Security+ Lab Series

Lab 02: Password Cracking with Linux

Document Version: 2018-11-01

Copyright © 2018 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, NETLAB+ Virtual Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Contents

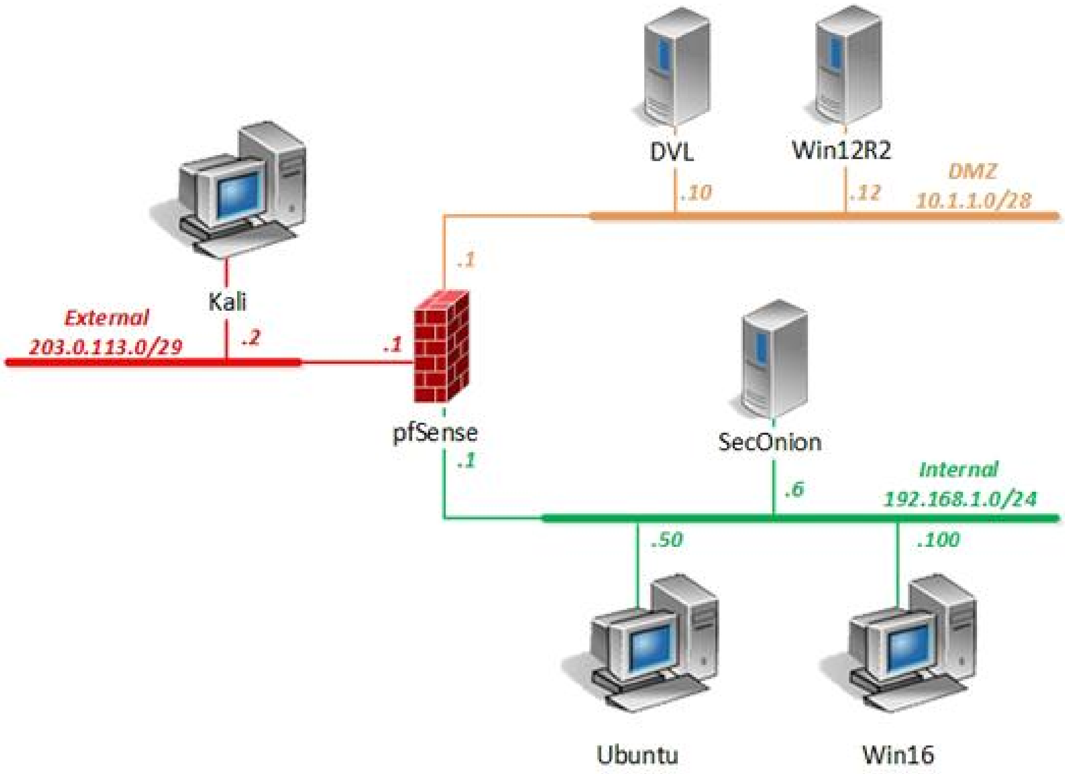
Introduction

In this lab, you will be conducting password-cracking techniques using various tools.

Objectives

- Summarize various types of attacks
- Analyze a scenario and select the appropriate type of mitigation and deterrent techniques

Lab Topology



Lab Settings

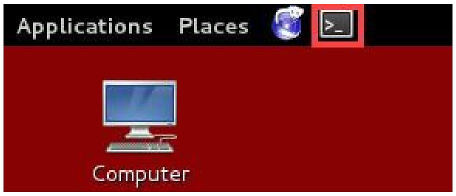
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
SecOnion	192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Train1ng$
Win16	192.168.1.100 /24	lab-user	Train1ng$
		Administrator	Train1ng$

1 Cracking Linux Passwords

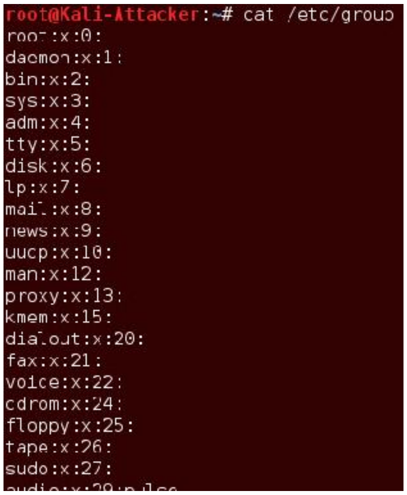
1.1 Creating User Accounts and Groups

1. Launch the **Kali** virtual machine to access the graphical login screen.
2. Log in as `root` with that password `toor`.
3. Open a new *terminal* window by clicking on the **terminal** icon located in the top menu pane.



4. Type the command below, followed by pressing the **Enter** key to view the groups on the system.

```
root@Kali-Attacker:~# cat /etc/group
```



```
root@Kali-Attacker:~# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:pulse
```

New groups and users will be created based on the tables below:

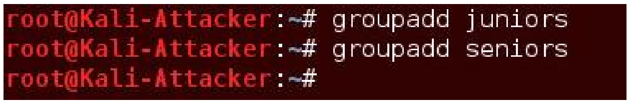
Group: seniors	
User	Password
elmo	123123
oscar	sanjose

Group: juniors	
User	Password
lisa	academic
homer	acapulco

5. Enter the command below to populate the group list by creating two new groups: **juniors** and **seniors**.

```
root@Kali-Attacker:~# groupadd juniors
```

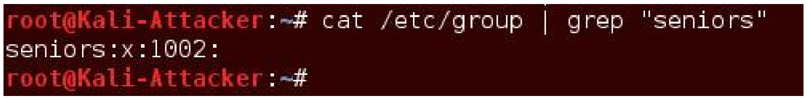
```
root@Kali-Attacker:~# groupadd seniors
```



```
root@Kali-Attacker:~# groupadd juniors
root@Kali-Attacker:~# groupadd seniors
root@Kali-Attacker:~#
```

6. Confirm that the groups have been added using *grep*.

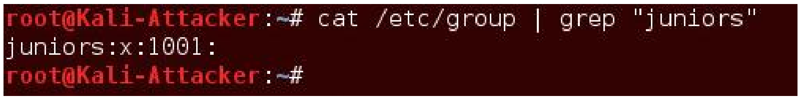
```
root@Kali-Attacker:~# cat /etc/group | grep “seniors”
```



```
root@Kali-Attacker:~# cat /etc/group | grep "seniors"
seniors:x:1002:
root@Kali-Attacker:~#
```

Notice the group ID for *seniors* in this example is *1002*.

```
root@Kali-Attacker:~# cat /etc/group | grep “juniors”
```

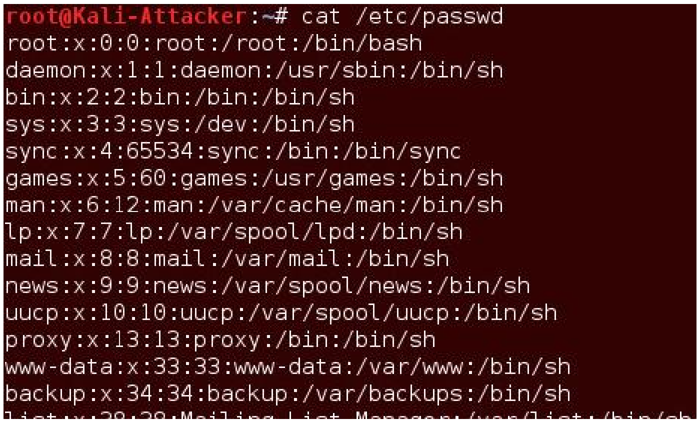


```
root@Kali-Attacker:~# cat /etc/group | grep "juniors"
juniors:x:1001:
root@Kali-Attacker:~#
```

Notice the group ID for *juniors* in this example is *1001*.

7. Enter the command below to view the user accounts on the system.

```
root@Kali-Attacker:~# cat /etc/passwd
```

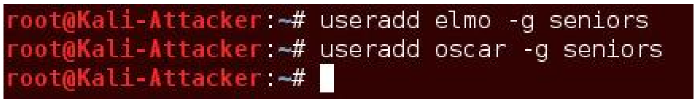


```
root@Kali-Attacker:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

8. Add users **elmo** and **oscar** to the system and assign them to the group **seniors**.

```
root@Kali-Attacker:~# useradd elmo –g seniors
```

```
root@Kali-Attacker:~# useradd oscar –g seniors
```



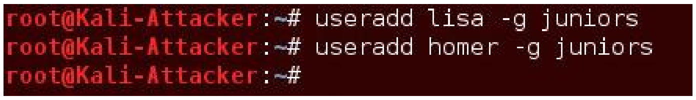
```
root@Kali-Attacker:~# useradd elmo -g seniors
root@Kali-Attacker:~# useradd oscar -g seniors
root@Kali-Attacker:~#
```

You may find it easier to press the up arrow while in the terminal to display the previous command entered and then revise the text to enter the new command should the commands be similar.

9. Add users **lisa** and **homer** and assign them to the group **juniors**.

```
root@Kali-Attacker:~# useradd lisa –g juniors
```

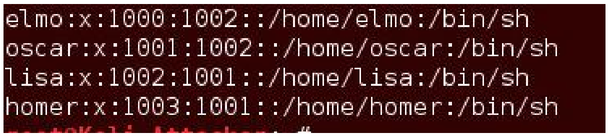
```
root@Kali-Attacker:~# useradd homer –g juniors
```



```
root@Kali-Attacker:~# useradd lisa -g juniors
root@Kali-Attacker:~# useradd homer -g juniors
root@Kali-Attacker:~#
```

10. View the **/etc/passwd** file once more to verify that all accounts are successfully created.

```
root@Kali-Attacker:~# cat /etc/passwd
```

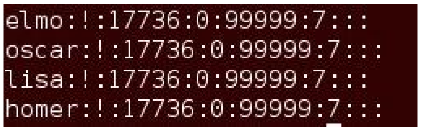


```
elmo:x:1000:1002::/home/elmo:/bin/sh
oscar:x:1001:1002::/home/oscar:/bin/sh
lisa:x:1002:1001::/home/lisa:/bin/sh
homer:x:1003:1001::/home/homer:/bin/sh
```

Notice the new accounts at the bottom of the list and how each is assigned to their respective group IDs mentioned. Note that the second ID field is assigned as the group ID. The first ID field is assigned as the user ID.

11. View the **/etc/shadow** file and observe the values next to the newly created accounts towards the bottom of the list.

```
root@Kali-Attacker:~# cat /etc/shadow
```



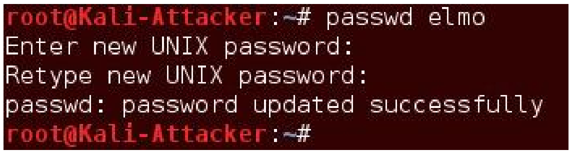
```
elmo:!:17736:0:99999:7:::
oscar:!:17736:0:99999:7:::
lisa:!:17736:0:99999:7:::
homer:!:17736:0:99999:7:::
```

The *shadow* file stores information such as password hashes for the user accounts on a *Linux* system.

12. Configure passwords for the users: **elmo**, **oscar**, **lisa,** and **homer**. First, begin by configuring the password for the **elmo** user account.

```
root@Kali-Attacker:~# passwd elmo
```

13. When prompted for the new password, type 123123 followed by pressing the **Enter** key. When prompted to retype the password, enter it again.



```
root@Kali-Attacker:~# passwd elmo
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@Kali-Attacker:~#
```

14. Configure the password for **oscar** next. When prompted, enter `sanjose` as the password.

```
root@Kali-Attacker:~# passwd oscar
```

15. Configure the password for **lisa**. When prompted, enter `academic` as the password.

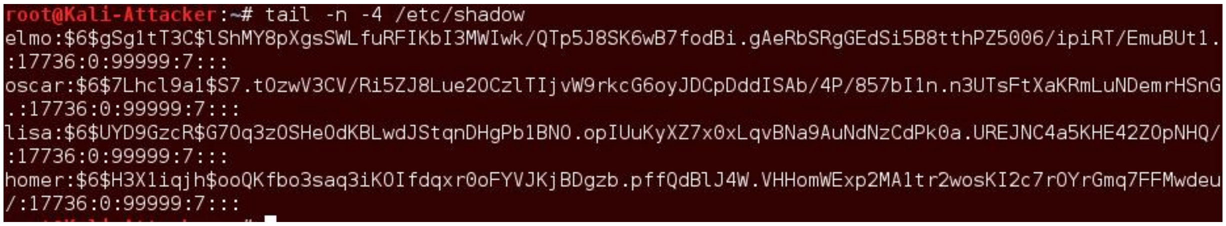
```
root@Kali-Attacker:~# passwd lisa
```

16. Configure the password for **homer**. When prompted, enter `acapulco` as the password.

```
root@Kali-Attacker:~# passwd homer
```

17. Type the command below to view the new user accounts along with their respective hashes in the **shadow** file. The command options used below will only output the last four accounts in the *shadow* file.

```
root@Kali-Attacker:~# tail –n -4 /etc/shadow
```



```
root@Kali-Attacker:~# tail -n -4 /etc/shadow
elmo:$6$gSg1tT3C$lShMY8pXgsSWLfuRFIKbI3MWIwk/QTp5J8SK6wB7fodBi.gAeRbSRgGEdSi5B8tthPZ5006/ipiRT/EmuBUt1.
:17736:0:99999:7:::
oscar:$6$7Lhcl9a1$S7.tOzwV3CV/Ri5ZJ8Lue20CzlTIjvW9rkcG6oyJDCpDddISAb/4P/857bI1n.n3UTsFtXaKRmLuNDemrHSnG
.:17736:0:99999:7:::
lisa:$6$UYD9GzcR$G70q3zOSHeOdKBLwdJStqnDHgPb1BNO.opIUuKyXZ7x0xLqvBNa9AuNdNzCdPk0a.UREJNC4a5KHE42ZOpNHQ/
:17736:0:99999:7:::
homer:$6$H3X1iqjh$ooQKfbo3saq3iKOIfdqxr0oFYVJKjBDgzb.pffQdBlJ4W.VHHomWExp2MA1tr2wosKI2c7rOYrGmq7FFMwdeu
/:17736:0:99999:7:::
```

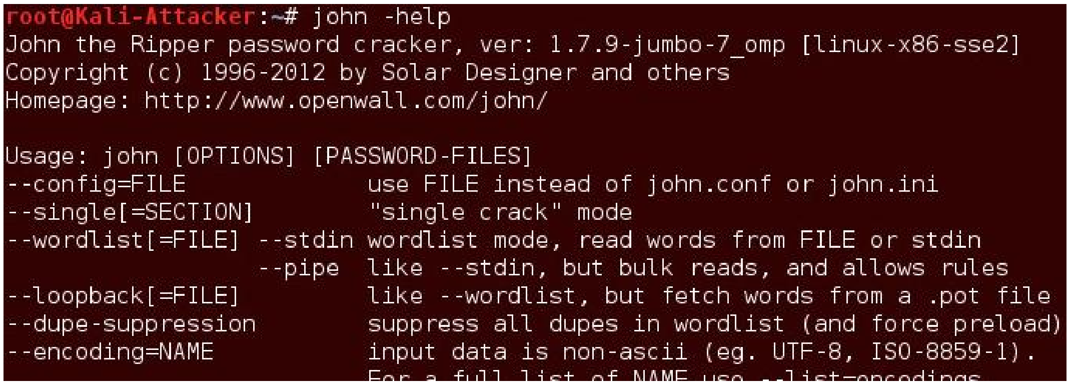
Notice how the fields next to the new user accounts have changed when compared to what was seen previously. They are now populated with password hashes.

18. Leave the *terminal* open to continue with the next task.

1.2 Cracking Passwords on a Linux System Using John the Ripper

1. Before using *John the Ripper*, using the terminal, type the command below to view the available options that can be used with the application. This is useful when using any command in *Linux*.

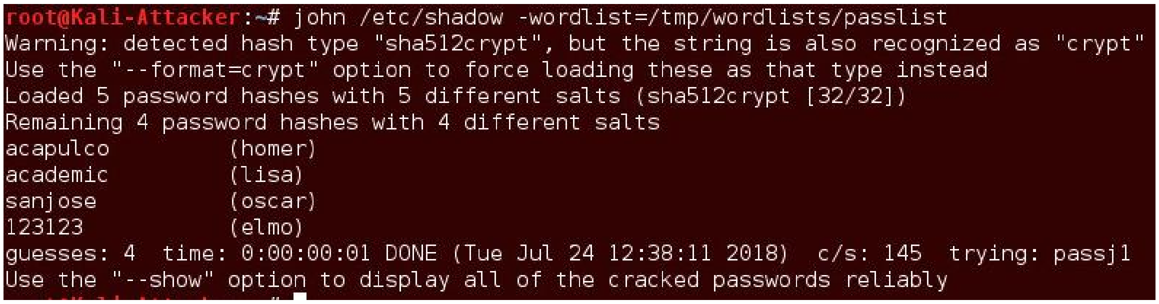
```
root@Kali-Attacker:~# john -help
```



```
root@Kali-Attacker:~# john -help
John the Ripper password cracker, ver: 1.7.9-jumbo-7_omp [linux-x86-sse2]
Copyright (c) 1996-2012 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
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but fetch words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--encoding=NAME           input data is non-ascii (eg. UTF-8, ISO-8859-1).
                          For a full list of NAME use --list=encodings
```

2. Run **John the Ripper** against the **/etc/shadow** file using a wordlist called **passlist**.

```
root@Kali-Attacker:~# john /etc/shadow –wordlist=/tmp/wordlists/passlist
```



```
root@Kali-Attacker:~# john /etc/shadow -wordlist=/tmp/wordlists/passlist
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 5 password hashes with 5 different salts (sha512crypt [32/32])
Remaining 4 password hashes with 4 different salts
acapulco         (homer)
academic         (lisa)
sanjose          (oscar)
123123           (elmo)
guesses: 4  time: 0:00:00:01 DONE (Tue Jul 24 12:38:11 2018)  c/s: 145  trying: passj1
Use the "--show" option to display all of the cracked passwords reliably
```

Notice the successful completion of cracking the passwords using JTR.

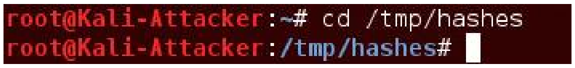
3. Leave the **terminal** open to continue with the next task.

2 Cracking Windows Passwords

2.1 Cracking Windows Passwords Using Hashcat

1. While on the **Kali** system, focus on the **terminal** window.
2. Change to the **/tmp/hashes** directory.

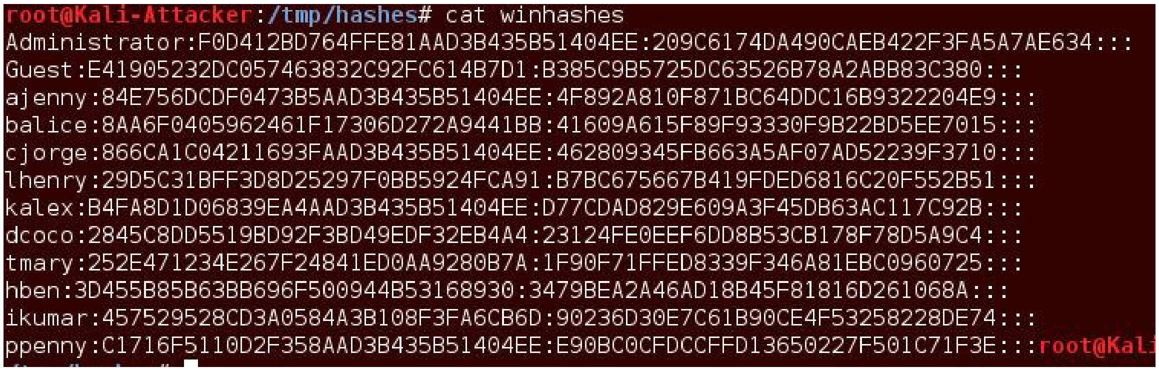
```
root@Kali-Attacker:~# cd /tmp/hashes
```



```
root@Kali-Attacker:~# cd /tmp/hashes
root@Kali-Attacker:/tmp/hashes#
```

3. View the **winhashes** file extracted from a *Windows* system. Notice the usernames listed along with the associated password hashes.

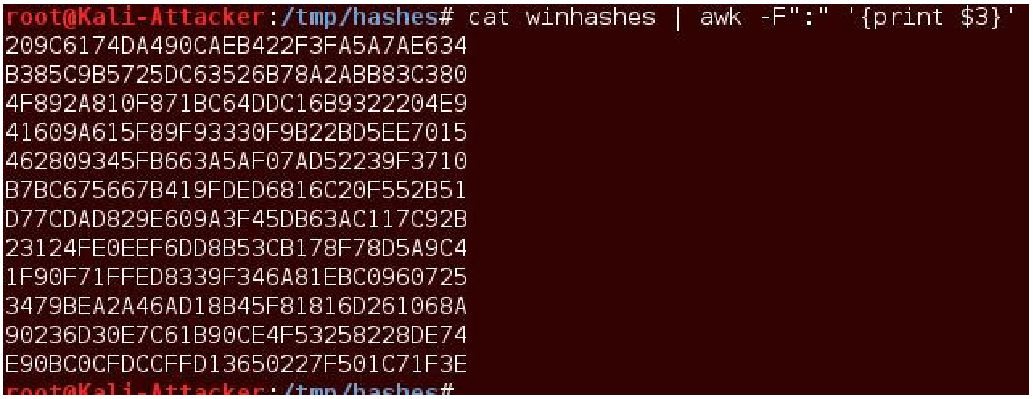
```
root@Kali-Attacker:/tmp/hashes# cat winhashes
```



```
root@Kali-Attacker:/tmp/hashes# cat winhashes
Administrator:F0D412BD764FFE81AAD3B435B51404EE:209C6174DA490CAEB422F3FA5A7AE634:::
Guest:E41905232DC057463832C92FC614B7D1:B385C9B5725DC63526B78A2ABB83C380:::
ajenny:84E756DCDF0473B5AAD3B435B51404EE:4F892A810F871BC64DDC16B9322204E9:::
balice:8AA6F0405962461F17306D272A9441BB:41609A615F89F93330F9B22BD5EE7015:::
cjorge:866CA1C04211693FAAD3B435B51404EE:462809345FB663A5AF07AD52239F3710:::
lhenry:29D5C31BFF3D8D25297F0BB5924FCA91:B7BC675667B419FDED6816C20F552B51:::
kalex:B4FA8D1D06839EA4AAD3B435B51404EE:D77CDAD829E609A3F45DB63AC117C92B:::
dcoco:2845C8DD5519BD92F3BD49EDF32EB4A4:23124FE0EEF6DD8B53CB178F78D5A9C4:::
tmary:252E471234E267F24841ED0AA9280B7A:1F90F71FFED8339F346A81EBC0960725:::
hben:3D455B85B63BB696F500944B53168930:3479BEA2A46AD18B45F81816D261068A:::
ikumar:457529528CD3A0584A3B108F3FA6CB6D:90236D30E7C61B90CE4F53258228DE74:::
ppenny:C1716F5110D2F358AAD3B435B51404EE:E90BC0CFDCCFFD13650227F501C71F3E:::root@Kali
```

4. Parse out the **NTHash** from the **winhashes** file.

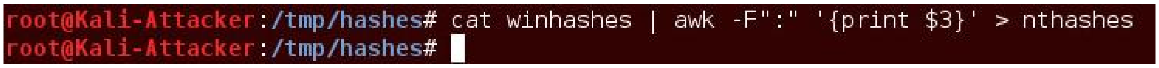
```
root@Kali-Attacker:/tmp/hashes# cat winhashes | awk –F”:” ‘{print $3}’
```



```
root@Kali-Attacker:/tmp/hashes# cat winhashes | awk -F":" '{print $3}'
209C6174DA490CAEB422F3FA5A7AE634
B385C9B5725DC63526B78A2ABB83C380
4F892A810F871BC64DDC16B9322204E9
41609A615F89F93330F9B22BD5EE7015
462809345FB663A5AF07AD52239F3710
B7BC675667B419FDED6816C20F552B51
D77CDAD829E609A3F45DB63AC117C92B
23124FE0EEF6DD8B53CB178F78D5A9C4
1F90F71FFED8339F346A81EBC0960725
3479BEA2A46AD18B45F81816D261068A
90236D30E7C61B90CE4F53258228DE74
E90BC0CFDCCFFD13650227F501C71F3E
root@Kali-Attacker:/tmp/hashes#
```

5. Now that we have confirmed what is needed to be parsed out, save the output to a file named **nthashes**.

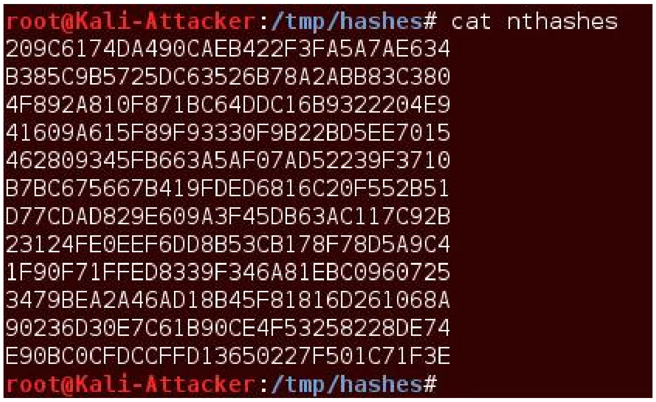
```
root@Kali-Attacker:~# cat winhashes | awk –F”:” ‘{print $3}’ > nthashes
```



```
root@Kali-Attacker:/tmp/hashes# cat winhashes | awk -F":" '{print $3}' > nthashes
root@Kali-Attacker:/tmp/hashes# 
```

6. Verify that the **NTHashes** have outputted correctly in the *nthashes* file.

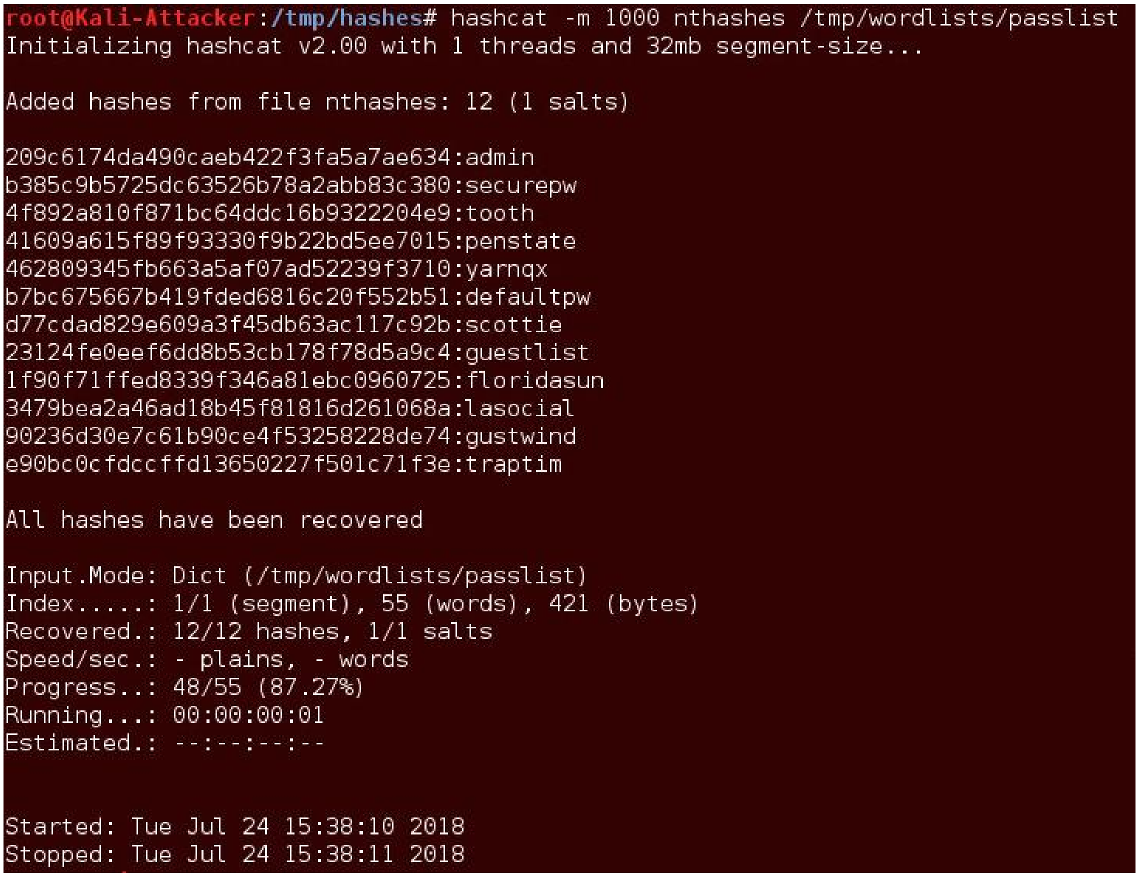
```
root@Kali-Attacker:/tmp/hashes# cat nthashes
```



```
root@Kali-Attacker:/tmp/hashes# cat nthashes
209C6174DA490CAEB422F3FA5A7AE634
B385C9B5725DC63526B78A2ABB83C380
4F892A810F871BC64DDC16B9322204E9
41609A615F89F93330F9B22BD5EE7015
462809345FB663A5AF07AD52239F3710
B7BC675667B419FDED6816C20F552B51
D77CDAD829E609A3F45DB63AC117C92B
23124FE0EEF6DD8B53CB178F78D5A9C4
1F90F71FFED8339F346A81EBC0960725
3479BEA2A46AD18B45F81816D261068A
90236D30E7C61B90CE4F53258228DE74
E90BC0CFDCCFFD13650227F501C71F3E
root@Kali-Attacker:/tmp/hashes#
```

7. Run the **Hashcat** password cracking program against the **nthashes** file with the help of the **passlist** dictionary file in an attempt to crack the *NTHashes* from a *Windows* system. If asked to accept a EULA, type **YES** followed by pressing **Enter**.

```
root@Kali-Attacker:/tmp/hashes# hashcat –m 1000 nthashes
/tmp/wordlists/passlist
```



```
root@Kali-Attacker:/tmp/hashes# hashcat -m 1000 nthashes /tmp/wordlists/passlist
Initializing hashcat v2.00 with 1 threads and 32mb segment-size...

Added hashes from file nthashes: 12 (1 salts)

209c6174da490caeb422f3fa5a7ae634:admin
b385c9b5725dc63526b78a2abb83c380:securepw
4f892a810f871bc64ddc16b9322204e9:tooth
41609a615f89f93330f9b22bd5ee7015:penstate
462809345fb663a5af07ad52239f3710:yarnqx
b7bc675667b419fded6816c20f552b51:defaultpw
d77cdad829e609a3f45db63ac117c92b:scottie
23124fe0eef6dd8b53cb178f78d5a9c4:guestlist
1f90f71ffed8339f346a81ebc0960725:floridasun
3479bea2a46ad18b45f81816d261068a:lasocial
90236d30e7c61b90ce4f53258228de74:gustwind
e90bc0cfdccffd13650227f501c71f3e:traptim

All hashes have been recovered

Input.Mode: Dict (/tmp/wordlists/passlist)
Index.....: 1/1 (segment), 55 (words), 421 (bytes)
Recovered.: 12/12 hashes, 1/1 salts
Speed/sec.: - plains, - words
Progress..: 48/55 (87.27%)
Running...: 00:00:00:01
Estimated.: --:--:--:--


Started: Tue Jul 24 15:38:10 2018
Stopped: Tue Jul 24 15:38:11 2018
```

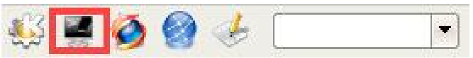
After a few seconds, a successful *hashcat* output should appear. Notice that all 12 *NTHashes* have been cracked with their associated passwords.

8. Leave the *terminal* open to continue with the next task.

3 Obtaining and Cracking Linux /etc/shadow

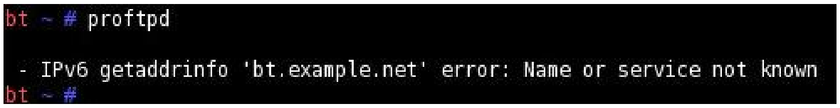
3.1 Obtaining the /etc/shadow Remotely

1. Launch the **DVL** virtual machine.
2. Log in as `root`, using `toor` as the password.
3. At the prompt, type `startx` followed by pressing the **Enter** key to launch the *GUI*.
4. Open a new terminal window by clicking on the **Terminal** icon located on the bottom menu pane.



5. Type the command below to initialize the FTP service.

```
bt ~# proftpd
```



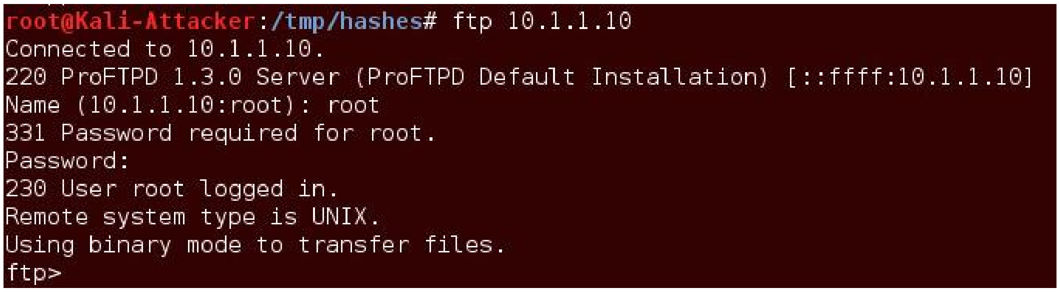
```
bt ~ # proftpd

 - IPv6 getaddrinfo 'bt.example.net' error: Name or service not known
bt ~ #
```

Please Note

Allow 30 seconds for it to load. Ignore the *IPv6* error message.

6. Change focus to the **Kali** system.
7. While on the **Kali** system, focus on the **terminal** window. Remotely **FTP** into the **DVL Server**. When asked for a username, type `root` followed by pressing **Enter**. When prompted for the password, type `toor` followed by pressing **Enter**.

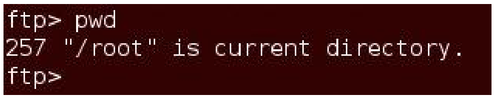
```
root@Kali-Attacker:/tmp/hashes# ftp 10.1.1.10
```



```
root@Kali-Attacker:/tmp/hashes# ftp 10.1.1.10
Connected to 10.1.1.10.
220 ProFTPD 1.3.0 Server (ProFTPD Default Installation) [::ffff:10.1.1.10]
Name (10.1.1.10:root): root
331 Password required for root.
Password:
230 User root logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

8. Once connected to the *DVL* system via *FTP*, print the current directory.

```
ftp> pwd
```

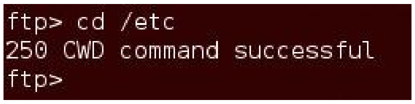


```
ftp> pwd
257 "/root" is current directory.
ftp>
```

Notice that the output points to the */root* directory.

9. Change to the **/etc** directory.

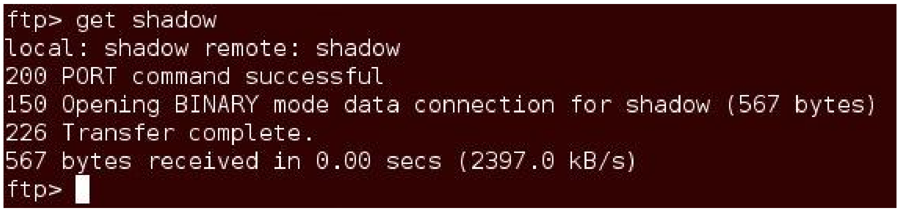
```
ftp> cd /etc
```



```
ftp> cd /etc
250 CWD command successful
ftp>
```

10. Download the local **shadow** file on the *DVL* system via *FTP*.

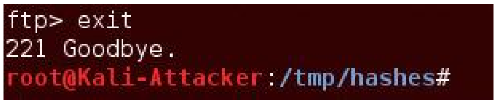
```
ftp> get shadow
```



```
ftp> get shadow
local: shadow remote: shadow
200 PORT command successful
150 Opening BINARY mode data connection for shadow (567 bytes)
226 Transfer complete.
567 bytes received in 0.00 secs (2397.0 kB/s)
ftp>
```

11. After the *shadow* file successfully downloads, close the **FTP** session.

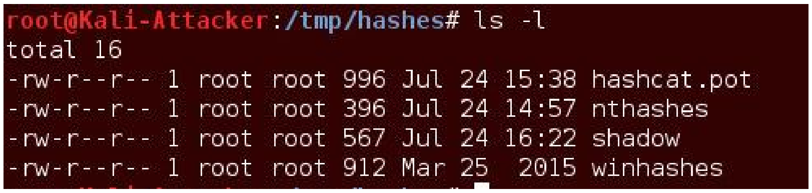
```
ftp> exit
```



```
ftp> exit
221 Goodbye.
root@Kali-Attacker:/tmp/hashes#
```

12. Verify that the *shadow* file has transferred into the current directory (*/tmp/hashes*).

```
root@Kali-Attacker:/tmp/hashes# ls -l
```



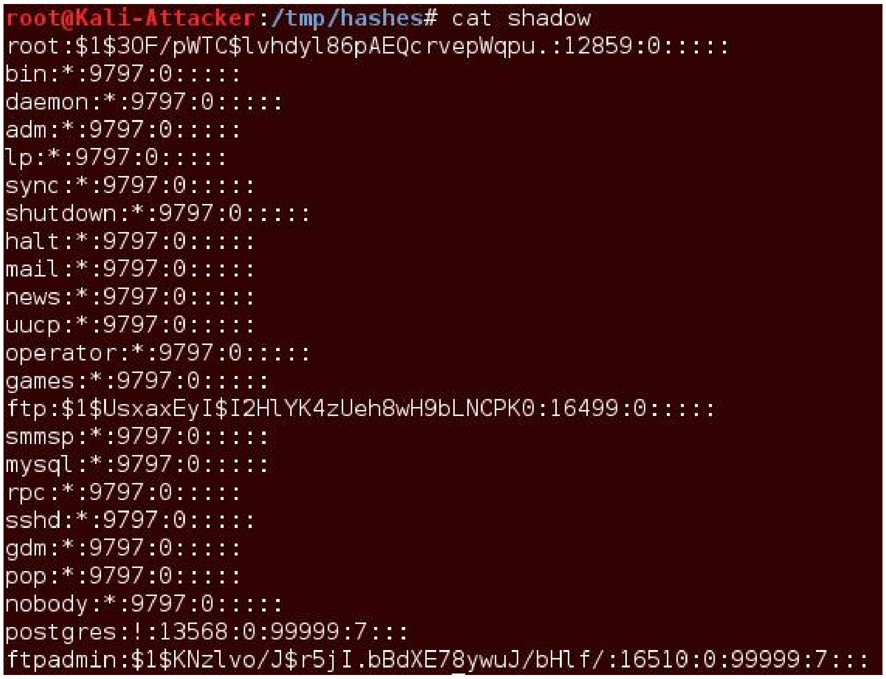
```
root@Kali-Attacker:/tmp/hashes# ls -l
total 16
-rw-r--r-- 1 root root 996 Jul 24 15:38 hashcat.pot
-rw-r--r-- 1 root root 396 Jul 24 14:57 nthashes
-rw-r--r-- 1 root root 567 Jul 24 16:22 shadow
-rw-r--r-- 1 root root 912 Mar 25  2015 winhashes
```

13. Leave the *terminal* open to continue with the next task.

3.2 Cracking /etc/shadow With Johnny

1. While on the *Kali* system, observe the content of the recently transferred **shadow** file. Notice the list of users.

```
root@Kali-Attacker:/tmp/hashes# cat shadow
```

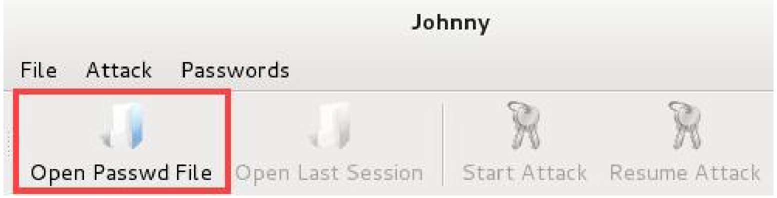


```
root@Kali-Attacker:/tmp/hashes# cat shadow
root:$1$30F/pWTC$lvhdyl86pAEQcrvepWqpu.:12859:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:$1$UsxaxEyI$I2HlYK4zUeh8wH9bLNCPK0:16499:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
sshd:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
nobody:*:9797:0:::::
postgres:!:13568:0:99999:7:::
ftpadmin:$1$KNzlvo/J$r5jI.bBdXE78ywuJ/bHlf/:16510:0:99999:7:::
```

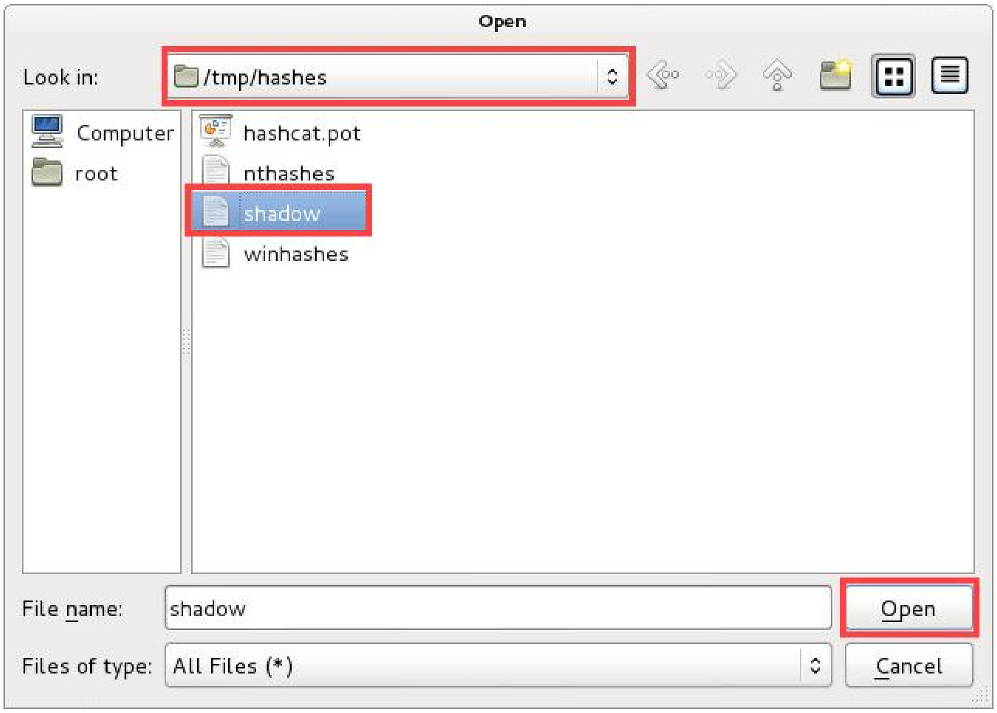
2. Start the *GUI* password cracking application, **johnny**. This is the same as John the Ripper but with a graphical user interface. Type the command below in the *terminal* window. Press **Enter**.

```
root@Kali-Attacker:/tmp/hashes# johnny
```

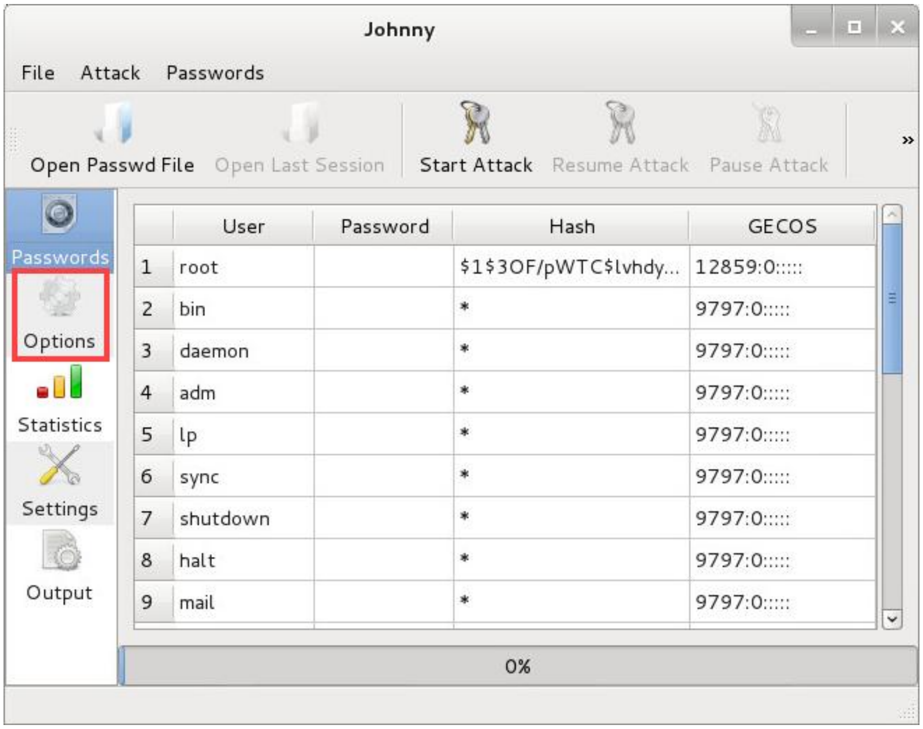
3. A new window appears. Click on the **Open Passwd File** icon.



4. In the new *Open* window, navigate to the **/tmp/hashes** directory. Select the **shadow** file and click on the **Open** button.

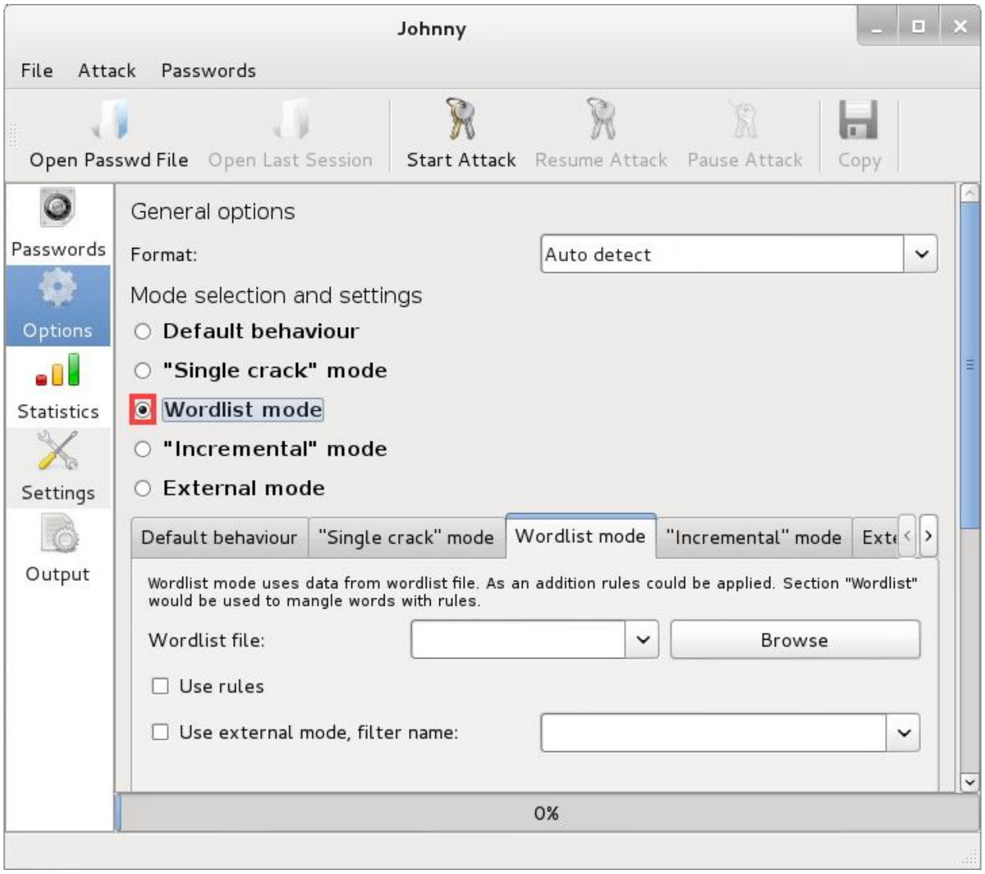


5. On the *Passwords* screen, notice how each column is populated with its associated values. Click on the **Options** icon located in the left pane.



	User	Password	Hash	GECOS
1	root		$1$3OF/pWTC$lvhdy...	12859:0:::::
2	bin		*	9797:0:::::
3	daemon		*	9797:0:::::
4	adm		*	9797:0:::::
5	lp		*	9797:0:::::
6	sync		*	9797:0:::::
7	shutdown		*	9797:0:::::
8	halt		*	9797:0:::::
9	mail		*	9797:0:::::

6. On the Options screen, select the radio button next to **Wordlist mode**. Notice the pane on the bottom changes to the *Wordlist* tab.



General options

Format: Auto detect

Mode selection and settings

○ Default behaviour

○ "Single crack" mode

● Wordlist mode

○ "Incremental" mode

○ External mode

Wordlist mode uses data from wordlist file. As an addition rules could be applied. Section "Wordlist" would be used to mangle words with rules.

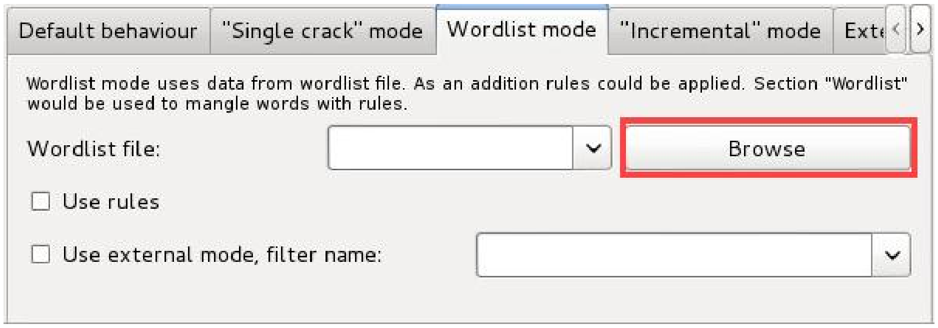
Wordlist file: Browse

□ Use rules

□ Use external mode, filter name:

0%

7. In the bottom pane, click on the **Browse** button.



Wordlist mode uses data from wordlist file. As an addition rules could be applied. Section "Wordlist" would be used to mangle words with rules.

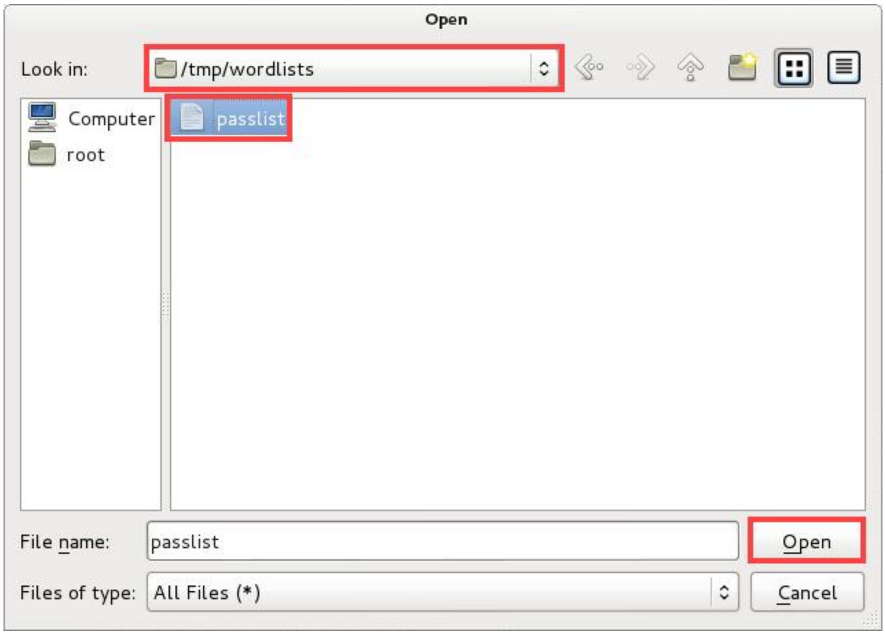
Wordlist file: Browse

□ Use rules

□ Use external mode, filter name:

Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com

8. In the *Open* window, navigate to the **/tmp/wordlists** directory. Select the **passlist** file and click on the **Open** button.

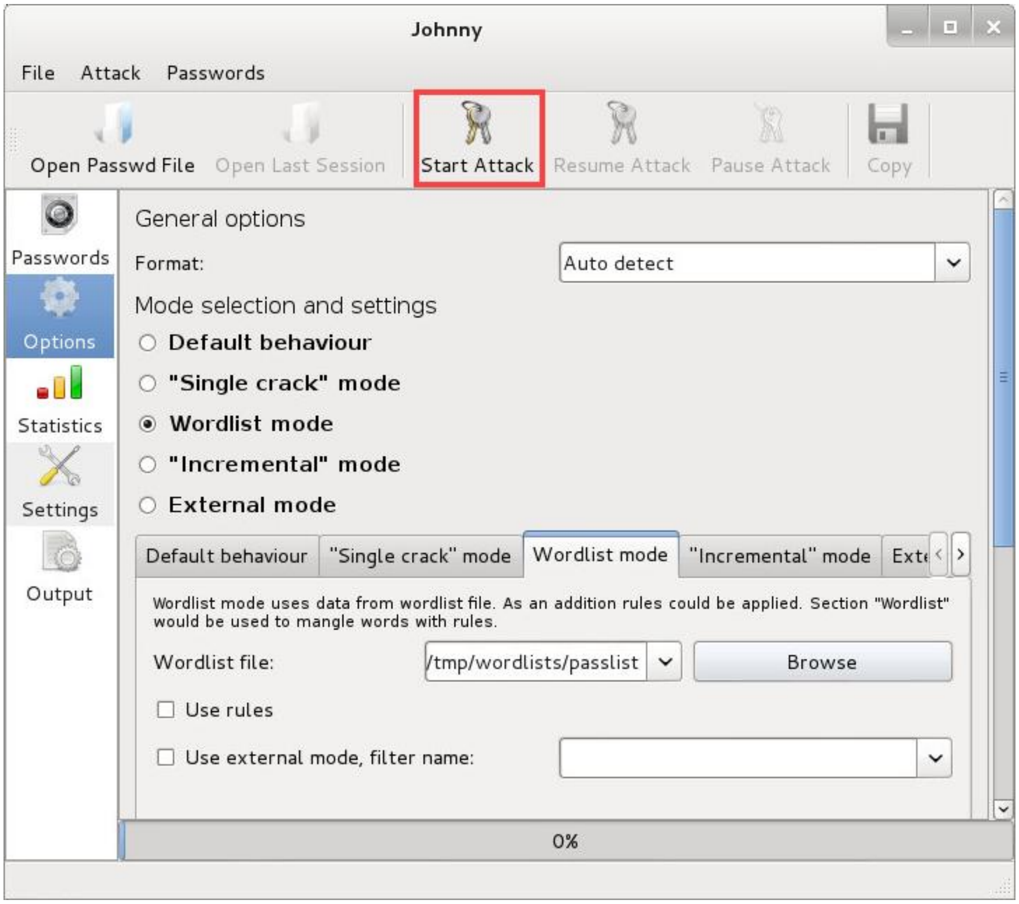


Look in: /tmp/wordlists

File name: passlist

Files of type: All Files (*)

9. Verify that the *Wordlist file* is assigned to **/tmp/wordlists/passlist**. Click the **Start Attack** icon located on the top menu.



General options

Format: Auto detect

Mode selection and settings

○ Default behaviour

○ "Single crack" mode

● Wordlist mode

○ "Incremental" mode

○ External mode

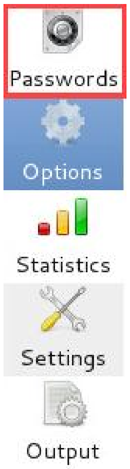
Wordlist mode uses data from wordlist file. As an addition rules could be applied. Section "Wordlist" would be used to mangle words with rules.

Wordlist file: /tmp/wordlists/passlist

☐ Use rules

☐ Use external mode, filter name:

10. Notice the progression bar at the bottom. When it reaches 100%, click the **Passwords** icon from the menu located on the left to view the results.



11. Notice the *Password* column for the usernames *root*, *ftp*, and *ftpadmin* have been cracked with the password printed in plain text.
12. The lab is now complete; you may end the reservation.

Copyright © 2018 Network Development Group, Inc. www.netdevgroup.com