



SECURITY+ LAB SERIES

Lab 8: Mitigation and Deterrent Techniques – Password Cracking

Document Version: **2015-09-24**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction	3
Lab Topology	4
Lab Settings	5
Pre-Lab Setup	6
1 Cracking Linux Passwords	7
1.1 Creating User Accounts and Groups	7
1.2 Cracking Passwords on a Linux System Using John the Ripper	10
2 Cracking Windows Passwords	11
2.1 Cracking Windows Passwords Using Hashcat	11
3 Obtaining and Cracking Linux /etc/shadow	14
3.1 Obtaining the /etc/shadow Remotely	14
3.2 Cracking /etc/shadow With Johnny	16



Introduction

The material in this lab aligns to the following learning objective:

- **Objective 3.2:** Summarize various types of attacks
- **Objective 3.6:** Analyze a scenario and select the appropriate type of mitigation and deterrent techniques

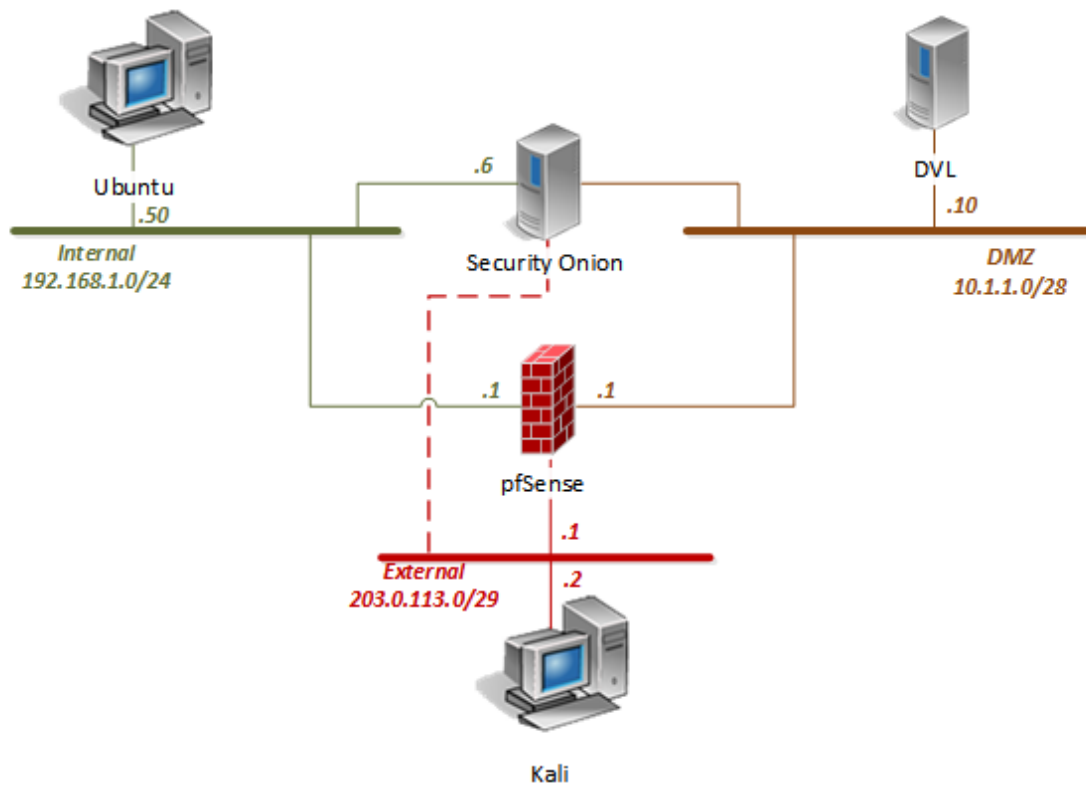
More information about individual objectives and their sections can be found in CompTIA document SY0-401, which is available from the CompTIA website.

In this lab, you will be conducting password-cracking techniques using various tools. You will be performing the following tasks:

1. Cracking Linux Passwords
2. Cracking Windows Passwords
3. Obtaining and Cracking Linux /etc/shadow



Lab 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.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Ubuntu	192.168.1.50	student	securepassword
DVL Server	10.1.1.10	root	toor
Security Onion	192.168.1.6	soadmin	mypassword
pfSense	192.168.1.1 10.1.1.1 203.0.113.1	admin	pfsense
Kali	203.0.113.2	root	toor



Pre-Lab Setup

Before continuing to Task 1, log into the following systems below as instructed.

I. Kali

1. On the login screen, select **Other**.
2. When presented with the username, type **root**. Press **Enter**.
3. When prompted for the password, type **toor**. Press **Enter**.
4. Minimize the *PC viewer* window.

II. DVL

1. On the login screen, type **root**. Press **Enter**.
2. When prompted for a password, type **toor**. Press **Enter**.
3. When presented with the user prompt, type **startx**. Press **Enter**.
4. Once the desktop boots close the *X Desktop* window.
5. Minimize the *PC viewer* window.



1 Cracking Linux Passwords

1.1 Creating User Accounts and Groups

1. Open the **Kali PC Viewer**. If closed, click on the **Kali** icon on the *Topology* page.



2. Open a new **Terminal** window by clicking on the **Terminal** icon located on the top menu pane.
3. Type the command below to view the groups on the system:

```
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:
```

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

4. Populate the group list first by adding two more groups: **juniors** and **seniors**.

```
groupadd juniors
```

```
groupadd seniors
```

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

5. Confirm that the groups have been added.

```
cat /etc/group | grep "seniors"
```

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

Notice the group ID *1002*.

```
cat /etc/group | grep "juniors"
```

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

Notice the group ID *1001*.

6. Type the command below to view the user accounts on the system.

```
cat /etc/passwd
```

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

```
useradd elmo -g seniors
```

```
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 in order to enter the next command.

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

```
useradd lisa -g juniors
```

```
useradd homer -g juniors
```

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


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

```
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 in *Task 1.1, Step 5*. Note that the second ID field is assigned as the group ID.

- View the **/etc/shadow** file and observe the entries next to the newly created accounts.

```
cat /etc/shadow
```

```
elmo:!:16541:0:99999:7:::
oscar:!:16541:0:99999:7:::
lisa:!:16541:0:99999:7:::
homer:!:16541:0:99999:7:::
```

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

- Configure passwords for the users: **elmo**, **oscar**, **lisa** and **homer**.

```
passwd elmo
```

- Type **123123** twice as the password.

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

```
passwd oscar
```

- Type **sanjose** twice as the password.

```
passwd lisa
```

- Type **academic** twice as the password.

```
passwd homer
```

- Type **acapulco** twice as the password.

16. Type the command below to view the created users in the **shadow** file.



```
tail -n -4 /etc/shadow
```

```
root@Kali-Attacker:~# tail -n -4 /etc/shadow
elmo:$6$9DX5VZ.a$r0EMGumIi6Zew25iEgqdLUItf7Mww3wDCBWH6pc1Adv0wZV4YRgAa8GcFc5Twu1Wdk6LZ.u0Iy19pQ3TIoW
IV/:16540:0:99999:7:::
oscar:$6$4VS2cP/. $jcoKKf5yBh8q4TLF0xLj7zRJ8cBw3ivfH.wPqRanbyJMdF2c6sEHaaxUH2Ke2pcXWjq5GRLLEIL8LYlNky
I0Y/:16540:0:99999:7:::
lisa:$6$7TQhC8uL$4/XPrUZBYdghw0kk87PBihxYn26z.ZwhBLJ57iaLiT1feanISDiP6Q2Yc4uvjbB7aMme04tX/mocEiLw4nj
LY/:16540:0:99999:7:::
homer:$6$bs.XDb6L$FQjsVJyNrSI.j0HXTS5K6s.z5oyhTSC.5i/.bdP3j5ZyI091z4AF/owVDaUKC/4qhnAcsQX3RNFdBb7305
i4S1:16540:0:99999:7:::
```

Notice how the fields next to the new user accounts have changed when compared to what was seen earlier in *Task 1, Step 11*. They are now populated with password hashes.

17. Leave the **Terminal** open for the next task.

1.2 Cracking Passwords on a Linux System Using John the Ripper

1. Before using *John the Ripper*, type the command below within a **Terminal** window to view the available options that can be used with the application.

```
john -help
```



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

```
john /etc/shadow -wordlist=/tmp/wordlists/passlist
```

```
root@Kali-Attacker:~# john /etc/shadow -wordlist=/tmp/wordlists/passlist
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypto"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 5 password hashes with 5 different salts (sha512crypt [32/32])
toor          (root)
acapulco      (homer)
sanjose       (oscar)
123123        (elmo)
academic      (lisa)
guesses: 5    time: 0:00:00:01 DONE (Thu Apr 16 16:01:50 2015) c/s: 162 trying:
123123
```

Notice the successfully cracked passwords.

3. Leave the **Terminal** window open for 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/hashtes** directory.

```
cd /tmp/hashtes
```

3. View the winhashes file extracted from a Windows system.

```
cat winhashes
```

```
root@Kali-Attacker:/tmp/hashtes# 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::
tmayr:252E471234E267F24841ED0AA9280B7A:1F90F71FFED8339F346A81EBC0960725::
nben:3D455B85B63BB696F500944B53168930:3479BEA2A46AD18B45F81816D261068A::
ikumar:457529528CD3A0584A3B108F3FA6CB6D:90236D30E7C61B90CE4F53258228DE74::
openny:C1716F5110D2F358AAD3B435B51404EE:E90BC0CFDCCFFD13650227F501C71F3E::root@
```

Notice the username list with their associated password hashes.

4. Parse out the **NTLM** hashes from the **winhashes** file.

```
cat winhashes | awk -F":" '{print $3}'
```

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

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

```
cat winhashes | awk -F":" '{print $3}' > ntlmhashes
```

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

- Verify that the **NTLM** hashes have outputted correctly.

```
cat ntlmhashes
```

```
root@Kali-Attacker:/tmp/hashes# cat ntlmhashes
209C6174DA490CAEB422F3FA5A7AE634
B385C9B5725DC63526B78A2ABB83C380
4F892A810F871BC64DDC16B9322204E9
41609A615F89F93330F9B22BD5EE7015
462809345FB663A5AF07AD52239F3710
B7BC675667B419F0ED6816C20F552B51
D77CDAD829E609A3F45DB63AC117C92B
23124FE0EEF6DD8B53CB178F78D5A9C4
1F90F71FFED8339F346A81EBC0960725
3479BEA2A46AD18B45F81816D261068A
90236D30E7C61B90CE4F53258228DE74
E90BC0CFDCCFFD13650227F501C71F3E
```



- Initiate **Hashcat** against the **ntlmhashes** file with the help of the **passlist** dictionary file.

```
hashcat -m 1000 ntlmhashes /tmp/wordlists/passlist
```

If asked to accept a EULA, type **YES** followed by pressing **Enter**.

```
1. All copyrights to this program are exclusively owned by the author --
atom

2. You may only use this software for legal purposes.

3. THIS PROGRAM IS DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS
EXPRESSED OR IMPLIED. YOU USE THIS SOFTWARE AT YOUR OWN RISK. THE AUTHOR
WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER
KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.

4. If your countries law(s) do not allow restrictions as in (3.) you
need to get an additional, written and individual license by the
copyright holder to use this software. Unless you have such a
license, you are not allowed to use the software.

5. You may not rent, lease, sell, modify, decompile, disassemble, or reverse
engineer this program or any subset of this program. Any such unauthorized
use shall result in immediate and automatic termination of this license and
may result in criminal and/or civil prosecution.

6. Redistribution of the original package, in whole or in part, or a modified
version as needed for distribution packaging is permitted without restrictions.

Enter YES in uppercase if you accept this EULA:
YES
```

```

root@Kali-Attacker:/tmp/hashe# hashcat -m 1000 ntlmhashes /tmp/wordlists/passlist
Initializing hashcat v0.49 with 1 threads and 32mb segment-size...

Added hashes from file ntlmhashes: 12 (1 salts)

NOTE: press enter for status-screen

209c6174da490caeb422f3fa5a7ae634:admin
b385c9b5725dc63526b78a2abb83c380:securepw
4f892a810f871bc64ddc16b9322204e9:tooth
41609a615f89f9330f9b22bd5ee7015:penstate
462809345fb663a5af07ad52239f3710:yarnqx
b7bc675667b419fdded6816c20f552b51: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), 54 (words), 410 (bytes)
Recovered.: 12/12 hashes, 1/1 salts
Speed/sec.: - plains, - words
Progress...: 44/54 (81.48%)
Running....: -:--:--:--
Estimated.: -:--:--:--

```

After a few seconds, a successful **Hashcat** output should appear. Notice that all 12 NTLM hashes have been cracked with their respective passwords.

8. Leave the **Terminal** window open for the next task.

3 Obtaining and Cracking Linux /etc/shadow

3.1 Obtaining the /etc/shadow Remotely

1. Open the **DVL PC Viewer**. If closed, click on the **DVL** icon on the *Topology* page.



2. While on accessing the *DVL Server*, open a new **Terminal** window by clicking on the **Terminal** icon located on the bottom menu pane.



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

```
proftpd
```

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

Ignore the IPv6 message.

4. Change focus to the **Kali** system.
5. While on the **Kali** system, navigate to the **Terminal** window.
6. Change to the **/tmp/hashes** directory.

```
cd /tmp/hashes
```

7. Remotely **FTP** into the **DVL Server**.

```
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>
```

- a. When asked for name, type **root** followed by pressing **Enter**.

- b. When prompted for the password, type **toor** followed by pressing **Enter**.
8. Print the current directory.

```
pwd
```

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

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

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

```
cd /etc
```

10. Start the download process in acquiring the **/etc/shadow** file.

```
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 (2782.5 kB/s)
ftp>
```

Notice the successful file transfer.

11. Close the **FTP** session.

```
exit
```

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

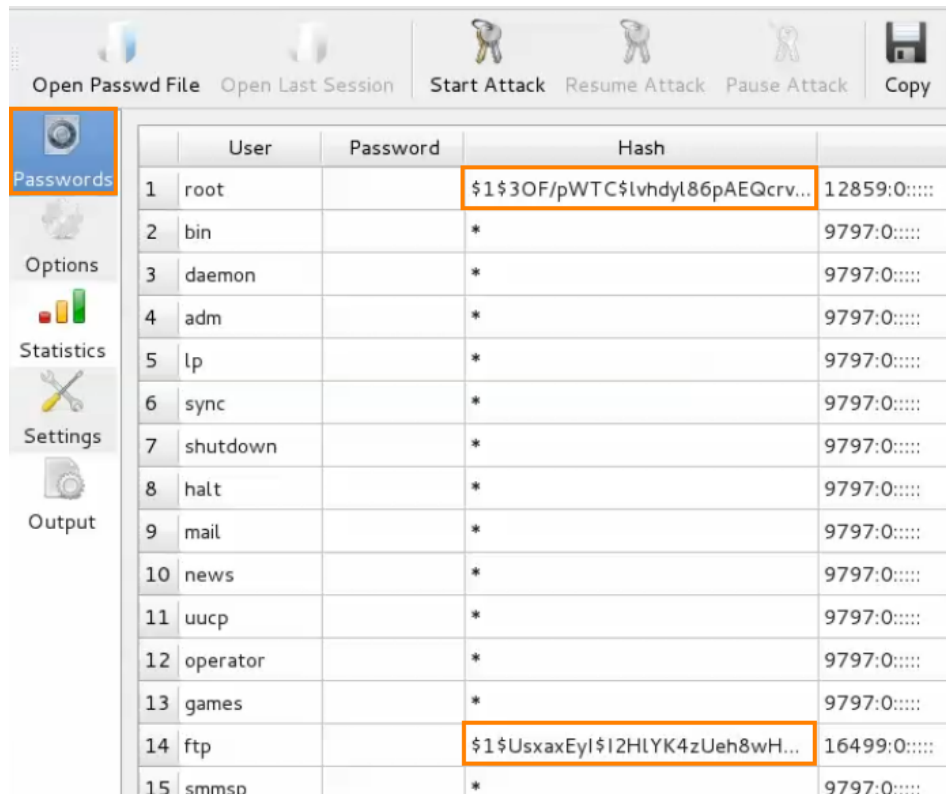
12. Verify that the **shadow** file has transferred into the current directory (**/tmp/hashes**).

```
ls -l
```

```
root@Kali-Attacker:/tmp/hashes# ls -l
total 16
-rw-r--r-- 1 root root 996 Apr 16 16:06 hashcat.pot
-rw-r--r-- 1 root root 396 Apr 16 16:04 ntlmhashes
-rw-r--r-- 1 root root 567 Apr 16 16:10 shadow
-rw-r--r-- 1 root root 912 Mar 25 15:27 winhashes
root@Kali-Attacker:/tmp/hashes#
```

13. Leave the **Terminal** open for the next task.

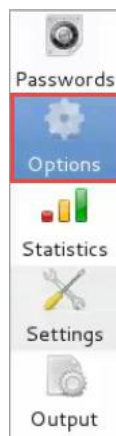
- Verify you are viewing the **Passwords** screen (if not, click the Passwords icon on the left).



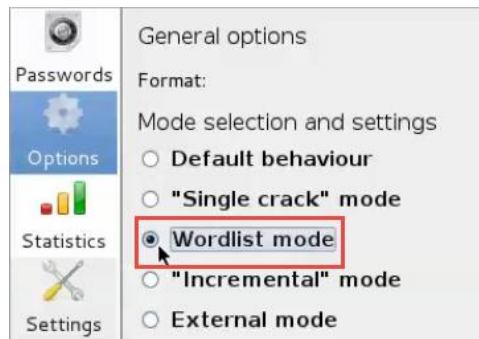
	User	Password	Hash	
1	root		\$1\$30F/pWTC\$lvhdyl86pAEQcrv...	12859:0:....
2	bin		*	9797:0:....
3	daemon		*	9797:0:....
4	adm		*	9797:0:....
5	lp		*	9797:0:....
6	sync		*	9797:0:....
7	shutdown		*	9797:0:....
8	halt		*	9797:0:....
9	mail		*	9797:0:....
10	news		*	9797:0:....
11	uucp		*	9797:0:....
12	operator		*	9797:0:....
13	games		*	9797:0:....
14	ftp		\$1\$UsxaxEyl\$I2HLYK4zUeh8wH...	16499:0:....
15	smmsp		*	9797:0:....

Notice how each column is populated with its respective values.

- Click on the **Options** icon as one of the left menu options.

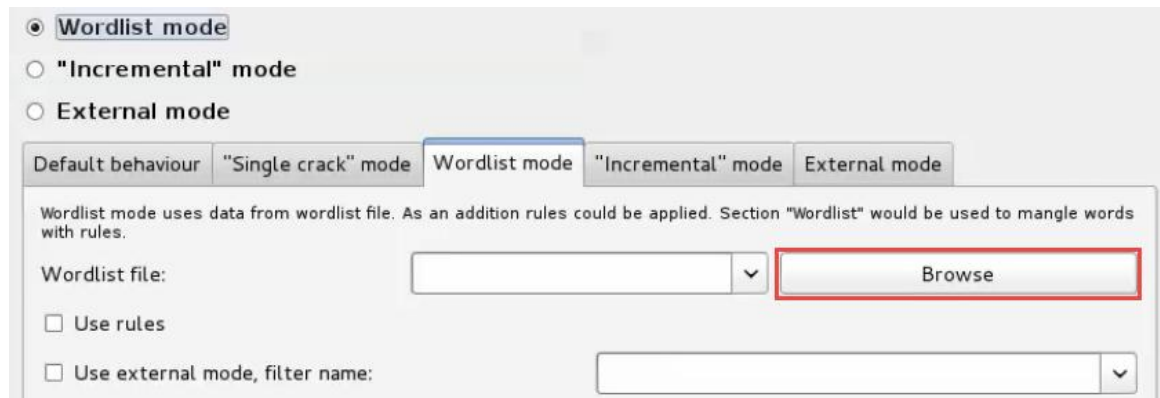


7. Select to use the **Wordlist** mode.

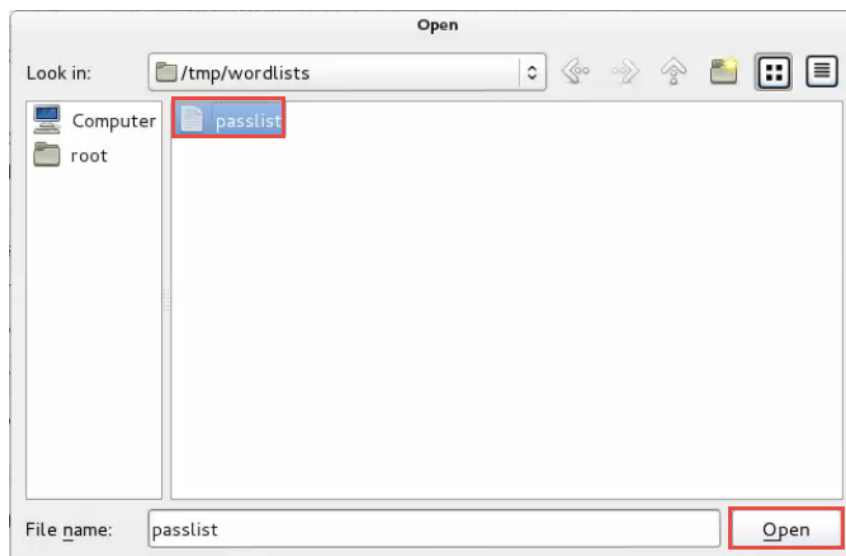


Notice the tab on the bottom change to *Wordlist mode*.

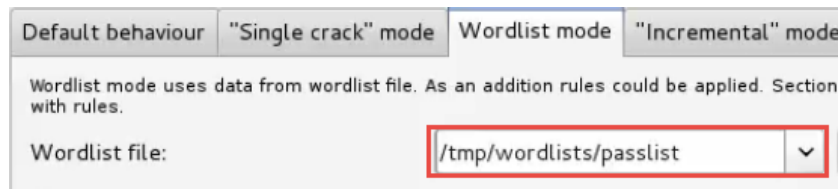
8. Within the tabbed area, click on the **Browse** button.



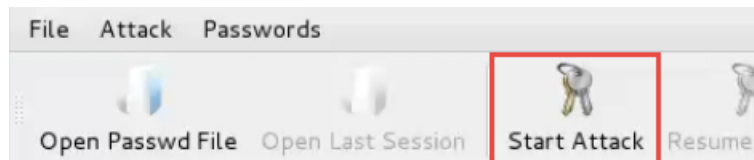
9. In the File Explorer window, navigate through **Computer > / > tmp > wordlists**. Select the **passlist** file and click on the **Open** button.



- Verify that the *Wordlist file* is assigned to **/tmp/wordlists/passlist**.

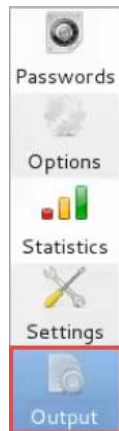


- Once verified, click the **Start** Attack icon located on the top menu.



After a couple of seconds, notice the progress bar located at the bottom of the window reach 100%.

- Click the **Output** icon from the menu located on the left to view the results.



- Notice the output with the successfully cracked password hashes.

```
guesses: 3 time: 0:00:00:00 DONE (Thu Apr 16 16:12:55 2015) c/s: 2400 trying: admin - passj1
Use the "--show" option to display all of the cracked passwords reliably
Loaded 3 password hashes with 3 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
toor      (root)
ftp       (ftpadmin)
ftp       (ftp)
```

- Close** the program and all remaining windows.