



ETHICAL HACKING LAB SERIES

Lab 5: Password Cracking with John the Ripper and Hashcat

Material in this Lab Aligns to the Following Certification Domains/Objectives		
Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives	SANS GPEN Objectives
5: System Hacking 18: Cryptography	15: Password Attacks	1: Advanced Password Attacks 2: Attacking Password Hashes 10: Password Attacks

Document Version: 2016-03-09

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

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

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC² is a registered trademark of EMC Corporation.

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Generating Password Lists for Password Cracking	6
2 Create User Accounts to be Cracked	8
3 Password Cracking Using John the Ripper	10
4 Password Cracking Using Hashcat	11

Introduction

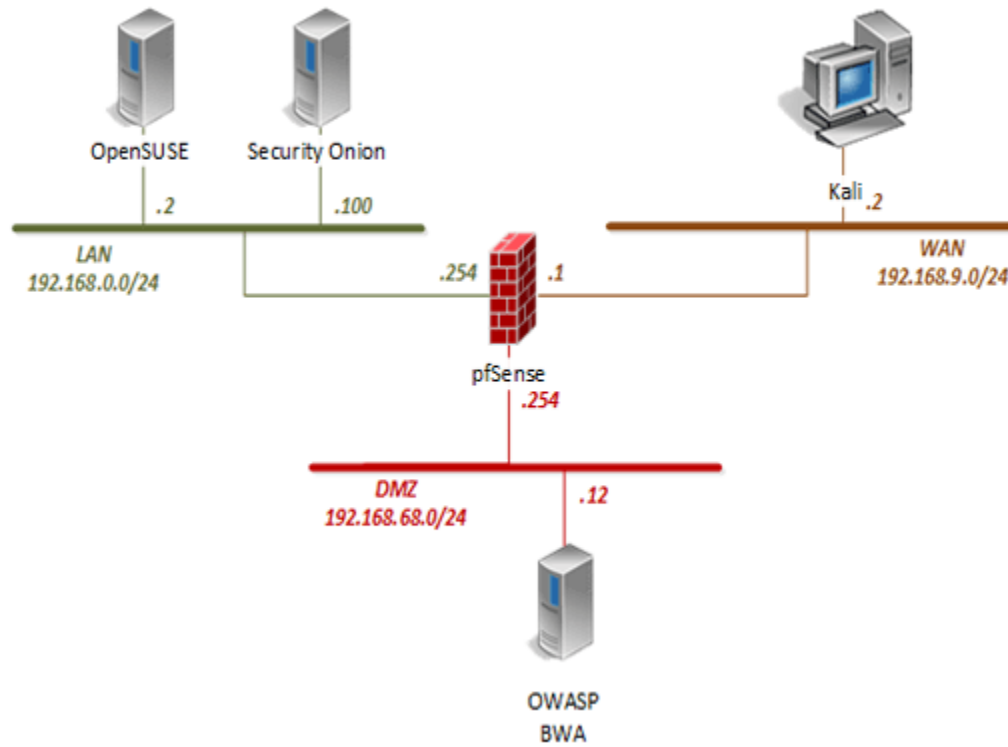
This lab introduces the methodologies used for cracking both Linux and Windows passwords using two different tools. In addition, this lab examines how to create supporting wordlists in order to create dictionaries for the tools.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Generating Password Lists for Password Cracking
2. Create User Accounts to be Cracked
3. Password Cracking Using John the Ripper
4. Password Cracking Using Hashcat

Pod 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)
Kali Linux	192.168.9.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Generating Password Lists for Password Cracking

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.



6. In the new *Terminal* window, observe the options available for the *cewl* tool. This tool is used to gather text from a website. Type the command below followed by pressing the **Enter** key.

```
cewl -help
```

7. Target the *OWASP* VM using the *cewl* tool and copy the text to a file named *owaspwords.txt*. Enter the command below.

```
cewl -w owaspwords.txt -d 2 -m 5 192.168.68.12
```

Wait about 1-2 minutes until the prompt reappears before continuing to the next step.

8. Once the prompt appears back on the screen, view the contents of the *owaspwords.txt* file. Enter the command below.

```
cat owaspwords.txt
```

Notice the amount of words in each single line. These can easily be used in the current format for password cracking.

9. *Crunch* is also another utility that can be used to generate passwords. At the prompt, type the command below followed by pressing the **Enter** key to receive generalized information about the crunch utility.

```
crunch
```

10. Using *crunch*, generate a set of passwords that are a minimum of **4** characters and a maximum of **8** characters in length, made up of all the **letters of the alphabet in lowercase** only. Enter the command below.

```
crunch 4 8 charset.lst lalpha -o list.txt
```

```
root@Kali2:~# crunch 4 8 charset.lst lalpha -o list.txt
Crunch will now generate the following amount of data: 429791427 bytes
409 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 48426741
crunch: 74% completed generating output
crunch: 100% completed generating output
```

11. Once *crunch* is finished generating passwords, combine the wordlist from the *OWASP* web server and the randomly generated *crunch* wordlist.

```
cat owaspwords.txt list.txt > mylist.txt
```

12. Add the password list from *John the Ripper* into the combined **mylist.txt** file.

```
cat /usr/share/john/password.lst >> mylist.txt
```

2 Create User Accounts to be Cracked

1. Create two fake user accounts. Enter the two commands below separately.

```
useradd fake3
```

```
useradd fake4
```

```
root@Kali2:~# useradd fake3
root@Kali2:~# useradd fake4
root@Kali2:~#
```

2. Assign the user **fake3** a new password by entering the command below.

```
passwd fake3
```

3. When prompted for a password, type **123456**. Press **Enter**.
4. When prompted to retype the password, type **123456** once more. Press **Enter**.

```
root@Kali2:~# passwd fake3
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@Kali2:~#
```

5. Assign the user **fake4** a new password by entering the command below.

```
passwd fake4
```

6. When prompted for a password, type **password**. Press **Enter**.
7. When prompted to retype the password, type **password** once more. Press **Enter**.

```
root@Kali2:~# passwd fake4
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@Kali2:~#
```

8. Confirm that the new users have passwords assigned to them in the **/etc/shadow** file.

```
cat /etc/shadow
```

```
fake3:$6$Cke4WPeU$9pb6yvU4VJLRJxjy5CQID0RDZKokxCSiuxuT1zQVQZV0j8536FCcQ61da4iFcx
net14n3UjcGC60mQ2MNe5AU0:16786:0:99999:7:::
fake4:$6$iSfnYQPJ$Qj3hB4XZVNytEkKI2D7aFrSkS/KIP8IpMxvJPi6ucCfDaq8BC.iEe.r0tI18Pl
teLXRbATTY4.Fimb3i8ER.B0:16786:0:99999:7:::
```

Notice the two names with hashed passwords.

9. Combine the two files that make updates to the user's credentials; both **/etc/passwd** and **/etc/shadow**.

```
unshadow /etc/passwd /etc/shadow > hashes.txt
```

10. Edit the hashes.txt file so that it is narrowed down to only two accounts that need to be cracked.

```
cat hashes.txt | grep fake* > hashes2.txt
```

11. View the contents of the **hashes2.txt** file.

```
cat hashes2.txt
```

3 Password Cracking Using John the Ripper

1. *John the Ripper* can be used either through the command line or the GUI version. Start by typing the command below to become familiarized with the command line version. Press **Enter**.

```
john
```



2. Use *John's* default password list to try to crack the passwords in the *hashes2.txt* file.

```
john -wordlist=/usr/share/john/password.lst hashes2.txt
```

Once finished, notice the successful password crack attempt given from the john output.

3. View the cracked passwords using john.

```
john --show hashes2.txt
```

```
root@Kali2:~# john --show hashes2.txt
fake3:123456:1002:1003::/home/fake3:/bin/sh
fake4:password:1003:1004::/home/fake4:/bin/sh

2 password hashes cracked, 0 left
```

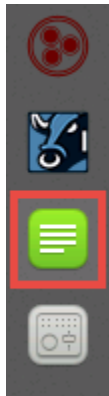
4 Password Cracking Using Hashcat

1. *Hashcat* can be used for advanced password cracking. Enter the command below to become familiarized with the options made available.

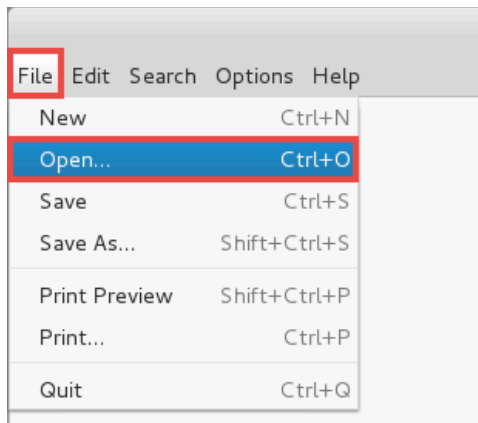
```
hashcat -help | more
```

Press the **Spacebar** to skip to the next page or the **Enter** key to skip by each line. Press **Q** to quit the help screen at any given time.

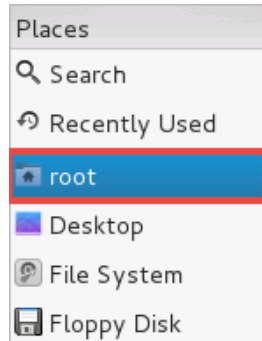
2. Click on the **Leafpad** icon located in the left panel to open the text editor.



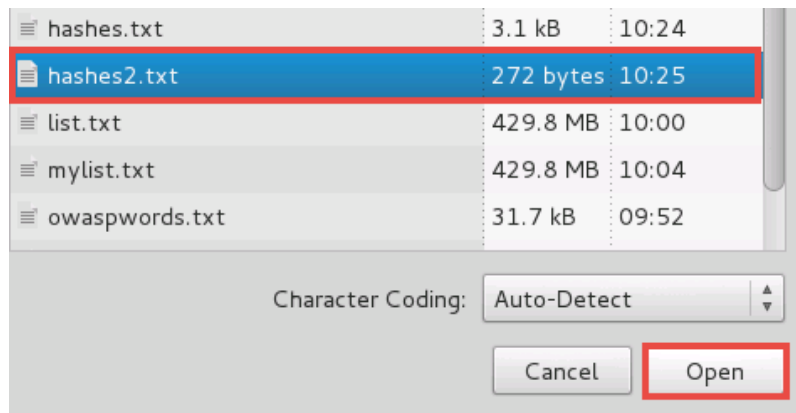
3. On the *Leafpad* window, click on the **File** tab and select **Open**.



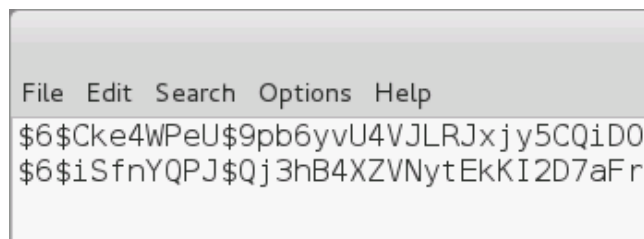
4. Click on the **root** file directory underneath *Places* in the left pane.



5. In the middle pane, select the **hashes2.txt** file and click **Open**.

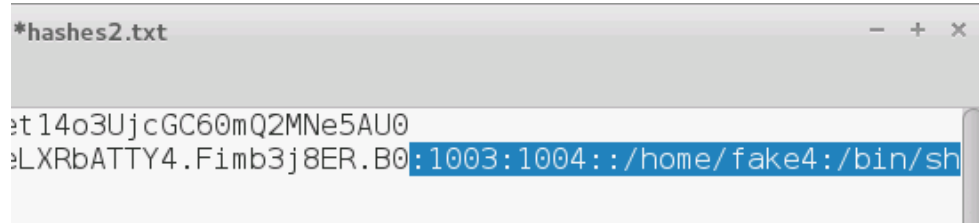


6. Using the file editor, remove the account names, **fake3** and **fake4**, along with the **colon** as shown below.



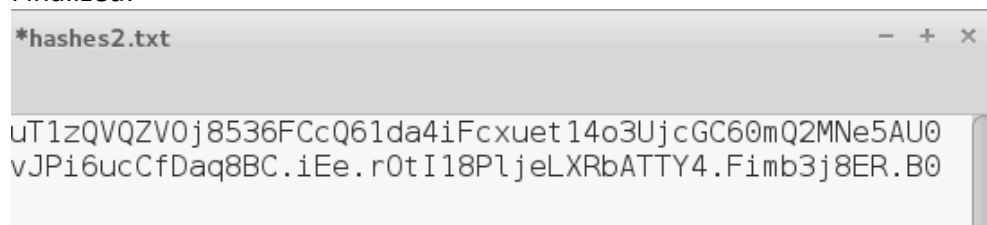
7. Using the arrows keys, move the cursor towards the right and remove all the information to the right of the colon ":" and the colon itself as shown below. Do this for both lines.

Remove the selected:



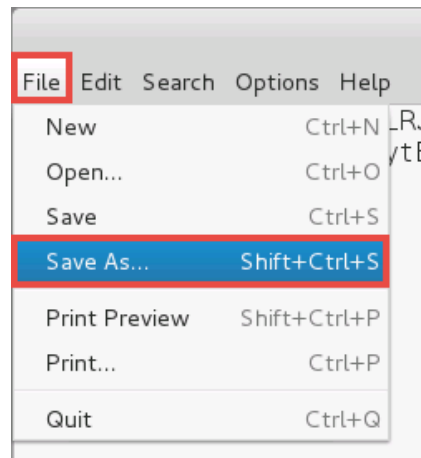
```
*hashes2.txt
:t 14o3UjcGC60mQ2MNe5AU0
:LXRbATTY4.Fimb3j8ER.B0:1003:1004::/home/fake4:/bin/sh
```

Finalized:

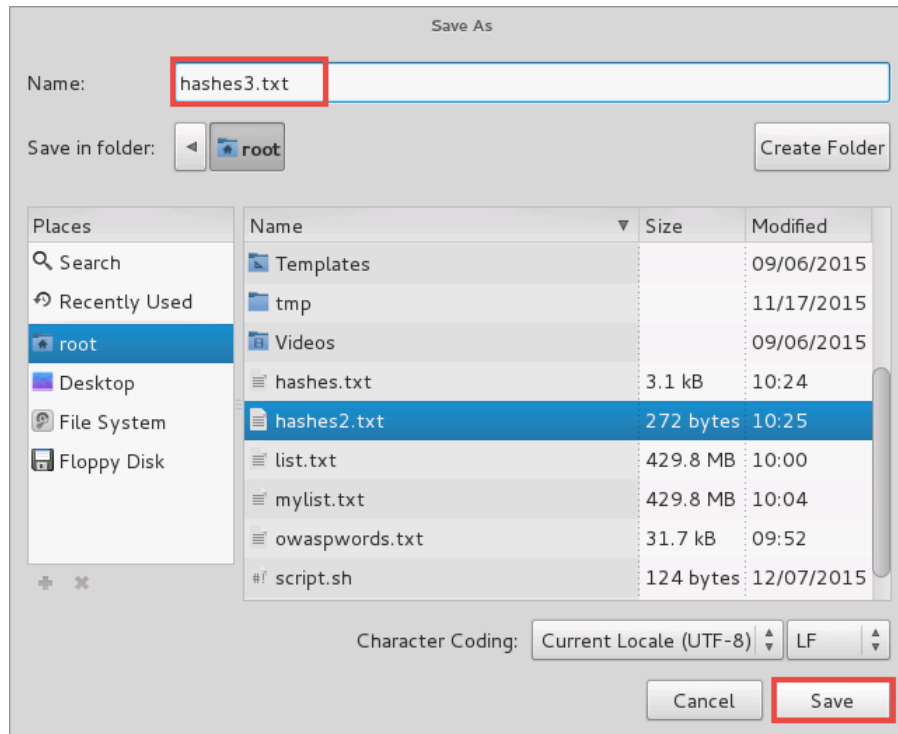


```
*hashes2.txt
uT1zQVQZV0j8536FCcQ61da4iFcxuett14o3UjcGC60mQ2MNe5AU0
vJPi6ucCfDaq8BC.iEe.r0tI18PljeLXRbATTY4.Fimb3j8ER.B0
```

8. After the modifications, click the **File** menu option and select **Saves As**.



9. In the *Save As* window, enter `hashes3.txt` in the *Name* text field and have the **root** file directory selected. Click **Save**.



10. Close the **Leafpad** window.
11. Navigate back to the Terminal window.
12. Enter the command below to use *Hashcat* in an attempt to password crack the two fake usernames in the **hashes3.txt** file using *John's* password dictionary.



```
hashcat -m 1800 -a 0 hashes3.txt /usr/share/john/password.lst
```

13. After successfully cracking the passwords, close the **Kali** PC viewer.