Matt Anderson U00628270 https://github.com/MattAndersonCEG3900

Laptop: Lenovo ThinkPad T400, 4 GB RAM, Intel Core 2 Duo

Phone: Samsung Galaxy S5 running Android 6.0.1

Task 1:

Screenshots/Status: Page 2-5

Task 2:

Screenshots/Status: Page 6-7

Task 3:

Screenshots/Status: Page 8

Task 4:

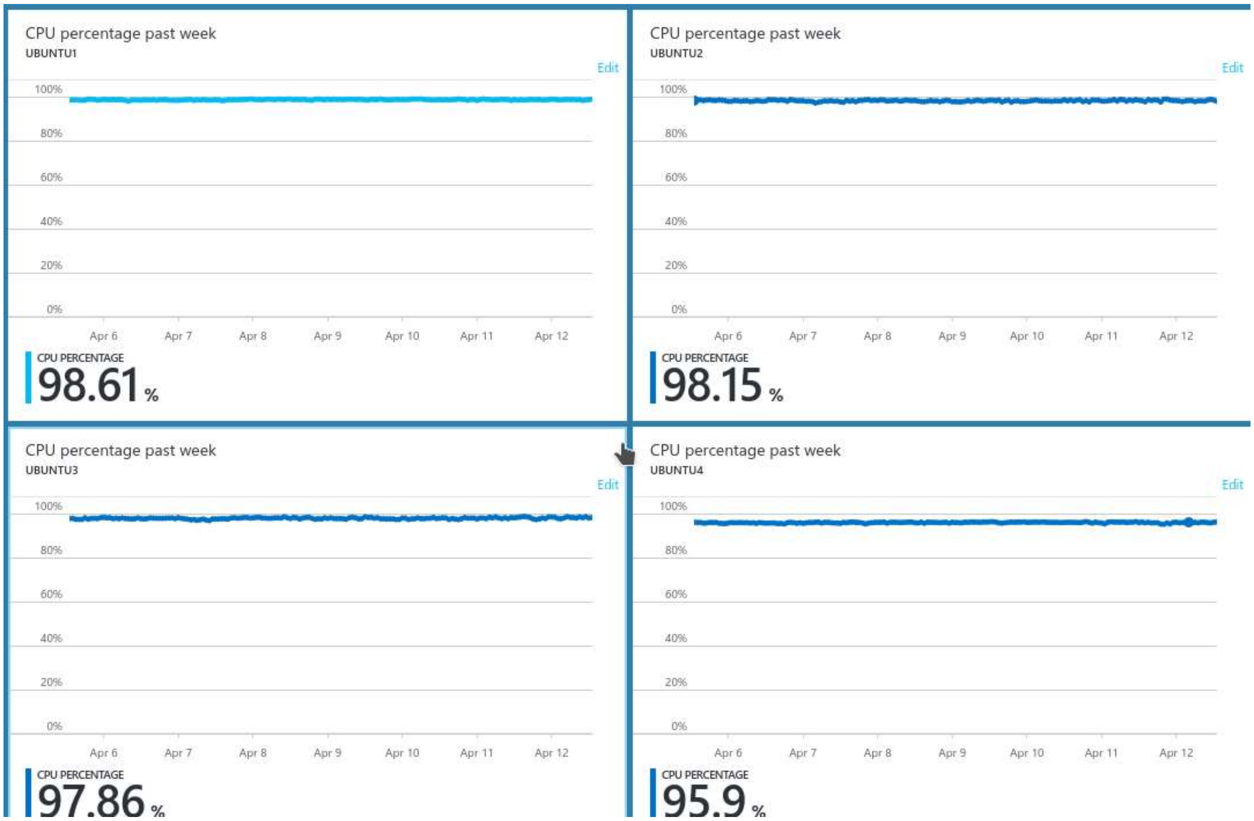
Screenshots/Status: Page 8-10

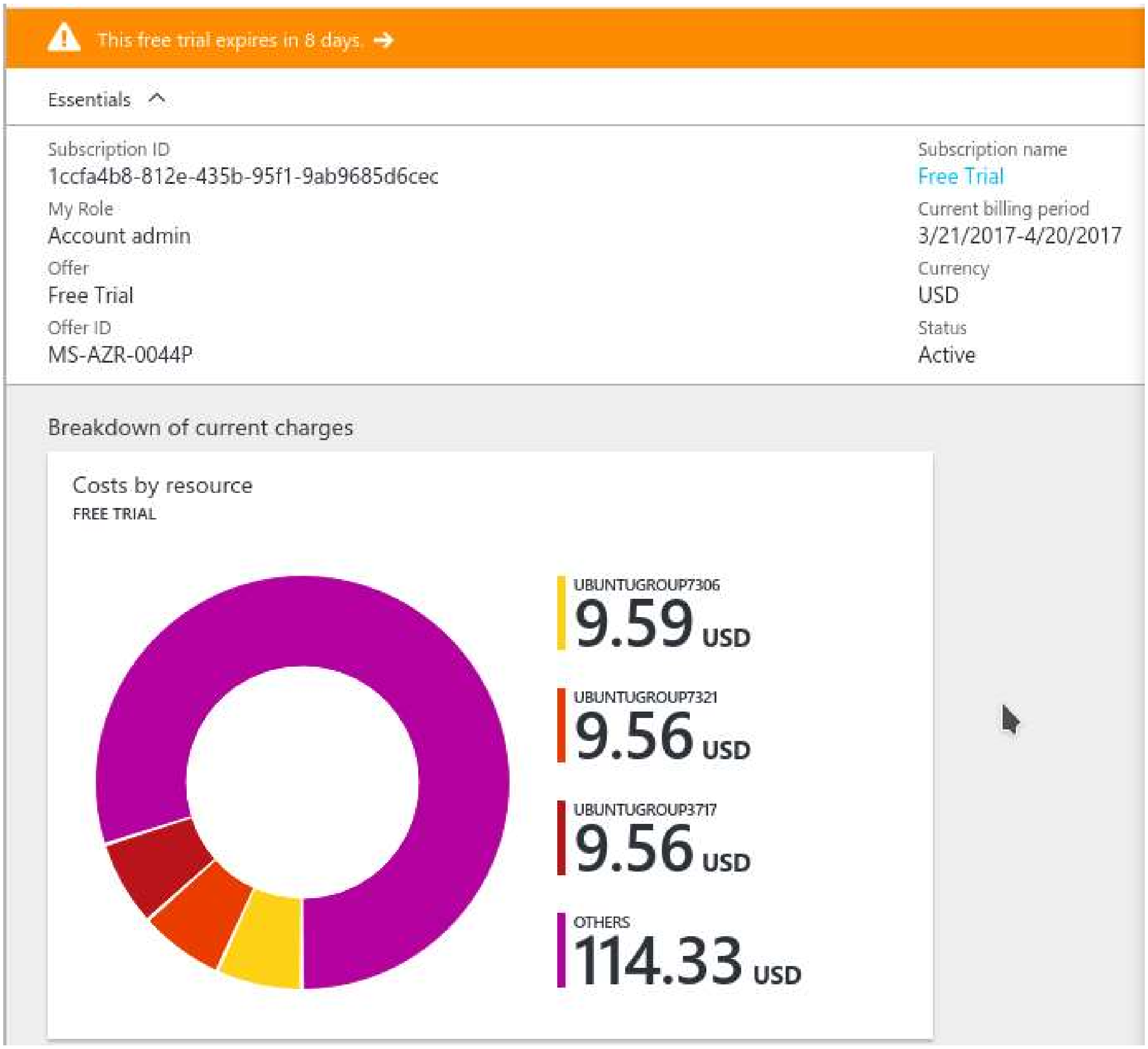
Task 5:

Screenshots/Status: Page 10-11

Task 1: Password Complexity Check with John-The-Ripper (5 hours)

I'm not sure if I've done something wrong, but my Azure VMs are still running John-The-Ripper. They were started Monday, March 27 at 3:30 PM and have hardly dropped below 90% CPU usage since. Each VM is running JTR on 13 passwords.





This free trial expires in 8 days. →

Essentials ^

Subscription ID
1ccfa4b8-812e-435b-95f1-9ab9685d6cec

My Role
Account admin

Offer
Free Trial

Offer ID
MS-AZR-0044P

Subscription name
Free Trial

Current billing period
3/21/2017-4/20/2017

Currency
USD

Status
Active

Breakdown of current charges

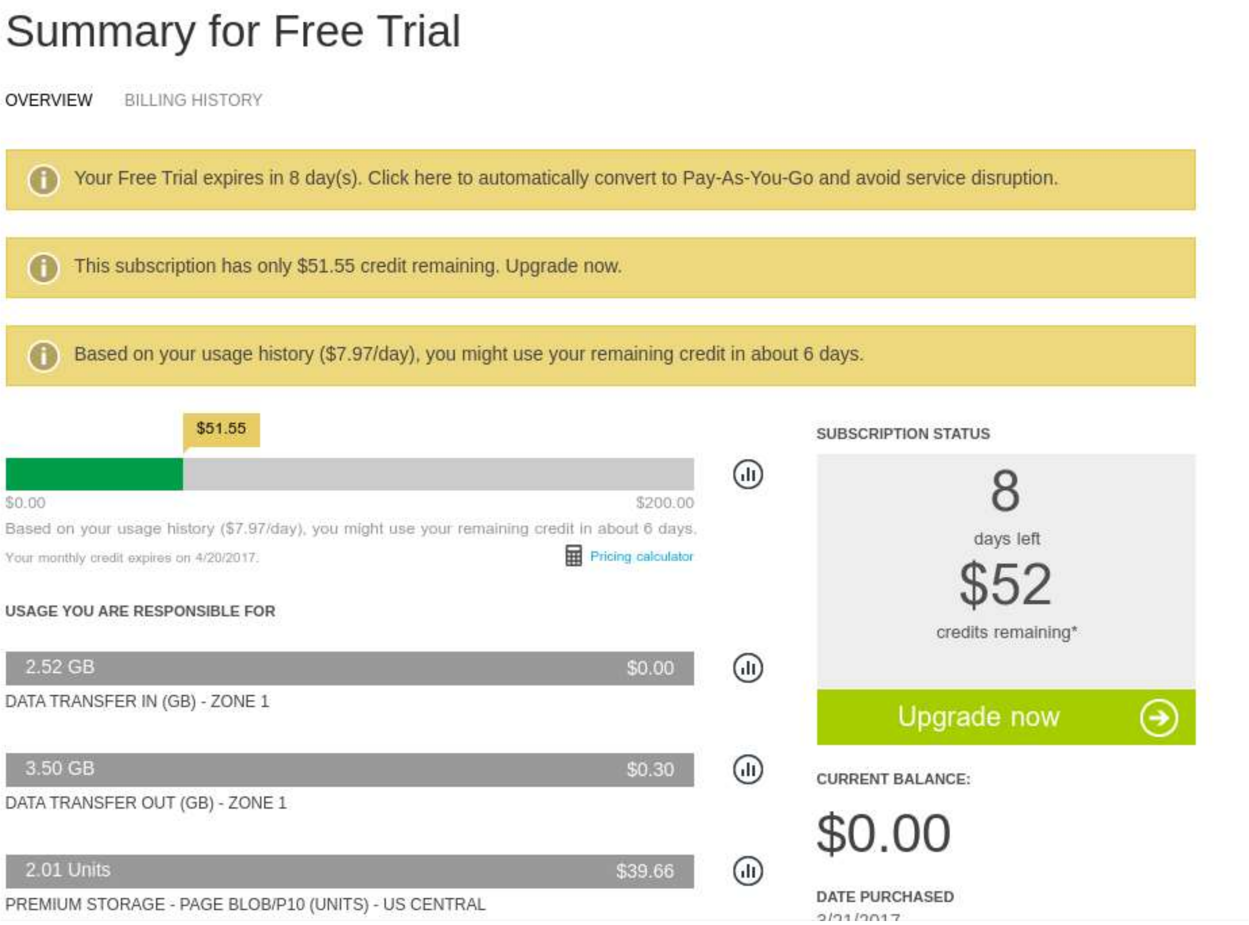
Costs by resource
FREE TRIAL

UBUNTUGROUP7306
9.59 USD

UBUNTUGROUP7321
9.56 USD

UBUNTUGROUP3717
9.56 USD

OTHERS
114.33 USD



Summary for Free Trial

OVERVIEW BILLING HISTORY

Your Free Trial expires in 8 day(s). Click here to automatically convert to Pay-As-You-Go and avoid service disruption.

This subscription has only $51.55 credit remaining. Upgrade now.

Based on your usage history ($7.97/day), you might use your remaining credit in about 6 days.

$51.55

$0.00 $200.00

Based on your usage history ($7.97/day), you might use your remaining credit in about 6 days.

Your monthly credit expires on 4/20/2017. Pricing calculator

USAGE YOU ARE RESPONSIBLE FOR

2.52 GB	$0.00
DATA TRANSFER IN (GB) - ZONE 1	
3.50 GB	$0.30
DATA TRANSFER OUT (GB) - ZONE 1	
2.01 Units	$39.66
PREMIUM STORAGE - PAGE BLOB/P10 (UNITS) - US CENTRAL	

SUBSCRIPTION STATUS

8

days left

$52

credits remaining*

Upgrade now

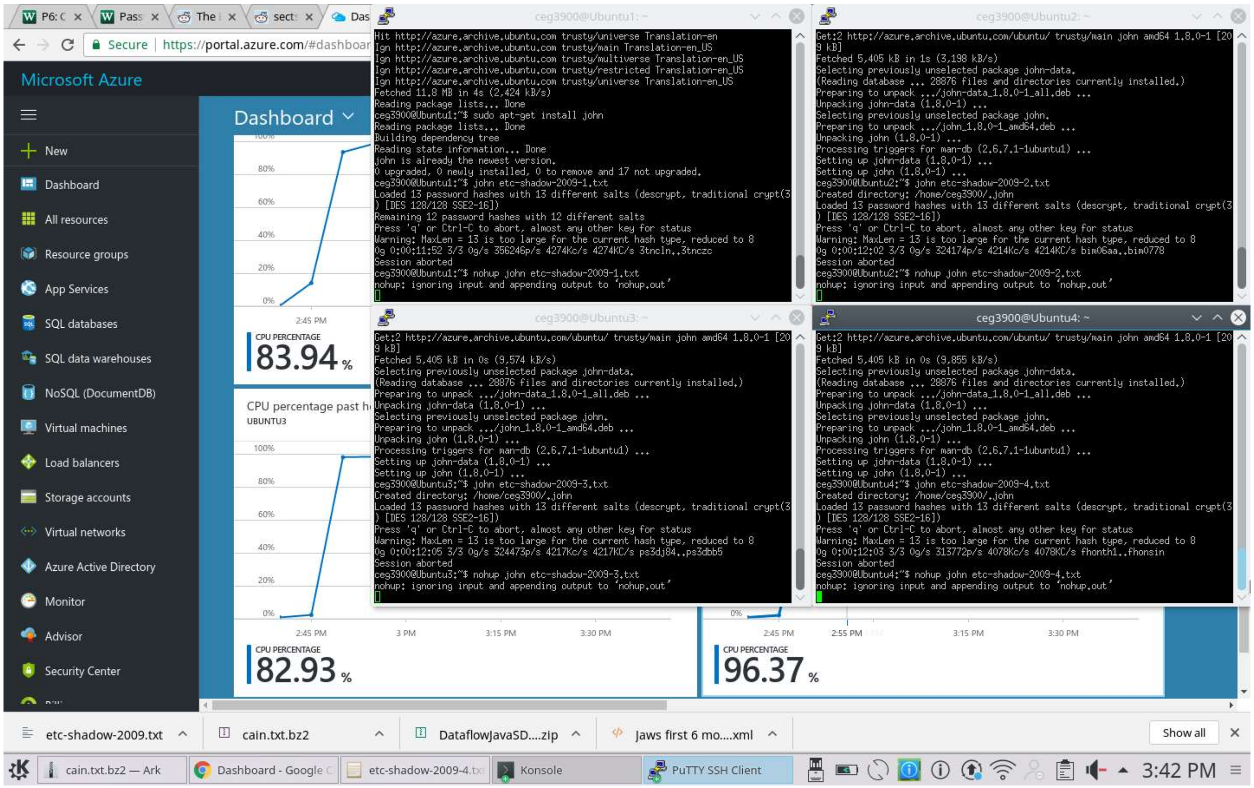
CURRENT BALANCE:

$0.00

DATE PURCHASED

3/21/2017

My computer was running for about the same duration until it froze and I've restarted JTR just in case. The program run for another 7 days and also did not complete. The bulk of this part of the assignment was in setting up Azure VMs and then installing necessary software on each of them.



```
Hit http://azure.archive.ubuntu.com trusty/universe Translation-en
Ign http://azure.archive.ubuntu.com trusty/main Translation-en_US
Ign http://azure.archive.ubuntu.com trusty/multiverse Translation-en_US
Ign http://azure.archive.ubuntu.com trusty/restricted Translation-en_US
Ign http://azure.archive.ubuntu.com trusty/universe Translation-en_US
Fetched 11.8 MB in 4s (2,424 kB/s)
Reading package lists... Done
ceg3900@Ubuntu1:~$ sudo apt-get install john
Reading package lists... Done
Building dependency tree
Reading state information... Done
john is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
ceg3900@Ubuntu1:~$ john etc-shadow-2009-1.txt
Loaded 13 password hashes with 13 different salts (descrypt, traditional crypt(3
) [DES 128/128 SSE2-16])
Remaining 12 password hashes with 12 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
0g 0:00:11:52 3/3 0g/s 356246p/s 4274Kc/s 4274KC/s 3tncln..3tnczc
Session aborted
ceg3900@Ubuntu1:~$ nohup john etc-shadow-2009-1.txt
nohup: ignoring input and appending output to ‘nohup.out’
```

```
Get:2 http://azure.archive.ubuntu.com/ubuntu/ trusty/main john amd64 1.8.0-1 [20
9 kB]
Fetched 5,405 kB in 1s (3,198 kB/s)
Selecting previously unselected package john-data.
(Reading database ... 28876 files and directories currently installed.)
Preparing to unpack .../john-data_1.8.0-1_all.deb ...
Unpacking john-data (1.8.0-1) ...
Selecting previously unselected package john.
Preparing to unpack .../john_1.8.0-1_amd64.deb ...
Unpacking john (1.8.0-1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up john-data (1.8.0-1) ...
Setting up john (1.8.0-1) ...
ceg3900@Ubuntu2:~$ john etc-shadow-2009-2.txt
Created directory: /home/ceg3900/.john
Loaded 13 password hashes with 13 different salts (descrypt, traditional crypt(3
) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
0g 0:00:12:02 3/3 0g/s 324174p/s 4214Kc/s 4214KC/s bim06aa..bim0778
Session aborted
ceg3900@Ubuntu2:~$ nohup john etc-shadow-2009-2.txt
nohup: ignoring input and appending output to ‘nohup.out’
```

```
Get:2 http://azure.archive.ubuntu.com/ubuntu/ trusty/main john amd64 1.8.0-1 [20
9 kB]
Fetched 5,405 kB in 0s (9,574 kB/s)
Selecting previously unselected package john-data.
(Reading database ... 28876 files and directories currently installed.)
Preparing to unpack .../john-data_1.8.0-1_all.deb ...
Unpacking john-data (1.8.0-1) ...
Selecting previously unselected package john.
Preparing to unpack .../john_1.8.0-1_amd64.deb ...
Unpacking john (1.8.0-1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up john-data (1.8.0-1) ...
Setting up john (1.8.0-1) ...
ceg3900@Ubuntu3:~$ john etc-shadow-2009-3.txt
Created directory: /home/ceg3900/.john
Loaded 13 password hashes with 13 different salts (descrypt, traditional crypt(3
) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
0g 0:00:12:05 3/3 0g/s 324473p/s 4217Kc/s 4217KC/s ps3dj84..ps3dbb5
Session aborted
ceg3900@Ubuntu3:~$ nohup john etc-shadow-2009-3.txt
nohup: ignoring input and appending output to ‘nohup.out’
```

```
Get:2 http://azure.archive.ubuntu.com/ubuntu/ trusty/main john amd64 1.8.0-1 [20
9 kB]
Fetched 5,405 kB in 0s (9,855 kB/s)
Selecting previously unselected package john-data.
(Reading database ... 28876 files and directories currently installed.)
Preparing to unpack .../john-data_1.8.0-1_all.deb ...
Unpacking john-data (1.8.0-1) ...
Selecting previously unselected package john.
Preparing to unpack .../john_1.8.0-1_amd64.deb ...
Unpacking john (1.8.0-1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up john-data (1.8.0-1) ...
Setting up john (1.8.0-1) ...
ceg3900@Ubuntu4:~$ john etc-shadow-2009-4.txt
Created directory: /home/ceg3900/.john
Loaded 13 password hashes with 13 different salts (descrypt, traditional crypt(3
) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
0g 0:00:12:03 3/3 0g/s 313772p/s 4078Kc/s 4078KC/s fhonth1..fhonsin
Session aborted
ceg3900@Ubuntu4:~$ nohup john etc-shadow-2009-4.txt
nohup: ignoring input and appending output to ‘nohup.out’
```

Task 2: Hashcat (9 hour)

Hashcat is still giving me the error that it requires OCL to use. In my research I have not been able to find a solution to this problem.. This shouldn't be a problem though, since we're supposed to be able to use the CPU to use Hashcat and aren't supposed to be required to use a GPU.

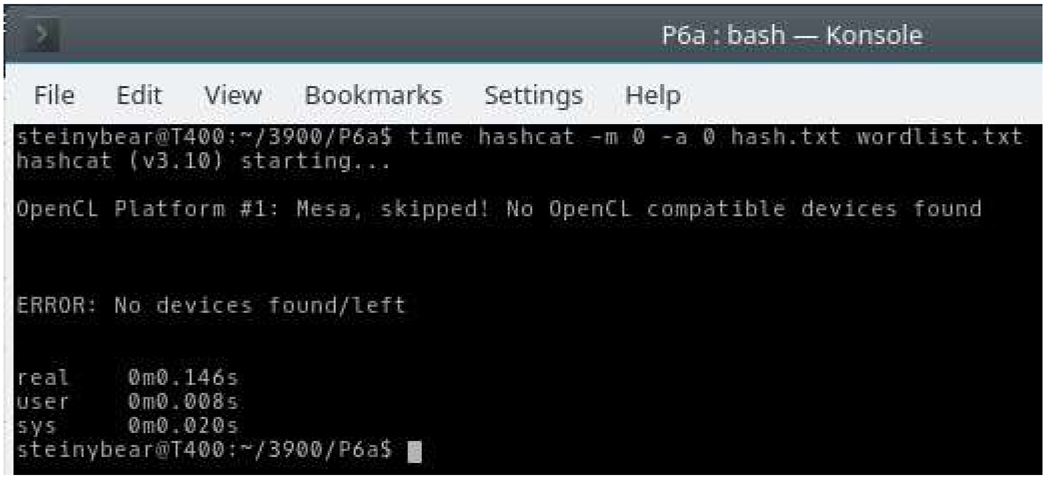
The "toggle2.rule" Hashcat rule is set up to try toggling 1 and 2 characters in the password at a time. Since the rule appears to be considering passwords of length 15 (indices 0 through E), this is a very incomplete rule. For example, if the password we are performing the rule on is "pass":

Tested Passwords: Pass, pAss, paSs, pasS, PAss, PaSs, PasS, pASs, pAsS, paSS

Untested Passwords: PASs, PAsS, pASS, PASS

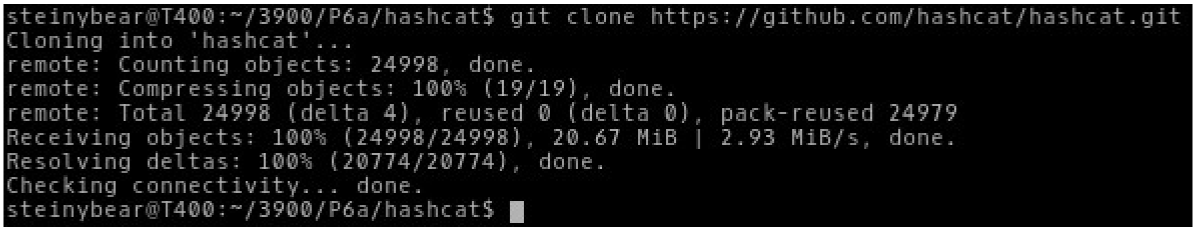
For each character in length that the password has above 2, more and more untested combinations exist.

Since I can't get Hashcat to run at all, I'm currently unable to create an APK that runs it.

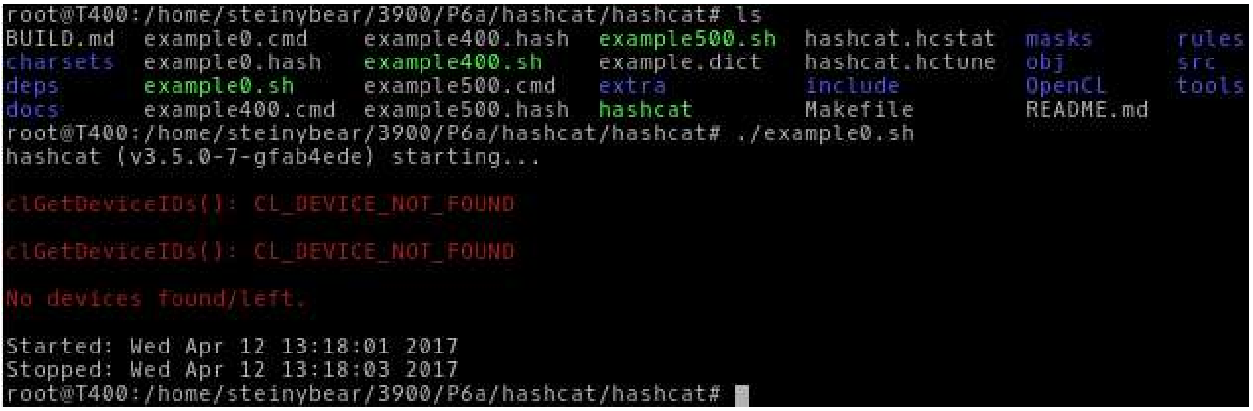


```
steinybear@T400:~/3900/P6a$ time hashcat -m 0 -a 0 hash.txt wordlist.txt
hashcat (v3.10) starting...

OpenCL Platform #1: Mesa, skipped! No OpenCL compatible devices found



ERROR: No devices found/left


real    0m0.146s
user    0m0.008s
sys     0m0.020s
steinybear@T400:~/3900/P6a$
```

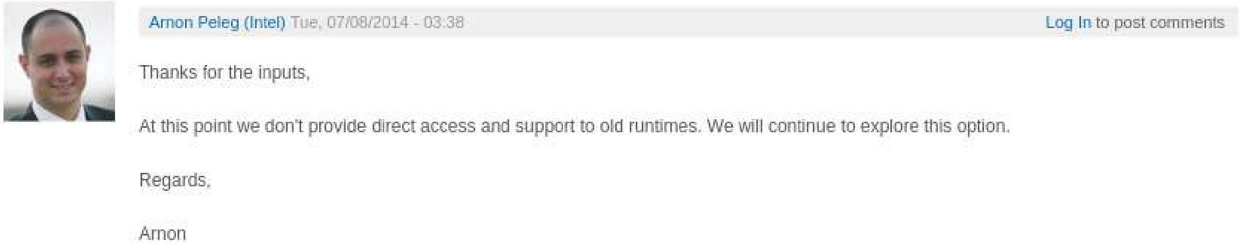
I spent a lot more time researching my error and the fact that it was requiring me to run OpenCL on my GPU instead of using my CPU and could not find a solution. I did confirm that my CPU does not support OpenCL (I do not have a dedicated graphics card). I also followed Dr. Mateti's suggestion of cloning the Hashcat repository for a more complete installation but ended up receiving the same errors.



```
steinybear@T400:~/3900/P6a/hashcat$ git clone https://github.com/hashcat/hashcat.git
Cloning into 'hashcat'...
remote: Counting objects: 24998, done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 24998 (delta 4), reused 0 (delta 0), pack-reused 24979
Receiving objects: 100% (24998/24998), 20.67 MiB | 2.93 MiB/s, done.
Resolving deltas: 100% (20774/20774), done.
Checking connectivity... done.
steinybear@T400:~/3900/P6a/hashcat$
```



```
root@T400:/home/steinybear/3900/P6a/hashcat/hashcat# ls
BUILD.md  example0.cmd    example400.hash  example500.sh  hashcat.hcstat  masks     rules
charsets  example0.hash   example400.sh    example.dict   hashcat.hctune  obj       src
deps      example0.sh     example500.cmd   extra          include         OpenCL    tools
docs      example400.cmd  example500.hash  hashcat        Makefile        README.md
root@T400:/home/steinybear/3900/P6a/hashcat/hashcat# ./example0.sh
hashcat (v3.5.0-7-gfab4ede) starting...

clGetDeviceIDs(): CL_DEVICE_NOT_FOUND

clGetDeviceIDs(): CL_DEVICE_NOT_FOUND

No devices found/left.

Started: Wed Apr 12 13:18:01 2017
Stopped: Wed Apr 12 13:18:03 2017
root@T400:/home/steinybear/3900/P6a/hashcat/hashcat#
```



Arnon Peleg (Intel) Tue, 07/08/2014 - 03:38

Thanks for the inputs,

At this point we don't provide direct access and support to old runtimes. We will continue to explore this option.

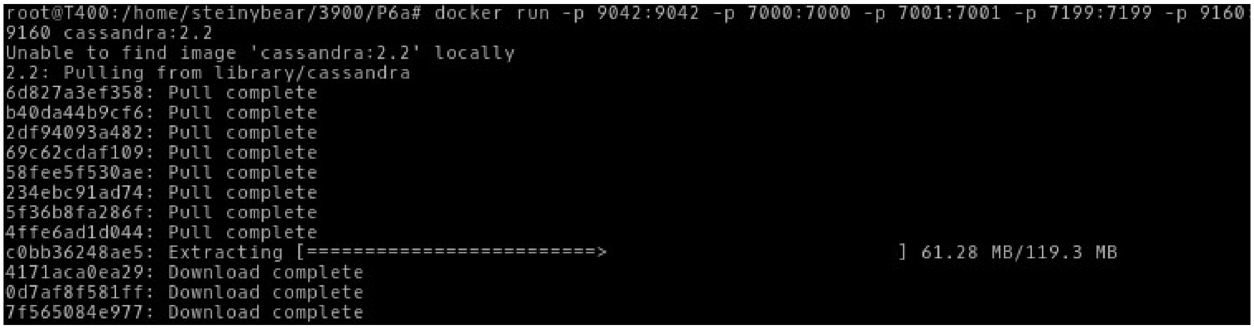
Regards,

Arnon

Task 3: Computing the Rainbow Tables in the Cloud

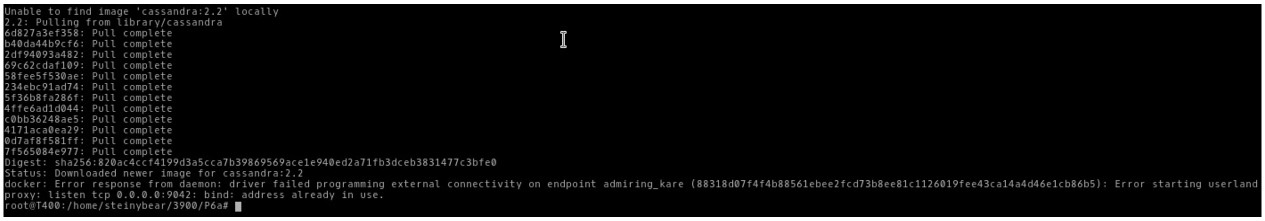
I’m unable to get Hashcat to run at all so all my time spent on Hashcat has been spent on Task 2 trying to get it running.

Task 4: Using Docker for Rainbow Tables (6 hours)



```
root@T400:/home/steinybear/3900/P6a# docker run -p 9042:9042 -p 7000:7000 -p 7001:7001 -p 7199:7199 -p 9160:
9160 cassandra:2.2
Unable to find image 'cassandra:2.2' locally
2.2: Pulling from library/cassandra
6d827a3ef358: Pull complete
b40da44b9cf6: Pull complete
2df94093a482: Pull complete
69c62cdaf109: Pull complete
58fee5f530ae: Pull complete
234ebc91ad74: Pull complete
5f36b8fa286f: Pull complete
4ffe6ad1d044: Pull complete
c0bb36248ae5: Extracting [=========================>                         ] 61.28 MB/119.3 MB
4171aca0ea29: Download complete
0d7af8f581ff: Download complete
7f565084e977: Download complete
```

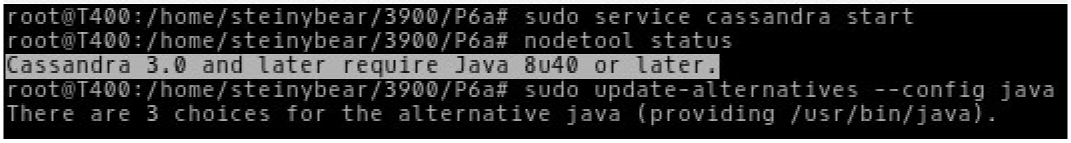
Getting all the software installed initially was no problem. The above screenshot is an attempt at running an example from the painbow documentation.



```
Unable to find image 'cassandra:2.2' locally
2.2: Pulling from library/cassandra
6d827a3ef358: Pull complete
b40da44b9cf6: Pull complete
2df94093a482: Pull complete
69c62cdaf109: Pull complete
58fee5f530ae: Pull complete
234ebc91ad74: Pull complete
5f36b8fa286f: Pull complete
4ffe6ad1d044: Pull complete
c0bb36248ae5: Pull complete
4171aca0ea29: Pull complete
0d7af8f581ff: Pull complete
7f565084e977: Pull complete
Digest: sha256:820ac4ccf4199d3a5cca7b39869569ace1e940ed2a71fb3dceb3831477c3bfe0
Status: Downloaded newer image for cassandra:2.2
docker: Error response from daemon: driver failed programming external connectivity on endpoint admiring_kare (88318d07f4f4b88561ebee2fcd73b8ee81c1126019fee43ca14a4d46e1cb86b5): Error starting userland
proxy: listen tcp 0.0.0.0:9042: bind: address already in use.
root@T400:/home/steinybear/3900/P6a#
```

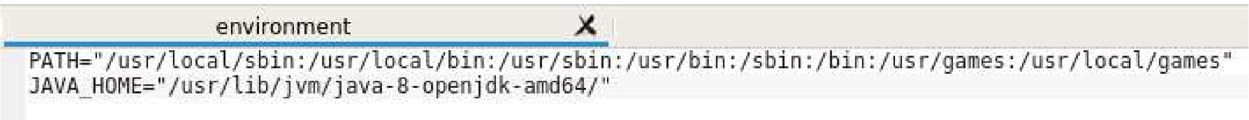
However, I couldn’t get Cassandra to launch. I tried starting it manually before running the docker command and it gave me an error that I wasn’t using Java 8. I confirmed with:

```
update-alternatives --config java
```



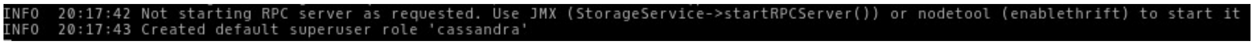
```
root@T400:/home/steinybear/3900/P6a# sudo service cassandra start
root@T400:/home/steinybear/3900/P6a# nodetool status
Cassandra 3.0 and later require Java 8u40 or later.
root@T400:/home/steinybear/3900/P6a# sudo update-alternatives --config java
There are 3 choices for the alternative java (providing /usr/bin/java).
```

But the error persisted. I found something online that suggested editing the /etc/environment file to force the usage of Java 8



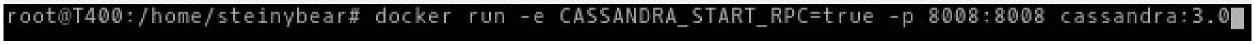
```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games"
JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64/"
```

The java version error is now gone but the RPC server won't start.



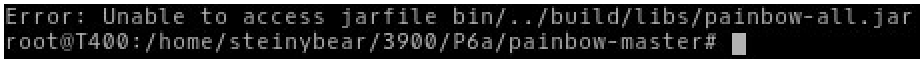
```
INFO  20:17:42 Not starting RPC server as requested. Use JMX (StorageService->startRPCServer()) or nodetool (enablethrift) to start it
INFO  20:17:43 Created default superuser role 'cassandra'
```

This doesn't appear to be a common error because I couldn't find anything relating to it directly. I did find an idea to try to run it and force the RPC to start.



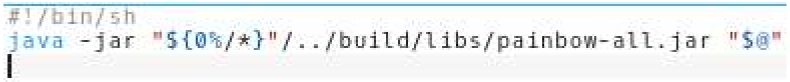
```
root@T400:/home/steinybear# docker run -e CASSANDRA_START_RPC=true -p 8008:8008 cassandra:3.0
```

Doing this launched the docker running Cassandra with no further errors. However, when I try to run painbow:



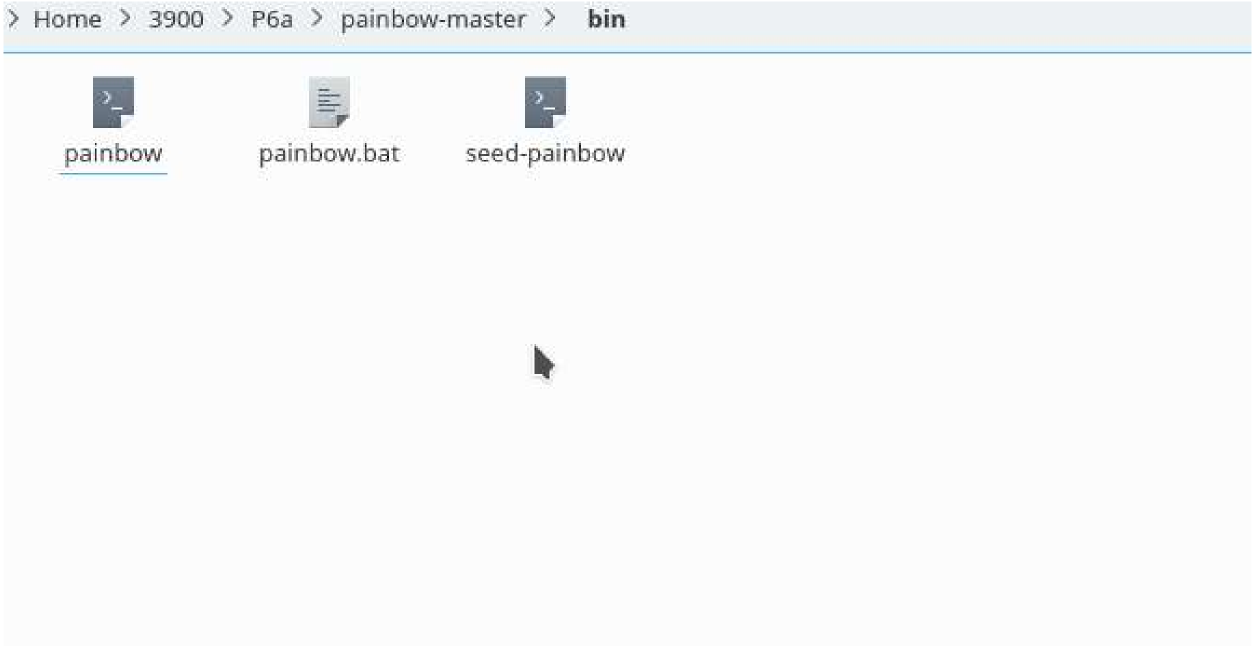
```
Error: Unable to access jarfile bin/../build/libs/painbow-all.jar
root@T400:/home/steinybear/3900/P6a/painbow-master#
```

Doing further research, it was suggested that I confirm the contents of the painbow script that I'm attempting to run.



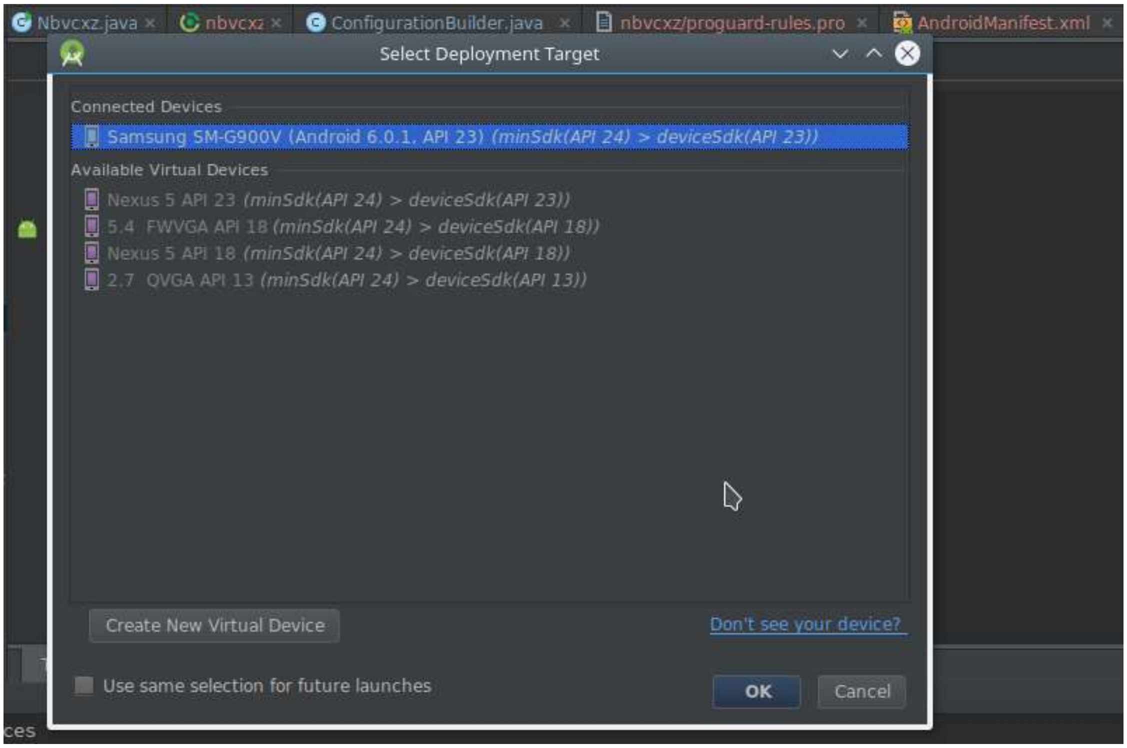
```
#!/bin/sh
java -jar "${0%/*}"/../build/libs/painbow-all.jar "$@"
```

The file does not exist and I'm unable to find it anywhere on my hard drive. Reinstalling did not place this jar anywhere on my machine either.



Task 5: Enhance Password-Help Task#5 of P5 (9 hours)

I took the PasswordHelper APK from P5 and imported nbvcxz as a module. I had to do a fair amount of wrestling for it to even accept the build. For a while, it kept telling me that Java 1.7 didn't permit lambdas even though I was using Java 1.8. Eventually I just removed the lambda functionality from the APK and it silenced the errors. Now it's telling me that nbvcxz requires API 24 to function.



Nbvcxz.java × | nbvcxz × | ConfigurationBuilder.java × | nbvcxz/proguard-rules.pro × | AndroidManifest.xml ×

Select Deployment Target

Connected Devices

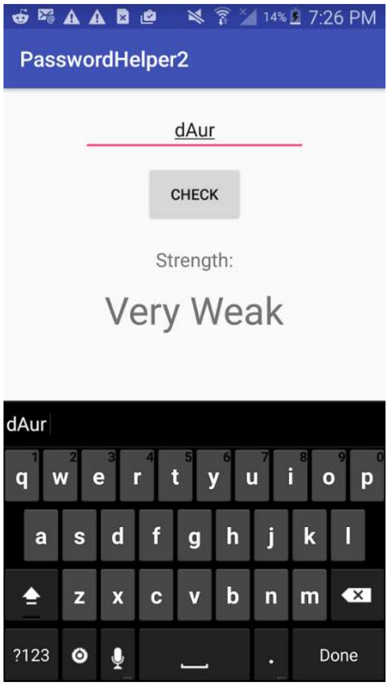
Samsung SM-G900V (Android 6.0.1, API 23) *(minSdk(API 24) > deviceSdk(API 23))*

Available Virtual Devices

Nexus 5 API 23 *(minSdk(API 24) > deviceSdk(API 23))*
5.4 FWVGA API 18 *(minSdk(API 24) > deviceSdk(API 18))*
Nexus 5 API 18 *(minSdk(API 24) > deviceSdk(API 18))*
2.7 QVGA API 13 *(minSdk(API 24) > deviceSdk(API 13))*

Create New Virtual Device
Don't see your device?
□ Use same selection for future launches
OK
Cancel

I gave up on trying to import the library and get it to function on my machine. I took some basic concepts of password strength and bits of entropy and applied it to my project.

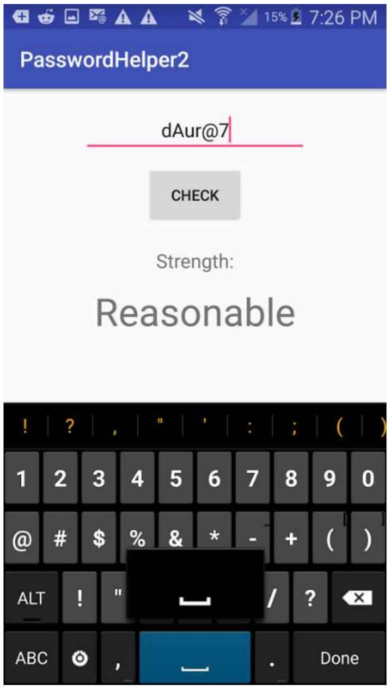


PasswordHelper2

dAur

Strength:

Very Weak

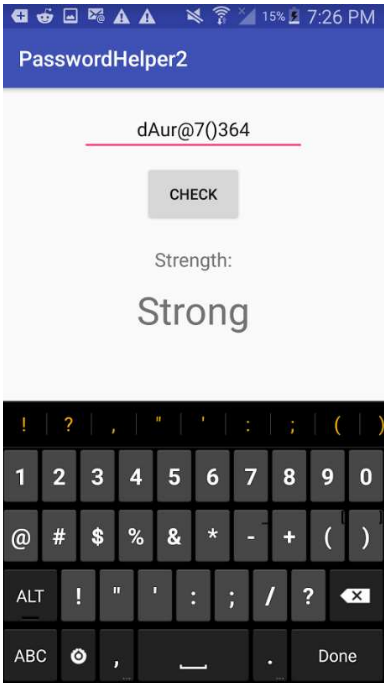


PasswordHelper2

dAur@7

Strength:

Reasonable



PasswordHelper2

dAur@7()364

Strength:

Strong

Total Time: About 29 hours (30 including making the report)