagerplus.com

+ New Alert Profile

1-25 of 64

25

Add/Remove Columns

NAME	CREATED ON	LAST MODIFIED ON	TICKETING	ALERTS	E-MAIL	BUSINESS HOUR	SEVERITY
Certificate Authority security or permission settings	Jun 20,2023 06:57:10 AM	Jun 20,2023 06:57:10 AM	Configure	View Alerts	Configure	No	Attention
Certificate template modified	Jun 20,2023 06:57:10 AM	Jun 20,2023 06:57:10 AM	Configure	View Alerts	Configure	No	Attention
Certificate Service audit filter	Jun 20,2023 06:57:10 AM	Jun 20,2023 06:57:10 AM	Configure	View Alerts	Configure	No	Attention
AdminSDHolder Permission Changes	Aug 19,2022 01:01:10 PM	Aug 19,2022 01:01:10 PM	Configure	View Alerts	Configure	No	Trouble
Unable to log Security log events for admanagerplus.com	Aug 19,2022 01:01:10 PM	Aug 19,2022 01:01:10 PM	Configure	View Alerts	Configure	No	Critical
Possible Ransomware activity detected at admanagerplus.com	Aug 19,2022 01:01:10 PM	Aug 19,2022 01:01:10 PM	Configure	View Alerts	Configure	No	Critical
AzureAD Password Modification in Audit-Only mode	Apr 22,2020 08:47:04 AM	Apr 22,2020 08:47:04 AM	Configure	View Alerts	Configure	No	Attention
LDAP Authentication	Apr 22,2020 08:47:04 AM	Apr 22,2020 08:47:04 AM	Configure	View Alerts	Configure	No	Attention
AzureAD Password Modification Failed	Apr 22,2020 08:47:04 AM	Apr 22,2020 08:47:04 AM	Configure	View Alerts	Configure	No	Attention
Disabled Users Enabled	Jan 10,2020 01:42:47 PM	Jan 10,2020 01:42:47 PM	Configure	View Alerts	Configure	No	Attention
Password Never Expire Enabled	Jan 10,2020 01:42:47 PM	Jan 10,2020 01:42:47 PM	Configure	View Alerts	Configure	No	Attention

Figure 9: Real-time alert profiles

Customized alerts: ADAudit Plus enables admins to define customized alerts based on specific criteria. For example, if a privileged user attempts to access sensitive data outside of business hours, or makes multiple failed login attempts, the system triggers an alert. This customization ensures that alerts are relevant and tailored to the organization's security policies.

Name

Non-Business hour changes on Files

Description

Severity

☒ Attention
 ☐ Trouble
 ☐ Critical

Category

☒ All
 ☐ GPO
 ☐ Printer

Report Profiles

File Modify

+

×

Alert Message

%ACCOUNT_NAME% has updated a file after business hours
 [\[Add\]](#)

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Advanced Configuration

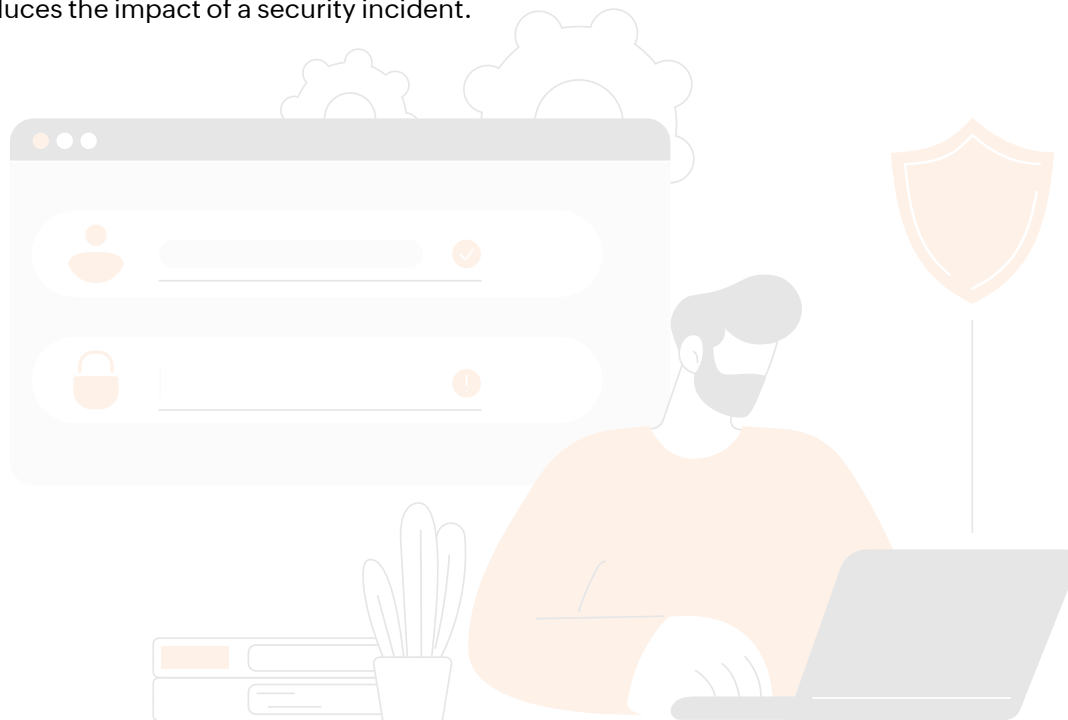
☐ Threshold Based Alerts

☒ Business Hour Alert

☐ Business Hours
 ☒ Non Business Hours

Figure 10: Custom alert profile creation

Automated responses: In addition to alerts, ADAudit Plus enables automated responses to certain triggers. For instance, if an alert indicates a suspicious change in system configuration, the system automatically reverts to a previously known state. This proactive approach minimizes potential damage and reduces the impact of a security incident.



Our Products

AD360 | Log360 | ADManager Plus | ADSelfService Plus | DataSecurity Plus | M365 Manager Plus

ManageEngine ADAudit Plus

ADAudit Plus is a UBA-driven auditor that helps keep your AD, Azure AD, file systems (including Windows, NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx for Windows, and QNAP), Windows servers, and workstations secure and compliant. ADAudit Plus transforms raw and noisy event log data into real-time reports and alerts, enabling you to get full visibility into activities happening across your Windows Server ecosystem in just a few clicks. For more information about ADAudit Plus, visit manageengine.com/active-directory-audit.

\$ Get Quote

⬇ Download