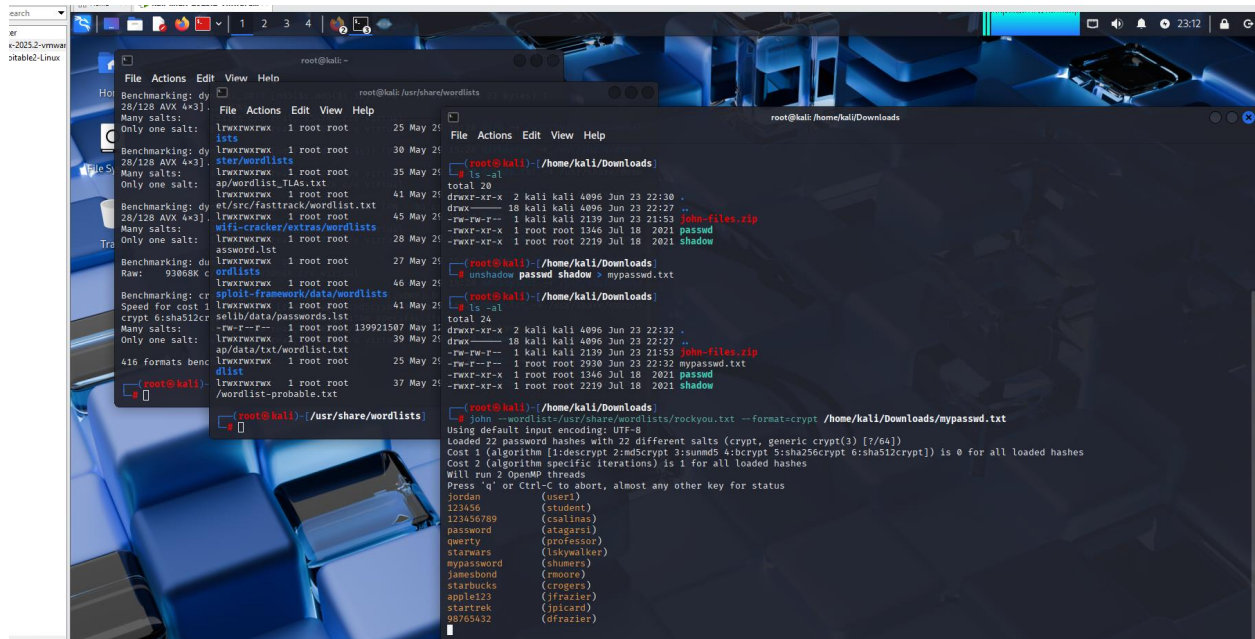


Fundamentals of Information Security: Cybersecurity (88252)

Ana Herrera Flores

Security Lab 6 - Cryptography Attacks



```
root@kali: ~  
File Actions Edit View Help  
root@kali: /usr/share/wordlists  
File Actions Edit View Help  
root@kali: /home/kali/Downloads  
File Actions Edit View Help  
root@kali: ~  
ls -al  
total 20  
drwxr-xr-x 2 kali kali 4096 Jun 23 22:30 .  
drwxr-xr-x 18 kali kali 4096 Jun 23 22:27 ..  
-rw-rw-r-- 1 kali kali 2139 Jun 23 21:53 john-files.zip  
-rw-rw-r-- 1 root root 1346 Jul 18 2021 passwd  
-rw-rw-r-- 1 root root 2219 Jul 18 2021 shadow  
root@kali: ~  
ls -al  
total 24  
drwxr-xr-x 2 kali kali 4096 Jun 23 22:32 .  
drwxr-xr-x 18 kali kali 4096 Jun 23 22:27 ..  
-rw-rw-r-- 1 kali kali 2139 Jun 23 21:53 john-files.zip  
-rw-rw-r-- 1 root root 2630 Jun 23 22:32 mypasswd.txt  
-rw-rw-r-- 1 root root 1346 Jul 18 2021 passwd  
-rw-rw-r-- 1 root root 2219 Jul 18 2021 shadow  
root@kali: ~  
john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt /home/kali/Downloads/mypasswd.txt  
Using default input encoding: UTF-8  
Loaded 22 password hashes with 22 different salts (crypt, generic crypt(3) [7/64])  
Cost 1 (algorithm [1:decrypt 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  
jordan (user)  
123456 (student)  
123456789 (csalinas)  
password (stagsari)  
querty (professor)  
starwars (lskywalker)  
mypassword (shumers)  
jamesbond (rmooze)  
starbucks (crogers)  
apple123 (jfrazier)  
startrek (jpicaard)  
00763632 (dfrazier)
```

This is a general screenshot of the steps in exercises 1 and 2.

Exercise 3 – Analysis and What to Turn-In

By default, “John the Ripper” will place the cracked accounts in the ~/.john directory. Since we ran this as “root”, we will find the files in /root/.john

From the root login shell.

```
cd /root/.john
```

```
ls -al
```

1- Notice above, we have 3 files. Do a cat on the 3 files and answer the following questions below. Example: cat john.log

a. Which one of the 3 files has the accounts that were cracked? Provide a snippet.

As we can see “cat john.log” is the file that contains those accounts that were cracked.

```
-rw-r--r-- 1 root root 243 Jun 23 23:13 john.rec
```

```
(root@kali)~/john
# cat john.log
0:00:00:00 Starting a new session
0:00:00:00 Loaded a total of 22 password hashes with 22 different salts
0:00:00:00 Sorting salts, for deterministic salt-resume
0:00:00:00 Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
0:00:00:00 Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
0:00:00:00 Command line: john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt /home/kali/Downloads/mypasswd.txt
0:00:00:00 - UTF-8 input encoding enabled
0:00:00:00 - Passwords will be stored UTF-8 encoded in .pot file
0:00:00:00 - Hash type: crypt, generic crypt(3) (min-len 0, max-len 24 [worst case UTF-8] to 72 [ASCII])
0:00:00:00 - Algorithm: ?/64
0:00:00:00 - Will reject candidates longer than 72 bytes
0:00:00:00 - Candidate passwords will be buffered and tried in chunks of 96
0:00:00:00 Proceeding with wordlist mode
0:00:00:00 - Wordlist file: /usr/share/wordlists/rockyou.txt
0:00:00:00 - memory mapping wordlist (139921507 bytes)
0:00:00:00 - No word mangling rules
0:00:00:00 - No stacked rules
0:00:00:04 + Cracked user1
0:00:00:05 + Cracked student
0:00:00:08 + Cracked csalinas
0:00:00:09 + Cracked atagarsi
0:00:00:15 + Cracked professor
0:00:01:37 + Cracked lskywalker
0:00:05:04 + Cracked shumers
0:00:06:32 + Cracked rmoore
0:00:07:11 + Cracked crogers
0:00:09:40 + Cracked jfrazier
0:00:12:57 + Cracked jpicaard
0:00:13:38 + Cracked dfrazier

(root@kali)~/john
#
```

b. Which one of the 3 files has the cracked hash values? Provide a snippet

As we can see "cat john.pot" is the one that provides the hash values of the accounts that were cracked.

```
(root@kali)~/john
# cat john.pot
$y$j9T$SPU97vfq0LhzYftoxke091$MpwJ.rGBhPgCCLa/ZI6mQh/zhIRqod0zyv7uXUaTI5.:jordan
$y$j9T$WSh/IqzfQM//wqdlktWuH.$FK9mp5uqTeKSFXaWwz4gJEAnh93/vlXRA1WFI5.pUM.:123456
$y$j9T$f/Ir/8EjUoMu9o7lICJAD/$/h6j1sJpMj0hZPxTPhuCiJEb7MTrC8.NrOIu7ZKMPXA:123456789
$y$j9T$fPwJBgP3kL7IgJyZhbaDi1$0yN9yLIXlfvt7kA8MxJyZ50lto6hJnDTY7yGMW9aXqD:password
$y$j9T$u.fjJcpzVoHLwrdKlivvg.$WGXyOZTP.TTdMWtBWp59i8C4ZvqjnyBbu1sZNcWdX42:qwerty
$y$j9T$lyY7chdOMApRwm58S2rWe1$kJKs3TXzGf/s2UCNFLE3BvxJckBbJgmuj4y.egI7ER8:starwars
$y$j9T$d1mWKa4kShibHJw0sh7a00$hi9le6d36FVNdX9SQmpZ4eXeyt2W/JzQLjIpz4kMzN2:mypassword
$y$j9T$LwUKV7jiWiz/GF4zew7bX0$r/vPve5FdfS2L..Iwt04HrBv2exoWgX4ndJXywXskvD:jamesbond
$y$j9T$nvjoIwTlEtUbCAAGMBX4z/$XEL.bSwsSX3jqo4/xVSE1wp2pR3udEBBy5zNS/oik55:starbucks
$y$j9T$xxvUdpEv/i8ksgCOP1TaLY1$WoQnhoC67XKk9lmqx/QLgc5zCNvv0y.Hgy5Lj4H9zu0:apple123
$y$j9T$Yf2SnDQgCMCB7GSSaYDce0$SS/c3uo83I8v18c8088wG4JXSf0M/lySeUiBe0xHpnA:startrek
$y$j9T$wPmCqQe8ySZ5lYH03lcAv/$hgoFE1HLWiRowvbx3jQ6qv6Gt0t5ivFPGsrL/D0Gu5:98765432

(root@kali)~/john
#
```

Extra file:

"Cat john.rec"

```
(root@kali)-[~/john]
# cat john.rec
RECC4
6
--wordlist=/usr/share/wordlists/rockyou.txt
/home/kali/Downloads/mypasswd.txt
--format=crypt
--input-encoding=UTF-8
--internal-codepage=UTF-8
2281
12
3f300
0
0
3f300
0
5a60
0
0
0
0
0
0
0
0
0
23136
slt-v2
b072f0cf6adb3acc9536715e587249a9
96
(root@kali)-[~/john]
```

As we can see, this last cat command shows the progress of the cracking process.

2- Next, use the “show” command with “John the Ripper”. In a “root” shell, type in the following:

- a. cd /home/kali/Downloads
- b. john --show mypasswd.txt

3- Notice that the output shows cracked passwords. Their username followed by a password that looks like the following below. Note: I only showed one crack, Kali itself. (Take a snippet and show the cracked passwords. Mine shows around 16 current passwords that were cracked).

```
File Actions Edit View Help
(root@kali)-[~/]
# cd /home/kali/Downloads
(root@kali)-[/home/kali/Downloads]
# john --show mypasswd.txt
user1:jordan:1002:1002:Jordan Smit,,,:/home/user1:/bin/bash
jfrazier:apple123:1003:1003:John Frazier,,,:/home/jfrazier:/bin/bash
student:123456:1004:1004:Good Student,,,:/home/student:/bin/bash
dfrazier:98765432:1006:1006:Dennis Frazier,,,:/home/dfrazier:/bin/bash
shumers:mypassword:1008:1008:Sharon Humers,,,:/home/shumers:/bin/bash
atagarsi:password:1010:1010:Arun Tagarsi,,,:/home/atagarsi:/bin/bash
crogers:starbucks:1011:1011:Cody Rogers,,,:/home/crogers:/bin/bash
csalinas:123456789:1012:1012:Chloe Salinas,,,:/home/csalinas:/bin/bash
lskywalker:starwars:1017:1017:Luke Skywalker,,,:/home/lskywalker:/bin/bash
jpickard:startrek:1018:1018:Jean-Luc Picard,bridge,,,:/home/jpickard:/bin/bash
rmoore:jamesbond:1021:1021:Roger Moore,007,,,:/home/rmoore:/bin/bash

11 password hashes cracked, 4 left
(root@kali)-[/home/kali/Downloads]
```

As we can see John the Ripper was able to crack 11 accounts with their 11 passwords. I let it run for 1 hour.