

Forum:[Hack Forums](#)

Thread: [\[Nmap & Metasploit\] Windows breaking & entering Port mapping & metasploit ICE #1](#)

slober - April 17, 2020, 4:34 pm

[Nmap & Metasploit] Windows breaking & entering Port mapping & metasploit ICE #1

Welcome, This is my first tutorial in a long time in this section. I've got some time on my hands these days and I think these tutorials could be beneficial to the community.

So here we go.

This one is tailored to getting to know how to work with Nmap and Metasploit on a windows system. Why windows well this computer is under spect for running virtual machines and well it's all I have at my disposal at this moment.

Please enjoy!

The reconnaissance fase

This step is an important one. Well, of course, it is important you need to know what ports are open on your victim/target computer so that you can deduct what kind of services are running on it.

A port doesn't necessarily mean that that specific service is running on that system but it gives an idea on what you could expect.

These are a few examples:

Code FTP - 20, 21

SSH - 22

TELNET - 23

SMTP - 25

DNS - 53

POP3-110

HTTP - 80

IMAP - 143

HTTPS - 443

RDP - 3389

How do we know what ports are open?

Well, that is a good question there is a tool for that. The one I'm using in this example is called Nmap. Nmap stands for Network mapper and it does work on windows.

Download:

Official website: <https://nmap.org/download.html>

Great, what are we going to do now? Well let's open the GUI.

Its pretty simple in the target textbox we can input the Ip address of the machine we're targetting. in my case, the IP address is 10.10.104.65

One of the advantages of the GUI is that it'll create the command for you depending on what type of scan you want to run you can edit this command and create custom variants but in this case, it isn't

necessary.

lets take a closer look at the command

Code `nmap -T4 -A -v 10.10.104.65`

nmap = the program

-T4 = timing (How fast should it scan.)

-A = OS detection (Tries to detect the Operating system)

-v = verbose (the output)

10.10.104.65 = The IP address it should scan.

After that, you should press the scan button. It can take a while but shouldn't take too long you should get an output similar to this:

If you scroll a bit back you can find more information about the ports, Operating system,...

The advantage of the GUI is that it'll organize some things for us when you press the host/ports tab you'll get an overview of the different services that should be running on set ports.

The one I'm interested in is the one used on port 8000 the Icecastserver it has some pretty decent vulnerabilities.

How can you know if a service is vulnerable?

You can search for it. Use google or a database like <https://www.cvedetails.com/>

An example for Icecast:

https://www.cvedetails.com/vulnerability-list/vendor_id-693/Icecast.html

Okay, what's next?

We're pretty much done with the recon we should now switch over to the gain access phase.

Gain access!

How can we exploit set vulnerabilities?

We need a software package that can run these exploits on the given system. A tool we can use for this is called metasploit and can be downloaded here it'll work on windows but it can be troublesome antiviruses will cause you trouble and the firewall will be an annoyance too. Don't give up you can do this ;) (if you must you can ignore a certain directory on your computer and give access to the meterpreter shell.

You can find more information here:

<https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers>

To run metasploit you should type msfconsole (it can take a while to run).

you should get something similar to this:

Now it's time to search for an exploit (we'll use the CVE-2004-1561). You can search for exploits using the search command.

Code `search icecast`

after this, we can use set exploit. bu using the command use, in this case, use 0
Code use 0

well, and how do we run this?

First, you'll need to know what kind of options you should give Metasploit you condo this by typing show options.

Code show options

Metasploit needs to know one single thing the rhosts. the r stands for remote it needs to know the target
in my case 10.10.104.65

We can set this value by typing set rhosts and then your IP
Code set rhosts 10.10.104.65

only one thing left to do we need to run the exploit we can do this by typing exploit
Code exploit

And you're done.

Thank you for reading through this tutorial the first of a series I'm planning on continuing I guess the next one will focus on something different I don't yet know what; If there is something you'll want to explore more in-depth please feel free to tell me or pm me about it.

Next on the list will probably be escalation and process migrating. ?