Windows Privilege Escalation Scripts & Techniques

Rahmat Nurfauzi Follow
Jan 21, 2018 · 4 min read

Privilege escalation is an important process part of post exploitation in a penetration test that allow an attacker to obtain a higher level of permissions on a system or network.

Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation.

An attacker can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or SYSTEM privileges. There are a few scripts in the under which makes it easy to do privilege escalation:

Windows-Exploit-Suggester

This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target. It also notifies the user if there are public exploits and Metasploit modules available for the missing bulletins.

GDSSecurity/Windows-Exploit-Suggester

Windows-Exploit-Suggester - This tool compares a targets patch levels against the Microsoft vulnerability database in...

github.com

SessionGopher

SessionGopher is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop. It can be run remotely or locally.

fireeye/SessionGopher

SessionGopher is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as...

github.com

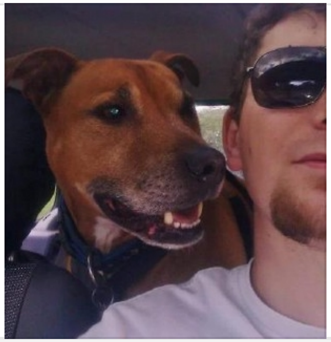
JAWS — Just Another Windows (Enum) Script

JAWS is PowerShell script designed to help penetration testers (and CTFers) quickly identify potential privilege escalation vectors on Windows systems. It is written using PowerShell 2.0 so 'should' run on every Windows version since Windows 7.

411Hall/JAWS

JAWS - Just Another Windows (Enum) Script

github.com



windows-privesc-check

Windows-privesc-check is standalone executable that runs on Windows systems. It tries to find misconfigurations that could allow local unprivileged users to escalate privileges to other users or to access local apps (e.g. databases).

pentestmonkey/windows-privesc-check

windows-privesc-check - Standalone Executable to Check for Simple Privilege Escalation Vectors on Windows Systems

github.com

Sherlock

PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.

rasta-mouse/Sherlock

Sherlock - PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.

github.com

Windows Privesc Check (WPC-PS)

After trying to fix the code of the original Windows Privesc Check tool and crying rivers of blood I decided to look for a more appropriate tool for the task. This is an experiment to implement similar functionality in Powershell, that is available by default in every Windows installation since Windows 7/Server 2008 R2.

silentsignal/wpc-ps

wpc-ps - Windows Privesc Check - PowerShell

github.com

PowerUp

PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations.

Running Invoke-AllChecks will output any identifiable vulnerabilities along with specifications for any abuse functions. The -HTMLReport flag will also generate a COMPUTER.username.html version of the report.

PowerShellMafia/PowerSploit

PowerSploit - A PowerShell Post-Exploitation Framework

github.com

Metasploit Windows Gather Applied Patches

post/windows/gather/enum_patches

This module will attempt to enumerate which patches are applied to a windows system based on the result of the WMI query: SELECT HotFixID FROM Win32_QuickFixEngineering

Metasploit Local Exploit Suggester Module

post/multi/recon/local_exploit_suggester

This module suggests local meterpreter exploits that can be used. The exploits are suggested based on the architecture and platform that the user has a shell opened as well as the available exploits in meterpreter. It's important to note that not all local exploits will be fired. Exploits are chosen based on these conditions: session type, platform, architecture, and required default options.

BeRoot

BeRoot(s) is a post exploitation tool to check common Windows misconfigurations to find a way to escalate our privilege.

AlessandroZ/BeRoot

BeRoot - Windows Privilege Escalation Tool

github.com

Privesc

Windows batch script that finds misconfiguration issues which can lead to privilege escalation. Script uses accesschk.exe from Sysinternals. This executable is mandatory. Few checks also use Listdlls.exe and pipelist.exe from Sysinternals. Those executables are optional.

enjoiz/Privesc

Privesc - Windows batch script that finds misconfiguration issues which can lead to privilege escalation.

github.com

Exploit Database (EDB)

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. exploit-db will help you to find out windows local exploit by searching through google or using tools like searchsploit.

By searching in google :

> *site:exploit-db.com privilege escalation windows 7*

Common Windows Privilege Escalation Vectors

1. Stored Credentials
2. Windows Kernel Exploit
3. DLL Injection
4. Unattended Answer File
5. Insecure File/Folder Permissions
6. Insecure Service Permissions
7. DLL Hijacking
8. Group Policy Preferences
9. Unquoted Service Path

10. Always Install Elevated

11. Token Manipulation

12. Insecure Registry Permissions

13. Autologon User Credential

14. User Account Control (UAC) Bypass

15. Insecure Named Pipes Permissions

Resources

https://github.com/SecWiki/windows-kernel-exploits

https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

https://www.insomniasec.com/downloads/publications/WindowsPrivEsc.ppt

http://toshellandback.com/2015/11/24/ms-priv-esc/

http://www.toshellandback.com/2015/08/30/gpp/

https://www.youtube.com/watch?v=DlJyKgfkoKQ

http://www.slideshare.net/chrisgates/windows-attacks-at-is-the-new-black-26672679

http://pwnwiki.io/#!privesc/windows/index.md

http://www.fuzzysecurity.com/tutorials/16.html

https://sec.mn/Archive/2016/April-Windows_Priv_Esc.pdf

https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/

http://resources.infosecinstitute.com/automating-windows-privilege-escalation http://resources.infosecinstitute.com/wp-content/uploads/Post-Exploitation-without-Automated-Tools1.pdf

https://zero-day.io/windows-privilege-escalation-exploit-suggester/

https://labs.mwrinfosecurity.com/assets/resourceFiles/DefCon25-UAC-0day-All-Day-v2.2.pdf

https://labs.mwrinfosecurity.com/assets/1089/original/Windows_Services_-_All_roads_lead_to_SYSTEM-1.1-oct15.pdf

Pentest Tools

264 claps

WRITTEN BY

Rahmat Nurfauzi

Follow

Security Consultant @ Xynexis. Red Team Operator & Pentester. Incident Responder, Purple Teaming & Threat Hunter.

See responses (1)

More From Medium

Related reads

The Hitchhiker’s Guide to Bug Bounty Hunting Throughout the Galaxy. v2

Nick Jenkins

Jan 30, 2018 · 9 min read

2K

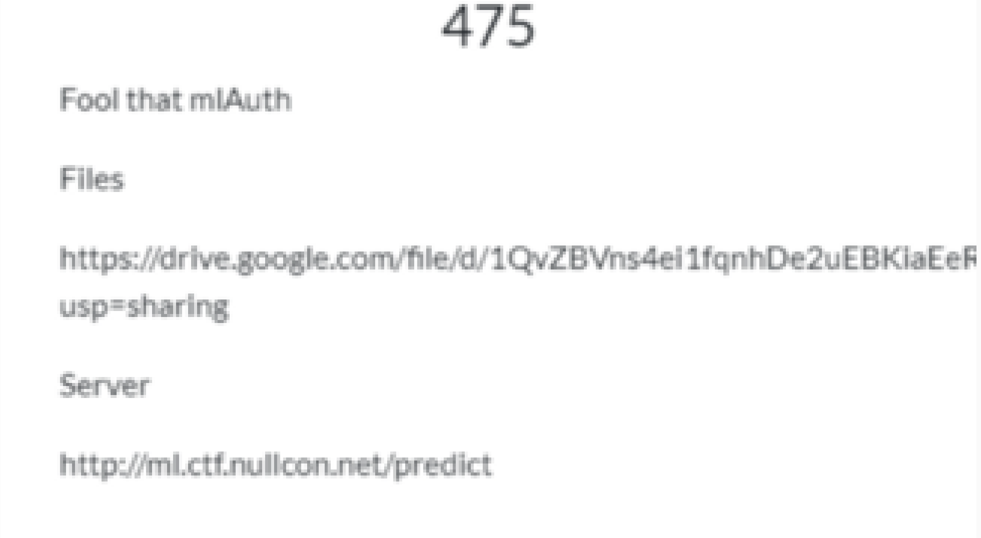
Related reads

Nullcon-HackIM CTF 2019- MLAuth-Misc(500) Writeup

Aagam shah in InfoSec Write-ups

Feb 3 · 4 min read

429



475

Fool that mlAuth

Files

https://drive.google.com/file/d/1QvZBVns4ei1fqnhDe2uEBKiaEeR
usp=sharing

Server

http://ml.ctf.nullcon.net/predict

Related reads

Remote Code Execution for Java Developers

Mitch Wasson in cisco-amp-technology

Apr 23 · 9 min read ★

143

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About Help Legal