windows privilege escalation cheat sheet

windows privilege escalation cheat sheet is an essential resource for cybersecurity professionals, penetration testers, and system administrators looking to understand and mitigate privilege escalation vulnerabilities in Windows environments. This comprehensive guide covers various techniques, tools, and methods used to gain higher privileges on Windows systems, which is critical for both offensive security testing and defensive hardening. By exploring common misconfigurations, vulnerable services, and exploitable binaries, this cheat sheet equips users with the knowledge to identify privilege escalation paths effectively. The content is structured to provide clear explanations and actionable insights, ensuring practical application during security assessments. From enumeration strategies to exploitation techniques, this article delves into the core aspects of Windows privilege escalation, making it a vital reference for anyone involved in Windows security. Below is a detailed table of contents outlining the main topics covered in this windows privilege escalation cheat sheet.

Enumeration Techniques

Effective privilege escalation begins with thorough enumeration of the target Windows system. Identifying system configurations, user privileges, installed software, and running services is critical to uncover potential weaknesses. Enumeration provides the foundational knowledge required for selecting appropriate escalation methods.

User and Group Information

Gathering details about local users, groups, and their privileges helps determine accounts with elevated permissions or those that can be leveraged for privilege escalation. Commands such as *net user* and *net localgroup* provide this information.

System Configuration and Patch Level

Understanding the Windows version, build number, and installed patches assists in identifying known vulnerabilities applicable to the system. Tools like *systeminfo* and the registry can reveal detailed configuration data.

Service and Process Enumeration

Listing running services and processes can expose misconfigured or vulnerable services that run with high privileges. Commands like *sc query* and PowerShell cmdlets such as *Get-Service* are useful for this purpose.

Network and Firewall Settings

Analyzing network interfaces, firewall rules, and open ports can reveal communication channels that might be exploited. Utilities like *netstat* and *Get-NetFirewallRule* assist in this assessment.

- net user / net localgroup
- systeminfo
- sc query / Get-Service
- netstat / Get-NetFirewallRule

Common Privilege Escalation Vulnerabilities

Windows systems often suffer from misconfigurations and vulnerabilities that can be exploited to escalate privileges. Recognizing these common issues is fundamental to successful exploitation and remediation.

Unquoted Service Paths

Services with unquoted executable paths that include spaces can be exploited by placing malicious executables in specific directories. This vulnerability allows attackers to execute code with service-level privileges.

Weak Service Permissions

Improperly set permissions on services may permit standard users to modify service binaries or configurations, enabling privilege escalation through service manipulation.

AlwaysInstallElevated Policy

If the Windows Installer policy "AlwaysInstallElevated" is enabled, users can install MSI packages with elevated privileges, potentially allowing execution of arbitrary code with SYSTEM rights.

Auto-Logon Configuration

Systems configured for automatic logon may store credentials in the registry or in memory, which can be extracted to gain higher privileges.

- Unquoted service paths
- Weak permissions on services
- AlwaysInstallElevated enabled
- Auto-logon credential exposure

Exploiting Misconfigured Services

Misconfigured Windows services are a prevalent vector for privilege escalation. Exploiting these services involves identifying weaknesses in their configuration, permissions, or execution environments.

Modifying Service Binaries

If a user has write permissions to a service executable or its directory, replacing the binary with a

malicious payload can result in code execution with the service's privileges.

Changing Service Configuration

Altering the service's executable path or parameters, when permissions allow, can redirect execution to attacker-controlled binaries.

Starting or Stopping Services

Users with rights to start or stop services can leverage this ability to trigger malicious payloads or manipulate service behavior to elevate privileges.

- Check service permissions with tools like AccessChk
- Modify service binaries if write access exists
- Alter service executable paths
- Control service start/stop actions

Abusing Scheduled Tasks and Jobs

Scheduled tasks and background jobs running with elevated privileges can be abused to execute arbitrary code. Identifying and manipulating these tasks is a key privilege escalation tactic.

Enumerating Scheduled Tasks

Using commands like *schtasks /query /fo LIST /v* or PowerShell cmdlets such as *Get-ScheduledTask*, one can list scheduled tasks and analyze their triggers, actions, and privileges.

Modifying or Creating Tasks

With appropriate permissions, users can modify existing tasks or create new ones configured to run with elevated privileges, enabling privilege escalation.

Exploiting Weak Permissions

Tasks with weak ACLs allow modification by non-privileged users, which can be leveraged to execute malicious payloads at scheduled times.

- Use schtasks and Get-ScheduledTask for enumeration
- Check permissions on tasks
- Modify or create tasks with elevated privileges
- Deploy payloads via scheduled jobs

Leveraging DLL Hijacking

DLL hijacking is a technique where an attacker places a malicious DLL in a location where a privileged process loads it instead of the legitimate one. This leads to code execution with elevated rights.

Understanding DLL Search Order

Windows searches for DLLs in a specific order, including the application directory and system directories. If a DLL with the same name as a required one exists earlier in the search path and is attacker-controlled, it will be loaded.

Identifying Vulnerable Applications

Applications lacking full path specification for DLLs or loading DLLs dynamically may be susceptible. Tools like Process Monitor can help identify DLL loading behavior.

Deploying Malicious DLLs

Placing a malicious DLL in the targeted directory or manipulating environment variables can trick the system into loading the attacker's DLL, resulting in privilege escalation.

- Analyze DLL search order
- Identify vulnerable applications
- Place malicious DLLs strategically
- Use tools like Process Monitor for analysis

Token Manipulation and Impersonation

Windows access tokens represent security contexts for users and processes. Manipulating or

impersonating tokens can grant an attacker elevated privileges within the system.

Token Stealing

Attackers can duplicate tokens from high-privilege processes to impersonate those users. This requires appropriate permissions and is often done using specialized tools or scripts.

Token Impersonation

Processes can impersonate tokens to execute actions under different security contexts. Exploiting this allows elevated command execution or access to restricted resources.

Using Tools for Token Manipulation

Utilities like Mimikatz and PowerSploit provide capabilities to manipulate tokens, extract credentials, and perform impersonation, aiding in privilege escalation.

- Duplicate tokens from SYSTEM or Administrator processes
- Impersonate tokens to elevate privileges
- Leverage tools like Mimikatz for token operations
- Ensure appropriate permissions exist for token manipulation

Useful Tools and Commands

Several built-in Windows commands and third-party tools facilitate enumeration, exploitation, and verification during privilege escalation activities. Mastery of these utilities enhances assessment efficiency.

Built-in Windows Commands

Commands such as *whoami*, *icacls*, *sc*, and *schtasks* provide crucial information about user privileges, permissions, service configuration, and scheduled tasks.

Third-Party Tools

Tools like AccessChk, PowerUp, WinPEAS, and Mimikatz automate privilege escalation checks, uncover misconfigurations, and facilitate exploitation steps, making them indispensable for security professionals.

PowerShell Cmdlets

PowerShell offers extensive cmdlets for system interrogation and manipulation, such as *Get-Process*, *Get-Service*, and *Get-ScheduledTask*, supporting detailed analysis and exploitation workflows.

- whoami, icacls, sc, schtasks
- AccessChk for permission auditing
- PowerUp and WinPEAS for automated checks
- Mimikatz for credential and token manipulation

- PowerShell cmdlets for in-depth enumeration

Frequently Asked Questions

What is a Windows privilege escalation cheat sheet?

A Windows privilege escalation cheat sheet is a concise reference guide that lists common techniques, commands, and tools used to identify and exploit privilege escalation vulnerabilities on Windows systems.

Why is privilege escalation important in Windows security testing?

Privilege escalation allows an attacker or tester to gain higher-level permissions, such as administrative rights, which can lead to full system control. It is crucial in security testing to identify and mitigate these vulnerabilities before they are exploited maliciously.

What are some common methods listed in a Windows privilege escalation cheat sheet?

Common methods include exploiting misconfigured services, weak file or folder permissions, vulnerable scheduled tasks, unquoted service paths, insecure registry permissions, and leveraging token impersonation or bypassing User Account Control (UAC).

Which built-in Windows commands are useful for privilege escalation enumeration?

Commands such as "whoami /priv", "net user", "systeminfo", "tasklist /v", "sc qc <service>", "icacls", and PowerShell cmdlets like "Get-Process" and "Get-Service" are often used for enumeration during privilege escalation analysis.

How can a cheat sheet help during a penetration test on a Windows machine?

A cheat sheet provides a quick and organized reference to common privilege escalation vectors and commands, saving time and ensuring thoroughness during penetration tests by guiding testers through systematic enumeration and exploitation steps.

Are there any tools recommended in Windows privilege escalation cheat sheets?

Yes, commonly recommended tools include PowerUp, Sherlock, WinPEAS, SharpUp, and BloodHound, which automate the discovery of privilege escalation opportunities on Windows systems.

Additional Resources

1. *Windows Privilege Escalation Essentials*
This book provides a comprehensive guide to understanding and exploiting privilege escalation vulnerabilities in Windows environments. It covers various techniques attackers use to gain higher privileges and offers defensive strategies for system administrators. Readers will find practical examples and step-by-step instructions to master privilege escalation methods.

2. *Mastering Windows Security and Privilege Escalation*
Focusing on Windows security mechanisms, this book delves into how privilege escalation occurs and how to prevent it. It includes detailed explanations of Windows internals, common misconfigurations, and exploitation techniques. Security professionals will benefit from the real-world case studies and mitigation tactics presented.

3. *The Windows Hacker's Handbook: Privilege Escalation Techniques*
This handbook is designed for ethical hackers and penetration testers seeking to understand Windows privilege escalation. It explores a variety of escalation paths, including token manipulation, service

misconfigurations, and kernel exploits. The book emphasizes hands-on labs and cheat sheets to enhance learning and application.

4. *Windows Privilege Escalation Cheat Sheet: Techniques and Tools*
A practical, concise reference guide, this cheat sheet compiles the most effective Windows privilege escalation techniques and tools. It is ideal for quick consultations during penetration tests or security assessments. The book also highlights common pitfalls and how to avoid detection.

5. *Advanced Windows Exploitation and Privilege Escalation*
Targeted at advanced users, this book explores sophisticated exploitation methods to escalate privileges on Windows systems. It includes coverage of kernel vulnerabilities, exploit development, and bypassing security controls like UAC and Windows Defender. Readers gain insight into cutting-edge attack vectors and protection mechanisms.

6. *Practical Windows Privilege Escalation for Penetration Testers*
This guide offers practical techniques tailored for penetration testers who need to escalate privileges in Windows environments. It breaks down complex concepts into actionable steps and includes numerous scripts and tools to automate tasks. The book also discusses post-exploitation tactics and cleanup procedures.

7. *Windows Security: From Fundamentals to Privilege Escalation*
Starting with fundamental Windows security concepts, this book gradually moves into the realm of privilege escalation. It explains how Windows handles permissions, user roles, and security policies, setting the stage for understanding escalation. The book is suited for beginners and intermediate readers aiming to build a solid foundation.

8. *Hacking Windows: Privilege Escalation and Persistence*
This book explores not only privilege escalation but also persistence techniques on Windows machines. It guides readers through various attack stages, from initial access to maintaining control with elevated privileges. The content is enriched with examples of common flaws and how attackers exploit them.

9. *The Blue Team’s Guide to Windows Privilege Escalation*

Written from a defender’s perspective, this book helps blue team members recognize and mitigate privilege escalation threats. It details detection strategies, logging configurations, and incident response tips specific to Windows environments. The guide empowers security teams to strengthen their defenses against attackers seeking elevated access.

Windows Privilege Escalation Cheat Sheet

Windows Privilege Escalation Cheat Sheet

Related Articles

- williams and company financial services
- window tinting training courses
- windsor associates in family medicine

Back to Home