INTERMEDIATE READ **1 min** Actionable advice coming up next.

What Is Privilege Escalation?

Definition, Types and Examples

LAST UPDATED ON **NOVEMBER 3, 2022**

ANDRA ANDRIOAIE (https://heimdalsecurity.com/blog/author/andra-andrioaie/) SECURITY ENTHUSIAST

in (http://www.linkedin.com/in/andra-andrioaie-627b1016b)

Privilege escalation might be a confusing cybersecurity term for many. That's why in this article we're going to shed a little bit more light on this topic. Keep reading to find out more about what is privilege escalation, how many types of privilege escalation exist, examples of privilege escalation attacks on Windows and Linux, and also what are the best practices to prevent it.

What Is Privilege Escalation?

Privilege escalation in cybersecurity is a malicious attempt to abuse an app or OS bug or error of configuration in order to gain unauthorized access to sensitive information. This happens by taking over a user's account that has the necessary privileges to view or make changes to confidential information that wouldn't normally be accessible to the current user.

By obtaining these types of rights, a malicious actor can perform a series of actions to the operating system or to the server such as running different commands or facilitating the infiltration of malware within the network, that could further lead to:

- business disruption,
- exposure of sensitive data, or system resources,
- and complete system takeover.

GO TO TOP

So shortly, this can be employed through misuse of privileges.

How Privilege Escalation Works

To perform a privilege escalation attack, a threat actor should first infiltrate the targeted network. This is usually done through abusing vulnerabilities in the system or through **social engineering (https://heimdalsecurity.com/blog/what-is-social-engineering/)** techniques for instance. This can also go both ways: either hackers find a **privileged account (https://heimdalsecurity.com/blog/superuser-accounts/)** from the beginning and perform a privilege escalation attack, or they gain access to a standard account in the initial phase. In the second scenario, they can perform surveillance on the network until it's time for the next move – gaining access to a privileged account – an account with special rights beyond those of a standard user, with access to critical data and infrastructure within an organization.

Types of Privilege Escalation

Privilege escalation can be split into two types: vertical privilege escalation and horizontal privilege escalation. In VPE (vertical privilege escalation), the attacker aims at taking over an account that has higher privileges. On the other hand, in HPE (horizontal privilege escalation) the hacker will first take over an account and then try to gain system-level rights. Both types of operations are achieved by taking advantage of existing operating system vulnerabilities.

Vertical Privilege Escalation

Vertical privilege escalation, also known as privilege elevation, is a term used in cybersecurity that refers to an attack that starts from a point of lower privilege, then escalates privileges until it reaches the level of the user or process it targets.

This type of attack takes advantage of the fact that most systems and networks are designed so that users at one privilege level can access resources at higher levels. For example, a system administrator may have access to resources normally reserved for kernel-level users, but may not have passwords for those resources. The attacker achieves this escalation by first gaining root-level access and then using those privileges to compromise other accounts with lesser access.

In vertical privilege escalation, you're dealing with the 'accountphage' type of behavior. Basically, the hacker chews the user out of his or her account.

A hacker can perform sensitive data and credentials theft, even downloading ransomware payloads and deploying them into the system, deleting files, or executing different code commands. The attacker can even leave without being noticed. How? Simply, they delete traces like access logs, nobody will even know they have been there, delaying thus the discovery of a **data breach (https://heimdalsecurity.com/blog/data-**

GO TO TOP

breach/), leading to harder recovery or more time for him to get whatever he wants related to that business.

VERTICAL PRIVILEGE ESCALATION EXAMPLE

Let's say that user A, who's working for company XYZ, has been given access to a financial database. Because user A is a finance officer, he's been cleared to perform a set of company-defined operations on the financial database (e.g., read, write, open, but not delete). Fellow B, who's in no way affiliated with XYZ, wishes to tap into the company's financial database for whatever malicious reason. Using various TTPs, B successfully takes over user A's account and gains access to the database. This is a great example of a vertical privilege escalation.

Horizontal Privilege Escalation

Horizontal privilege escalation means that a user will achieve access permissions belonging to another user that owns the same access level as the user that has started the cyberattack. Horizontal privilege escalations are a bit more challenging compared to vertical ones since they require a deep understanding of how operating systems work.

In VPE, you don't need to elevate rights (i.e. obtain the credentials necessary to access another informational class) because the account you're about to take over has all the credentials necessary to access that particularly sensitive area. In HPE, you will need to take over and, at the same time, elevate those privileges. No doubt some 'Mission Impossible' right there, but very doable if a hacker has the right tools. In most case HEP cases, the attacker would rely on **phishing (https://heimdalsecurity.com/blog/phishing-attack/)** or **spearphishing (https://heimdalsecurity.com/blog/what-is-spear-phishing/)** to infiltrate the victim's machine and hacking tools such as Metasploit to gain SYSTEM-level (root) access. And that's where the fun begins.

Privilege Escalation Risks

Privilege escalation is one of the most dangerous types of attacks in cybersecurity because it grants attackers access to everything in an organization's IT infrastructure.

It lets your sensitive data fall in the wrong hands

A major risk associated with privilege escalation is that it might mean that a malicious hacker has achieved access to sensitive and confidential data they shouldn't have access to.

GO TO TOP

It can be the path to other cyberattacks

Even if a privilege escalation attack itself poses a risk to your organization’s infrastructure’s security, it can be the path to other cyberattacks through which threat actors can deploy a malicious payload in the system that is targeted. So, whenever privilege escalation is detected, you should look further into the problem to see if it doesn’t go deeper into the organization’s system by searching for indicators of malicious activity.

Privilege Escalation Attack Examples

I’ve described above how generally privilege escalation works. Now, let’s illustrate a more practical part of this topic. Let’s see some privilege escalation attack examples depending on the operating system. In the following lines, I am going to give you examples of Windows privilege escalation attacks and also examples of Linux privilege escalation attacks. These examples come along with recommended mitigation measures.

Windows Privilege Escalation

Windows Privilege escalation can be achieved in many ways. Let’s see 3 examples of windows privilege escalation attacks and what you can do about them.

WINDOWS STICKY-KEY ATTACK

The so-to-say “beauty” of this kind of privilege escalation attack lies in its simplicity. A hacker doesn’t really need that computer native to carry it out. Here’s the gig: using the ‘enable sticky keys feature’ the threat actor can bypass normal endpoint auth and gain system-level privileges. Sounds crazy, but it really works. From here, he can create a (fake) admin account, install a secret backdoor, and much more.

Windows Sticky Key Attack Mitigation Measure: prevent the launch of sticky keys. Go to HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys\Flags in your Windows registry and change the value from “510” to “510”. This will add encryption protection to your Windows partition.

CREDENTIAL DUMPING (PURLOINING STORED CREDENTIALS)

Credential dumping is a great way of recovering (**hashed (https://heimdalsecurity.com/blog/what-is-hashing/)**) credentials from key system locations. Compared to the sticky-key attack, credential dumping is a bit more challenging since it requires tools, time, and, of course, the nose of a bloodhound. So, how does this work? Well, all machines running Windows cache login credentials are in various locations. Basically, if you know where to look, you can easily pull out stuff like admin login passwords, master passwords for local passphrase vaults, and so on.

GO TO TOP

The hacker still needs to figure out a way to 'unhash' those passwords. Think of it this way – credential dumping is like searching every trash can in your city, hoping that you come across a piece of paper that holds the key code to the warehouse housing your dream PC or something.

Credential Dumping Attack Mitigation Measure: increase password complexity, enable PPL (Protect Process Light) for LSA, check Domain controller backups, restrictor disable NTLM, and add a user to the Protected Users list in your Access Directory.

ACCESS TOKEN MANIPULATION

Through token manipulation, an attacker can perform 3 types of privilege escalation techniques, as Red Team Notes specified in their **article (https://dmcxblue.gitbook.io/red-team-notes/privesc/access-token-manipulation)**: token theft, this method involves the creation of a new access token for the purpose of **impersonating (https://heimdalsecurity.com/blog/online-impersonation/)** a legitimate token, generating process via token creation, where the threat actor creates a token and uses it to force-run a process on the victim's machine. This process will operate under a legit security context, one associated with a legit user and also the make&bake technique where once the legit user logs off, the threat actor will invoke a new logon session (usually using the LogonUser command in a CMD window). The function will then pass the threat actor a copy of the session's token. Finally, this newly-obtained token can be tied to a thread.

Access Token Manipulation Prevention Measure: Bar user groups or users from creating tokens. Enforce the **least-privilege principle (https://heimdalsecurity.com/blog/what-is-the-principle-of-least-privilege-polp/)** and police admin accounts.

NTLM RELAY OR HOT-TATER ATTACK

The Hot-tater attack is a highly sophisticated attack that involves exploiting vulnerabilities found in the NTML relay and the local NBNS Spoofer. The scope is to obtain NT AUTHORITY\SYSTEM privileges on the victim's machine. 'Hot-tatting' a target is a triphasic process: interrogating the NBNS spoofer, requesting a fake WPAD proxy server, and MITMing the NTLM protocol. The result: the threat actor persuades the victim's machine to authenticate via the NTML protocol. The auth process's details are sent to the attacker who, by this time, would have gained system-level privileges.

Hot-Tater Attack Prevention Measure: Enable **SMB Signing (https://hedgehogsecurity.co.uk/blog/2019/01/19/fixing-smb-signing-not-required/)** (however, not yet proven).

GO TO TOP

Linux Privilege Escalation

When talking about Linux privilege escalation, a process dubbed “enumeration” is used by hackers. This will help them detect vulnerabilities that will further permit the unfolding of a privileged escalation attack. For this, a series of automated tools are employed. Threat actors get more knowledge about the system through port scanning, Google searches, or direct interaction or they might look for available Perl or Phython, which are basically two high-level programming languages that will permit them to deploy an exploit code into the system.

There are two techniques associated with Linux privilege escalation: kernel exploit and SUDO rights exploitation.

KERNEL EXPLOIT

A kernel exploit attack is possible if there are flaws in the Linux kernel that let the hacker abuse them in order to achieve **Linux (https://heimdalsecurity.com/blog/linux-patch-management/)** root system access.

Kernel Exploit Mitigation Measure: According to **MITRE ATT&CK (https://attack.mitre.org/techniques/T1068/)**, in this case, **Linux (https://heimdalsecurity.com/blog/linux-patch-management-challenges/)** updates and patches should be installed in a timely manner. Files such as FTP, SCP or curl that permit file transfer actions should be restricted or removed or they should be simply associated with just a handful of users or IPs, to prevent an exploit infiltration.

SUDO RIGHTS EXPLOITATION

What is SUDO? It stands basically for a Linux program that will give different users the ability to run programs by means of privileged rights that belong to somebody else who will grant them access to do so. The risk of command execution with root privileges would be the consequence in this case.

SUDO Right Exploitation Mitigation Measure: According to **MITRE ATT&CK (https://attack.mitre.org/techniques/T1548/003/)**, compilers, interpreters, or editors should never be granted rights that allow access to programming language compiler, and neither different programs that facilitate a shell running action should not have these kinds of special rights.

Wrapping Up…

Data breaches caused by credential privilege escalation can lead to serious problems in a system and network applications. Although protecting a system against cyberattacks and ever-increasing privilege escalation efforts becomes exceedingly challenging, Privileged Access Management (PAM) security mechanisms designed to prevent both internal and external threats offer a significant advantage when it comes to end-to-end data and access protection.

GO TO TOP

How Can Heimdal® Help?

Our **Privileged Access Management (https://heimdalsecurity.com/enterprise-security/products/privileged-access-management?partner=Blog)** solution stands out through the following characteristics:

When used together with our **Nex-Gen Antivirus (https://heimdalsecurity.com/enterprise-security/products/endpoint-antivirus?partner=Blog)**, it becomes the only software that automatically de-escalates user rights, should any threats be detected on the machine.

A very efficient approval/denial flow;

Flexibility: wherever you are now, with our PAM you can either escalate or deescalate user rights;

Settings in terms of AD group rights, escalation period customization, local admin rights removal, session tracking, system files elevation blocking, and many more characterize our product;

Stunning graphics with details like hostname, the average escalation duration will support your audit strategy, making you able to prove NIST AC-5 and NIST AC-1,6 compliance and build a trustworthy relationship with your partners.

Combine it also with our **Application Control (https://heimdalsecurity.com/enterprise-security/products/application-control?partner=Blog)** module, which lets you perform application execution approval or denial or live session customization to further ensure business safety. Need I say more?

Managing privileges is a fundamental aspect of any cybersecurity strategy. Make sure you have the proper PAM tool and be a step ahead of hackers!

GO TO TOP

Feel free to drop a comment below if you's want to add anything. Also, don't forget to follow us on **LinkedIn (https://www.linkedin.com/company/heimdal-security/)**, **Twitter (https://twitter.com/HeimdalSecurity?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor)**, **Facebook (https://www.facebook.com/HeimdalSec/)**, **Youtube (https://www.youtube.com/c/Heimdalsecuritycompany)**, or **Instagram (https://www.instagram.com/heimdalsecurity/?hl=en)** to keep up to date with everything we post!

This article was written in collaboration with my colleague, **Vladimir Unterfingher (https://heimdalsecurity.com/blog/author/vladimir/)**.

RELATED

What Is the Principle of Least Privilege (POLP)? (https://heimdalsecurity.com/blog/what-is-the-principle-of-least-privilege-polp/)

Just-in-Time Access Explained. What It Means, Benefits and Best Practices of JIT (https://heimdalsecurity.com/blog/what-is-just-in-time-access-jit/)

What Is Privileged Access Management (PAM)? (https://heimdalsecurity.com/blog/privileged-access-management-pam/)

What Is Privileged Account and Session Management (PASM)? (https://heimdalsecurity.com/blog/privileged-account-and-session-management-pasm/)

What Is Endpoint Privilege Management? (https://heimdalsecurity.com/blog/what-is-endpoint-privilege-management/)

Comments

Melih ON DECEMBER 5, 2022 AT 8:53 PM **(https://heimdalsecurity.com/blog/privilege-escalation/#comment-693498)**

This is just a feedback. I guess the part below has a minor mistake.

Windows Sticky Key Attack Mitigation Measure: prevent the launch of sticky keys. Go to HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys\Flags in your Windows registry and change the value from "510" to "510". This will add encryption protection to your Windows partition.

Reply

GO TO TOP

Leave a Reply

Your email address will not be published. Required fields are marked *

COMMENT: *

NAME: *

EMAIL: *

□ SAVE MY NAME, EMAIL, AND WEBSITE IN THIS BROWSER FOR THE NEXT TIME I COMMENT.

POST COMMENT

SECURITY PRODUCTS FOR HOME USERS

FREE SOFTWARE UPDATER (HTTPS://HEIMDALSECURITY.COM/PRODUCTS/FREE-SOFTWARE-UPDATER)

THREAT PREVENTION SOFTWARE (HTTPS://HEIMDALSECURITY.COM/PRODUCTS/THREAT-PREVENTION-SOFTWARE)

ANTIVIRUS SOFTWARE (HTTPS://HEIMDALSECURITY.COM/PRODUCTS/ANTIVIRUS-SOFTWARE)

PREMIUM SECURITY SUITE (HTTPS://HEIMDALSECURITY.COM/PRODUCTS/PREMIUM-SECURITY-SUITE)

SECURITY PRODUCTS FOR BUSINESSES

THREAT PREVENTION ENDPOINT (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/THREAT-PREVENTION)

PAM SOFTWARE (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/PRIVILEGED-ACCESS-MANAGEMENT)

APPLICATION CONTROL (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/APPLICATION-CONTROL)

PATCH MANAGEMENT SOFTWARE (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/PATCH-MANAGEMENT-SOFTWARE)

EMAIL FRAUD PREVENTION (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/EMAIL-FRAUD-PROTECTION)

EMAIL SECURITY (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/EMAIL-SECURITY)

ENDPOINT ANTIVIRUS (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/ENDPOINT-ANTIVIRUS)

RANSOMWARE ENCRYPTION PROTECTION (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/RANSOMWARE-ENCRYPTION-PROTECTION)

REMOTE DESKTOP SOFTWARE (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/PRODUCTS/REMOTE-DESKTOP)

GO TO TOP

EDR SOFTWARE (HTTPS://HEIMDALSECURITY.COM/ENTERPRISE-SECURITY/ENDPOINT-DETECTION-AND-RESPONSE-EDR-SOFTWARE)

FREE SECURITY RESOURCES

CYBER SECURITY COURSE FOR BEGINNERS (HTTP://CYBERSECURITYCOURSE.CO/)

INTERMEDIATE READ **1 min** Actionable advice coming up next.

THE ULTIMATE WINDOWS 10 SECURITY GUIDE (HTTPS://HEIMDALSECURITY.COM/WINDOWS-10-SECURITY-GUIDE)

CYBER SECURITY GLOSSARY (HTTPS://HEIMDALSECURITY.COM/GLOSSARY)

THE DAILY SECURITY TIP (HTTPS://DAILYSECURITYTIPS.COM/)

CYBER SECURITY FOR SMALL BUSINESS OWNERS (HTTPS://LEARNINFOSEC.CO.UK/)

CYBERSECURITY WEBINARS (HTTPS://HEIMDALSECURITY.COM/WEBINARS)

COMPANY

ABOUT HEIMDAL (HTTPS://HEIMDALSECURITY.COM/ABOUT)

MEDIA CENTER (HTTPS://HEIMDALSECURITY.COM/MEDIA-CENTER)

WRITE FOR US (HTTPS://HEIMDALSECURITY.COM/BLOG/WRITE-FOR-US/)

RESELLER PROGRAM (HTTPS://HEIMDALSECURITY.COM/PARTNER-WITH-US)

AFFILIATE PROGRAM (HTTPS://HEIMDALSECURITY.COM/ONLINE-AFFILIATE-PROGRAM)