Question 1.

١.

```
0 0
                                                                                     0
                                   root@osboxes: /home
 File Edit View Search Terminal Help
                                  prefix directory where are located the /etc/*
      --prefix PREFIX DIR
les
                                  remove any SELinux user mapping for the user
  -Z, --selinux-user
root@osboxes:~# userdel ole westby
root@osboxes:~# useradd -m -G sudo ole westby
 coot@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: ~
                                                                                                        0 0
File Edit View Search Terminal Help
               :~# cat /etc/shadow
root:$6$Q8uKtWWm/dptau2a$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT/10JT4rtBACAm4NlEFV4n4x6ndTN3
wD9A5uH0jEQQ/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:::
tkit:*: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
q3ByyDNdBrIfIwT3<u>a</u>GBfbHok0:18558:0:99999:7:::
      osboxes:~#
```

III.

```
:~# cd /root/Documents
             :~/Documents# john --wodlist=/usr/share/wordlists/sqlmap.txt passwords.txt
Unknown option: "--wodlist=/usr/share/wordlists/sqlmap.txt
            :~/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
             :~/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 ^{\mathsf{N}}\mathbf{1}^{\mathsf{IS}} (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
       sboxes:~/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
     @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
                              4096 Sep 3 2019 Desktop
drwxr-xr-x 2 root root
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
                             4096 Sep 3 2019 Public
4096 Sep 3 2019 Templates
4096 Sep 3 2019 Videos
drwxr-xr-x 2 root root
drwxr-xr-x 2 root root
drwxr-xr-x 2 root root
root@osboxes:~# sudo chmod g=rw Ex-dir
root@osboxes:~# ls -l
total 40
                             4096 Sep 3 2019 Desktop
4096 Oct 23 10:02 Documents
drwxr-xr-x 2 root root
drwxr-xr-x 2 root root
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
                              4096 Sep 3 2019 Music
4096 Oct 23 10:09 Pictures
drwxr-xr-x 2 root root
drwxr-xr-x 2 root root
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
```

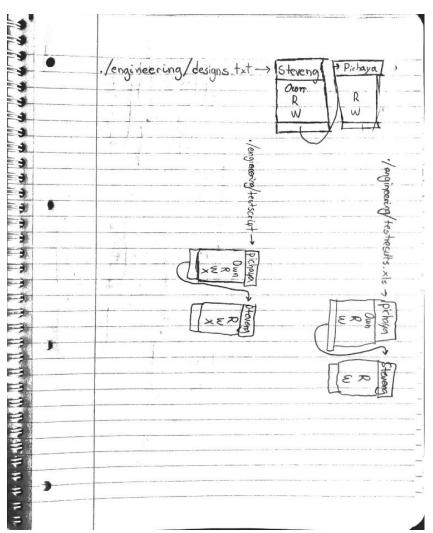
```
root@osboxes:~# ole westby
bash: ole: command not found
root@osboxes:~# su Guest3
$ ls Ex-dir/
ls: cannot open directory 'Ex-dir/': Permission denied
$
```

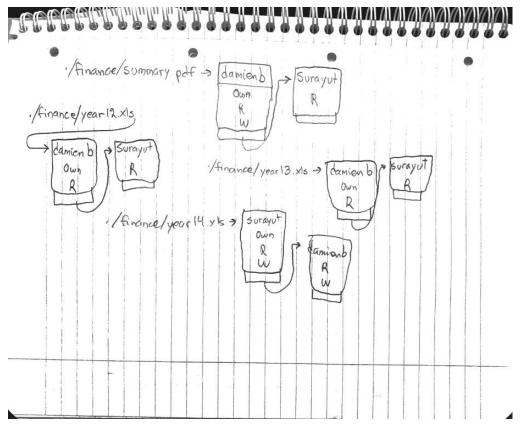
```
-rw-rw-rw- 1 root root 3 Oct 23 10:29 file1.txt
root@osboxes:~# ls -l
total 40
drwxr-xr-x 2 root root
                         4096 Sep 3
                                      2019 Desktop
drwxr-xr-x 2 root root
                         4096 Oct 23 10:02 Documents
drwxr-xr-x 2 root root
        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

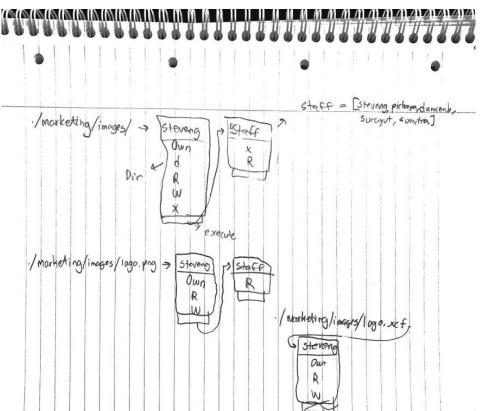
Guest3 can't read/write to files, as it only has execution rights.

Question 4.

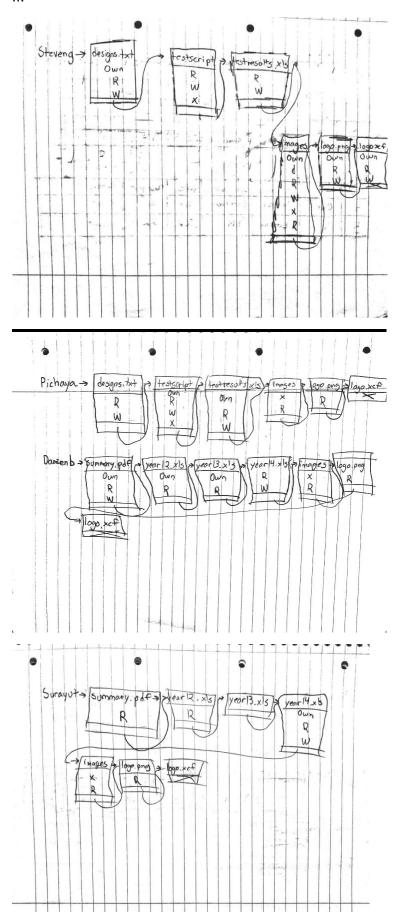
١.

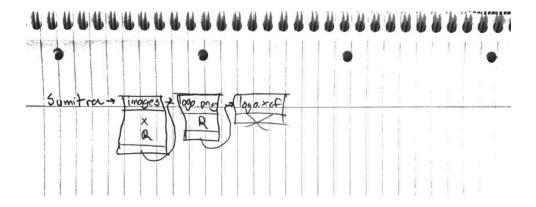






П.





III.

Read logo.xef Write loop.xef Pichayon Read designs.txt Write designs.txt Own testscript Read testscript Write testscript Compared testscript Compared testscript Read testscript Read testscript Read testscript And testresults.xb		ı		
Steveng Dun Designs. +x+ Steveng Bead Designs. +x+ Steveng Bead Designs. +x+ Steveng Bead test-script Steveng Bead test-script Steveng Brec test-script Steveng Brech test-results xls Steveng Bread images Steveng Dun images Steveng Dun images Steveng Bread images Steve				
Steveng Dun Designs. +x+ Steveng Bead Designs. +x+ Steveng Bead Designs. +x+ Steveng Bead test-script Steveng Bead test-script Steveng Brec test-script Steveng Brech test-results xls Steveng Bread images Steveng Dun images Steveng Dun images Steveng Bread images Steve		Subject	Access Made	Object
Storing Write Designs. 124 Storing Write Designs. 124 Storing Write Designs. 124 Storing Dead testscript Storing Exec testscript Storing Read testresults xls Storing Read images Storing Read images Storing Read images Storing Read images Storing Exec images Storing Exec images Own logo. prog Read logo. prog Write loop. prog Write loop. xcf Read logo. xcf Read logo. xcf Read logo. xcf Write loop. xcf Write loop. xcf Read logo. xcf Write loop. xcf Read logo. xcf Write loop.		Stevens		Designs +x+
Storing write lesigns text Storing Deal testscript Storing Write testscript Storing Read testresults xls Storing Read images Storing Read images Storing Read images Storing Read images Storing Read images Storing Read images Storing Read images Storing Read images Write images Write loop pag Write loop pag Write loop xcf Write designs tot Write designs tot Write designs tot Write testscript Read testscript Ener testscript Own testresults x b Read testreoutts x		Sharens		Deslans +x+
Steveng Dead testscript Stoveng Write testscript Stoveng Exec testscript Stoveng Read testresults xls Steveng Write testresults xls Steveng Write testresults xls Steveng Read images Stoveng Read images Stoveng Read images Stoveng Exec images Stoveng Exec images Write logo.png Write logo.png Write logo.xcf Read logo.xcf Write logo.xcf Write logo.xcf Write logo.xcf Write logo.xcf Write logo.xcf Write logo.xcf Read designs.bct Write losgo.xcf		Stevens		Designs tet
Stoveng, write testscript Stoveng, Exec testscript Stoveng, Read testresults xls Stoveng, Read testresults xls Stoveng, Write testresults xls Stoveng, Read images Stoveng, Read images Stoveng, Read images Stoveng, Exec images Own logo.png		Stovena		testscript
Steveng Exec testscript Steveng Read testresults xls Steveng Write testresults xls Steveng Own images Steveng Read images Steveng Read images Steveng Exec images Steveng Exec images Own logo.png Read logo.png Write logo.xcf Read logo.xcf Read logo.xcf Pichaya Read designs.txt Write designs.txt Read testscript Exec testscript Exec testscript		Stovena		testscript
Storang Read testresults xls Sherang Write testresults xls Storang Own images Storang Read images Storang Read images Shorang Exec images Own logo.png		Stereng	Exec	testscript
Stereng Write testresults x/s Stereng Own images Stereng Read images Stereng Read images Stereng Write images Stereng Exec images Own logo.png Read logo.png Write logo.xcf Read logo.xcf Read logo.xcf Write logo.xcf Pichayan Read designs.tet Write designs.tet Read testscript Exec testscript Exec testscript Exec testscript Exec testscript				testresults xls
Steveng Own images Steveng Read images Steveng Read images Steveng Write images Steveng Exec images Own logo.png Read logo.png Own logo.xcf Read logo.xcf Read logo.xcf Pichaya Read designs.tet Write designs.tet Write designs.tet Own testscript Read testscript Exec testscript Own testresults.xb Read testreouts.xb			Write	
storing Read images storing Write images Storing Exec images Own logo.png Read logo.png Write logo.xcf Read logo.xcf Read logo.xcf Write logo.xcf Write logo.xcf Pichaya Read designs.txt Write designs.txt Own testscript Read testscript Exec testscript Own testresylls.xb			Own	
sterring Write images Sterring Exec images Own logu.p.ng Read logo.png Write logo.xcf Dwn logo.xcf Read logo.xcf Write logo.xcf Viele logo.xcf Write designs.txt Write designs.txt Write designs.txt Write designs.txt Write testscript Read testscript Write testscript Read testscript Own testscript Dwn testscript Exec testscript And testresults.xb				images
Shoreng Exec images Own logo.png Read logo.png write logo.png Dwn logo.xcf Read logo.xcf Write loop.xcf Pichaya Read designs.but Write designs.but Tendo testscript Read testscript Exec testscript Dwn testresults.xb Read testresults.xb	****			
Own logs.png Read logs.png Write logs.png Dwn logs.xcf Read logs.xcf Write logs.xcf Pichayan Read designs.bd Write designs.bd Own testscript Read testscript Read testscript Ease testscript Ease testscript Rad testresults.xb Rad testresults.xb		Shoveng	Exec	images
Read logo.prg write logo.prg write logo.xcf Read logo.xcf Write loop.xcf Pichayon Read designs.bct Write designs.bct Own testscript Read testscript write testscript write testscript Dwn testscript Exac testscript Dwn testrayibs.xb	-7	\ -·-'	Own	logo pag
Dun loge xcs Read loge xcs Write loop xcf Write loop xcf Pichayon Read designs but Write designs tut Own testscript Read testscript Write testscript Write testscript Own testscript Read testscript Dun testscript Read testscript Read testscript			The state of the s	1090.pm
Dun loge xcf Read loge xcf Write loop xcf Write loop xcf Pichayon Read designs but Write designs tut Own testscript Read testscript Write testscript Exact testscript Own testrapy The control of the control			Write	logo-pag
Pichayon Read designs but Write designs but Write designs but Own trustscript Read testscript Write testscript Ease testscript Own testrapy Ease testscript And testrapy Read testscript Ease testscript Ease testscript	verg	~ -		loge.xcs
Pichayon Read designs but Write designs but Own trustscript Read testscript Write designs but Own trustscript Read testscript Ease trustscript Own testresulfs x 4 Read testreouts		<u> </u>		logo.xef
Vichayon Read designs but Write designs but Own test script Read test script Write test script Ease test sospit Own test results x y Read test results x	0	<u> </u>		loop.xrf
Write designs tot Own testscript Read testscript Write testscript Earc testscript Own testresults x 4 Read testresults x		Pichaya		cesigns but
Own testscript Read testscript Write testscript Earc testscript Own testresults x b Read testreouts		,	Write	designs but
Resid testscript Write testscript Ease testscript Own testresids x b Read testreouts x			Own	testscript
Write testscript Earce testscript Own testresults x b Read testresults x				testscript
Own testresults .x 4 Read testresults .x			The second secon	testscript
- Read testreauts x			Earec	testsonipt
1.0.1.40				testresits .x 1
			The second secon	testreauts ;
1			Write	testresuling

	Did	Exte	mages	
	Pichaya Pichaya	Real		
	Pichaya	Read	I mages	
		Reac	loso.prg	
	Damien b	Own	logo.xcf Summary pdf	
	Damien o	Read	Summery port	
		Write	Summary pot Summary pot	
		Own	year Rx15	
		Read	year R. xls	
		Own	year 13. xls	
		Read	year13 x15	
		Reac	year 14. xls	
		- Write	year 14. xls	
		- Exec	0 /	
		Rea	d ingges	
m - 14,8 8 - 1581 - 1581		Rea	è logo pro	
aring garage sections			(Ugo.xc+	
	Surayut	rea	d Summary, pdf	
			d year 12 xls	
Jacquista Compania Management		- re		trapa bada a attractiva are
ANNE PAR ILLEGO			n year 14.xls	
			ad year M.Xb	
C164 15 - pc - c-			rite year 14,xls	
against the court of the state			eab Images	
and the second second				
			ear logo, prog × logo, xcf	
	MICO R. P. I. MICH T. T. LAMBERT COMMISSION		- Tugo xc1	
and to again as an entire	to the second se			
Š	imitra	Exec	Images Images logo prog logo, xcf	
+=		Read	mages	
+=		Read	1090 pm	
-		×	lugo, xcf	
			U	
-			commenced and the second and the sec	
-	270			

Question 5.

١.

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 > ...
       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.

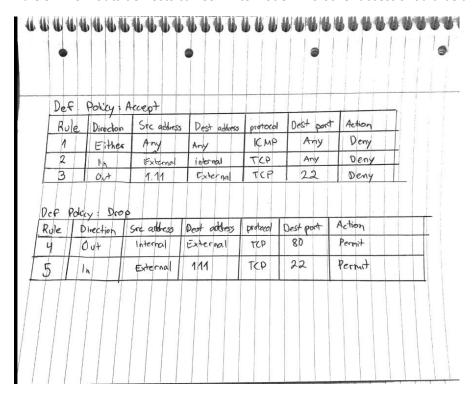
Rule 3: Prevent Node1 from SSHing to any outside nodes

- 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



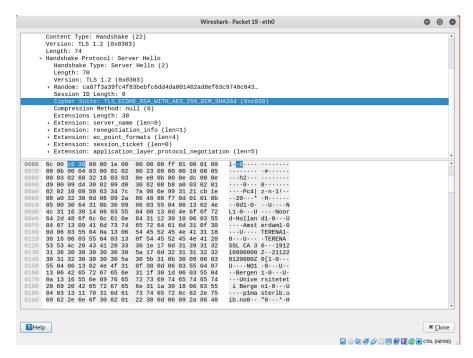
Question 8.

١.

```
Cipher Suites Length: 28

* Cipher Suites (14 suites)
Cipher Suites (14 suites)
Cipher Suite: TIS_AB_128_GCM_SHA256 (0x1301)
Cipher Suite: TIS_AB_128_GCM_SHA256 (0x1301)
Cipher Suite: TIS_AB_128_GCM_SHA256 (0x1301)
Cipher Suite: TIS_ECOME_ECOMS_MATH AES_128_GCM_SHA256 (0x0027)
Cipher Suite: TIS_ECOME_ECOMS_MATH AES_128_GCM_SHA354 (0x0030)
Cipher Suite: TIS_ECOME_ECOMS_MATH AES_256_GCM_SHA394 (0x0030)
Cipher Suite: TIS_ECOME_EXA_WITH AES_256_GCM_SHA394 (0x0030)
Cipher Suite: TIS_EXA_WITH AES_256_GCM_SHA394 (0x0030
```

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.