Internal Pentest (POC)

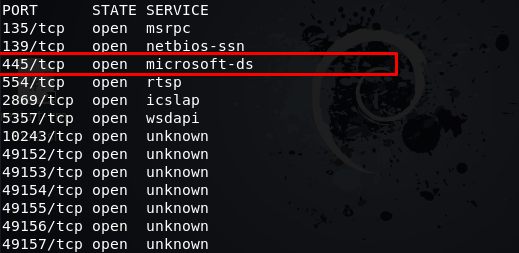
Attacker using machine kali linux 2018.2

Victim windows 7 64 bits

Information gathering using nmap:



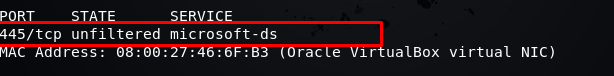
**Figure 1: using this parameter to get a information on windows 7**



**Figure 2:we found the victims machine running port 445**



Figure 3: To get a clearly information about the port 445 and firewall issue

****

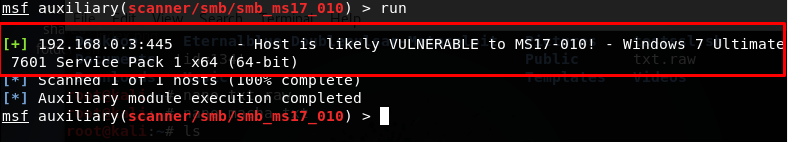
**Figure 4: We got clearly about the port is filter or not and the port 445 detail**



**Figure 5:we try this auxiliary scanner to check vulnerable on port 445(smb service)**

1.set RHOST IP ADDRESS VICTIM

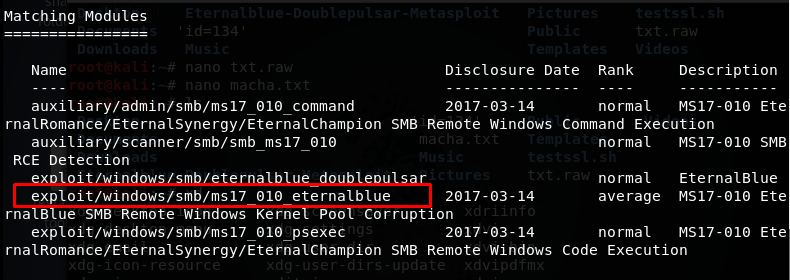
2.run



**Figure 6:woo it is likely vulnerable for MS17-010**



**Figure 7: search for eternal blue exploit**



**Figure 8:Try using this type of exploit**



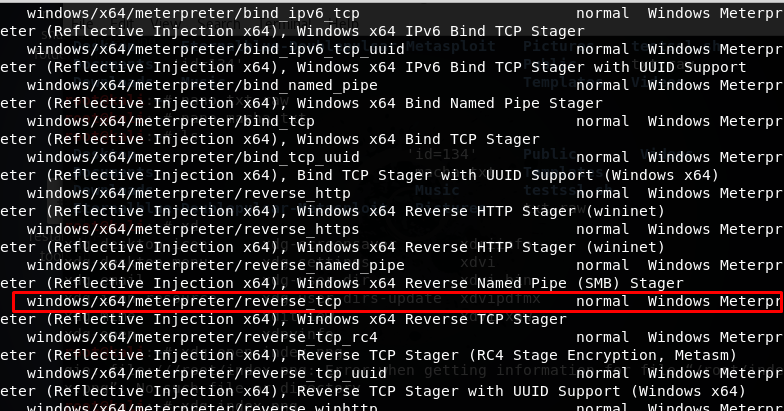
**Figure 9: choose this type of attack**



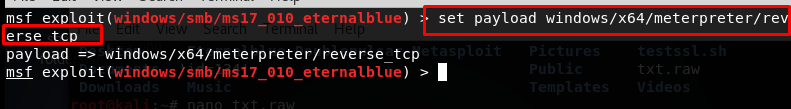
**Figure 10:Set the RHOST (VICTIM IP ADDRESS)**



**Figure 11:show payload to see and choose suitable payload to get a shell and reverse**



**Figure 12:U see a lot of payloads in this case we use windows/64/meterpreter/reverse\_tcp**



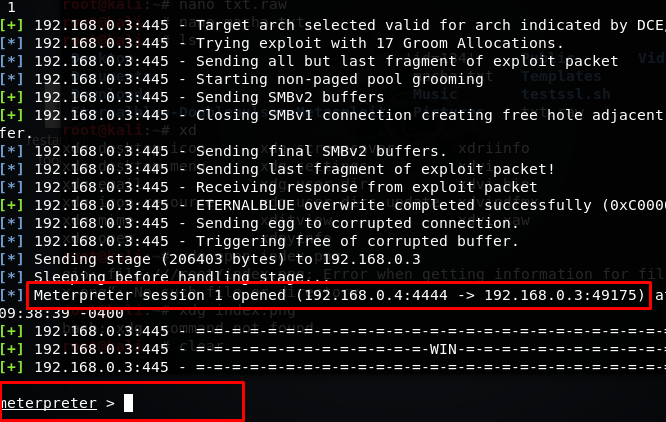
**Figure 13: set the payload to use**



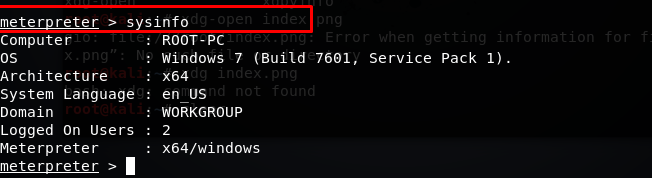
**Figure 14:Set a LHOST (YOUR MACHINE IP ADDRESS)**



**Figure 15:Ok now exploit**

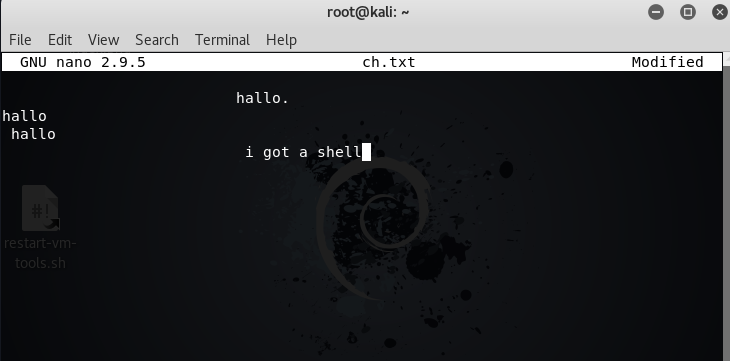


**Figure 16: orite attacker success back door the windows 7 and got a shell happy**

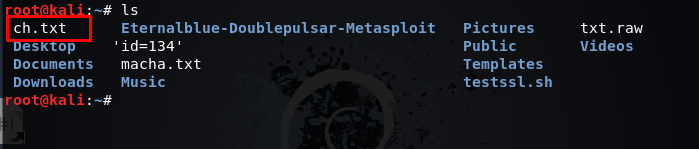


**Figure 17: sysinfo (system info) to make sure attacker success backdoor on port 445**

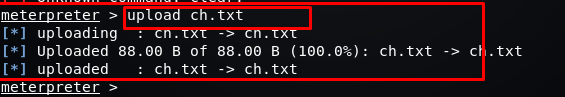
Let’s upload the file into the victim machine.



**Figure 18:create the dummy txt**



**Figure 19: copy this file name**



**Figure 20:upload the file the attacker create**

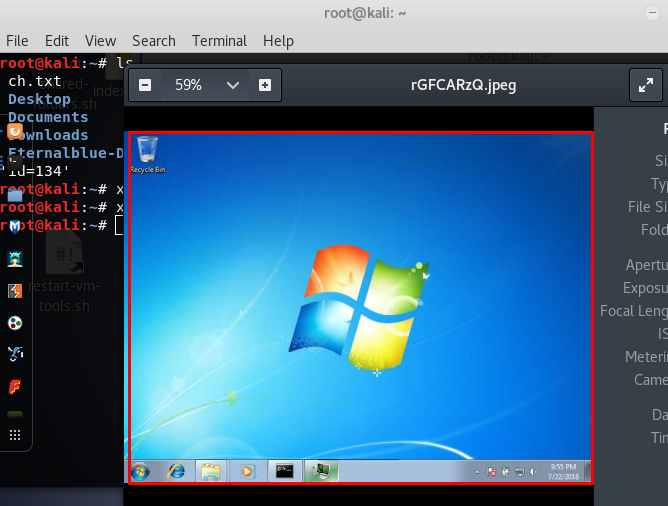
Let’s see the victim machine desktop



**Figure 21:just execute screenshot command and the file will be save on attacker machine**



**Figure 22: run this command to see screen screenshot victim machine**



**Figure 23 : haha attacker success see what the victim do with using their laptop**