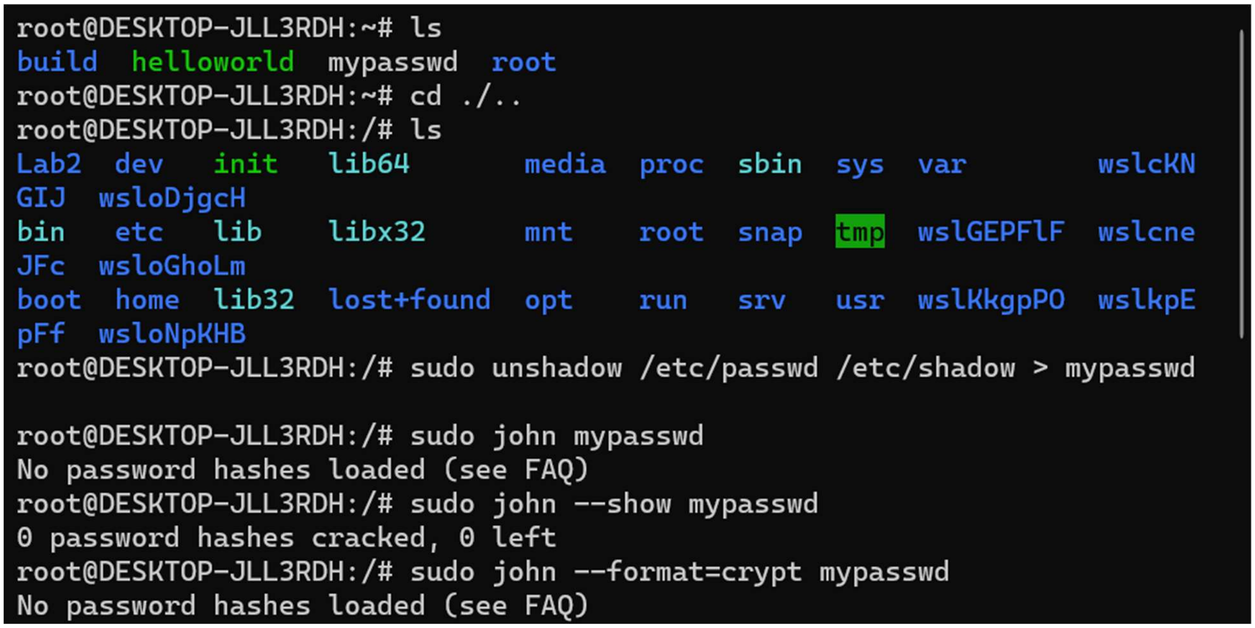
Mark Shinozaki
HW02 – Observations Report

Assignment Details:

- Screenshots proving you did perform the tutorial tasks i.e. activities, challenges, and questions
- Report any bugs, typos, broken links etc.
- A brief discussion on the skills you've learned from the tutorial (7 lines maximum)

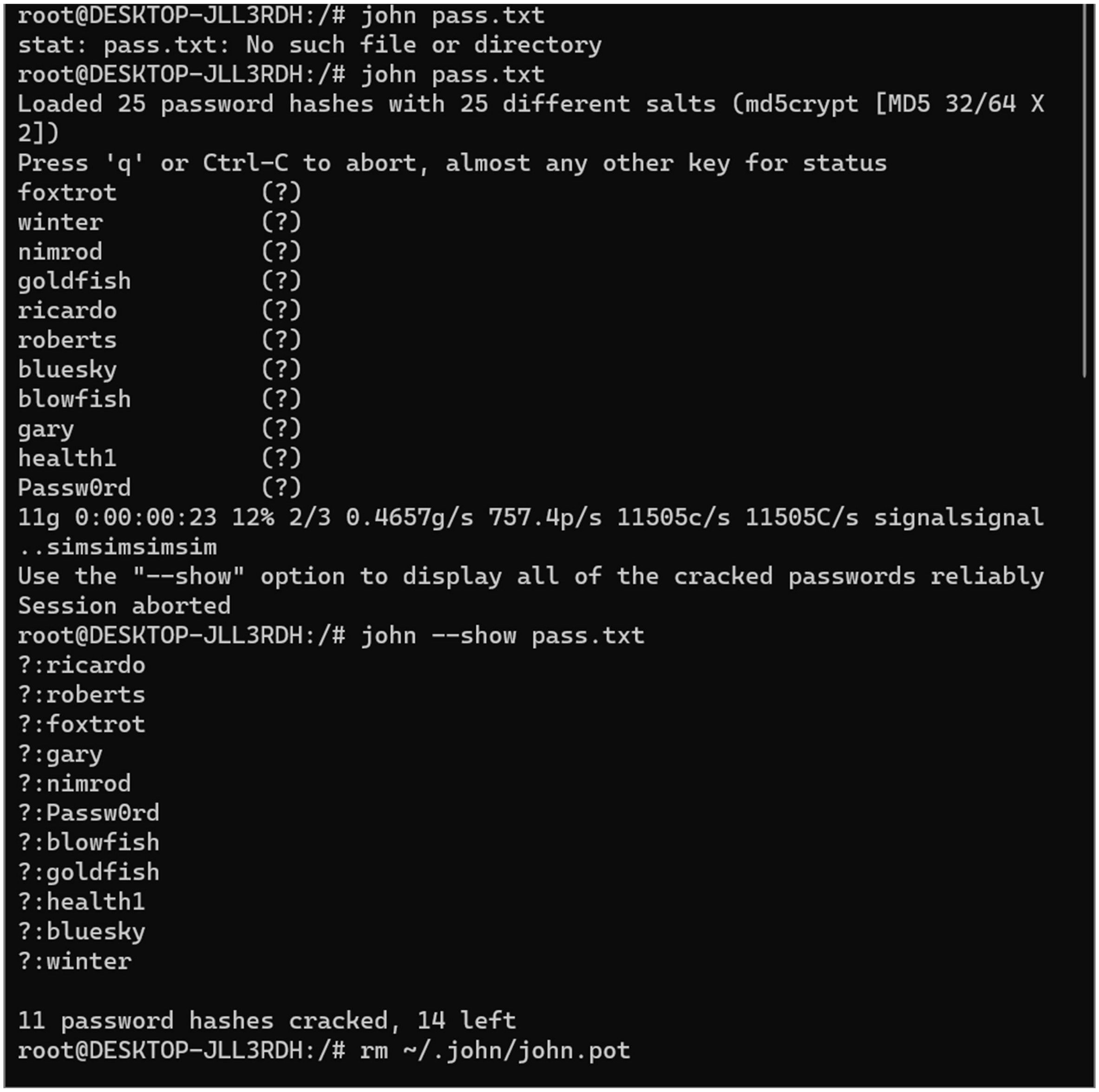
8 – Unshadowing the password file

- I tried my best to figure out why I could see the cracked passwords, but everything else in my observation report worked perfectly, If you could explain why this didn't work properly that would be great.



```
root@DESKTOP-JLL3RDH:~# ls
build  helloworld  mypasswd  root
root@DESKTOP-JLL3RDH:~# cd ./..
root@DESKTOP-JLL3RDH:/# ls
Lab2  dev   init  lib64       media  proc  sbin  sys  var        wslcKN
GIJ  wsloDjgcH
bin   etc   lib   libx32      mnt    root  snap  tmp  wslGEPFlF  wslcne
JFc  wsloGhoLm
boot  home  lib32  lost+found  opt    run   srv   usr  wslKkgpPO  wslkpE
pFf  wsloNpKHB
root@DESKTOP-JLL3RDH:/# sudo unshadow /etc/passwd /etc/shadow > mypasswd

root@DESKTOP-JLL3RDH:/# sudo john mypasswd
No password hashes loaded (see FAQ)
root@DESKTOP-JLL3RDH:/# sudo john --show mypasswd
0 password hashes cracked, 0 left
root@DESKTOP-JLL3RDH:/# sudo john --format=crypt mypasswd
No password hashes loaded (see FAQ)
```

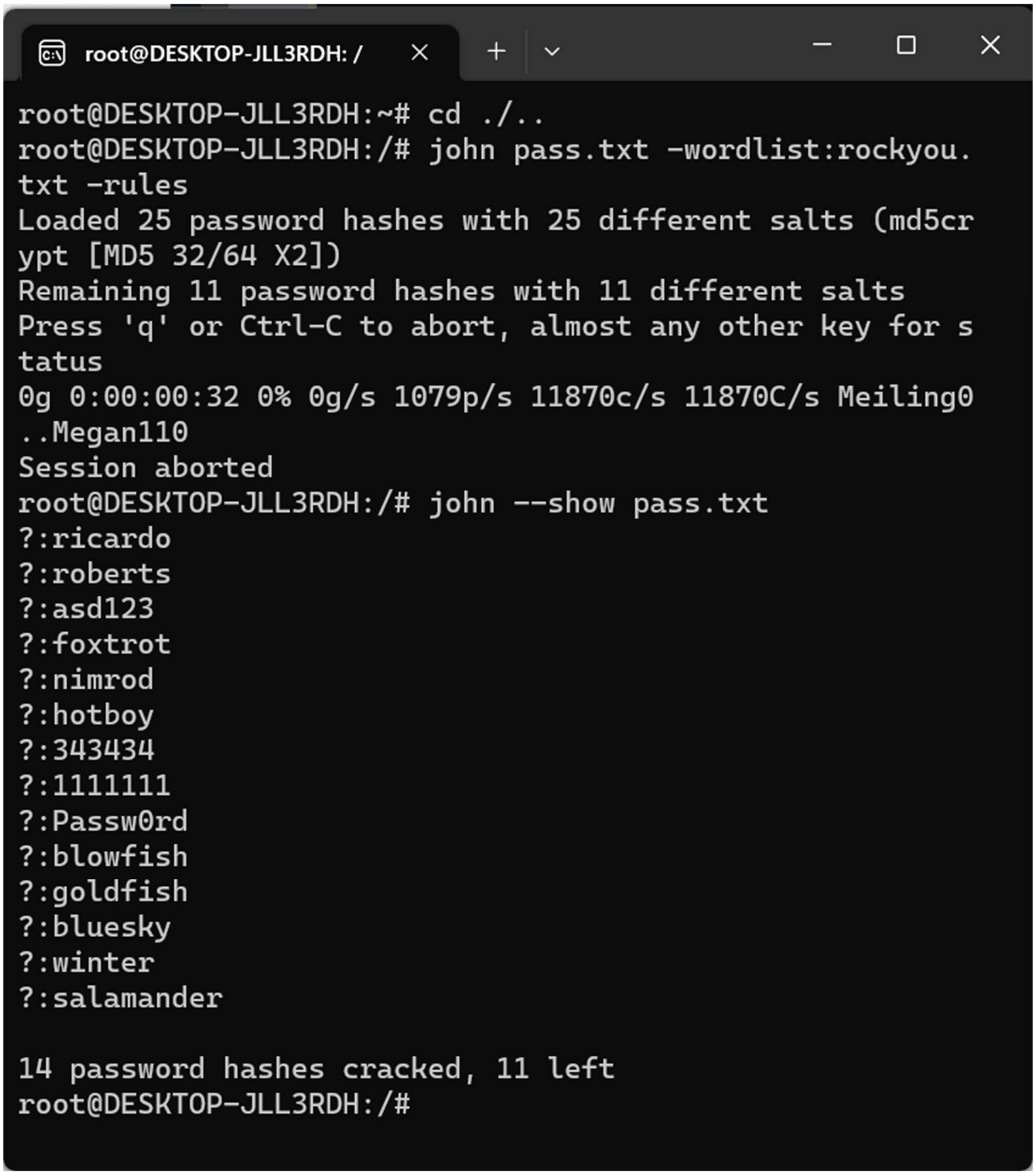
9 – Cracking MD5 Hashes by Default



```
root@DESKTOP-JLL3RDH:/# john pass.txt
stat: pass.txt: No such file or directory
root@DESKTOP-JLL3RDH:/# john pass.txt
Loaded 25 password hashes with 25 different salts (md5crypt [MD5 32/64 X
2])
Press 'q' or Ctrl-C to abort, almost any other key for status
foxtrot          (?)
winter           (?)
nimrod           (?)
goldfish         (?)
ricardo          (?)
roberts          (?)
bluesky          (?)
blowfish         (?)
gary             (?)
health1          (?)
Passw0rd         (?)
11g 0:00:00:23 12% 2/3 0.4657g/s 757.4p/s 11505c/s 11505C/s signalsignal
..simsimsimsim
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@DESKTOP-JLL3RDH:/# john --show pass.txt
?:ricardo
?:roberts
?:foxtrot
?:gary
?:nimrod
?:Passw0rd
?:blowfish
?:goldfish
?:health1
?:bluesky
?:winter

11 password hashes cracked, 14 left
root@DESKTOP-JLL3RDH:/# rm ~/.john/john.pot
```

Mark Shinozaki
HW02 – Observations Report

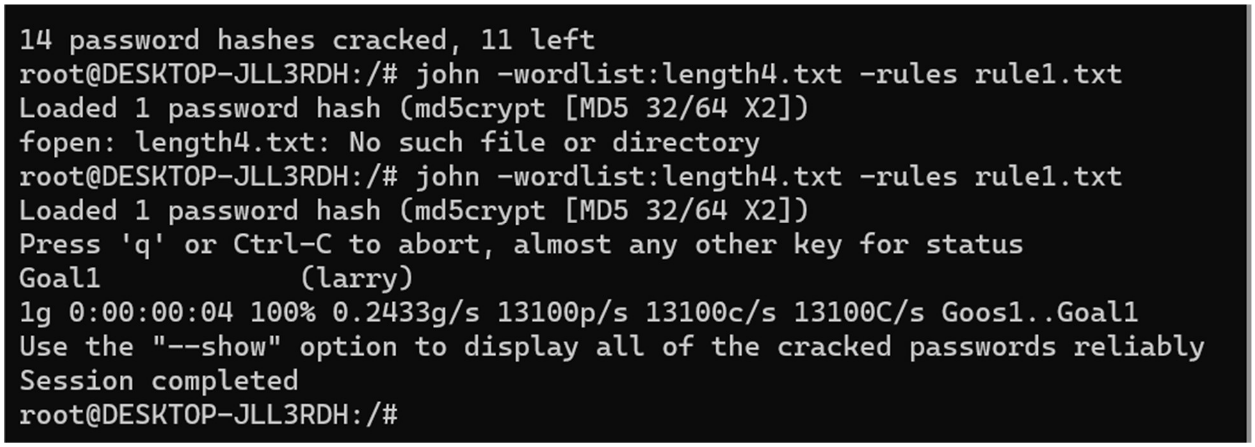
10 – Cracking MD5 Hashes with a wordlist



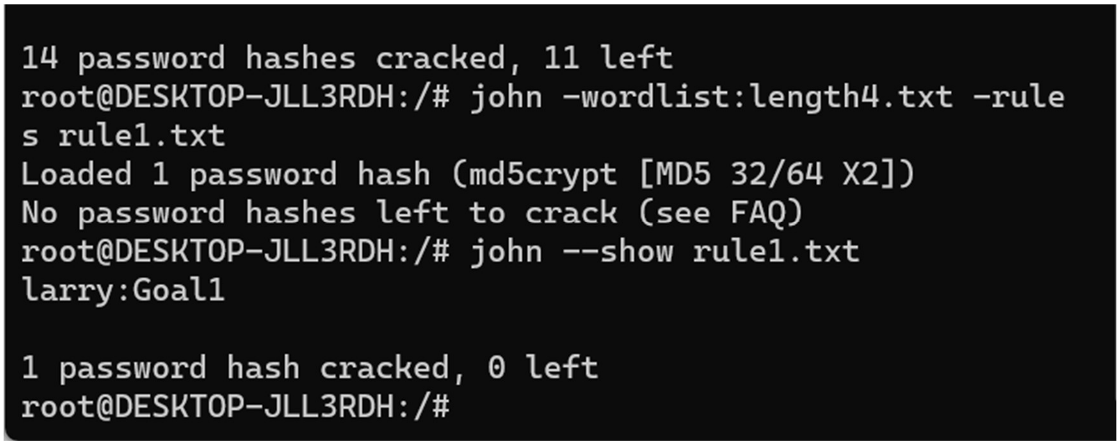
```
root@DESKTOP-JLL3RDH:~# cd ./..
root@DESKTOP-JLL3RDH:/# john pass.txt -wordlist:rockyou.
txt -rules
Loaded 25 password hashes with 25 different salts (md5cr
ypt [MD5 32/64 X2])
Remaining 11 password hashes with 11 different salts
Press 'q' or Ctrl-C to abort, almost any other key for s
tatus
0g 0:00:00:32 0% 0g/s 1079p/s 11870c/s 11870C/s Meiling0
..Megan110
Session aborted
root@DESKTOP-JLL3RDH:/# john --show pass.txt
?:ricardo
?:roberts
?:asd123
?:foxtrot
?:nimrod
?:hotboy
?:343434
?:1111111
?:Passw0rd
?:blowfish
?:goldfish
?:bluesky
?:winter
?:salamander

14 password hashes cracked, 11 left
root@DESKTOP-JLL3RDH:/#
```

Mark Shinozaki
HW02 – Observations Report

12 – Cracking MD5 Hashes by Specifying Rules



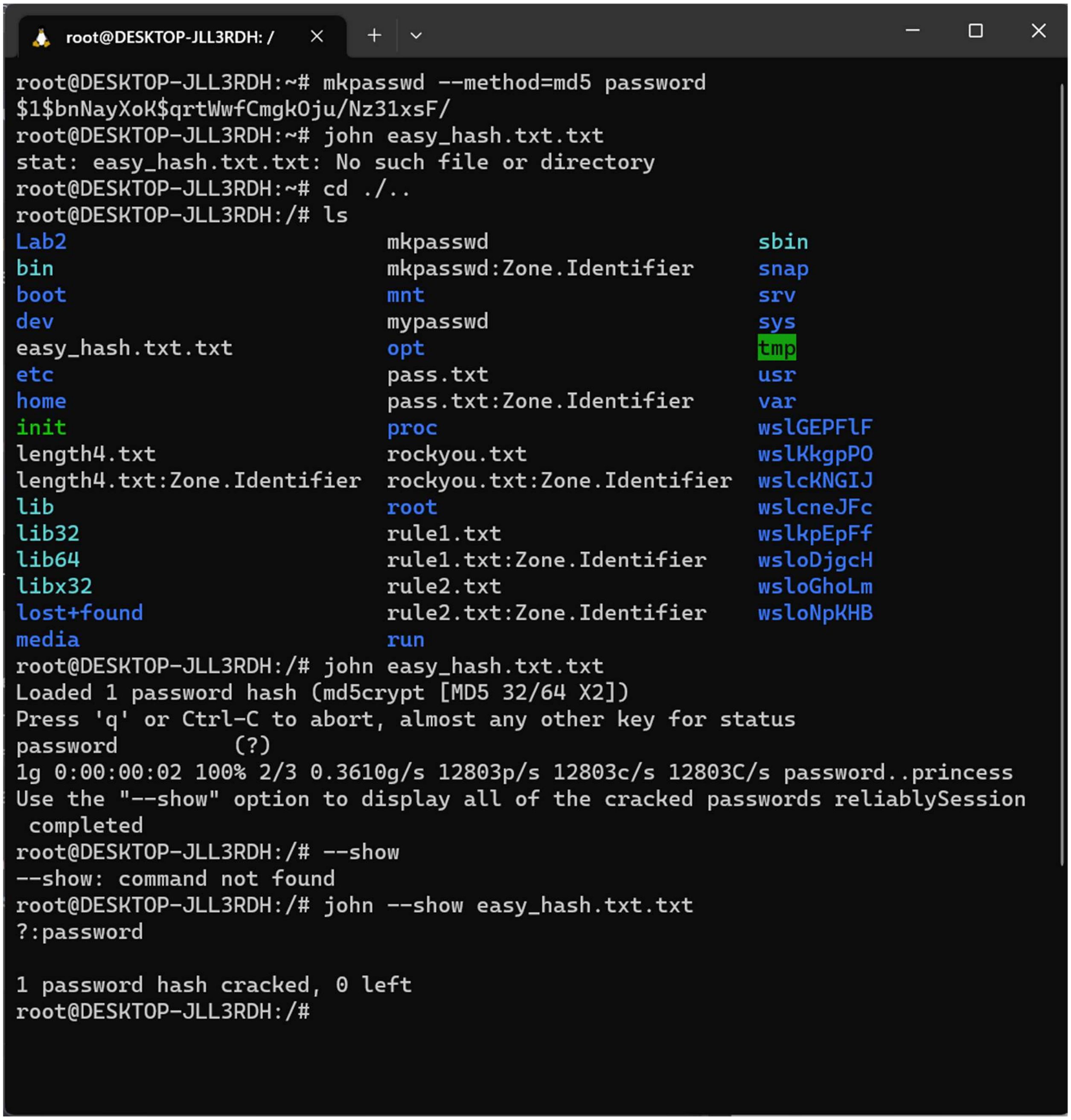
```
14 password hashes cracked, 11 left
root@DESKTOP-JLL3RDH:/# john -wordlist:length4.txt -rules rule1.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
fopen: length4.txt: No such file or directory
root@DESKTOP-JLL3RDH:/# john -wordlist:length4.txt -rules rule1.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
Goal1            (larry)
1g 0:00:00:04 100% 0.2433g/s 13100p/s 13100c/s 13100C/s Goos1..Goal1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@DESKTOP-JLL3RDH:/#
```



```
14 password hashes cracked, 11 left
root@DESKTOP-JLL3RDH:/# john -wordlist:length4.txt -rule
s rule1.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
No password hashes left to crack (see FAQ)
root@DESKTOP-JLL3RDH:/# john --show rule1.txt
larry:Goal1

1 password hash cracked, 0 left
root@DESKTOP-JLL3RDH:/#
```

Mark Shinozaki
HW02 – Observations Report

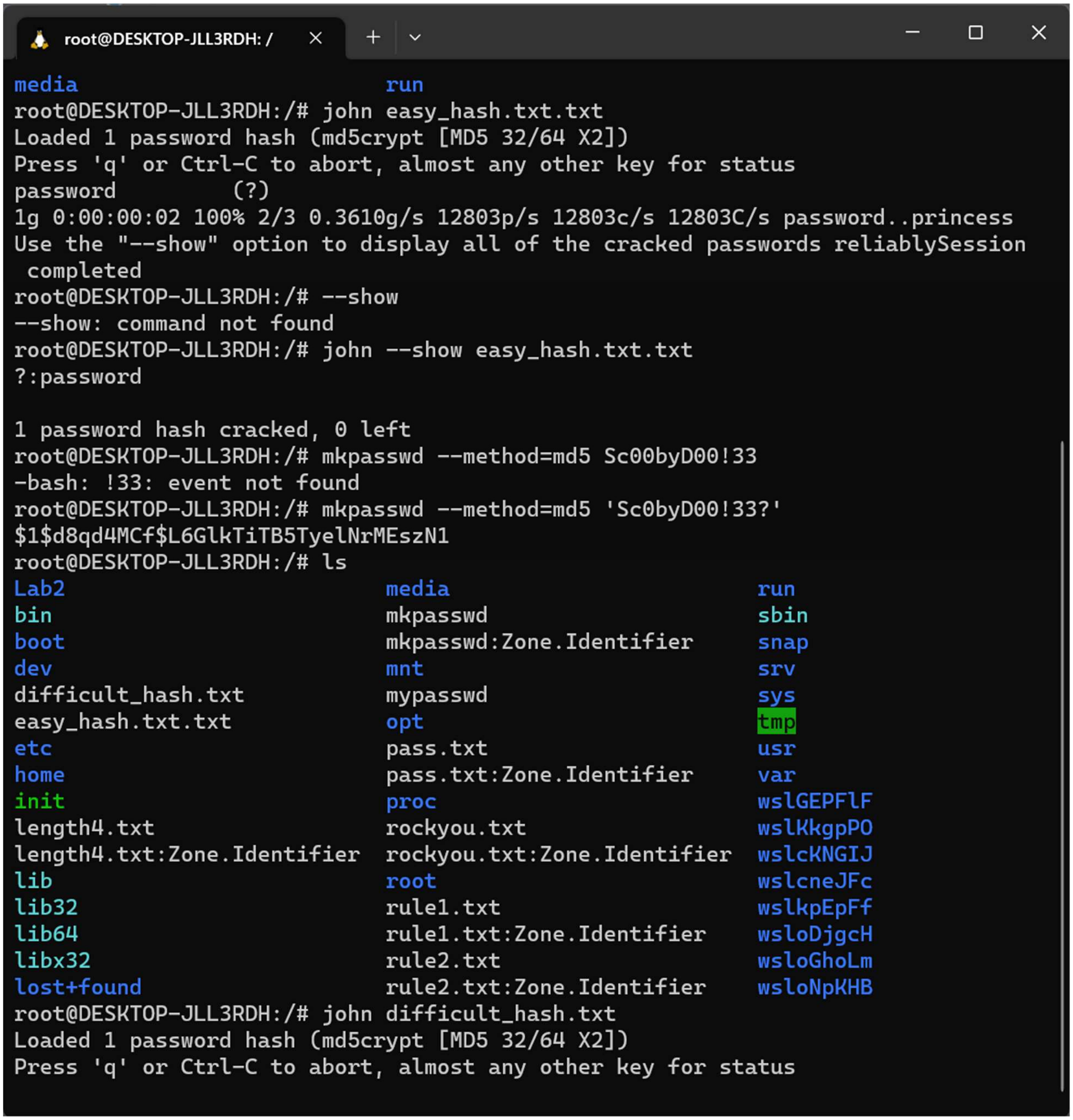
13 – Challenge 1 – part 1 (easy)



```
root@DESKTOP-JLL3RDH:~# mkpasswd --method=md5 password
$1$bnNayXoK$qrtWwfCmgkOju/Nz31xsF/
root@DESKTOP-JLL3RDH:~# john easy_hash.txt.txt
stat: easy_hash.txt.txt: No such file or directory
root@DESKTOP-JLL3RDH:~# cd ./..
root@DESKTOP-JLL3RDH:/# ls
Lab2                         mkpasswd                     sbin
bin                          mkpasswd:Zone.Identifier     snap
boot                         mnt                          srv
dev                          mypasswd                     sys
easy_hash.txt.txt            opt                          tmp
etc                          pass.txt                     usr
home                         pass.txt:Zone.Identifier     var
init                         proc                         wslGEPFlF
length4.txt                  rockyou.txt                  wslKkgpPO
length4.txt:Zone.Identifier  rockyou.txt:Zone.Identifier  wslcKNGIJ
lib                          root                         wslcneJFc
lib32                        rule1.txt                    wslkpEpFf
lib64                        rule1.txt:Zone.Identifier    wsloDjgcH
libx32                       rule2.txt                    wsloGhoLm
lost+found                   rule2.txt:Zone.Identifier    wsloNpKHB
media                        run
root@DESKTOP-JLL3RDH:/# john easy_hash.txt.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:02 100% 2/3 0.3610g/s 12803p/s 12803c/s 12803C/s password..princess
Use the "--show" option to display all of the cracked passwords reliablySession
 completed
root@DESKTOP-JLL3RDH:/# --show
--show: command not found
root@DESKTOP-JLL3RDH:/# john --show easy_hash.txt.txt
?:password

1 password hash cracked, 0 left
root@DESKTOP-JLL3RDH:/#
```

Mark Shinozaki
HW02 – Observations Report

13 – challenge 1 – part 2 (difficult)



```
media                        run
root@DESKTOP-JLL3RDH:/# john easy_hash.txt.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:02 100% 2/3 0.3610g/s 12803p/s 12803c/s 12803C/s password..princess
Use the "--show" option to display all of the cracked passwords reliablySession
 completed
root@DESKTOP-JLL3RDH:/# --show
--show: command not found
root@DESKTOP-JLL3RDH:/# john --show easy_hash.txt.txt
?:password

1 password hash cracked, 0 left
root@DESKTOP-JLL3RDH:/# mkpasswd --method=md5 Sc00byD00!33
-bash: !33: event not found
root@DESKTOP-JLL3RDH:/# mkpasswd --method=md5 'Sc0byD00!33?'
$1$d8qd4MCf$L6GlkTiTB5TyelNrMEszN1
root@DESKTOP-JLL3RDH:/# ls
Lab2                         media                        run
bin                          mkpasswd                     sbin
boot                         mkpasswd:Zone.Identifier     snap
dev                          mnt                          srv
difficult_hash.txt           mypasswd                     sys
easy_hash.txt.txt            opt                          tmp
etc                          pass.txt                     usr
home                         pass.txt:Zone.Identifier     var
init                         proc                         wslGEPFlF
length4.txt                  rockyou.txt                  wslKkgpPO
length4.txt:Zone.Identifier  rockyou.txt:Zone.Identifier  wslcKNGIJ
lib                          root                         wslcneJFc
lib32                        rule1.txt                    wslkpEpFf
lib64                        rule1.txt:Zone.Identifier    wsloDjgcH
libx32                       rule2.txt                    wsloGhoLm
lost+found                   rule2.txt:Zone.Identifier    wsloNpKHB
root@DESKTOP-JLL3RDH:/# john difficult_hash.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Mark Shinozaki
HW02 – Observations Report

14 – Challenge 2 – Wasn’t able to crack the password in the time I had available, but I followed all necessary steps to crack it, I created a file called custom-rules.txt with

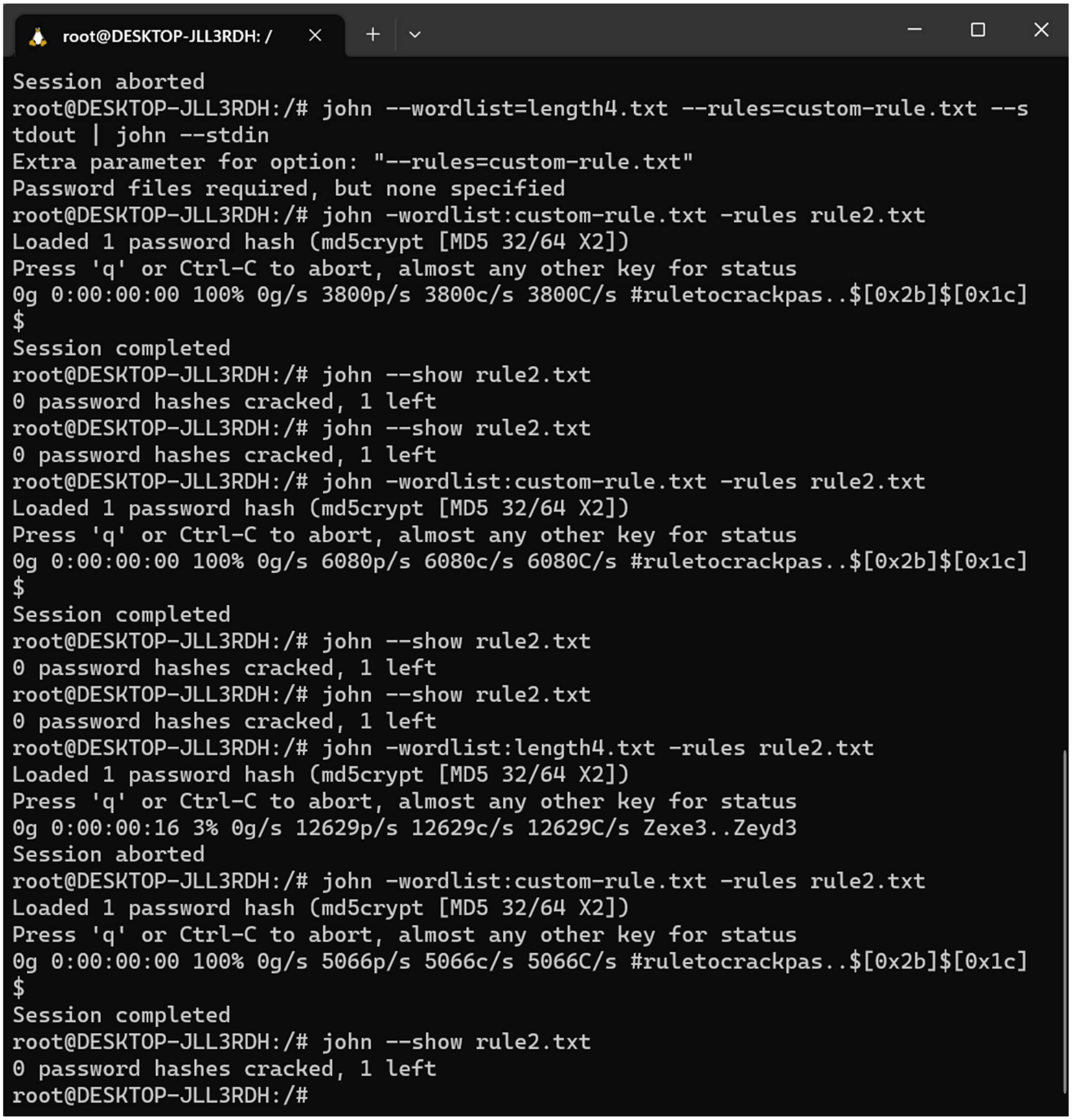
# custom-rule.txt

# Rule to crack passwords starting with "+" and ending with "8"

[PrefixRule]

$[0x2b] $[0x1c] $[0x18]

And this is the result that I received from the commands



```
Session aborted
root@DESKTOP-JLL3RDH:/# john --wordlist=length4.txt --rules=custom-rule.txt --s
tdout | john --stdin
Extra parameter for option: "--rules=custom-rule.txt"
Password files required, but none specified
root@DESKTOP-JLL3RDH:/# john -wordlist:custom-rule.txt -rules rule2.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 100% 0g/s 3800p/s 3800c/s 3800C/s #ruletocrackpas..$[0x2b]$[0x1c]
$
Session completed
root@DESKTOP-JLL3RDH:/# john --show rule2.txt
0 password hashes cracked, 1 left
root@DESKTOP-JLL3RDH:/# john --show rule2.txt
0 password hashes cracked, 1 left
root@DESKTOP-JLL3RDH:/# john -wordlist:custom-rule.txt -rules rule2.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 100% 0g/s 6080p/s 6080c/s 6080C/s #ruletocrackpas..$[0x2b]$[0x1c]
$
Session completed
root@DESKTOP-JLL3RDH:/# john --show rule2.txt
0 password hashes cracked, 1 left
root@DESKTOP-JLL3RDH:/# john --show rule2.txt
0 password hashes cracked, 1 left
root@DESKTOP-JLL3RDH:/# john -wordlist:length4.txt -rules rule2.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:16 3% 0g/s 12629p/s 12629c/s 12629C/s Zexe3..Zeyd3
Session aborted
root@DESKTOP-JLL3RDH:/# john -wordlist:custom-rule.txt -rules rule2.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 100% 0g/s 5066p/s 5066c/s 5066C/s #ruletocrackpas..$[0x2b]$[0x1c]
$
Session completed
root@DESKTOP-JLL3RDH:/# john --show rule2.txt
0 password hashes cracked, 1 left
root@DESKTOP-JLL3RDH:/#
```

Mark Shinozaki
HW02 – Observations Report

15 – Questions

1. What is an example of one cryptographic hashing algorithm besides MD5 that should not be used to hash passwords? What should be used in their place?
    - A hashing algorithm that should not be used is SHA-1, its just considered weak for password hashing because its vulnerable to collision attacks, two different inputs can produce the same hash value. Bcrypt; is a widely recommended password hashing algorithm known for its security. It incorporates a work factor (cost factor) that can be adjusted to make hashing slower and more resistant to brute-force and dictionary attacks

2. Is the default cracking mode or the wordlist mode more effective at cracking passwords? Why is this the case ?
    - Wordlist Mode: is typically more effective when you have a high-quality wordlist that includes common passwords and patterns. It is efficient for cracking passwords that are weak and present in the wordlist. If a target password is a common dictionary word or a simple variation of one, wordlist mode is the way to go. Default cracking, is useful when you have no information about the passwords structure and you're dealing with complex and strong passwords. It systematically generates and tests all possible combinations, starting with shorter passwords and gradually moving to longer ones. A combination of both modes, where you start with wordlist mode and then move to default mode if needed is often used for efficient password cracking

3. Can you crack any possible password with a brute-force attack? If so, what would this require?
    - In theory a brute force attack can crack any possible password given enough time and resources. However, the feasibility of such an attack depends on several factors, including:
        - Password length: as the length grows, the # of combinations grow
        - Character set: the character set used in the password, affects the complexity of the brute-force attack. The larger and more diverse the character set, the more combinations need to be tested
        - Computational resources: the speed and efficiency of the attackers hardware impact the success of the attack.
        - Time: A brute force attack can take an impractically long time to crack complex passwords. For example, cracking a strong password with sufficient length and complexity could take centuries or longer
        - In practice, modern password security standards make brute-force attacks infeasible by encouraging the use of more complex passwords and hashing algorithms.