

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] ~ Post Exploitation Part II: System Information Gathering](#)

Goodies - March 18, 2014, 7:10 pm

Hello everyone! :D

Today, I'll be writing a tutorial on Windows Post-exploitation. If you followed the last tutorial [LOCATED HERE](#) you have an NT AUTHORITY meterpreter shell running regardless of the user's privileges on the box. Now, we're going to use this to our advantage and find out some information about the box.

Part II: System Information Gathering

What is information Gathering?

Essentially, we want to gather information pertaining to this machine. This can mean passwords as well as files or network information.

What is a Backdoor?

A backdoor is an application that sits idly on the victim's computer until we intrude and connect to it.

1. Sysinfo

Upon running sysinfo, we can see:

- Computer Name
- Operating System & Build
- Architecture
- Language
- Meterpreter Payload Type

2. Shell and Windows Scripting

Typing shell in the meterpreter session will spawn a windows system shell. Here, you can see that running net users shows me the users of the computer.

Okay, great! How about we look at some users.

net user goodies

Just getting a feel for the owner

3. Hashdump

run hashdump will dump both the password hints and the password hashes.

In my case, the password hint is the password. However, you can use JTR, Hashcat, or simply use

googledorks to try and crack the hash. This is not what that tutorial is about though :P That will have to be done on your own time.

This can also possibly be used, in an NTLM authenticated SMB usershare, to log into other machines via pass the hash, psexec, or smbexec.

4. Packet Sniffing

My personal favorite :)

First, run ipconfig so we can see which interface has the IP address assigned to it.

In my case, it's Intel® PRO/1000 MT Desktop Adapter. That's important, remember that.

Next, load the sniffer module by typing use sniffer . You can then type help to show the commands specific to the sniffer module.

running sniffer_interfaces shows that interface ID 2 is what I must use for the sniffing.

Let's start the sniffer:

```
sniffer_start 2 100000
```

100000 = The max number of packets allowed capture.

After a while, when you want to dump it, you can dump it by running:

```
sniffer_dump 2 /tmp/something.pcap
```

where 2 is the ID and /tmp/something.pcap is the pcap file that will be created and saved.

Stop and flush the sniffer with:

```
sniffer_stop 2
```

```
sniffer_release 2
```

Thank You for Reading Part II

I Am Sexy Boys - March 19, 2014, 5:15 am

Note: If you "reset" the password then no Encrypted files will work unless you have the original password (I can't remember the exact windows terminology but I think it's like bitlocker or something)

XBatt - March 19, 2014, 9:00 am

Great tutorial, very useful, thanks.

prokeen - March 19, 2014, 9:34 am

Thanks for this man, well-made and useful tutorial!

WheredYouGo - March 19, 2014, 11:53 am

This will be very helpful whenever I can find out how to get VMware for free. Thanks :D

prokeen - March 19, 2014, 1:10 pm

(Mar 19, 2014 11:53 AM)WheredYouGo Wrote: [\[CITE\]](#) This will be very helpful whenever I can find out how to get VMware for free. Thanks :D

You can use VirtualBox, it's a virtualization software just like VMWare but it's free :)

<https://www.virtualbox.org/wiki/Downloads>

Or, I heard there are some people sharing VMWare on some torrent sites lol

Good luck! ?

SIM-5561 - March 19, 2014, 2:06 pm

Nice tut. Hope to see more of these HQ tuts in this section :)

WheredYouGo - March 19, 2014, 8:57 pm

(Mar 19, 2014 01:10 PM)prokeen Wrote: [\[CITE\]](#) You can use VirtualBox, it's a virtualization software just like VMWare but it's free :) <https://www.virtualbox.org/wiki/Downloads>

Or, I heard there are some people sharing VMWare on some torrent sites lol

Good luck! ?

Hey thanks! Haven't heard of Virtualbox, but I'd still need to get a \$100 copy of windows 7 in order to use it though right? Sorry for posting off topic :/ Would pm if I could

Goodies - March 19, 2014, 9:44 pm

(Mar 19, 2014 08:57 PM)WheredYouGo Wrote: [\[CITE\]](#) Hey thanks! Haven't heard of Virtualbox, but I'd still need to get a \$100 copy of windows 7 in order to use it though right? Sorry for posting off topic :/ Would pm if I could

If you're looking for a legal copy, sure. The. Pirate. Bay. Dot. Se.

WheredYouGo - March 20, 2014, 4:42 am

(Mar 19, 2014 09:44 PM)Goodies Wrote: [\[CITE\]](#) If you're looking for a legal copy, sure. The. Pirate. Bay. Dot. Se.

Alright thanks, think I might as well just buy a \$300 windows laptop. Great tutorial though!