CYSE 270: Linux System for Cybersecurity

Assignment: Lab 5 – Password cracking

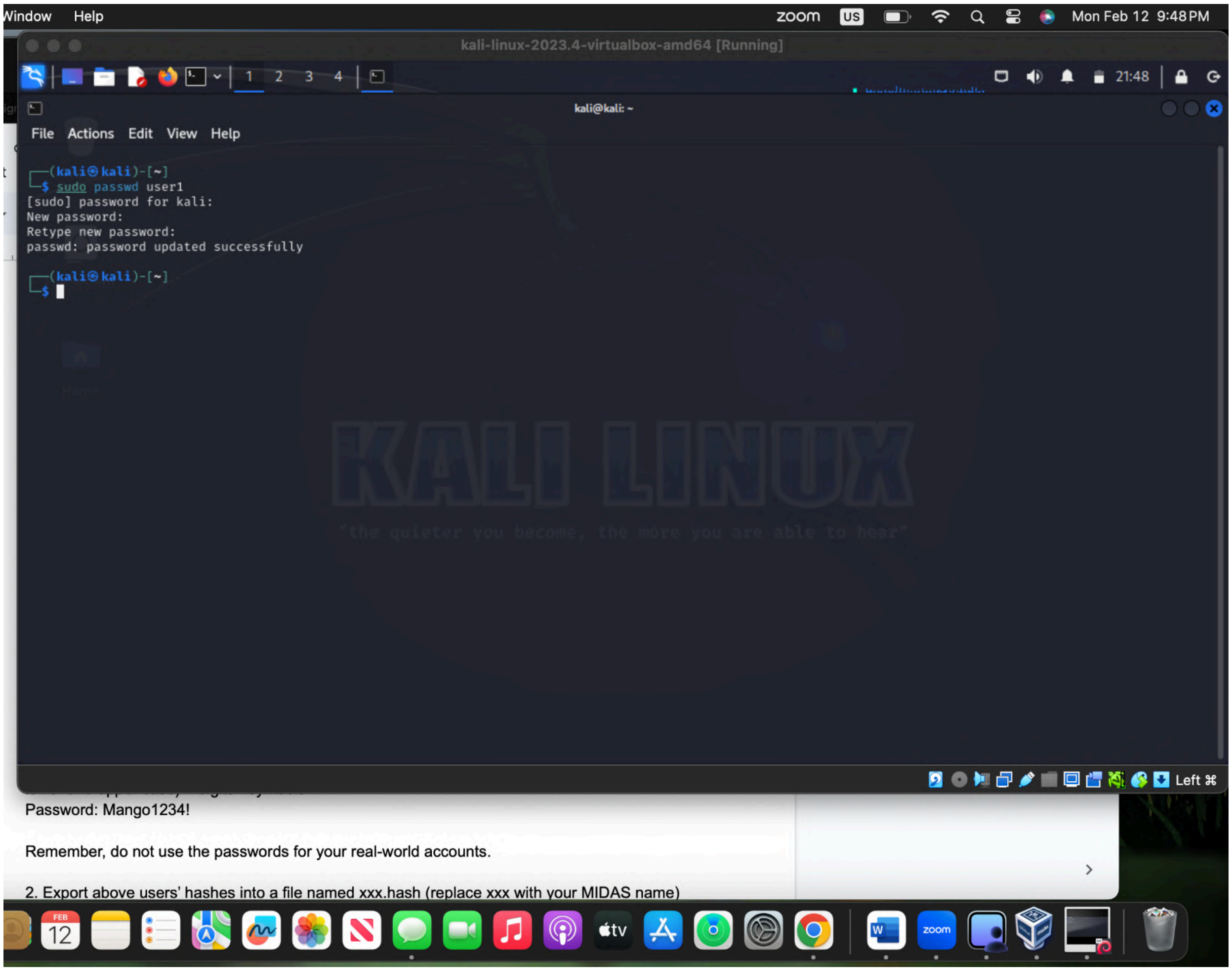
CYSE 270: Linux System for Cybersecurity

The goal of this lab is to test the strength of different passwords.

Task A – Password Cracking

1. Create 6 users in your Linux Terminal, then set the password for each user that meets the followingcomplexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30points]

1. For user1, the password should be a simple dictionary word (all lowercase)



```
┌──(kali㉿kali)-[~]
└─$ sudo passwd user1
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ 
```

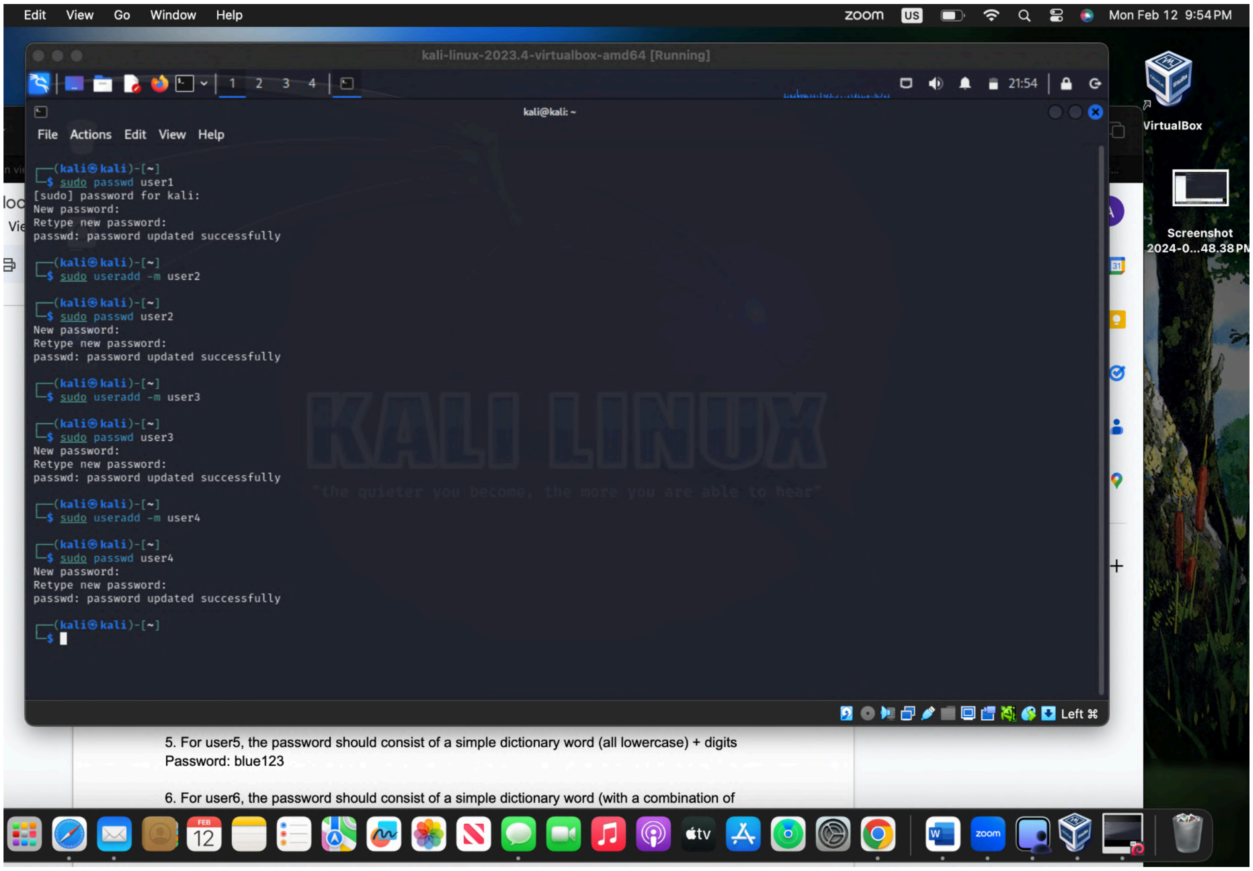
Password: Mango1234!

Remember, do not use the passwords for your real-world accounts.

2. Export above users' hashes into a file named xxx.hash (replace xxx with your MIDAS name)

Password: apple

2. For user2, the password should consist of 4 digits


Edit View Go Window Help
zoom
Mon Feb 12 9:54 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
1 2 3 4
21:54
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Left ⌘
VirtualBox
Screenshot 2024-0...48.38 PM

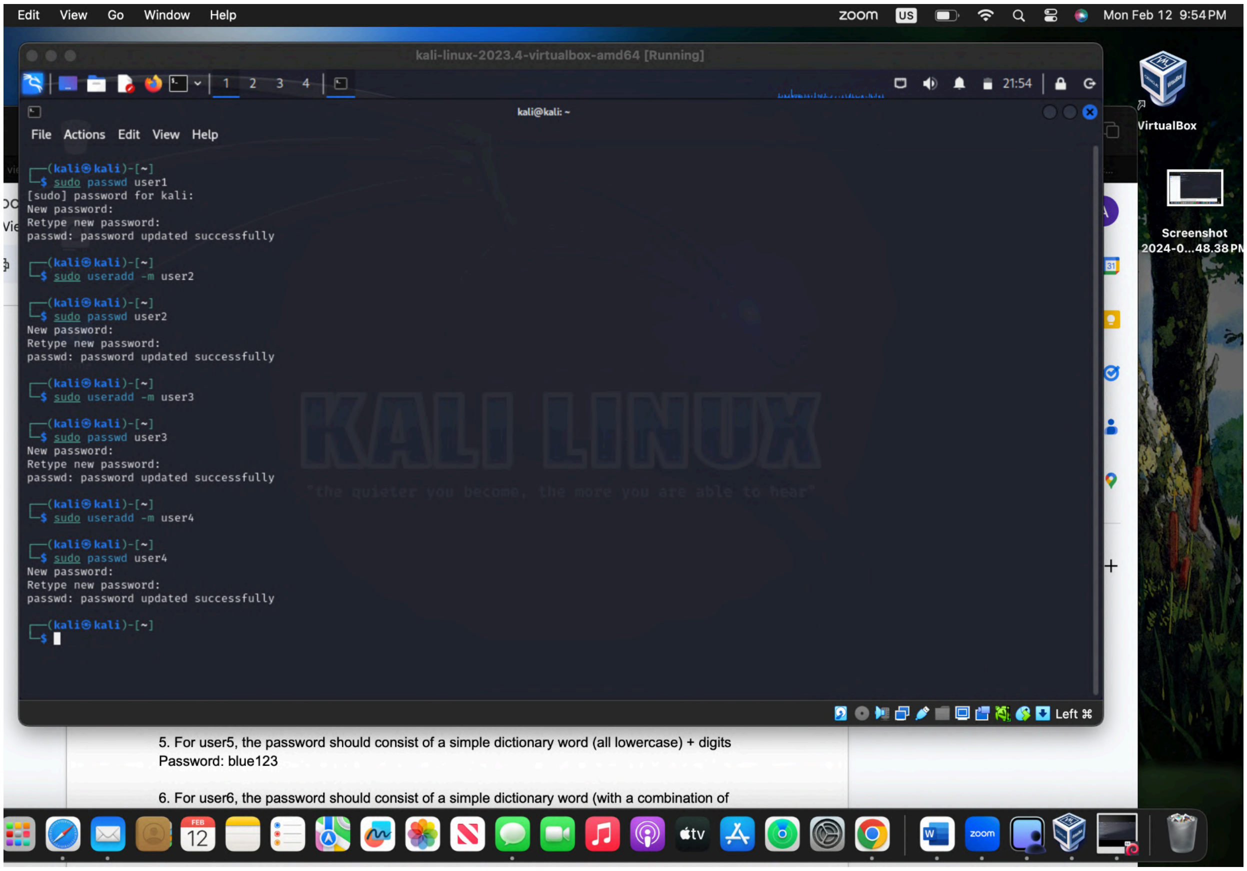
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd user1
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user2

┌──(kali㉿kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user3

┌──(kali㉿kali)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user4

┌──(kali㉿kali)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ █
```

5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits
Password: blue123

6. For user6, the password should consist of a simple dictionary word (with a combination of

Password: 1234

3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits


Edit
View
Go
Window
Help
zoom
Mon Feb 12 9:54 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
1 2 3 4
21:54
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Left ⌘
VirtualBox
Screenshot 2024-0...48.38 PM

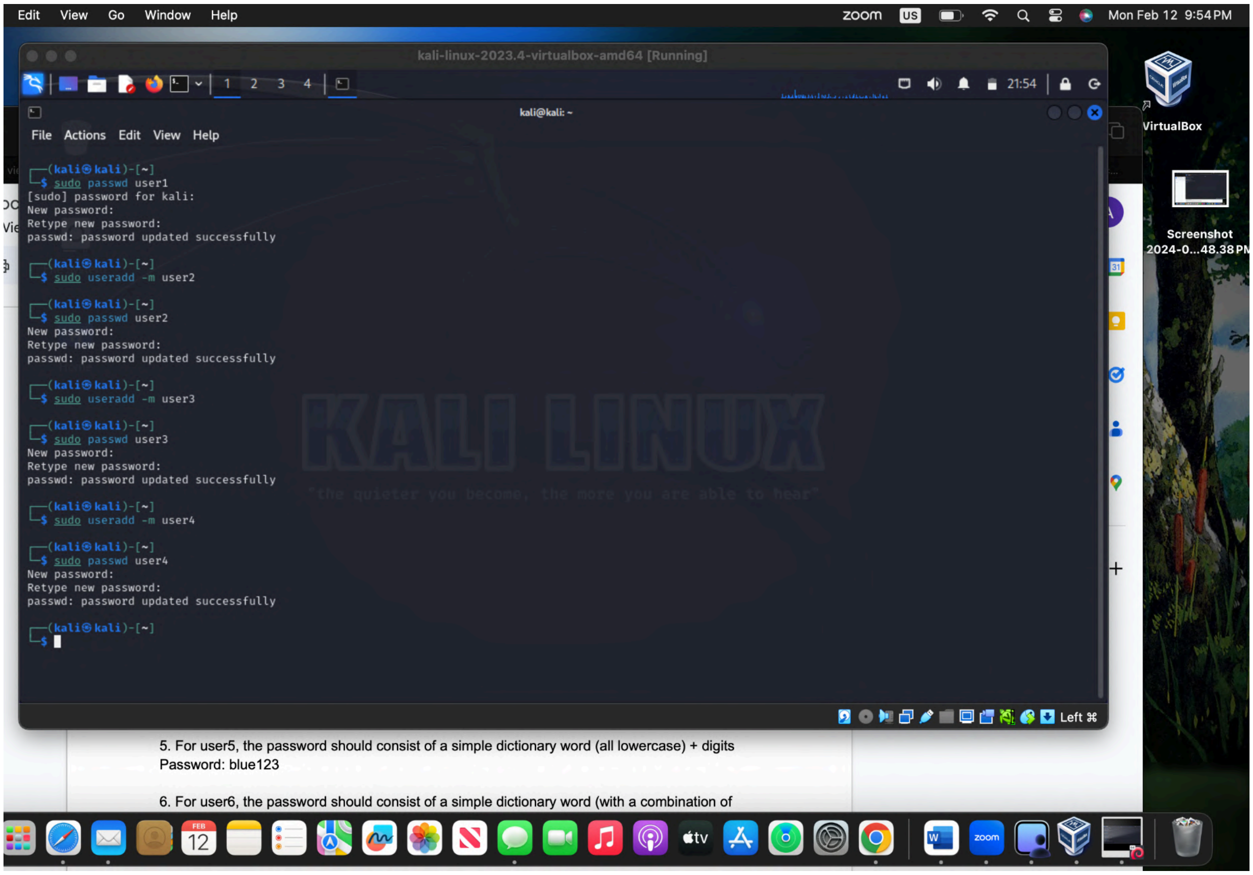
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd user1
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user2

┌──(kali㉿kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user3

┌──(kali㉿kali)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user4

┌──(kali㉿kali)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ 
```

5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits
Password: blue123

6. For user6, the password should consist of a simple dictionary word (with a combination of

Password: pink123

4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits +symbols


Edit View Go Window Help
zoom
Mon Feb 12 9:54 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
21:54
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Left ⌘
VirtualBox
Screenshot 2024-0...48.38 PM

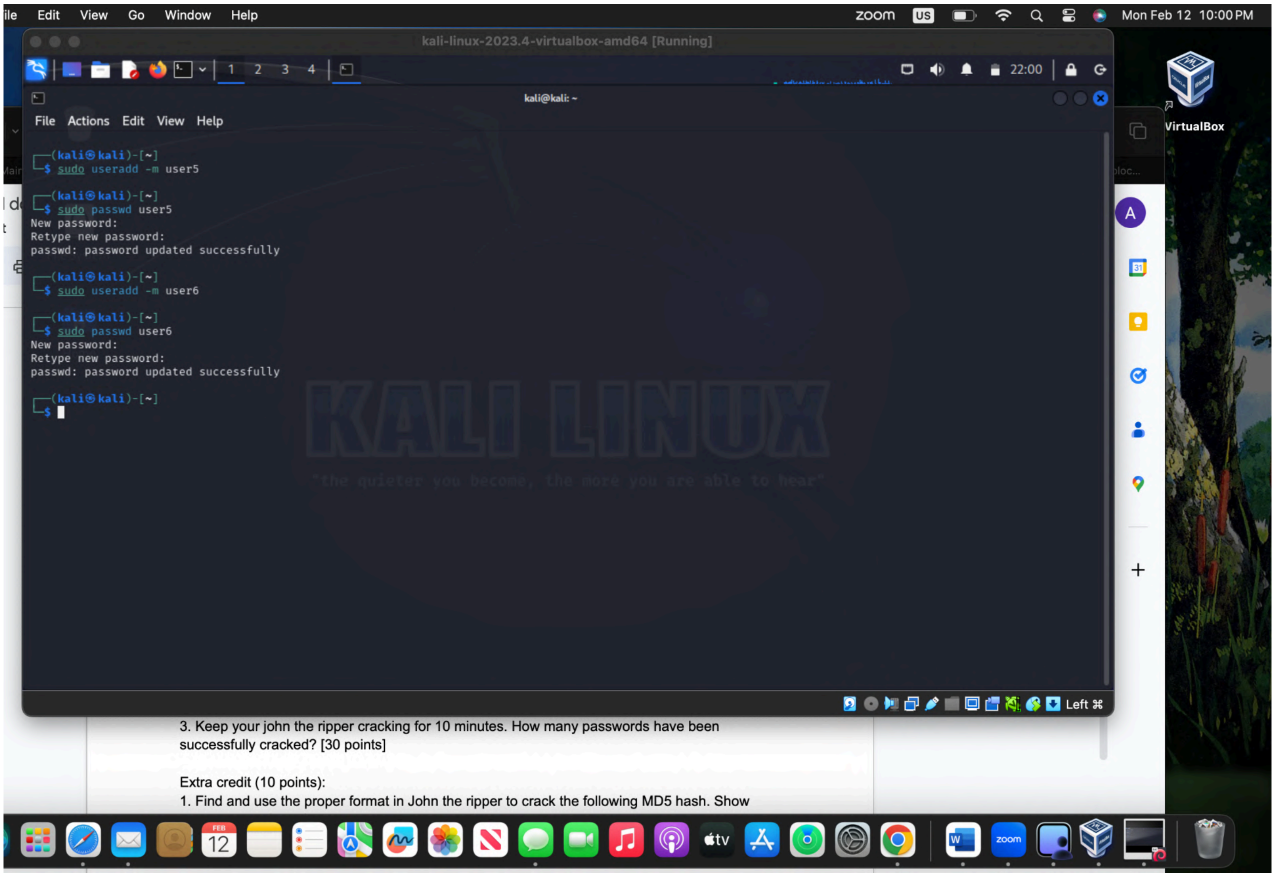
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd user1
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user2

┌──(kali㉿kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user3

┌──(kali㉿kali)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user4

┌──(kali㉿kali)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ █
```

5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits
Password: blue123

6. For user6, the password should consist of a simple dictionary word (with a combination of

Password: yellow123!

5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits


ile Edit View Go Window Help
zoom
US
Mon Feb 12 10:00 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
1 2 3 4
22:00
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
VirtualBox
Left ⌘

```
┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user5

┌──(kali㉿kali)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user6

┌──(kali㉿kali)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ █
```

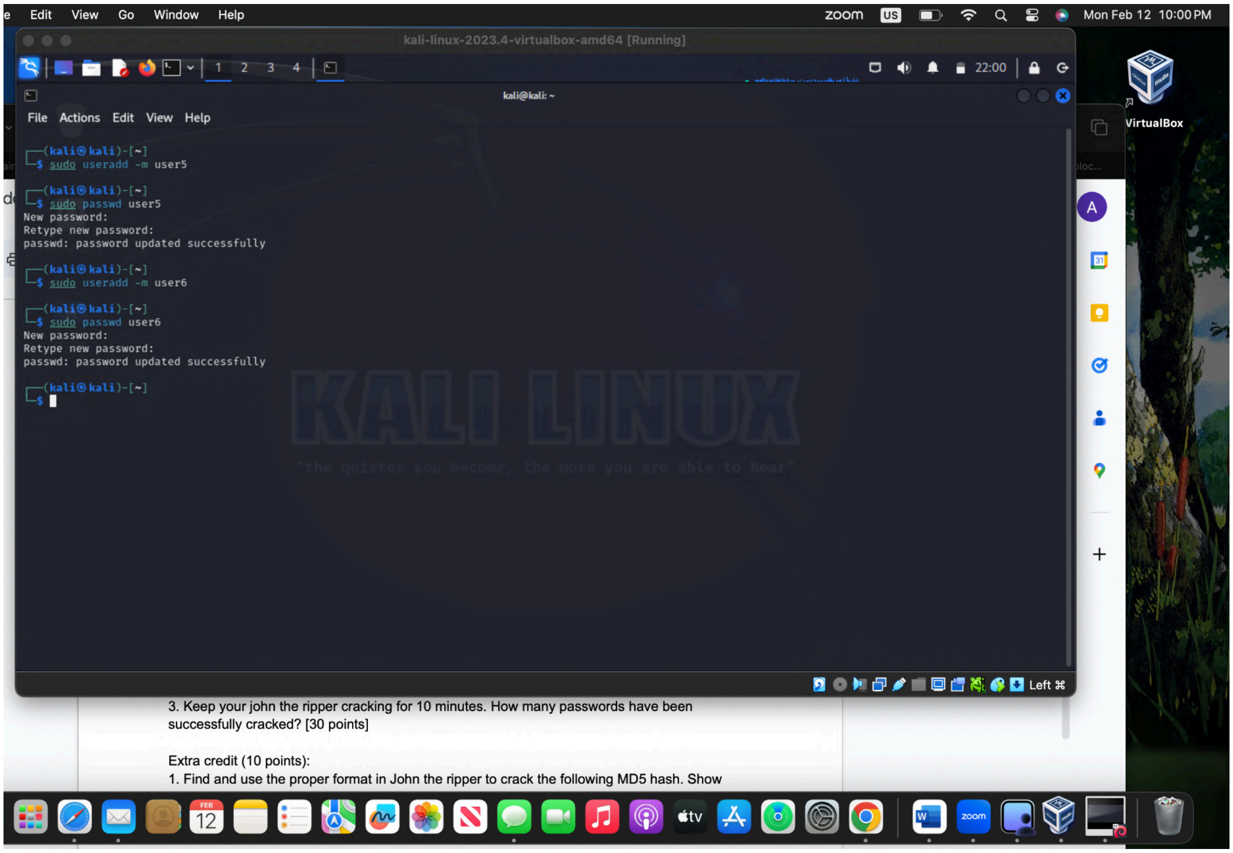
3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? [30 points]

Extra credit (10 points):

1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show

Password: blue123

6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits +symbols


Edit View Go Window Help
zoom
Mon Feb 12 10:00 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
22:00
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
VirtualBox
Left ⌘

```
┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user5

┌──(kali㉿kali)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo useradd -m user6

┌──(kali㉿kali)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$
```

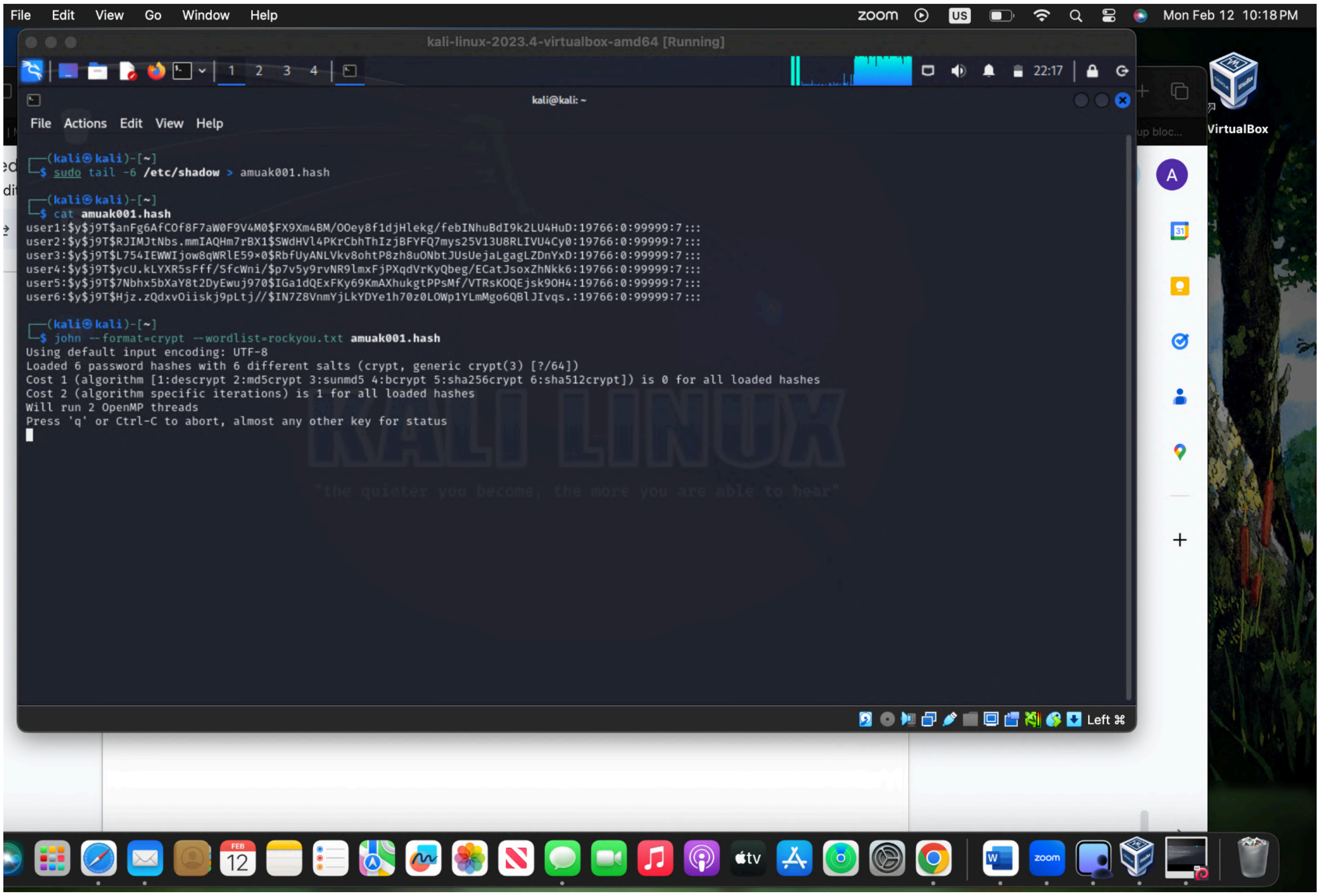
3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? [30 points]

Extra credit (10 points):
1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show

Password: Mango1234!

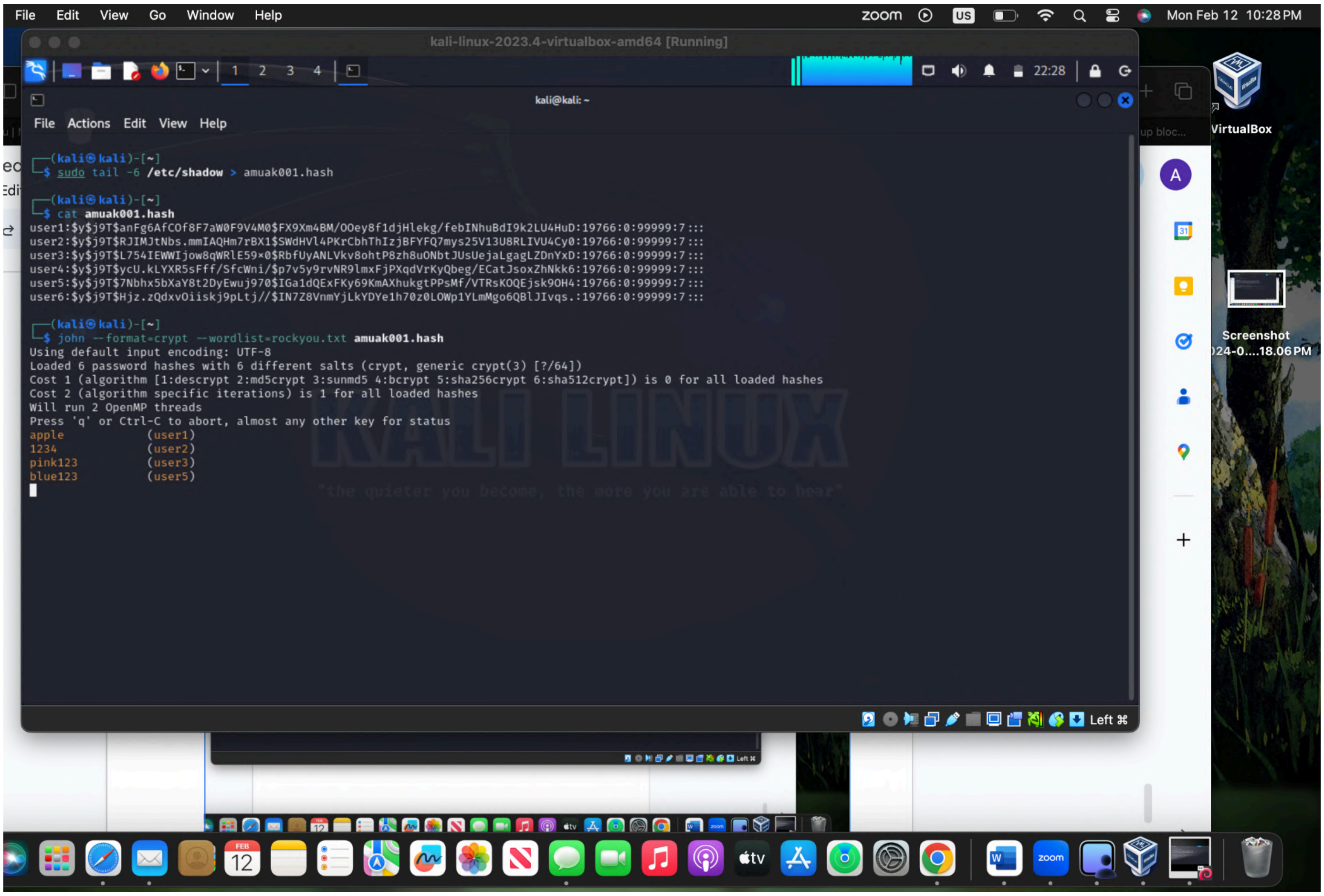
Remember, do not use the passwords for your real-world accounts.

2. Export above users' hashes into a file named xxx.hash (replace xxx with your MIDAS name) and use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt). [40 points]


File Edit View Go Window Help
Mon Feb 12 10:18 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
22:17
kali@kali: ~
File Actions Edit View Help
VirtualBox
Left ⌘

```
┌──(kali㉿kali)-[~]
└─$ sudo tail -6 /etc/shadow > amuak001.hash

┌──(kali㉿kali)-[~]
└─$ cat amuak001.hash
user1:$y$j9T$anFg6AfCOf8F7aW0F9V4M0$FX9Xm4BM/OOey8f1djHlekg/febINhuBdI9k2LU4HuD:19766:0:99999:7:::
user2:$y$j9T$RJIMJtNbs.mmIAQHm7rBX1$SWdHVl4PKrCbhThIzjBFYFQ7mys25V13U8RLIVU4Cy0:19766:0:99999:7:::
user3:$y$j9T$L754IEWWIjow8qWRlE59×0$RbfUyANLVkv8ohtP8zh8uONbtJUsUejaLgagLZDnYxD:19766:0:99999:7:::
user4:$y$j9T$ycU.kLYXR5sFff/SfcWni/$p7v5y9rvNR9lmxFjPXqdVrKyQbeg/ECatJsoxZhNkk6:19766:0:99999:7:::
user5:$y$j9T$7Nbhx5bXaY8t2DyEwuj970$IGa1dQExFKy69KmAXhukgtPPsMf/VTRsKOQEjsk9OH4:19766:0:99999:7:::
user6:$y$j9T$Hjz.zQdxvOiiskj9pLtj//$IN7Z8VnmYjLkYDYe1h70z0LOWp1YLmMgo6QBlJIvqs.:19766:0:99999:7:::

┌──(kali㉿kali)-[~]
└─$ john --format=crypt --wordlist=rockyou.txt amuak001.hash
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
█
```

3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? [30 points]

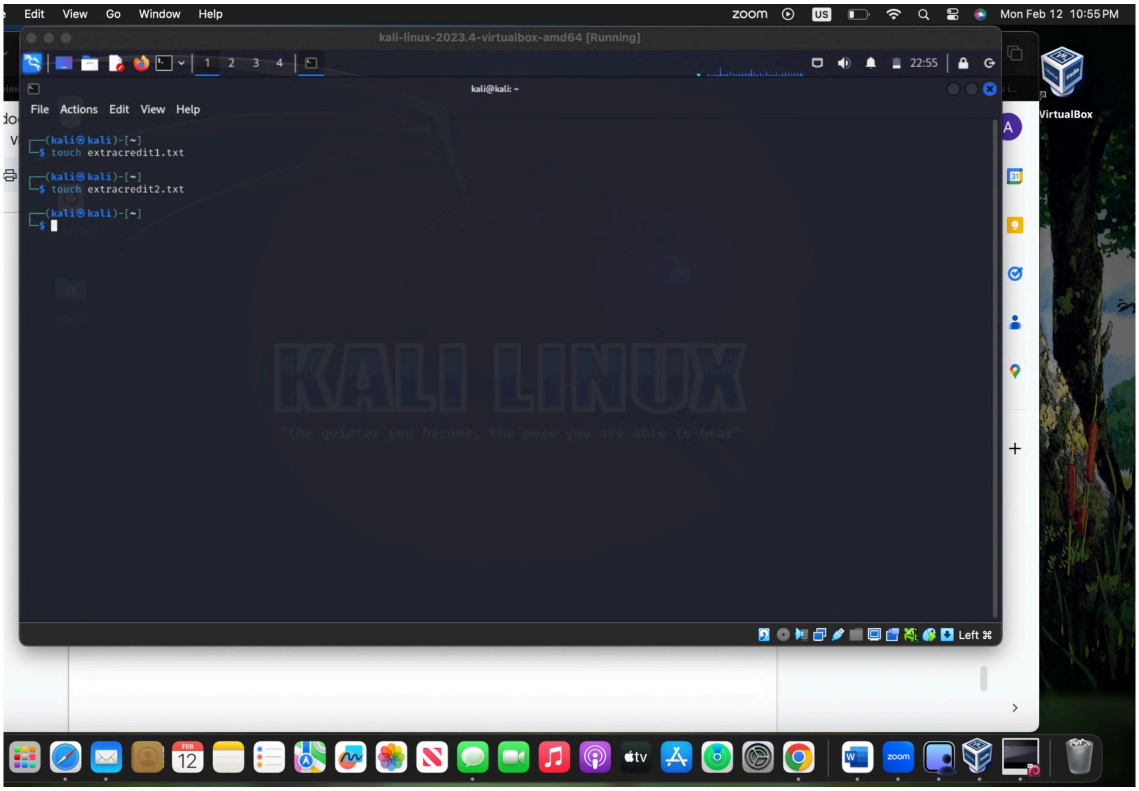

File Edit View Go Window Help
zoom
Mon Feb 12 10:28 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
22:28
kali@kali: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"
Left ⌘
VirtualBox
Screenshot
)24-0....18.06 PM

```
┌──(kali㉿kali)-[~]
└─$ sudo tail -6 /etc/shadow > amuak001.hash

┌──(kali㉿kali)-[~]
└─$ cat amuak001.hash
user1:$y$j9T$anFg6AfCOf8F7aW0F9V4M0$FX9Xm4BM/OOey8f1djHlekg/febINhuBdI9k2LU4HuD:19766:0:99999:7:::
user2:$y$j9T$RJIMJtNbs.mmIAQHm7rBX1$SWdHVl4PKrCbhThIzjBFYFQ7mys25V13U8RLIVU4Cy0:19766:0:99999:7:::
user3:$y$j9T$L754IEWWIjow8qWRlE59×0$RbfUyANLVkv8ohtP8zh8uONbtJUsUejaLgagLZDnYxD:19766:0:99999:7:::
user4:$y$j9T$ycU.kLYXR5sFff/SfcWni/$p7v5y9rvNR9lmxFjPXqdVrKyQbeg/ECatJsoxZhNkk6:19766:0:99999:7:::
user5:$y$j9T$7Nbhx5bXaY8t2DyEwuj970$IGa1dQExFKy69KmAXhukgtPPsMf/VTRsKOQEjsk9OH4:19766:0:99999:7:::
user6:$y$j9T$Hjz.zQdxvOiiskj9pLtj//$IN7Z8VnmYjLkYDYe1h70z0LOWp1YLmMgo6QBlJIvqs.:19766:0:99999:7:::

┌──(kali㉿kali)-[~]
└─$ john --format=crypt --wordlist=rockyou.txt amuak001.hash
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
apple            (user1)
1234             (user2)
pink123          (user3)
blue123          (user5)
```

Extra credit (10 points):

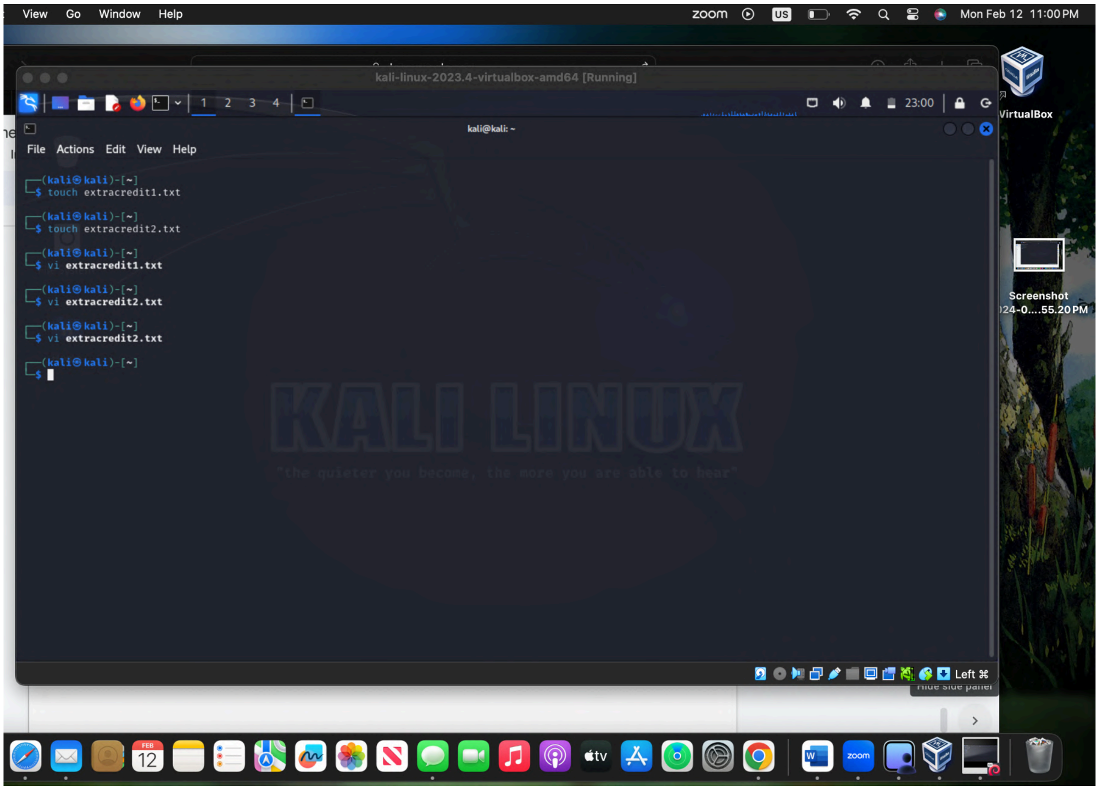
1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show your steps and results.

- 5f4dcc3b5aa765d61d8327deb882cf99
- 63a9f0ea7bb98050796b649e85481845

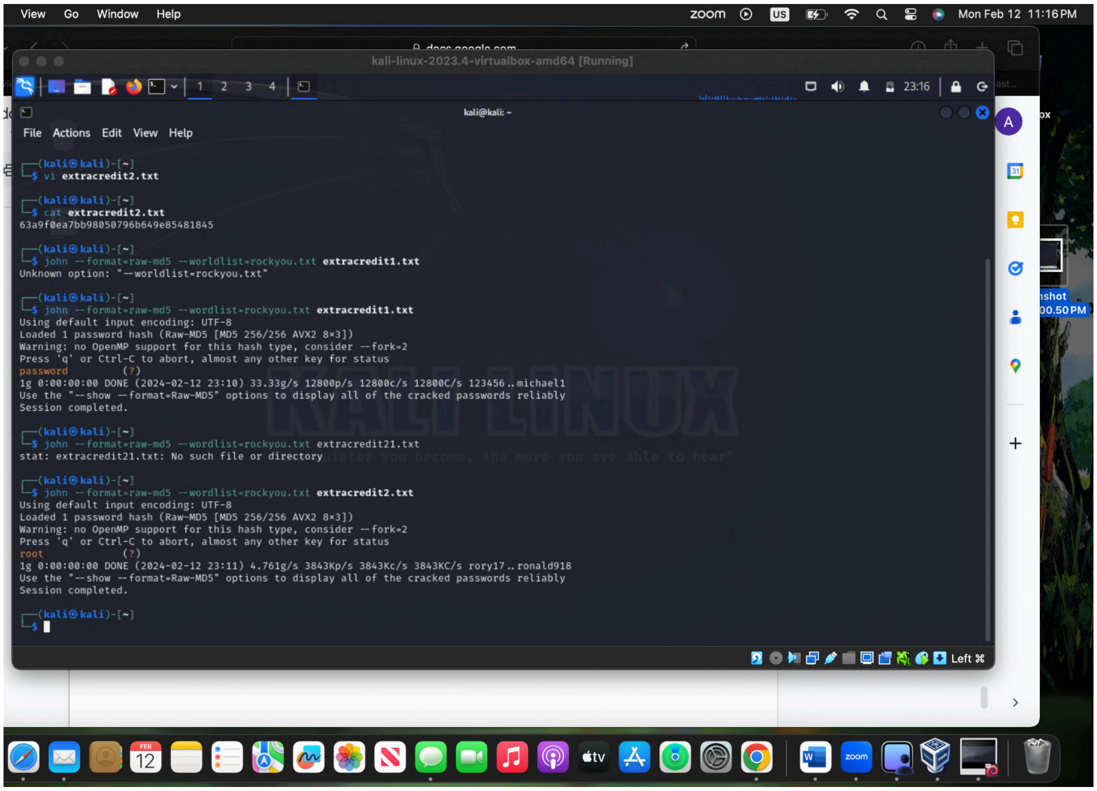


Edit View Go Window Help
zoom
Mon Feb 12 10:55 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
1 2 3 4
22:55
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Left ⌘
VirtualBox

```
┌──(kali㉿kali)-[~]
└─$ touch extracredit1.txt

┌──(kali㉿kali)-[~]
└─$ touch extracredit2.txt

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ touch extracredit1.txt

┌──(kali㉿kali)-[~]
└─$ touch extracredit2.txt

┌──(kali㉿kali)-[~]
└─$ vi extracredit1.txt

┌──(kali㉿kali)-[~]
└─$ vi extracredit2.txt

┌──(kali㉿kali)-[~]
└─$ vi extracredit2.txt

┌──(kali㉿kali)-[~]
└─$ 
```


View Go Window Help
Mon Feb 12 11:16 PM
kali-linux-2023.4-virtualbox-amd64 [Running]
23:16
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ vi extracredit2.txt

┌──(kali㉿kali)-[~]
└─$ cat extracredit2.txt
63a9f0ea7bb98050796b649e85481845

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --worldlist=rockyou.txt extracredit1.txt
Unknown option: "--worldlist=rockyou.txt"

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=rockyou.txt extracredit1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:00 DONE (2024-02-12 23:10) 33.33g/s 12800p/s 12800c/s 12800C/s 123456..michael1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=rockyou.txt extracredit21.txt
stat: extracredit21.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=rockyou.txt extracredit2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
root             (?)
1g 0:00:00:00 DONE (2024-02-12 23:11) 4.761g/s 3843Kp/s 3843Kc/s 3843KC/s rory17..ronald918
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ 
```

citation:
https://www.youtube.com/watch?v=h_cxbMuHAfE