


| | | | |
|---|---|---------------------------|---|
| Generalitat de Catalunya Departament d'Educació INS Provençana | Mòdul 6: Seguretat informàtica | Curs 2023-2024 |  |
| Departament d'informàtica Grup SMX2C | UF5 - Tallafocs i monitoratge de xarxes | Nota | |
| | NF1 - Monitoratge de xarxes | Data: 30 de Gener de 2024 | |

Professors: Laura Montesinos

Alumne:

Instruccions

Lliurament:

1. Poseu el **nom i cognoms** dins del document que lliureu.
2. Heu de lliurar un **únic document** en format **pdf**.
3. Heu de fer captures de pantalla per demostrar que heu realitzar l'exercici. Les captures de pantalla han d'anar annexades en aquest document.

Consell: Cada apartat té exercicis de diferent dificultat (feu primer els que sapiguen).

4. Durada: **2** hores.

- Pots consultar tot el material que consideris adient (també Internet)
- Tots els exercicis valen el mateix.
- Cada apartat té exercicis de diferent dificultat (fes primer els fàcils)

Crea una màquina virtual amb el teu nom (enlloc de Alumne) i el codi **alumne-245**

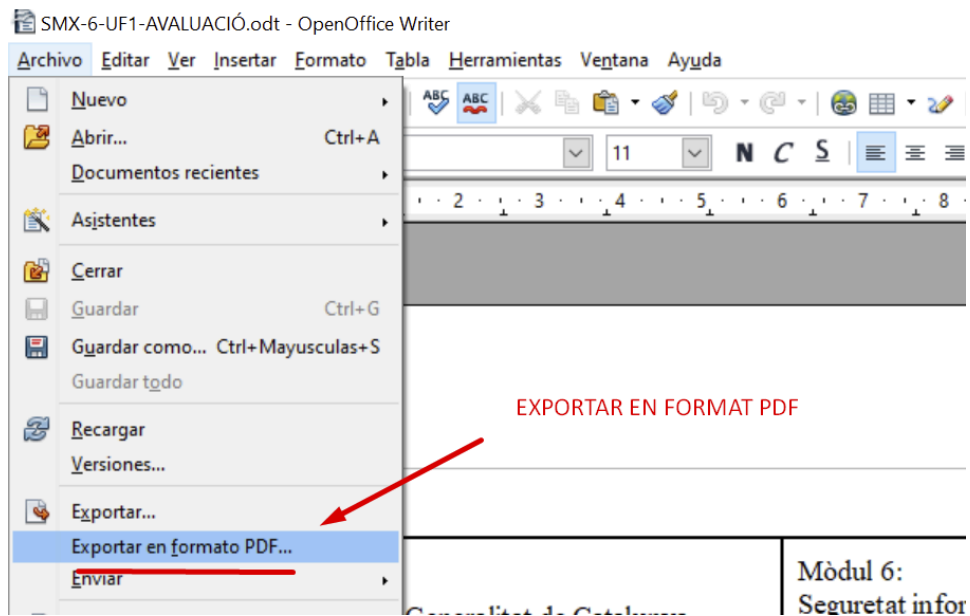
Arrenca la màquina configurant --cpu i --memory :

Inicieu la màquina.

Important. "Aneu al VirtualBox i poseu-hi adaptador pont".
box.exe code laura-245 -c 4 -m 8000

| | | | |
|---------|------------|---------------|------------|
| C01-F25 | Versió 1.0 | Pàgina 1 de 2 | 10-09-2020 |
|---------|------------|---------------|------------|

El document l'has d'exportar a PDF:



Exercicis

1. Docker-emmagatzematge- 25%

- 1.1. Borra tots els **contenidors** i verifica amb un docker ps.
- 1.2. Arrenca un contenidor apache amb l'opció **-p 8000:80** perquè poguem connectar-nos des de fora del host. Verifica la pàgina d'inici del teu contenidor apache
- 1.3. Crea una carpeta amb el nom web i crea la pàgina d'inici amb el missatge "**La meva WEB: Nom_alumne**"
- 1.4. Torna a crear un nou contenidor **apache_web** montant la carpeta **web**
- 1.5. Fes un `curl` a localhost pots veure que ara respon amb el teu fitxer `index.html` no amb l'index d'inici, que has fet perquè això passi?

2. Docker-xarxes 25%

Per evitar problemes, primer elimina totes les xarxes que no s'estan fent servir:

```
docker network prune -f
```

- 2.1. Crea dues xarxes virtuals amb les següents ips:

net-1→10.0.10.0/24

net-2→ 10.0.20.0/24

- 2.2. Mostreu el resultat amb **docker network ls**.

| | | | |
|---------|------------|---------------|------------|
| C01-F25 | Versió 1.0 | Pàgina 1 de 2 | 10-09-2020 |
|---------|------------|---------------|------------|

2.3. Arrenca un contenidor amb nginx connectat a la primera xarxa-net-1

2.4. Arrenca un contenidor amb apache connectat a la segona xarxa-net-2.

2.4.1. Verifica els contenidors

2.5. Crear un contenidor amb nom **explorer amb alpine**

2.5.1. Connecta el contenidor explorer a les dues xarxes amb **docker network connect** i arrenca els contenidors:

2.6. Verifica les interfícies disponibles del docker

docker exec explorer ip -f inet -4 -o add

3. Nmap 30%

3.1. Feu un escaneig del domini (escull un domini: ibm.es, movistar.es, telefonica.es) i explica els resultats més rellevants:

Primer fem un update i instal·lem el nmap:

Amb la comanda:

- sudo apt install -y nmap

-nmap movistar.es per escanejar la màquina:

```
box@roc-245: ~$ nmap movistar.es
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-30 18:03 UTC
Nmap scan report for movistar.es (81.47.192.13)
Host is up (0.023s latency).
rDNS record for 81.47.192.13: 13.red-81-47-192.staticip.rima-tde.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds
```

3.2. Mostra las ip's activas cercanas al domini XXXX/28 seleccionat abans.

Utilitzem la següent comanda per saber les ip's actives properes:

`nmap -sL movistar.es/28`

```
box@roc-245:~$ nmap -sL movistar.es/28
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-30 18:19 UTC
Nmap scan report for 0.red-81-47-192.staticip.rima-tde.net (81.47.192.0)
Nmap scan report for 1.red-81-47-192.staticip.rima-tde.net (81.47.192.1)
Nmap scan report for 2.red-81-47-192.staticip.rima-tde.net (81.47.192.2)
Nmap scan report for 3.red-81-47-192.staticip.rima-tde.net (81.47.192.3)
Nmap scan report for 4.red-81-47-192.staticip.rima-tde.net (81.47.192.4)
Nmap scan report for 5.red-81-47-192.staticip.rima-tde.net (81.47.192.5)
Nmap scan report for 6.red-81-47-192.staticip.rima-tde.net (81.47.192.6)
Nmap scan report for 7.red-81-47-192.staticip.rima-tde.net (81.47.192.7)
Nmap scan report for 8.red-81-47-192.staticip.rima-tde.net (81.47.192.8)
Nmap scan report for 9.red-81-47-192.staticip.rima-tde.net (81.47.192.9)
Nmap scan report for 10.red-81-47-192.staticip.rima-tde.net (81.47.192.10)
Nmap scan report for 11.red-81-47-192.staticip.rima-tde.net (81.47.192.11)
Nmap scan report for 12.red-81-47-192.staticip.rima-tde.net (81.47.192.12)
Nmap scan report for movistar.es (81.47.192.13)
rDNS record for 81.47.192.13: 13.red-81-47-192.staticip.rima-tde.net
Nmap scan report for 14.red-81-47-192.staticip.rima-tde.net (81.47.192.14)
Nmap scan report for 15.red-81-47-192.staticip.rima-tde.net (81.47.192.15)
Nmap done: 16 IP addresses (0 hosts up) scanned in 0.02 seconds
box@roc-245:~$
```

3.3. El domini **seleccionat** resuelve la IP XXXXXXXXX? . Indica a quien pertenece el servidor detrás de la IP?

Ho busquem amb la comanda:

`whois 81.47.192.13:`

I ens dirà el propietari del servidor: Telefonica

Per saber si el domini resolt la ip fem un nslookup:

```
box@roc-245:~$ nslookup movistar.es
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   movistar.es
Address: 81.47.192.13
```

```

box@roc-245:~$ whois 81.47.192.13
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '81.47.192.0 - 81.47.192.255'

% Abuse contact for '81.47.192.0 - 81.47.192.255' is 'nemesys@telefonica.es'

inetnum:        81.47.192.0 - 81.47.192.255
netname:        RIMA
descr:          Telefonica de Espana SAU
descr:          Red de servicios IP
descr:          Spain
country:        ES
admin-c:        ATdE1-RIPE
tech-c:         TTdE1-RIPE
status:         ASSIGNED PA
remarks:        INFRA-AW
mnt-by:         MAINT-AS3352
created:        2003-04-28T10:42:14Z
last-modified:  2009-08-19T11:27:20Z
source:         RIPE # Filtered

role:           Administradores Telefonica de Espana
address:        Ronda de la Comunicacion s/n
address:        Edificio Norte 1, planta 6
address:        28050 Madrid
address:        SPAIN
org:            ORG-TDE1-RIPE
admin-c:        KIX1-RIPE
tech-c:         TTDE1-RIPE
nic-hdl:        ATDE1-RIPE
mnt-by:         MAINT-AS3352
abuse-mailbox:  nemesys@telefonica.es
created:        2006-01-18T12:24:41Z
last-modified:  2018-09-18T10:36:42Z
source:         RIPE # Filtered

role:           Tecnicos Telefonica de Espana
address:        Ronda de la Comunicacion S/N
address:        28050-MADRID
address:        SPAIN
org:            ORG-TDE1-RIPE
admin-c:        TTE2-RIPE
tech-c:         TTE2-RIPE
nic-hdl:        TTdE1-RIPE
mnt-by:         MAINT-AS3352
abuse-mailbox:  nemesys@telefonica.es
created:        2006-01-18T12:39:59Z
last-modified:  2018-09-18T12:08:51Z
source:         RIPE # Filtered

% Information related to '81.47.0.0/16AS3352'

route:          81.47.0.0/16
descr:          RIMA (Red IP Multi Acceso)
origin:         AS3352
mnt-by:         MAINT-AS3352
created:        2002-03-26T11:55:32Z
last-modified:  2002-03-26T11:55:32Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.109.1 (DEXTER)

```

3.4. - Crea aquest fitxer docker-compose.yml

```
version: "3.5"
services:
  httpd:
    image: httpd:2.4.55
  nginx:
    image: nginx:1.22
  redis:
    image: redis:7.0.8-alpine
```

Primer instal·lem el docker: `sudo apt -y install docker-compose` y `sudo apt install docker`

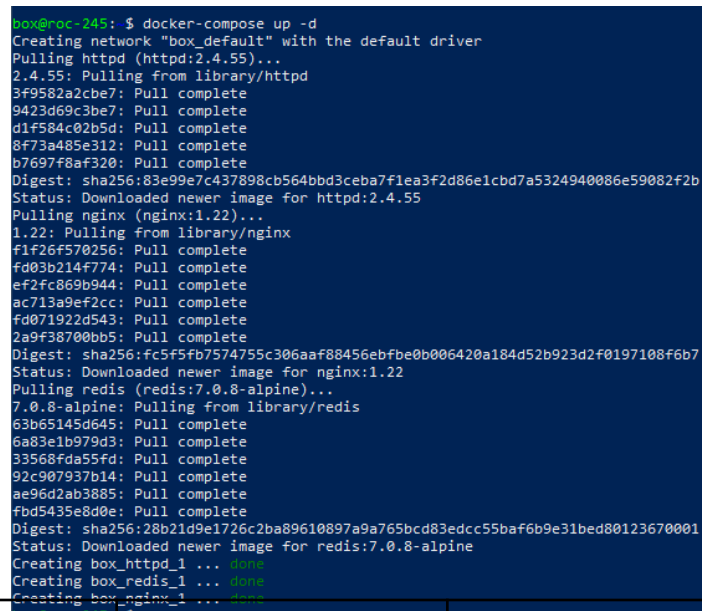
Ara fem un nano i l'anomenem docker-compose.yml:



```
GNU nano 6.2                                docker-compose.yml *
version: "3.5"
services:
  httpd:
    image: httpd:2.4.55
  nginx:
    image: nginx:1.22
  redis:
    image: redis:7.0.8-alpine
```

3.5. Executa la comanda docker-compose up en el mateix directori per aixecar el serveis definits en la configuració.

Un cop el tenim així l'hem d'executar: `docker-compose up -d`



```
box@roc-245: $ docker-compose up -d
Creating network "box_default" with the default driver
Pulling httpd (httpd:2.4.55)...
2.4.55: Pulling from library/httpd
3f9582a2cbe7: Pull complete
9423d69c3be7: Pull complete
d1f584c02b5d: Pull complete
8f73a485e312: Pull complete
b7697f8af320: Pull complete
Digest: sha256:83e99e7c437898cb564bbd3ceba7f1ea3f2d86e1cbd7a5324940086e59082f2b
Status: Downloaded newer image for httpd:2.4.55
Pulling nginx (nginx:1.22)...
1.22: Pulling from library/nginx
f1f26f570256: Pull complete
fd03b214f774: Pull complete
ef2fc869b944: Pull complete
ac713a9ef2cc: Pull complete
fd071922d543: Pull complete
2a9f38700bb5: Pull complete
Digest: sha256:fc5f5fb7574755c306aaf88456ebf0b006420a184d52b923d2f0197108f6b7
Status: Downloaded newer image for nginx:1.22
Pulling redis (redis:7.0.8-alpine)...
7.0.8-alpine: Pulling from library/redis
63b65145d645: Pull complete
6a83e1b979d3: Pull complete
33568fda55fd: Pull complete
92c907937b14: Pull complete
ae96d2ab3885: Pull complete
fbd5435e8d0e: Pull complete
Digest: sha256:28b21d9e1726c2ba89610897a9a765bcd83edcc55baf6b9e31bed80123670001
Status: Downloaded newer image for redis:7.0.8-alpine
Creating box_httpd_1 ... done
Creating box_redis_1 ... done
Creating box_nginx_1 ... done
```

3.6. Mostra els dockers actius.

Per mostrar els docker actius utilitzem docker ps:

```
box@roc-245:~$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS        NAMES
f3a7133f1f09   redis:7.0.8-alpine "docker-entrypoint.s..." 2 minutes ago Up 2 minutes 6379/tcp     box_redis_1
1a30ff369c85   nginx:1.22     "/docker-entrypoint..." 2 minutes ago Up 2 minutes 80/tcp       box_nginx_1
038f6fd6b34a   httpd:2.4.55   "httpd-foreground"       2 minutes ago Up 2 minutes 80/tcp       box_httpd_1
box@roc-245:~$
```

3.7. Obre un terminal interactiu en un contenidor i escaneja la xarxa privada

```
apt install -y nmap iproute2
```

Obrim un contenidor del que ja tenim actiu:

```
box@roc-245:~$ docker exec -it box_nginx_1 bash
root@1a30ff369c85:/#
```

```
root@1a30ff369c85:/# apt install -y nmap iproute2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dbus libapparmor1 libatm1 libblas3 libbpf0 libcap2 libcap2-bin libdbus-1-3 libelf1 liblinear4 liblua5.3-0 libmn10 libpam-cap
  libpcap0.8 libxtables12 lua-lpeg nmap-common
Suggested packages:
  default-dbus-session-bus | dbus-session-bus iproute2-doc liblinear-tools liblinear-dev ncat ndiff zenmap
```

Mirem la xarxa privada:

```
box@roc-245:~$ ip -brief addr | grep enp0s8
enp0s8          UP          192.168.56.19/24 fe80::a00:27ff:fe94:5a37/64
box@roc-245:~$
```

```
docker exec -it box_nginx_1 bash
```

```
box@roc-245:~$ docker exec -it box_nginx_1 bash
root@1a30ff369c85:/# nmap 192.168.56.19
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-30 18:59 UTC
Nmap scan report for roc-245 (192.168.56.19)
Host is up (0.000018s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```


3.8. Explica la topografia de la xarxa privada/24 (ip, port , servei). Omple la següent taula.

| Host Name | Port | IP | Service | |
|-----------|------|----|---------|--|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

3.9. Elimina tots els contenidors

Així boreu tots els contenidors: `docker rm -vf $(docker ps -a -q)`

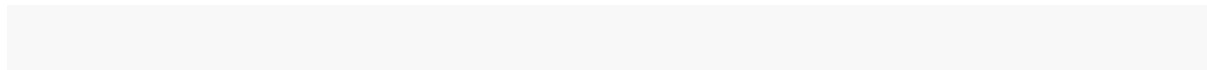
```
box@roc-245:~$ docker rm -vf $(docker ps -a -q)
f3a7133f1f09
1a30ff369c85
038f6fd6b34a
```

4. TCPDUMP 20%

01 - tcpdump

4.1. Mostra les interfícies que tens a la màquina.

4.2. Obre un nou terminal i executa la comanda per veure tot el tràfic **en una** interfície



- 4.3. Explica el resultat més importants del punt anterior
- 4.4. En un altre terminal executa un nslookup a google.es:
- 4.5. Executa la comanda que filtra el tràfic de totes les interfícies cuyo destí es dns
excluyen el port ssh