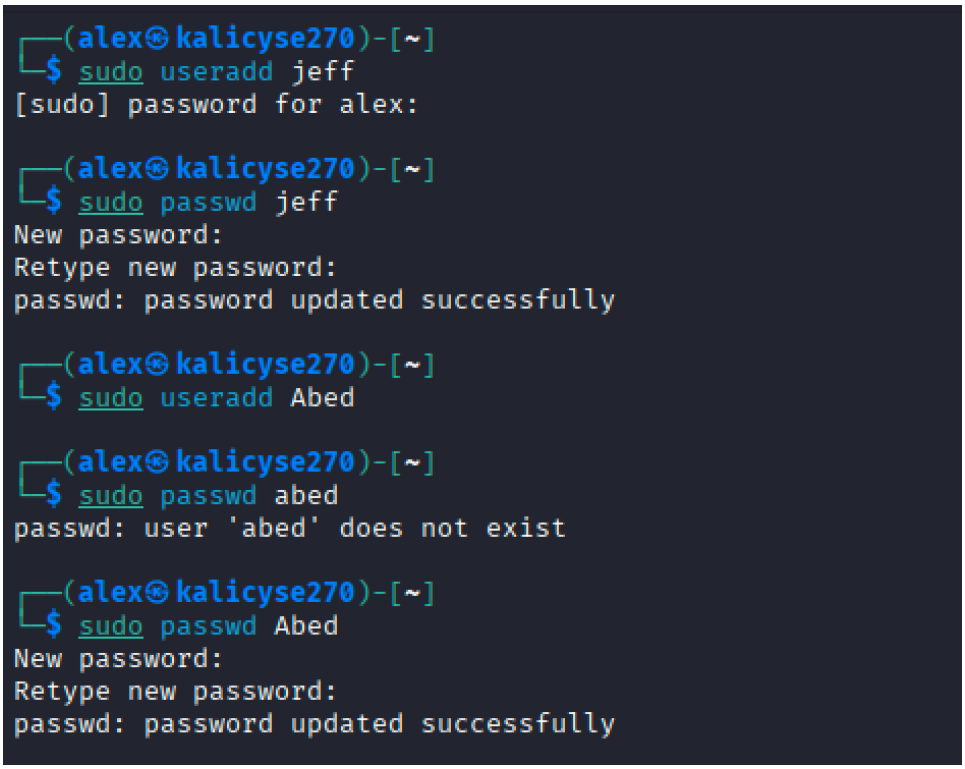
CYSE 270 Lab 5 – Password Cracking

Alex Bretana

Step 1 – create 6 users (sudo useradd ____, sudo passwd *USER* ____)

1. Jeff - community
2. Abed - 1984
3. Pierce – balding1945
4. Troy – cha$eth3m0ney
5. Britta – woman23
6. Annie – Pr3D@t0R%751



```
┌──(alex㉿kalicyse270)-[~]
└─$ sudo useradd Pierce

┌──(alex㉿kalicyse270)-[~]
└─$ sudo passwd Pierce
New password:
Retype new password:
passwd: password updated successfully

┌──(alex㉿kalicyse270)-[~]
└─$ sudo useradd Troy

┌──(alex㉿kalicyse270)-[~]
└─$ sudo passwd Troy
New password:
Retype new password:
passwd: password updated successfully
```

```
┌──(alex㉿kalicyse270)-[~]
└─$ sudo useradd Britta

┌──(alex㉿kalicyse270)-[~]
└─$ sudo passwd Britta
New password:
Retype new password:
passwd: password updated successfully

┌──(alex㉿kalicyse270)-[~]
└─$ sudo useradd Annie

┌──(alex㉿kalicyse270)-[~]
└─$ sudo passwd Annie
New password:
Retype new password:
passwd: password updated successfully

┌──(alex㉿kalicyse270)-[~]
└─$
```

Step 2A: export user's hashes to abret003.hash

"Tail -6 /etc/passwd " shows the 6 most recent created users (hence -6)
"sudo tail -6 /etc/shadow > abret003.hash" takes the 6 most recent hashes from etc/shadow and imports them to a new file named abret003.hash
"cat abret003.hash" checks the file to ensure it was copied properly

```
┌──(alex㉿kalicyse270)-[~]
└─$ tail -6 /etc/passwd
jeff:x:1007:1008::/home/jeff:/bin/sh
Abed:x:1008:1009::/home/Abed:/bin/sh
Pierce:x:1009:1010::/home/Pierce:/bin/sh
Troy:x:1010:1011::/home/Troy:/bin/sh
Britta:x:1011:1012::/home/Britta:/bin/sh
Annie:x:1012:1013::/home/Annie:/bin/sh
```

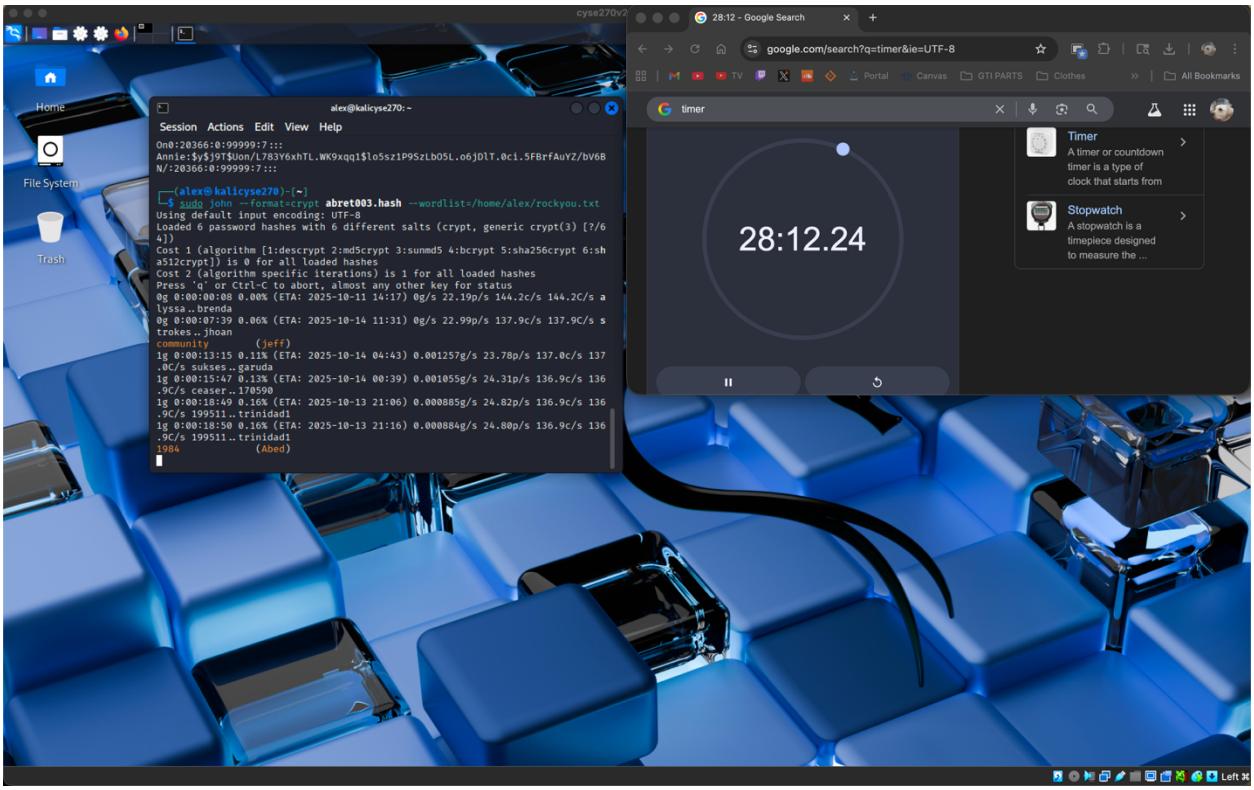
```
┌──(alex㉿kalicyse270)-[~]
└─$ sudo tail -6 /etc/shadow > abret003.hash

┌──(alex㉿kalicyse270)-[~]
└─$ cat abret003.hash
jeff:$y$j9T$P82AC7H0CNgIgUEDR8wCw1$.kwKYSTneVGa3/x7lLAIf2Gdplz8HMdcVu8OYnJbRW
.:20366:0:99999:7:::
Abed:$y$j9T$VNbnhoyWudTvVJlO6/yhE0$PAWZ2236QreA5ozHhap0gqcel2/qY9/WlVEzLersoL
/:20366:0:99999:7:::
Pierce:$y$j9T$L14zW/OzG55cFnGnjA3i6/$RcUmi2NiMPRgilj78RpmMEWFZhHbnCauCWJSMvXl
twA:20366:0:99999:7:::
Troy:$y$j9T$xrE/0KQFyqPZQN3kcWHLH1$VQ9cue9QDzwO1kJ4IcBSFhbiImR5F/FQwpOMZEiz2j
7:20366:0:99999:7:::
Britta:$y$j9T$zgn.r8ZjY3gjxJnETnkpP.$aJA/C8f/QWuBy1aaubRw7uOrv.rWpZJd1E04MJ..
On0:20366:0:99999:7:::
Annie:$y$j9T$Uon/L783Y6xhTL.WK9xqq1$lo5sz1P9SzLbO5L.o6jDlT.0ci.5FBrfAuYZ/bV6B
N/:20366:0:99999:7:::

┌──(alex㉿kalicyse270)-[~]
└─$
```

Step 2B: run john the ripper on the file (sudo john –format=crypt abret003.hash –wordlist=/home/alex/rockyou.txt)

```
┌──(alex㉿kalicyse270)-[~]
└─$ sudo john --format=crypt abret003.hash --wordlist=/home/alex/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/6
4])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh
a512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 0.00% (ETA: 2025-10-11 14:17) 0g/s 22.19p/s 144.2c/s 144.2C/s a
lyssa..brenda
```

Step 3: how many passwords have been cracked after 10 minutes?

In my case, only one password was cracked at 26 minutes in, and it was the simplest one: Jeff's password, "community." It would take days to crack the harder ones. EDIT: at 27 minutes, it cracked the 2nd password, Abed's password: "1984."



EXTRA CREDIT: echo 5f4dcc3b5aa765d61d8327deb882cf99 > extracredit.txt

echo 63a9f0ea7bb98050796b649e85481845 >> extracredit.txt

```
┌──(alex㉿kalicyse270)-[~]
└─$ echo 63a9f0ea7bb98050796b649e85481845 >> extracredit.txt
```

```
┌──(alex㉿kalicyse270)-[~]
└─$ echo 5f4dcc3b5aa765d61d8327deb882cf99 > extracredit.txt
```

cat extracredit.txt

```
┌──(alex㉿kalicyse270)-[~]
└─$ cat extracredit.txt
5f4dcc3b5aa765d61d8327deb882cf99
63a9f0ea7bb98050796b649e85481845
```

John –format=raw-md5 –wordlist=/home/alex/rockyou.txt extracredit.txt

John –show –format=Raw-MD5 extracredit.txt

```
┌──(alex㉿kalicyse270)-[~]
└─$ john --format=raw-md5 --wordlist=/home/alex/rockyou.txt extracredit.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD
4×2])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
root             (?)
2g 0:00:00:00 DONE (2025-10-05 20:21) 22.22g/s 8965Kp/s 8965Kc/s 9011KC/s sal
ecorazon..room1234
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.

┌──(alex㉿kalicyse270)-[~]
└─$ john --show --format=Raw-MD5
Password files required, but none specified

┌──(alex㉿kalicyse270)-[~]
└─$ john --show --format=Raw-MD5 extracredit.txt
?:password
?:root

2 password hashes cracked, 0 left

┌──(alex㉿kalicyse270)-[~]
└─$
```