

Forum:[Hack Forums](#)

Thread: [Basic Windows Privilege Escalation](#)

CyberStrike - September 28, 2017, 7:59 am

Elevating Privileges in Windows:

Windows localhost it is important that one understands the mechanisms behind the scenes in order to be successful.

The Game Plan for Windows Privilege Escalation

User => More Privileged User/Admin

Admin => Domain Admin/Enterprise Admin

Elevating Privileges:

Windows localhost it is important that one understands the mechanisms behind the scenes in order to be successful. For example for a user to be able to install software "always_install_elevated" can allow a program to be installed and that program may run at a higher privilege than the user whom installed it. So backdooring such a program with an embeded trojan is an option. Remember to be resourceful!

Edit: More to come more post exploitation tutorials/persistence in Windows & Linux

Escalation from a normal user to an admin on your localhost has some very simple steps although they may seem daunting at first glance. Trust me they are not!

User to more privileged user or Administrator:

Each process or thread on Windows has a token associated with it and anytime an application or process is started on a machine Windows does a few things, first there is a check of the access security function, secondly a check of the DACL. There are a few basic rules to any undertaking, first ask yourself do I need Administrator or elevated privileges in order to accomplish my tasks, for example if you already have a meterpreter session to a machine which belongs to a sales representative do you really need admin? Probably not you may just want to use a keylogger in order to garner actionable information, such as customer data. If you can accomplish tasks without needing admin then you should do so. But let's assume that we need that admin account and we are on that lonely sales representative's machine, how do we get admin on a completely unprivileged user?

The Game Plan for Windows Privilege Escalation

Credentials in file

Always worth a search to check if there is a password file since there are so many credentials that most users either reuse or place off their credentials in a file.

Code `dir /b /s *pass*`

`dir /b /s web.config`

`dir /b /s unattend.xml`

```
dir /b /s sysprep.inf
dir /b /s sysprep.xml
findstr /si password *.txt | *.xml | *.ini
```

Escalation of Privilege Bugs

Windows as is with most operating systems do have flaws, many times patching is done for more serious vulnerabilities such as RCE, but even then some patches are not applied or completely discarded to never be thought of again until an attacker is on a machine.

You will want to enumerate patches/updates of the local machine which you have landed on. Metasploit does have this as one of the post modules in `post/multi/recon/local_exploit_suggester`, which will greatly speed up your enumeration process. In addition `post/windows/enum_patches` is another quick post module to use to speed up enumeration.

If you are in a shell on the target machine you can use powershell or cmd to gather the same information.

Enumerating Patches

You may use Powershell also by using :

Code `Get-Package -AllVersions`
In cmd use the following:

Code `wmic qfe list`
Weak file/folder permission and orphaned executables and dlls

This is one of those techniques that the sysinternals suite using AutoRuns will greatly help you discover orphaned executables and dlls in the registry, which will be covered further below.

Weak file/folder permissions

One must remember that in `Windows\system32` you will not be able to write. Sysinternals `accesschk.exe` is required and it is strongly suggested that you take the time to get familiar with this suite of powerful tools in order to make your job easier. By default an "Authenticated User" may write/read/append data and files so this is what we will be exploiting. Taking a screenshot of the system is recommended as these generally run as SYSTEM, which you maybe able to target injecting your session and quickly gaining the elevated privileges. In addition if you are able to locate a program in autostart you may trojan that program as it will have higher privileges.

Checking the write permissions is important in cmd you may use :

Code `cacls \dir`
Checking the owner

Code `dir /q`
Appending/Writing to a file which you do not own can be accomplished as follows:

Code `echo text > file.ext`
This can be used in order to overwrite the file.

In order to check access to a file or directory you use the following command:

Code accesschk.exe -qvv \path\dir\fileWeak permissions for directory
Code accesschk -uwdqs users c:\

accesschk -uwdqs "Authenticated Users" c:\Weak file permissions
Code accesschk -uwdqs users c:*.*

accesschk -uwdqs "Authenticated Users" c:*.*

accesschk.exe -uwcqv *Checking the access to Program Files if the Users group is able to write
Code calcs "c:\Program Files" /T |findstr UsersEnumerating Autoruns

This is where you will need Sysinternals AutoRuns application in order to find orphaned files which will be highlighted in red. After locating a suitable orphaned file or dll you will want to check if you are able to write to that directory using the methods above if you are able to then you will trojanize an executable or dll and place it in the directory. If you need to you can create relatively the correct directory structure in order for the path to be correct according to the AutoRuns application and your backdoor will be started upon a REBOOT.

ProcMon is also a good application which can help you enumerate dll's called outside of Windows and thus directories which after checking access you maybe able to write and inject your own trojanized dll.

Checking Scheduled Tasks as these also maybe trojanized or can be used to issue a command for example here we will add a new user although the service will fail our command will not.

Code sc BinName.exe binpath= "net user NewUser /add" An attacker does have the option to install programs by using metasploit's post module exploit/windows/local/always_install_elavated

Checking the Registry

OEM Install

Code c:\sysprep.inf cleartext

c:\sysprep\sysprep.xml (Base64)The registry hold credentials for certain applications which as was stated earlier users reuse credentials, and may help you quickly gain an Administrator account.

Code \HKCU\SOFTWARE\ORL\WinVNC3\Password

Autologin - readable by any user

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
clear txt cred shell key UserInit key

SNMP can help you garner information

HKLM\SYSTEM\CurrentControlSet\Services\SNMP

Putty a ssh client

HKCU\Software\Username\PuTTY\Sessions

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

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

reg query "keyname"Clip is command which is used with citrix clients, which is often used for remote administration with in corporations. VNC.ini and ultravnc.ini will have hashed password which are easily decrypted, so one should be on alert for these files on a target machine.

Edit: Added code tags

Baud - September 28, 2017, 11:19 am

This is an interesting and useful thread, especially for beginners who need an introduction to more advanced hacking topics such as privilege escalation, so good work, I can tell from your other posts as well you know your stuff. Just a little suggestion, use the code tags to make the thread more readable, some users might close it without reading it because it's not easy to look at. Other than that very well done.

CyberStrike - September 28, 2017, 3:59 pm

Excellent Baud I will keep this in mind and use code tags, thank you.

bash_bunny - October 12, 2017, 1:54 pm

hmm might be on to something here

AnomalyX - October 12, 2017, 5:30 pm

Sirru5h you have been posting alot of HQ content everywhere, and i am very grateful for you passing on some knowledge to us newcomers! Keep up the good work!

CyberStrike - October 13, 2017, 1:20 pm

(Oct 12, 2017 05:30 PM)AnomalyX Wrote: [\[CITE\]](#) Sirru5h you have been posting alot of HQ content everywhere, and i am very grateful for you passing on some knowledge to us newcomers! Keep up the good work!

Thank you AnomalyX, I appreciate the positive feedback, I am always glad to help.

Puller - October 13, 2017, 4:41 pm

This thread is filled with a lot of good information and one of the better threads I've seen in this section. A linux version of this one would be interesting to follow up with. Keep up the good work.

CyberStrike - October 13, 2017, 5:58 pm

(Oct 13, 2017 04:41 PM)Puller Wrote: [\[CITE\]](#) This thread is filled with a lot of good information and one of the better threads I've seen in this section. A linux version of this one would be interesting to follow up with. Keep up the good work.

Awesome I appreciate the positive comments yeah I did a few tutorials on Windows and Red Team Structure, which I have linked to below. Next is Linux and will be composed of:

- Linux Information Gathering and Situational Awareness,
- Linux Post exploitation and Persistence
- Linux Privilege Escalation

Then on to OSX following the same structure and finally a tutorial on how to build a domain reputation, which is helpful during phishing campaigns. Then we put it all together with a write up on Dirty Exploitation/Post Exploitation Tricks, which will encompass all of the tutorials and how to implement the technical information with practical uses. (I am about 1 week behind because of a minor accident with my computer which had the most recent version of my notes, this weekend I will be trying to recover my old hard disk)

Windows Post Exploitation & AD Hunting

<https://hackforums.net/showthread.php?tid=5726592>

Red Team Structure (Post Exploitation)

<https://hackforums.net/showthread.php?tid=5728866>

Windows Information Gathering and Situational Awareness

<https://hackforums.net/showthread.php?tid=5733292>

bader965 - *October 14, 2017, 9:41 am*

Thank you I enjoyed reading in writing Dear

CyberStrike - *October 15, 2017, 4:50 pm*

Excellent glad you enjoyed it bader965

imscheurkie - *October 16, 2017, 8:00 am*

Nice tutorial. I'll give it a try later.

CyberStrike - *October 16, 2017, 6:06 pm*

Excellent just create a windows 7 vm create a regular user account run a backdoor on that account Microsoft has VMs for free btw .

stripcheese - *November 5, 2017, 3:24 pm*

This is a very well written and detailed post! Thanks!

lowfatcheeze - *November 6, 2017, 8:03 pm*

Amazing write-up. But how exactly can you take advantage of orphaned DLLs?

CyberStrike - *November 6, 2017, 8:32 pm*

We can create our own backdoored DLL and providing we have the ability to append we can write our backdoored DLL to the path which is referred to now will be run with system level privileges. If we look at say the search order for Windows when it comes to DLL's.

[https://msdn.microsoft.com/en-us/library/windows/desktop/ms682586\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms682586(v=vs.85).aspx)

lowfatcheeze - *November 7, 2017, 9:36 am*

That makes sense, thank you!

CyberStrike - *November 7, 2017, 11:42 am*

(Nov 7, 2017 10:36 AM)lowfatcheeze Wrote: [\[CITE\]](#) That makes sense, thank you!

Always glad to help I do have multiple other tutorials which I have posted as well on Windows and Linux, next I am on to OSX.