Project 12: Cracking Linux Password Hashes with Hashcat (15 pts.)

What You Need for This Project

- A Kali Linux machine, real or virtual

Getting Hashcat 2.00

Hashcat updated to 3.00 and it won't run in a virtual machine anymore. The simplest solution is to use the old version.

In a Terminal window, execute these commands:

```
cd
mkdir hash
cd hash
wget https://hashcat.net/files_legacy/hashcat-2.00.7z
7z e hashcat-2.00.7z
./hashcat-cli32.bin -V
```

Troubleshooting

If that link doesn't work, use this one:

wget https://samsclass.info/123/proj10/hashcat-2.00.7z

Creating a Test User

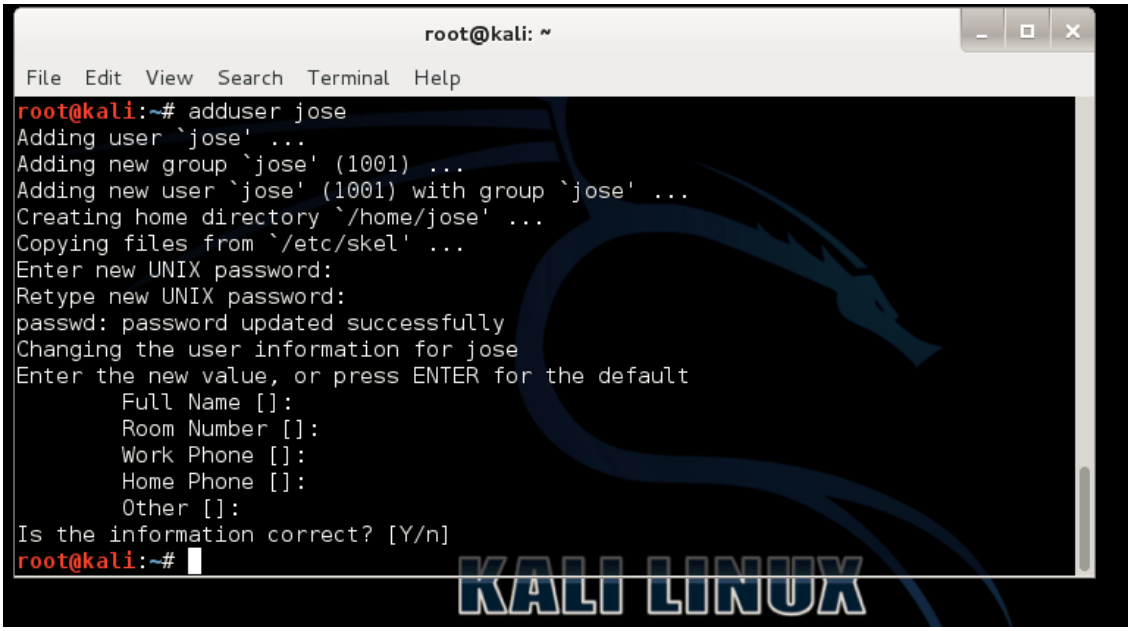
In a Terminal window, execute this command:

```
adduser jose
```

At the "Enter new UNIX password" enter a password of **password**

At the "Retype new UNIX password" enter a password of **password**

Press Enter to accept defaults for the other options, as shown below:



Viewing the Password Hash

In a Terminal window, execute this command:

```
tail /etc/shadow
```

The last line shows the password hash for jose, as shown below (your hash will be different):

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# tail /etc/shadow
postgres:*:15772:0:99999:7:::
sshd:*:15772:0:99999:7:::
rtkit:*:15772:0:99999:7:::
snmp:*:15772:0:99999:7:::
stunnel4:!:15772:0:99999:7:::
statd:*:15772:0:99999:7:::
sslh:!:15772:0:99999:7:::
saned:*:15772:0:99999:7:::
Debian-gdm:*:15772:0:99999:7:::
jose:$6$CqiOcwyE$Rutm7Vt7yuALGpkYfFT3p5zqywaMsbK74/u7vz/aIj1Mz3LftQsgUnpFBfVjDv/
IMKPBuuiRBd85QrRKvOU1R/:15871:0:99999:7:::
root@kali:~#
```

Finding Your Salt Value

Look at the salt following the username "jose". The 6 value indicates a type 6 password hash (SHA-512, many rounds). The characters after 6, up to the next $, are the SALT.

In my example, the SALT is **CqiOcwyE**

Understanding the Hash Algorithm

The hash algorithm is defined in the file /etc/login.defs. To see the portion of that file discussing the password hash algorithm, execute this grep command to see 18 lines after the line containing the string "ENCRYPT_METHOD":

```
grep -A 18 ENCRYPT_METHOD /etc/login.defs
```

As you can see, Kali Linux uses SHA-512 hashes, with the default value of 5000 rounds:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
#
ENCRYPT_METHOD SHA512

#
# Only used if ENCRYPT_METHOD is set to SHA256 or SHA512.
#
# Define the number of SHA rounds.
# With a lot of rounds, it is more difficult to brute forcing the password.
# But note also that it more CPU resources will be needed to authenticate
# users.
#
# If not specified, the libc will choose the default number of rounds (5000).
# The values must be inside the 1000-999999999 range.
# If only one of the MIN or MAX values is set, then this value will be used.
# If MIN > MAX, the highest value will be used.
#
# SHA_CRYPT_MIN_ROUNDS 5000
# SHA_CRYPT_MAX_ROUNDS 5000

################ OBSOLETED BY PAM ##############
#                                              #
# These options are now handled by PAM. Please #
# edit the appropriate file in /etc/pam.d/ to  #
root@kali:~#
```

Making a Hash File

In a Terminal window, execute these commands:

```
tail -n 1 /etc/shadow > crack1.hash

nano crack1.hash
```

In the nano text editor, carefully delete the username **jose** and the colon after it, and all the text at the end of the file, including all the colons, leaving only the hash, as shown below:

```
root@kali: ~/hash
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                File: crack1.hash                          Modified

$6$CqiOcwyE$Rutm7Vt7yuALGpkYfFT3p5zqywaMsbK74/u7vz/aIj1Mz3LftQsgUnpFBfVjDv/IMKPBuuiRBd85QrRKvOU1R/

^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Page   ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page   ^U UnCut Text  ^T To Spell
```

Press **Ctrl+X**, **Y**, **Enter** to save the file.

Dowloading a Wordlist

We'll use a very small list of 500 common passwords.

In a Terminal window, execute these commands:

```
curl http://www.scovetta.com/download/500_passwords.txt > 500_passwords.txt

head 500_passwords.txt
```

You should see the first ten passwords, as shown below:

```
root@kali: ~/hash
File  Edit  View  Search  Terminal  Help
root@kali:~/hash# wget http://www.scovetta.com/download/500_passwords.txt
--2013-06-16 14:37:47--  http://www.scovetta.com/download/500_passwords.txt
Resolving www.scovetta.com (www.scovetta.com)... 216.227.213.152
Connecting to www.scovetta.com (www.scovetta.com)|216.227.213.152|:80... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 3492 (3.4K) [text/plain]
Saving to: `500_passwords.txt'

100%[=====================================>] 3,492       --.-K/s   in 0s

2013-06-16 14:37:48 (266 MB/s) - `500_passwords.txt' saved [3492/3492]

root@kali:~/hash# head 500_passwords.txt
123456
password
12345678
1234
pussy
12345
dragon
qwerty
696969
mustang
root@kali:~/hash#
```

Troubleshooting

If that link doesn't work, use this one:

curl https://samsclass.info/123/proj10/500_passwords.txt > 500_passwords.txt

Cracking the Hash

In a Terminal window, execute these commands:

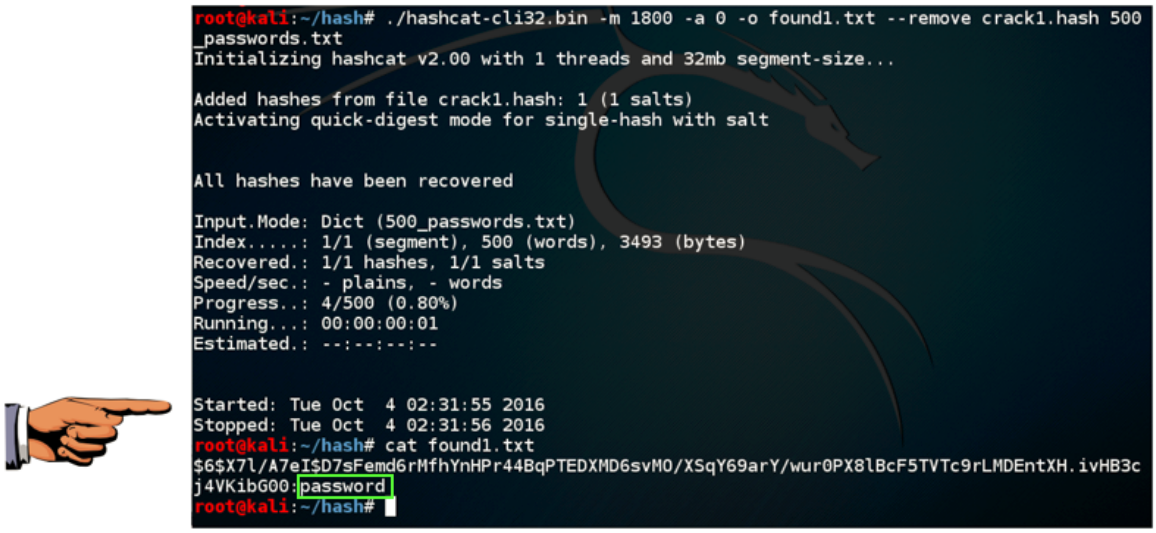
```
./hashcat-cli32.bin -m 1800 -a 0 -o found1.txt --remove crack1.hash 500_passwords.txt

cat found1.txt
```

Explanation: This uses hashcat with these options:

- Unix type 6 password hashes (-m 1800)
- Using a dictionary attack (-a 0)
- Putting output in the file **found1.txt**
- Removing each hash as it is found
- Getting hashes from **crack1.hash**
- Using the dictionary **500_passwords.txt**

You should see the hash, with the cracked password of "**password**" at the end, as shown below:



Saving a Screen Image

Make sure the Terminal window is visible, showing the cracked password of "**password**".

Click on the host machine's desktop, outside the virtual machine to make the host machine's desktop active.

Press the PrintScrn key to copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT.

In the host machine, open Paint and paste in the captured image. Save it as "**Your Name Proj12a**".

Getting the crack2.hash List

In a Terminal window, execute these commands:

```
curl https://samsclass.info/123/proj10/crack2.hash > crack2.hash

cat crack2.hash
```

You should see four password hashes, as shown below:

```
root@kali: ~/hash
File  Edit  View  Search  Terminal  Help
root@kali:~/hash# wget http://samsclass.info/123/proj10/crack2.hash
--2013-06-16 15:02:50--  http://samsclass.info/123/proj10/crack2.hash
Resolving samsclass.info (samsclass.info)... 141.101.117.152, 141.101.116.152, 240
0:cb00:2048:1::8d65:7498, ...
Connecting to samsclass.info (samsclass.info)|141.101.117.152|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 396 [text/plain]
Saving to: `crack2.hash'

100%[=====================================>] 396         --.-K/s   in 0s

2013-06-16 15:02:51 (69.7 MB/s) - `crack2.hash' saved [396/396]

root@kali:~/hash# cat crack2.hash
$6$NShHCRTL$lAe9dI1rtpAXQkiMPqncpCQ69gE7Y25TgKRDvtfIOdLVTlG4cMAp9LQE9eEZuboS4tO6ip
pBnOIFE8zgqOvGP0
$6$ssMb25ys$yuyoQKJaaGeRVhwsklDAvWnJLcgZxiTX7mrxH.8xCslnGcCbB3S0gLic3qlyOGWCZImFI3
KW29p1Ht7ny9Jwo/
$6$sH2VWpHm$cEvtk3IffFilT73amGGv7/6j2LRWHQ7df4vjgoSuOSEt8QZDeDDYxCqlly.cU8/AfL/ulY
mX/42QI.etA8fdV1
$6$E5s/79nO$HLNy0xElpbp7Dx4537KCsAlAER.wULMLLS1vzgmkVyp1ZK/fK/.td819Ea1RFhMBLfsQXv
FM0HfMW3k3oF4ob.
root@kali:~/hash#
```

Cracking the Hashes

In a Terminal window, execute these commands:

```
./hashcat-cli32.bin -m 1800 -a 0 -o found2.txt --remove crack2.hash 500_passwords.txt

cat found2.txt
```

You should see the hashes, with the found passwords at the end of each line as shown below. (I redacted the passwords.)

```
root@kali:~/hash# ./hashcat-cli32.bin -m 1800 -a 0 -o found2.txt --remove crack2.h
ash 500_passwords.txt
Initializing hashcat v2.00 with 1 threads and 32mb segment-size...

Added hashes from file crack2.hash: 4 (4 salts)


All hashes have been recovered

Input.Mode: Dict (500_passwords.txt)
Index.....: 1/1 (segment), 500 (words), 3493 (bytes)
Recovered.: 4/4 hashes, 4/4 salts
Speed/sec.: - plains, 248 words
Progress..: 500/500 (100.00%)
Running...: 00:00:00:02
Estimated.: --:--:--:--


Started: Tue Oct  4 02:37:02 2016
Stopped: Tue Oct  4 02:37:04 2016
root@kali:~/hash# cat found2.txt
$6$NShHCRTL$lAe9dI1rtpAXQkiMPqncpCQ69gE7Y25TgKRDvtfIOdLVTlG4cMAp9LQE9eEZuboS4tO6ip
pBnOIFE8zgqOvGP0:[redacted]
$6$ssMb25ys$yuyoQKJaaGeRVhwsklDAvWnJLcgZxiTX7mrxH.8xCslnGcCbB3S0gLic3qlyOGWCZImFI3
KW29p1Ht7ny9Jwo/:[redacted]
$6$sH2VWpHm$cEvtk3IffFilT73amGGv7/6j2LRWHQ7df4vjgoSuOSEt8QZDeDDYxCqlly.cU8/AfL/ulY
mX/42QI.etA8fdV1:[redacted]
$6$E5s/79nO$HLNy0xElpbp7Dx4537KCsAlAER.wULMLLS1vzgmkVyp1ZK/fK/.td819Ea1RFhMBLfsQXv
FM0HfMW3k3oF4ob.:[redacted]
root@kali:~/hash#
```

Saving a Screen Image

Make sure the Terminal window is visible, showing the found passwords.

Click on the host machine's desktop, outside the virtual machine to make the host machine's desktop active.

Press the PrintScrn key to copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT.

In the host machine, open Paint and paste in the captured image. Save it as "**Your Name Proj12b**".

Turning in Your Project

Email the images to **cnit.123@gmail.com** with a subject line of "**Proj 12 From Your Name**", replacing "Your Name" with your own first and last name. Send a Cc to yourself.

Sources

http://www.vidarholen.net/contents/junk/files/sha512crypt.bash

http://hashcat.net/files/hashcat_user_manual.pdf

http://contest-2010.korelogic.com/wordlists.html

http://www.scovetta.com/article-2.html

Last modified 10-19-16