Question 1.

I.

```
root@osboxes: /home
File  Edit  View  Search  Terminal  Help
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* fi
les
  -Z, --selinux-user            remove any SELinux user mapping for the user

root@osboxes:~# userdel ole_westby
root@osboxes:~# useradd -m -G sudo ole_westby
```

```
root@osboxes:~# passwd ole_westby
New password:
Retype new password:
passwd: password updated successfully
root@osboxes:~# cd /home
root@osboxes:/home# ls
lost+found  ole_westby
```

II.

```
root@osboxes: ~
File  Edit  View  Search  Terminal  Help
root@osboxes:~# cat /etc/shadow
root:$6$Q8uKtWWm/dptau2a$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT/1OJT4rtBACAm4NlEFV4n4x6ndTN3
wD9A5uHOjEQQ/JJqN./:18142:0:99999:7:::
daemon:*:18135:0:99999:7:::
bin:*:18135:0:99999:7:::
sys:*:18135:0:99999:7:::
sync:*:18135:0:99999:7:::
games:*:18135:0:99999:7:::
man:*:18135:0:99999:7:::
lp:*:18135:0:99999:7:::
mail:*:18135:0:99999:7:::
news:*:18135:0:99999:7:::
uucp:*:18135:0:99999:7:::
proxy:*:18135:0:99999:7:::
www-data:*:18135:0:99999:7:::
backup:*:18135:0:99999:7:::
list:*:18135:0:99999:7:::
irc:*:18135:0:99999:7:::
gnats:*:18135:0:99999:7:::
nobody:*:18135:0:99999:7:::
_apt:*:18135:0:99999:7:::
systemd-timesync:*:18135:0:99999:7:::
systemd-network:*:18135:0:99999:7:::
systemd-resolve:*:18135:0:99999:7:::
mysql:!:18135:0:99999:7:::
ntp:*:18135:0:99999:7:::
messagebus:*:18135:0:99999:7:::
arpwatch:!:18135:0:99999:7:::
Debian-exim:!:18135:0:99999:7:::
uuidd:*:18135:0:99999:7:::
redsocks:!:18135:0:99999:7:::
tss:*:18135:0:99999:7:::
rwhod:*:18135:0:99999:7:::
iodine:*:18135:0:99999:7:::
stunnel4:!:18135:0:99999:7:::
miredo:*:18135:0:99999:7:::
dnsmasq:*:18135:0:99999:7:::
sslh:!:18135:0:99999:7:::
postgres:*:18135:0:99999:7:::
usbmux:*:18135:0:99999:7:::
rtkit:*:18135:0:99999:7:::
_rpc:*:18135:0:99999:7:::
```

```
_rpc:*:18135:0:99999:7:::
Debian-snmp:!:18135:0:99999:7:::
statd:*:18135:0:99999:7:::
inetsim:*:18135:0:99999:7:::
sshd:*:18135:0:99999:7:::
pulse:*:18135:0:99999:7:::
speech-dispatcher:!:18135:0:99999:7:::
avahi:*:18135:0:99999:7:::
saned:*:18135:0:99999:7:::
colord:*:18135:0:99999:7:::
geoclue:*:18135:0:99999:7:::
king-phisher:*:18135:0:99999:7:::
Debian-gdm:*:18135:0:99999:7:::
dradis:*:18135:0:99999:7:::
beef-xss:*:18135:0:99999:7:::
systemd-coredump:!!:18142::::::
ole_westby:$6$57NPhKr7YG8QpVZ0$yDLHpdAVJjm8QcFF5IAfruM8Di4dhGLg1xTN.2zAzJTJCvksH.8tL3/S2Vn/P
q3ByyDNdBrIfIwT3aGBfbHok0:18558:0:99999:7:::
root@osboxes:~#
```

III.

```
root@osboxes:~# cd /root/Documents
root@osboxes:~/Documents# john --wodlist=/usr/share/wordlists/sqlmap.txt passwords.txt
Unknown option: "--wodlist=/usr/share/wordlists/sqlmap.txt"
root@osboxes:~/Documents# john --wordlist=/usr/share/wordlists/sqlmap.txt passwords.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
fopen: /usr/share/wordlists/sqlmap.txt: No such file or directory
root@osboxes:~/Documents# john --wordlist=/usr/share/wordlists/fasttrack.txt passwords.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2020-10-23 10:07) 0g/s 1585p/s 1585c/s 1585C/s admin..starwars
Session completed
root@osboxes:~/Documents# ole westby
```

Question 2.

I.

In MAC, the system specifies which subjects could access data objects. It's discretionary because control of access is based on the discretion of the owner.

In DAC, the owner of the object specifies which subjects can access data objects. MAC is based on security labels. Subjects have a security clearance, and the data objects are given classification.

II.

764 means that the user has read, write and execute permissions. Group has read and write permissions. While Others have only read permissions. Permission 764 as rwxrw-r—means:

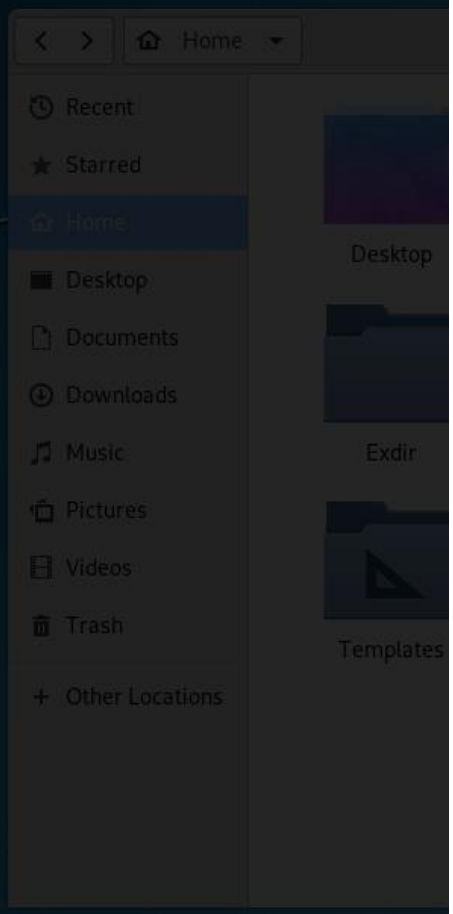
Read, write, execute permission to User/owner.

Read and write permission for the group.

Read only for others.

Question 3.

```
root@osboxes:~# mkdir Ex-dir
root@osboxes:~# touch Ex-dir/file1.txt
root@osboxes:~# ls -l Ex-dir/
total 4
-rw-rw-rw- 1 root root 3 Oct 23 10:29 file1.txt
root@osboxes:~# sudo chgrp Guest2 Ex-dir/
chgrp: invalid group: 'Guest2'
root@osboxes:~# useradd -m -G sudo Guest2
root@osboxes:~# useradd -m -G sudo Guest3
root@osboxes:~# sudo chgrp Guest2 Ex-dir/
root@osboxes:~# ls -l Ex-dir/
total 4
-rw-rw-rw- 1 root root 3 Oct 23 10:29 file1.txt
root@osboxes:~# sudo chgrp Guest2 Ex-dir/
root@osboxes:~# ls -l
total 40
drwxr-xr-x 2 root root   4096 Sep  3  2019 Desktop
drwxr-xr-x 2 root root   4096 Oct 23 10:02 Documents
drwxr-xr-x 2 root root   4096 Sep  3  2019 Downloads
drwxr-xr-x 2 root Guest2 4096 Oct 23 10:29 Ex-dir
drwxr-xr-x 2 root root   4096 Oct 23 10:29 Exdir
drwxr-xr-x 2 root root   4096 Sep  3  2019 Music
drwxr-xr-x 2 root root   4096 Oct 23 10:09 Pictures
drwxr-xr-x 2 root root   4096 Sep  3  2019 Public
drwxr-xr-x 2 root root   4096 Sep  3  2019 Templates
drwxr-xr-x 2 root root   4096 Sep  3  2019 Videos
root@osboxes:~# sudo chmod g=rw Ex-dir
root@osboxes:~# ls -l
total 40
drwxr-xr-x 2 root root   4096 Sep  3  2019 Desktop
drwxr-xr-x 2 root root   4096 Oct 23 10:02 Documents
drwxr-xr-x 2 root root   4096 Sep  3  2019 Downloads
drwxrw-r-x 2 root Guest2 4096 Oct 23 10:29 Ex-dir
drwxr-xr-x 2 root root   4096 Oct 23 10:29 Exdir
drwxr-xr-x 2 root root   4096 Sep  3  2019 Music
drwxr-xr-x 2 root root   4096 Oct 23 10:09 Pictures
drwxr-xr-x 2 root root   4096 Sep  3  2019 Public
drwxr-xr-x 2 root root   4096 Sep  3  2019 Templates
drwxr-xr-x 2 root root   4096 Sep  3  2019 Videos
root@osboxes:~# sudo Guest2
sudo: Guest2: command not found
root@osboxes:~# su Guest2
$ touch Ex-dir/file2.txt
touch: cannot touch 'Ex-dir/file2.txt': Permission denied
$ exit
root@osboxes:~# sudo chmod o=+x Ex-dir/
root@osboxes:~# ls -l Ex-dir/
total 4
-rw-rw-rw- 1 root root 3 Oct 23 10:29 file1.txt
```



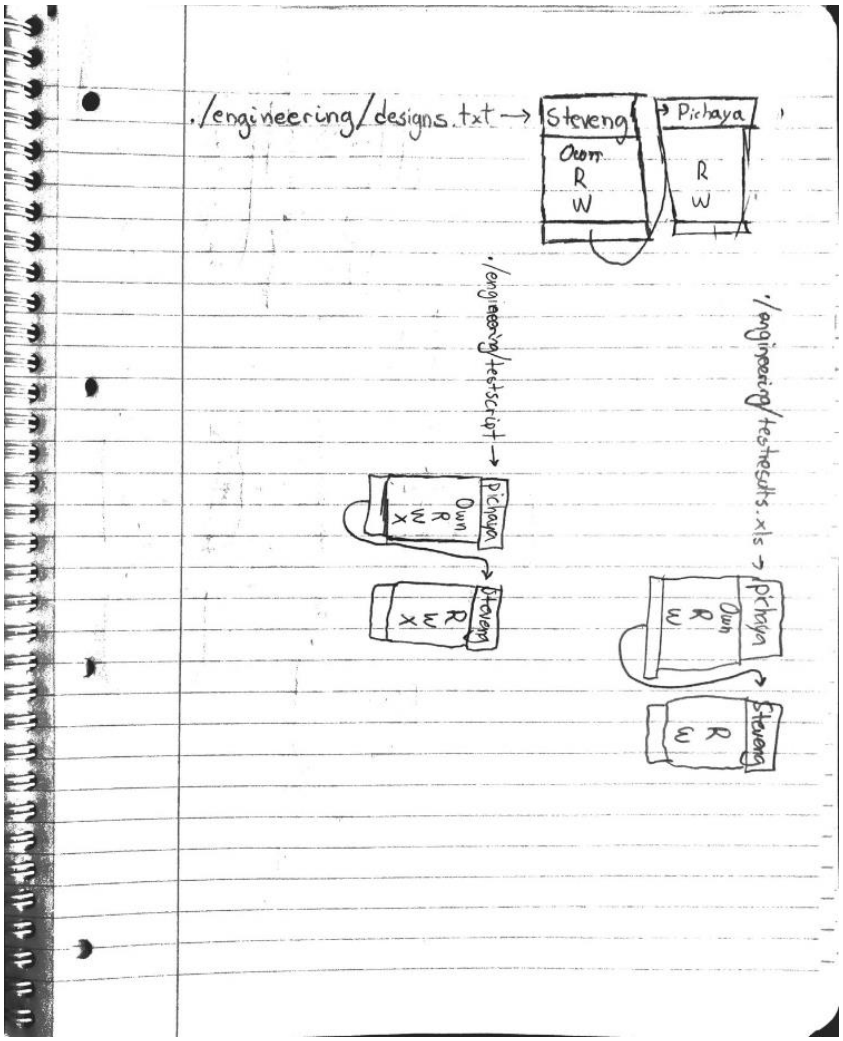

```
root@osboxes:~# ole westby
bash: ole: command not found
root@osboxes:~# su Guest3
$ ls Ex-dir/
ls: cannot open directory 'Ex-dir/': Permission denied
$
```

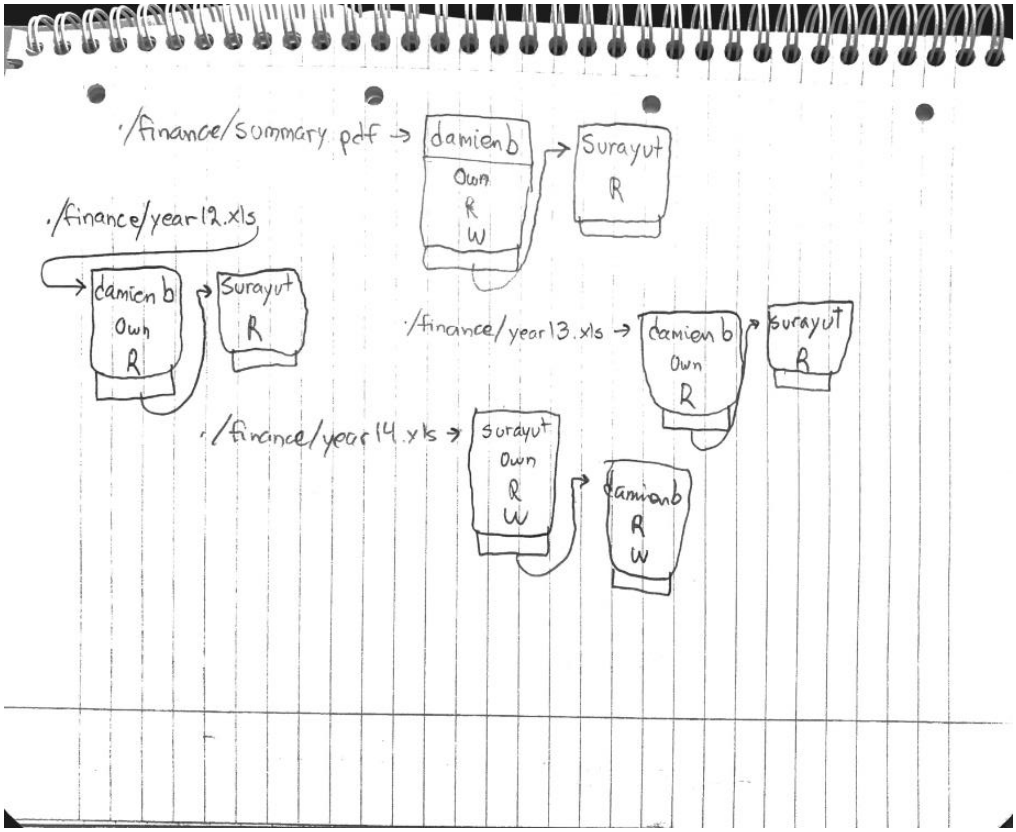
```
-rw-rw-rw- 1 root root 3 Oct 23 10:29 file1.txt
root@osboxes:~# ls -l
total 40
drwxr-xr-x 2 root root   4096 Sep  3  2019 Desktop
drwxr-xr-x 2 root root   4096 Oct 23 10:02 Documents
drwxr-xr-x 2 root root   4096 Sep  3  2019 Downloads
drwxrw---x 2 root Guest2 4096 Oct 23 10:29 Ex-dir
drwxr-xr-x 2 root root   4096 Oct 23 10:29 Exdir
drwxr-xr-x 2 root root   4096 Sep  3  2019 Music
drwxr-xr-x 2 root root   4096 Oct 23 10:09 Pictures
drwxr-xr-x 2 root root   4096 Sep  3  2019 Public
drwxr-xr-x 2 root root   4096 Sep  3  2019 Templates
drwxr-xr-x 2 root root   4096 Sep  3  2019 Videos
root@osboxes:~# ole westby
```

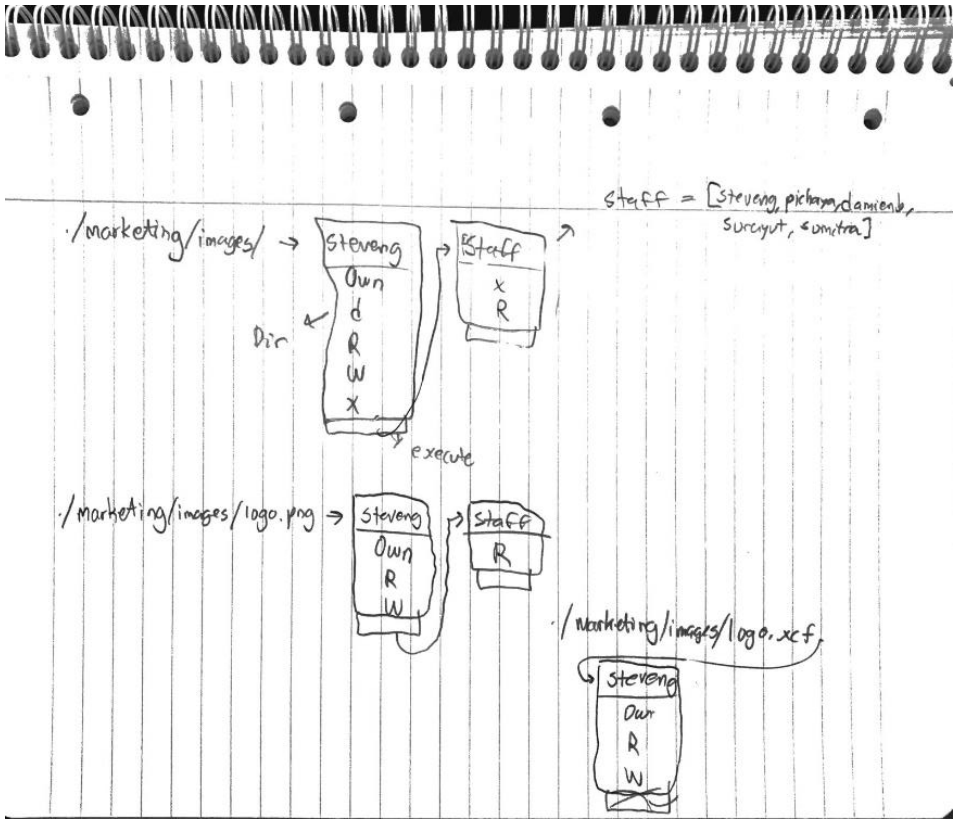
Guest3 can’t read/write to files, as it only has execution rights.

Question 4.

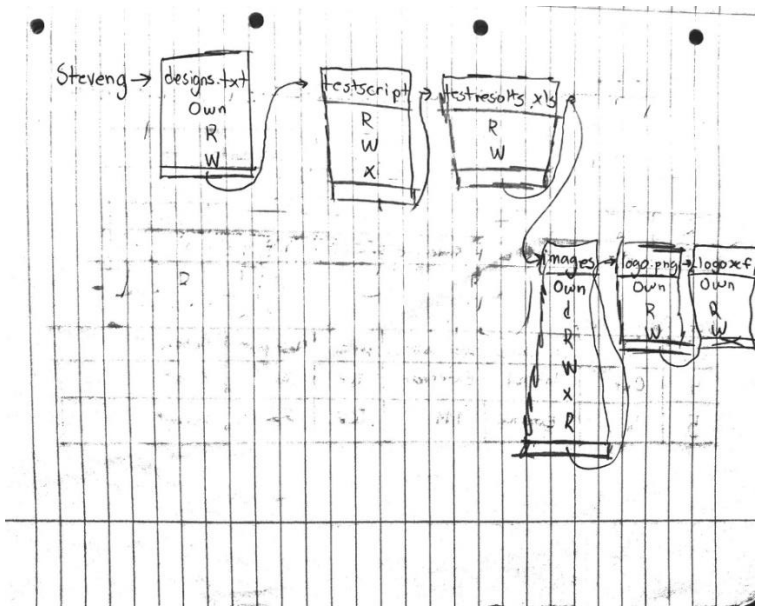
I.

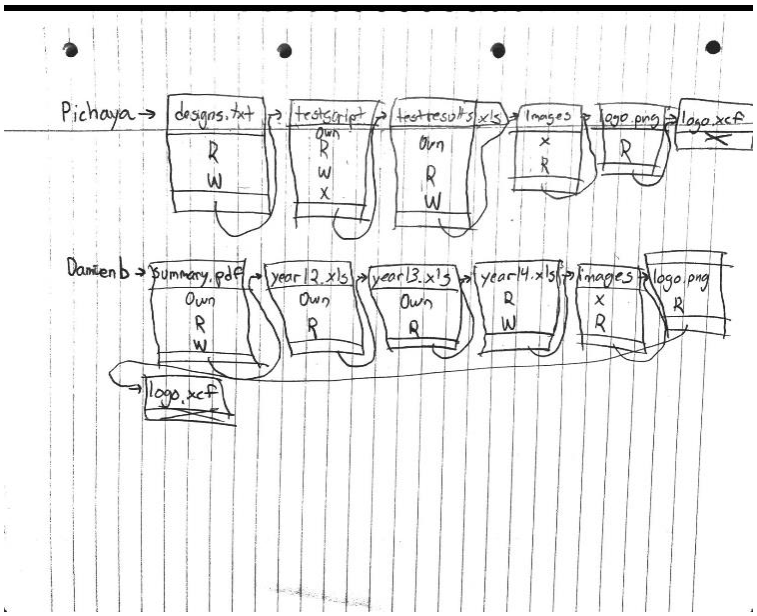


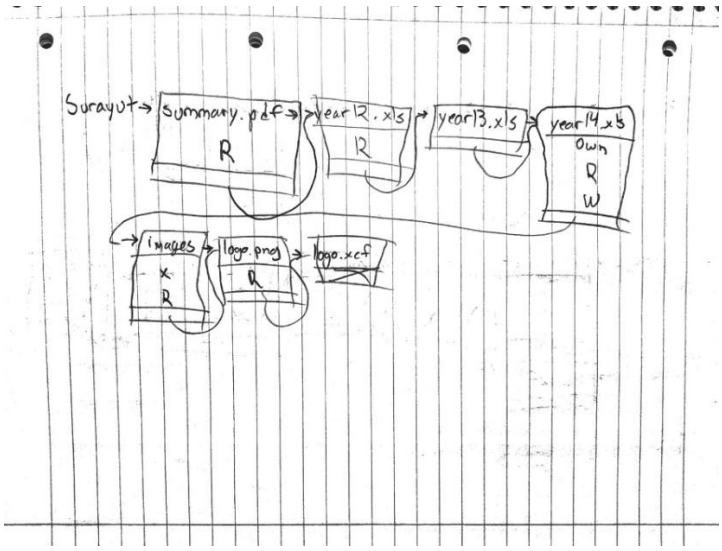

./finance/summary.pdf
damienb
Own
R
W
Surayut
R
./finance/year12.xls
damienb
Own
R
Surayut
R
./finance/year13.xls
damienb
Own
R
Surayut
R
./finance/year14.xls
surayut
Own
R
W
damienb
R
W

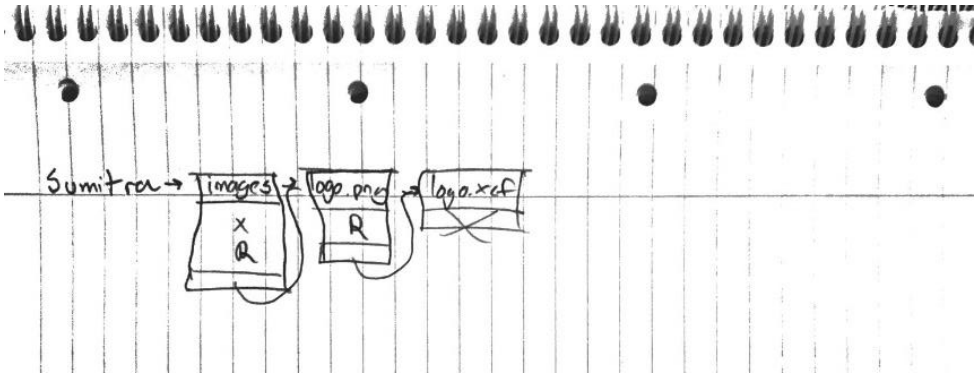

staff = [steveng, pichaya, damienb, surayut, umitra]
./marketing/images/
steveng
Own
d
R
W
X
Dir
execute
Staff
X
R
./marketing/images/logo.png
steveng
Own
R
W
Staff
R
./marketing/images/logo.xcf
steveng
Own
R
W

II.


Steveng
designs.txt
Own
R
W
testscript
R
W
X
testresolts.xls
R
W
images
Own
d
R
W
X
R
logo.png
Own
R
W
logo.xcf
Own
R
W


Pichaya
designs.txt
R
W
testscript
Own
R
W
X
testresolts.xls
Own
R
W
images
X
R
logo.png
R
logo.xcf
Damien b
summary.pdf
Own
R
W
year12.xls
Own
R
year13.xls
Own
R
year14.xls
R
W
images
X
R
logo.png
R
logo.xcf


Surayut
summary.pdf
R
year12.xls
R
year13.xls
year14.xls
Own
R
W
images
X
R
logo.png
R
logo.xcf



III.

Subject	Access Mode	Object
Steveng	Own	Designs.txt
Steveng	Read	Designs.txt
Steveng	Write	Designs.txt
Steveng	Read	testscript
Steveng	Write	testscript
Steveng	Exec	testscript
Steveng	Read	testresults.xls
Steveng	Write	testresults.xls
Steveng	Own	images
Steveng	Read	images
Steveng	Write	images
Steveng	Exec	images
— · · —	Own	logo.png
— · · —	Read	logo.png
— · · —	Write	logo.png
Steveng — · —	Own	logo.xcf
— · · —	Read	logo.xcf
— · · —	Write	logo.xcf
Pichayn	Read	designs.txt
— · —	Write	designs.txt
— · —	Own	testscript
— · —	Read	testscript
— · · —	Write	testscript
— · · —	Exec	testscript
— · · —	Own	testresults.xls
— · —	Read	testresults.xls
— —	Write	testresults.xls

Pichaya	Exec	Images
Pichaya	Read	Images
— · —	Read	logo.png
— · · —	✗	logo.xcf
Damien b	Own	summary.pdf
— · —	Read	Summary.pdf
— · —	Write	Summary.pdf
— · —	Own	yearR.xls
— · —	Read	yearR.xls
— · · —	Own	year13.xls
— · · —	Read	year13.xls
— · —	Read	year14.xls
— · · —	Write	year14.xls
— · · —	Exec	images
— · · —	Read	images
— · · —	Read	logo.png
— · · —	✗	logo.xcf
Surayut	read	Summary.pdf
— · · —	read	year12.xls
— · · —	read	year13.xls
— · · —	own	year14.xls
— · · —	read	year14.xls
— · · —	write	year14.xls
— · · —	Exec	images
— · · —	Read	Images
— · · —	Read	logo.png
— · · —	✗	logo.xcf

Sumitra	Exec	Images
— · · —	Read	Images
— · · —	Read	logo.png
— · · —	✗	logo.xcf

Question 5.

I.

In a virus, the malware takes the form of a virus that infects executable files by attaching its code into them.

In a worm, the malware takes the form of a self-replicating worm (it multiplies), that spreads to different parts of the network by itself. This is done by exploiting software vulnerabilities.

In social engineering, you trick a user in the system to bypass security and install the malware. Usually, the malware is disguised behind for example, useful software, a tool or application.

II.

A normal virus infects files on the system. This is done by attaching its code to them. It can easily be detected by an anti-virus.

Polymorphic virus changes its appearance when it propagates. This makes it harder to detect the virus, because the signature isn't consistent.

Metamorphic virus rewrites its own code as it propagates. It changes its structure and compared to the polymorphic virus; they do more than just change the appearance by encryption. Their whole code structure changes frequently, which make them quite difficult to detect.

Question 6.

Ole.Westby_inf100-uke-09 > quine2.py > ...

```python
a= "print('a = ' + chr(34) + a + chr(34) + chr(10) + a)"

t = ['Ole Westby']
print("t = ['Ole Westby']")

print('a = ' + chr(34) + a + chr(34) + chr(10) + a)

b = 'b = %r\nprint(b %% b)'

print(b % b)

c= 'c = {!r};print(c.format(c))';print(c.format(c))
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 2: Python

```
print('a = ' + chr(34) + a + chr(34) + chr(10) + a)
b = 'b = %r\nprint(b %% b)'
print(b % b)
c = 'c = {!r};print(c.format(c))';print(c.format(c))
PS C:\Users\owe05\Desktop\INF100-prosjekter> & C:/Users/owe05/AppData/Local/Programs/Python/Pytho
n38-32/python.exe c:/Users/owe05/Desktop/INF100-prosjekter/Ole.Westby_inf100-uke-09/quine2.py
t = ['Ole Westby']
a = "print('a = ' + chr(34) + a + chr(34) + chr(10) + a)"
print('a = ' + chr(34) + a + chr(34) + chr(10) + a)
b = 'b = %r\nprint(b %% b)'
print(b % b)
c = 'c = {!r};print(c.format(c))';print(c.format(c))
PS C:\Users\owe05\Desktop\INF100-prosjekter> & C:/Users/owe05/AppData/Local/Programs/Python/Pytho
n38-32/python.exe c:/Users/owe05/Desktop/INF100-prosjekter/Ole.Westby_inf100-uke-09/quine2.py
t = ['Ole Westby']
a = "print('a = ' + chr(34) + a + chr(34) + chr(10) + a)"
print('a = ' + chr(34) + a + chr(34) + chr(10) + a)
b = 'b = %r\nprint(b %% b)'
print(b % b)
c = 'c = {!r};print(c.format(c))';print(c.format(c))
PS C:\Users\owe05\Desktop\INF100-prosjekter>
```

https://git.app.uib.no/Ole.Westby/quine-moment

Question 7.

Rule 1: Block ping packets from being forwarded between two subnets

1.1 Block ping on the server, if facing DDoS attacks.
1.2 Iptables controls the incoming and outgoing packages.
1.3 Iptables will run without any rules, and we can edit the rules to them.

Rule 2: Block ping packets coming into the firewall

2.1. Firewall rules consists of services that describe the different types of traffic used by this type of traffic.

2.2. There are already-defined collections of firewall rules on each profile. You cannot alter these, and on some accounts, you can only apply more rules. You may not be able to apply rules of your own choosing to said profiles.

Rule 3: Prevent Node1 from SSHing to any outside nodes

3.1. Change the default policy as DROP and write packet filtering rules for the following goals

3.2. You can use strong passwords.

3.3. Limit SSH Access.

3.4. Individual clients.

3.5. Deactivate root login.

Rule 4: Allow inside hosts can access outside websites

4.1. Ping domain to check the IP.

4.2. Check port.

4.3. Logs.

Rule 5: Allow outside hosts can SSH into Node1. No other access should be allowed

Def. Policy: Accept

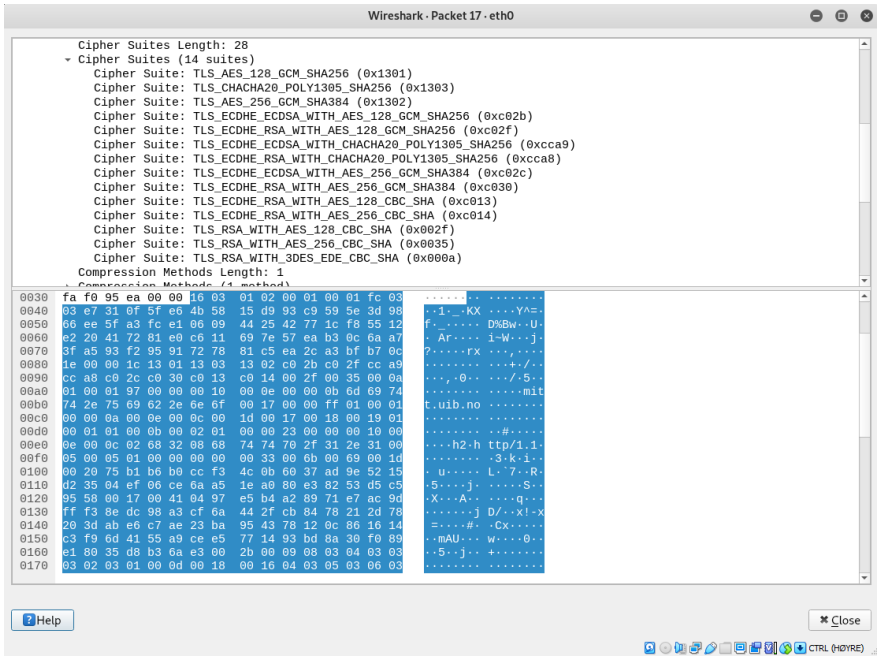
Rule	Direction	Src address	Dest address	protocol	Dest port	Action
1	Either	Any	Any	ICMP	Any	Deny
2	In	External	internal	TCP	Any	Deny
3	Out	1.11	External	TCP	22	Deny

Def Policy: Drop

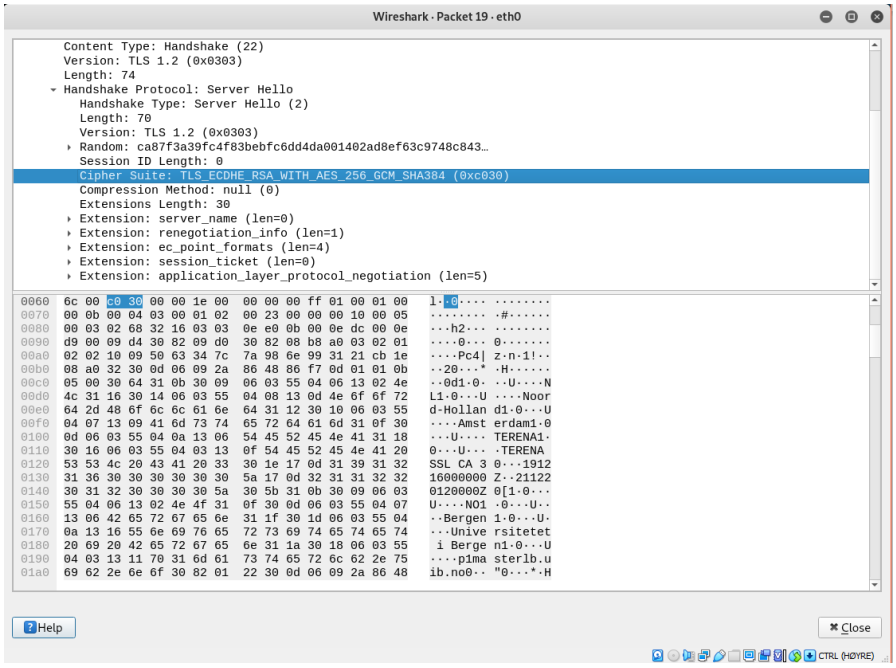
Rule	Direction	Src address	Dest address	protocol	Dest port	Action
4	Out	Internal	External	TCP	80	Permit
5	In	External	111	TCP	22	Permit

Question 8.

I.



II.



The TSL handshake requires the client and server to share the same capabilities so they can find the cryptographic features they both supports. This ensures the cipher suite in server handshake will protect subsequent HTTP traffic.