0

Lab-3: Cracking password with John

1. Once you connect to your VM using RDP or SSH, and run the ssudo apt-get purge john -y && sudo snap install john-the-ripper && sudo reboot command in you VM.
2. Your VM will be closed but you cna re-establish you session via ssh and RDp to access the VM.
3. Next, go ahead and unzip the folder (you can use the unzip command) and take a look at the files (using ls). You should have:

- crackA.txt
- crackB.txt
- crackC.txt
- crackChallenge.txt
- lower.lst

4. Once you do that run the following command to get the wordlists from the web in the terminal
   wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

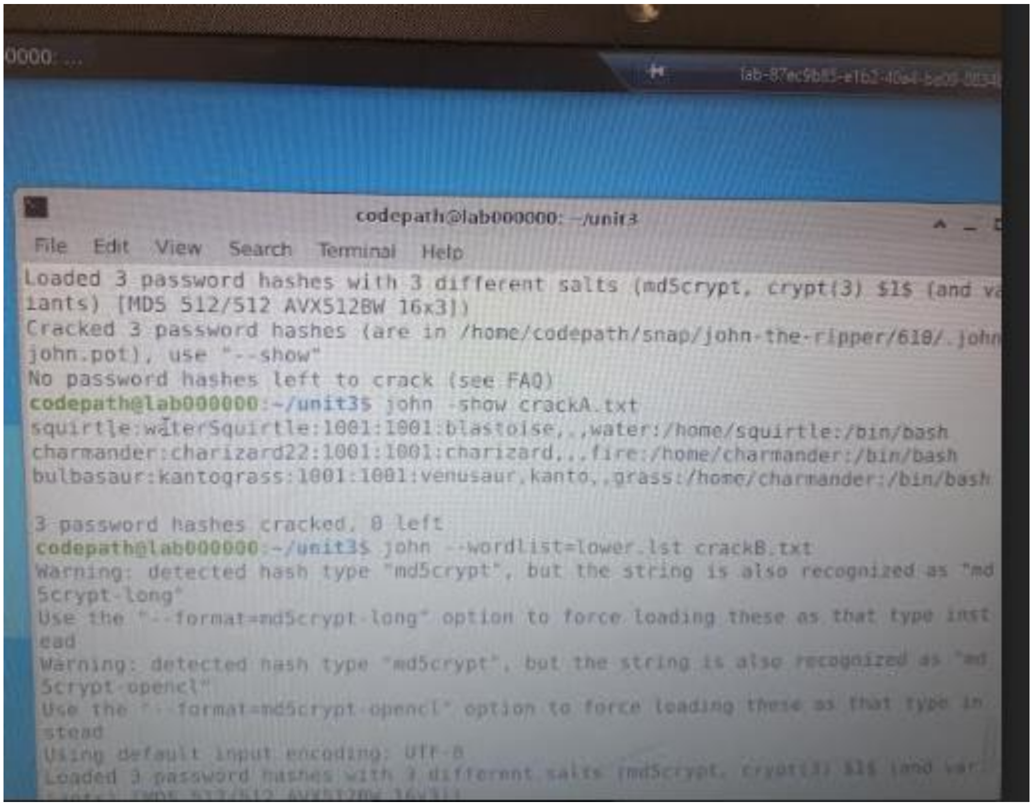
5. You should have the following files in your unti3 folder.

   ```
   codepath@lab000001:~/unit3$ ls
   crackfiles.zip rockyou.txt cp_leak.txt
   ```

6. Run the following command: less -N ./rockyou.txt and you should see a big word list showing up. You can search for a word using & and look up its form such as &puppy.

7. Now, it seems that this word list is ok. Let’s try to crack passwords

8. For crackA.txt,run the following command john --single crackA.txt and you should be able to crack the passwords.

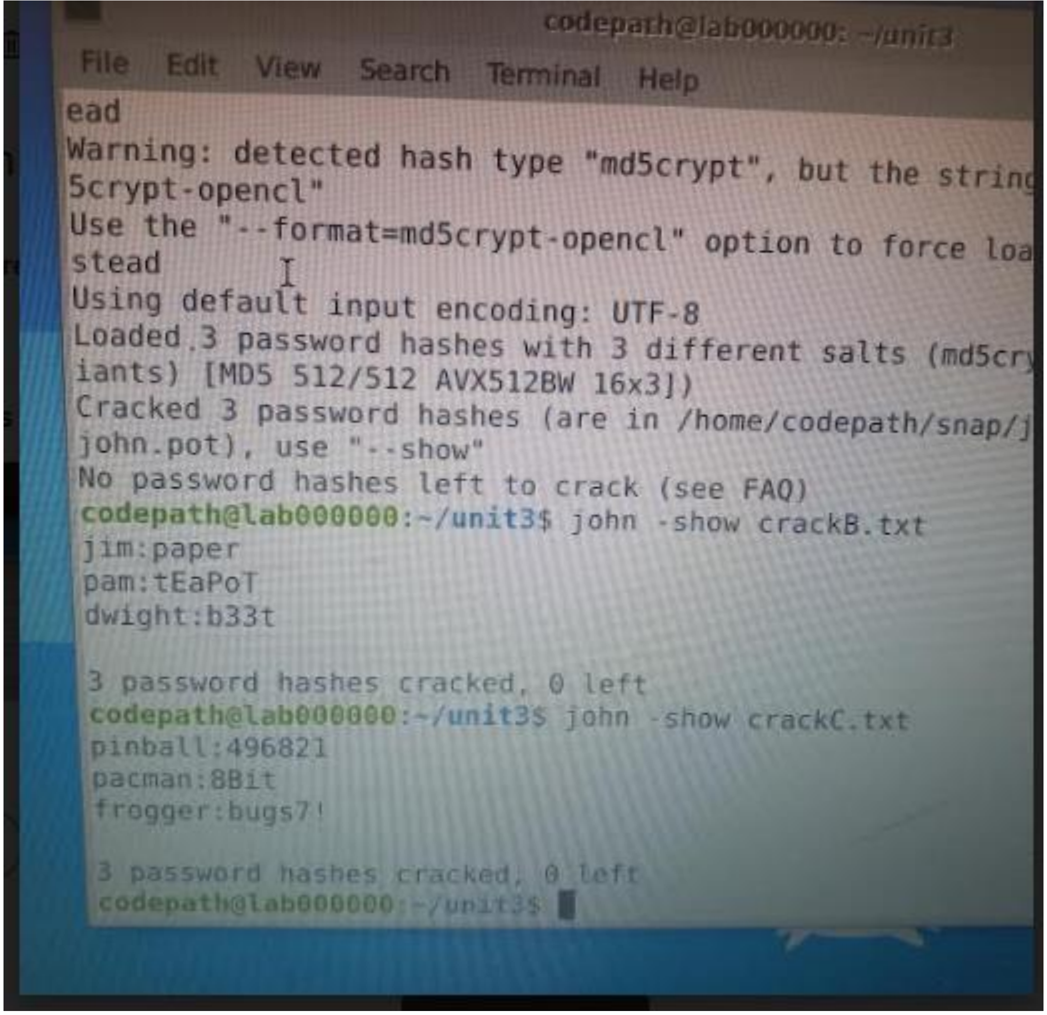


```
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and va
iants) [MD5 512/512 AVX512BW 16x3])
Cracked 3 password hashes (are in /home/codepath/snap/john-the-ripper/618/.john
john.pot), use "--show"
No password hashes left to crack (see FAQ)
codepath@lab000000:~/unit3$ john -show crackA.txt
squirtle:waterSquirtle:1001:1001:blastoise,,,water:/home/squirtle:/bin/bash
charmander:charizard22:1001:1001:charizard,,,fire:/home/charmander:/bin/bash
bulbasaur:kantograss:1001:1001:venusaur,kanto,,grass:/home/charmander:/bin/bash

3 password hashes cracked, 0 left
codepath@lab000000:~/unit3$ john --wordlist=lower.lst crackB.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md
5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type inst
ead
Warning: detected hash type "md5crypt", but the string is also recognized as "md
5crypt-opencl"
Use the "--format=md5crypt-opencl" option to force loading these as that type in
stead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and var
iants) [MD5 512/512 AVX512BW 16x3])
```

9. For crackB txt, run john --wordlist=lower.lst crackB.txt to crack Jim’s password, john --wordlist=lower.lst crackB.txt --rules=l33t to crack Dwight’s password, and john --wordlist=lower.lst crackB.txt --rules=shifttoggle

to crack Pam’s password.


codepath@lab000000: ~/unit3
File Edit View Search Terminal Help

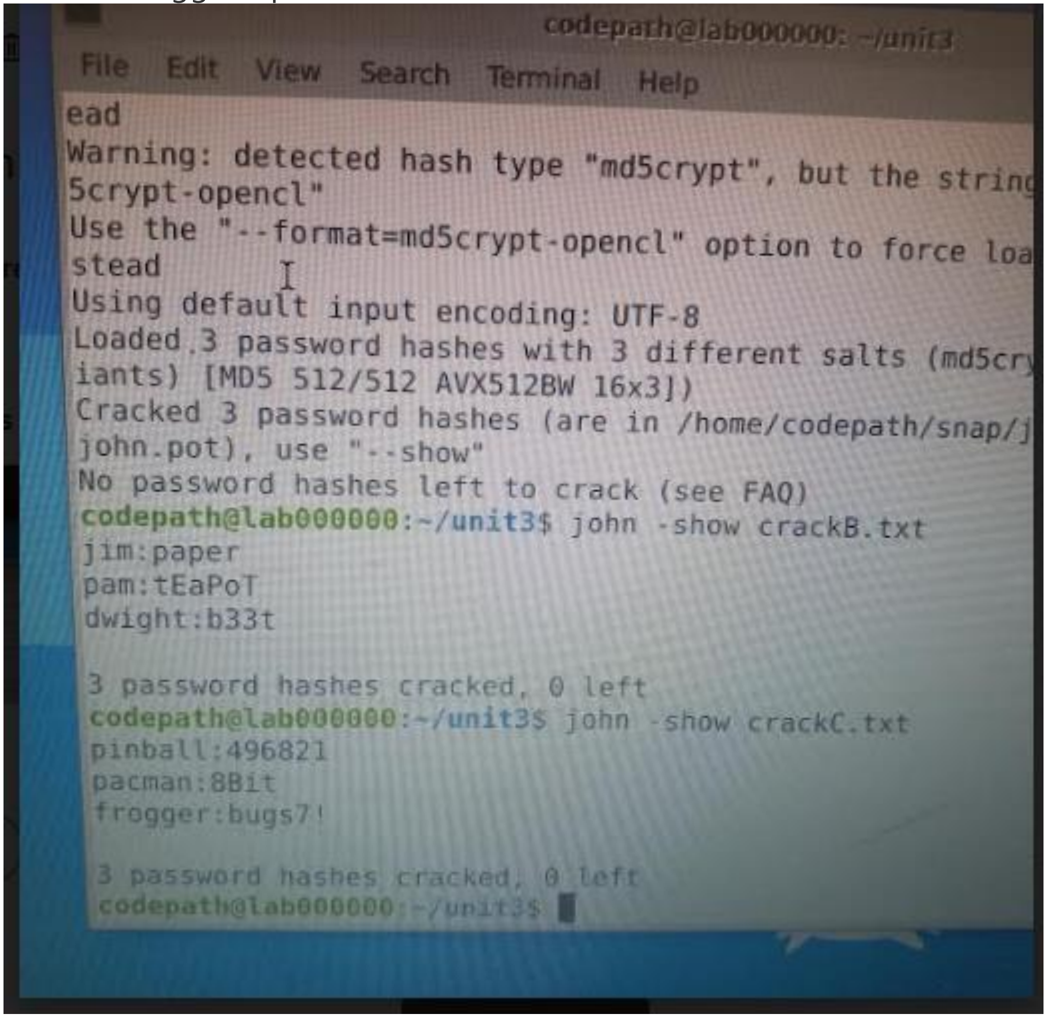
```
ead
Warning: detected hash type "md5crypt", but the strin
5crypt-opencl"
Use the "--format=md5crypt-opencl" option to force loa
stead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5cr
iants) [MD5 512/512 AVX512BW 16x3])
Cracked 3 password hashes (are in /home/codepath/snap/j
john.pot), use "--show"
No password hashes left to crack (see FAQ)
codepath@lab000000:~/unit3$ john -show crackB.txt
jim:paper
pam:tEaPoT
dwight:b33t

3 password hashes cracked, 0 left
codepath@lab000000:~/unit3$ john -show crackC.txt
pinball:496821
pacman:8Bit
frogger:bugs7!

3 password hashes cracked, 0 left
codepath@lab000000:~/unit3$
```

10. For crackC.txt, we can run john --incremental=digits --min-length=4 --max-length=6 crackC.txt to crack pinball’s passwords, john --mask=?d?u?l?l crackC.txt to crack pacman’s passwords, and john --mask=?l?l?l?l?d! crackC.txt

to crack frogger’s password.


codepath@lab000000: ~/unit3
File Edit View Search Terminal Help

```
ead
Warning: detected hash type "md5crypt", but the string
5crypt-opencl"
Use the "--format=md5crypt-opencl" option to force loa
stead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5cr
iants) [MD5 512/512 AVX512BW 16x3])
Cracked 3 password hashes (are in /home/codepath/snap/j
john.pot), use "--show"
No password hashes left to crack (see FAQ)
codepath@lab000000:~/unit3$ john -show crackB.txt
jim:paper
pam:tEaPoT
dwight:b33t

3 password hashes cracked, 0 left
codepath@lab000000:~/unit3$ john -show crackC.txt
pinball:496821
pacman:8Bit
frogger:bugs7!

3 password hashes cracked, 0 left
codepath@lab000000:~/unit3$
```

11. You can see your passwords in using ~~/snap/john-the-ripper/610/.john/john.pot command and use less to see the passwords you cracked.

Expand allBack to topGo to bottom

Select a repo

Edit Note Details

Change note title, set tags, cover photos, and other metadata here.

SkipNext