Pràctica 3: Seguretat lògica - Seguretat perimetral

1- Objectius de la pràctica

Aquesta activitat té com objectius adquirir els següents resultats d'aprenentatge i continguts marcats al currículum de la UF a DOGC:

- RA1 i C1 →
  - RA1.8 --> Aplica tècniques criptogràfiques en l'emmagatzematge i la transmissió de la informació.
  - C1.4 → Amenaces. Tipus: Amenaces físiques. Amenaces lògiques

Un altre objectiu de l'activitat és avaluar si s'han assolit correctament aquests coneixements per mitjà d'una pràctica.

Per desenvolupar aquests objectius:

- L'alumne haurà de llegir i entendre la documentació. Per resoldre qualsevol dubte sobre la documentació, es durà a terme una sessió a classe per explicar els conceptes més importants i resoldre els dubtes que hagin aparegut durant la lectura de la documentació.
- L'alumne haurà de lliurar una pràctica funcionant d'acord a allò que es demani a l'enunciat.

2- Conceptes de seguretat perimetral

La seguretat perimetral és el conjunt de mecanismes i sistemes de control de:

- L'accés físic de persones a les instal·lacions: Autenticació per mitjà de targetes d'accés amb foto verificades per un vigilant de seguretat, càmares CCTV, detectors de moviment, tanques de seguretat, etc..
- La detecció i prevenció d'intrusions per mitjà de firewalls, sistemes IDS/IPS (sistemes de detecció i i prevenció d'instrussions), honeypots, sistemes anti-DDoS, antivirus, aplicacions antispam.

3- Documentació sobre el Firewall UFW de Linux

1- Alguns exemples
2- Doumentació comunitat ubuntu sobre ufw
3- Documentació ufw sobre Ubuntu/Debian d'Ocean-I
4- Documentació ufw sobre Ubuntu/Debian d'Ocean-II
5- Documentació ufw sobre Ubuntu/Debian d'Ocean-III
6- Prioritat de les regles d'ufw
7- Drop vs Reject
8- Tràfic sortint
9- Principals caràcterísitiques. Arxius de configuració

4- Abans de començar la pràctica

a) Comprova que tens instal·ltats i en execució els servidor **apache2** i **SSH**. Executa:

```
systemctl status apache2
systemctl status apache2
```

i comprova que tots 2 es troben en estat **active (running)**.

```
aptitude search ^apache2$ ^coreutils$ ^wget$
```

i el resultat ha de ser:

```
i   A  apache2                        - Apache HTTP Server
i   A  coreutils                      - GNU core utilities
i   A  wget                           - retrieves files from the web
```

b) Comprova que el paquet **net-tools** es troba instal·lat en el sistema. Executa:

```
aptitude search ^net-tools$
```

i el resultat ha de ser:

```
i   A  net-tools                      - NET-3 networking tool
```

c) Comprova que el **servidor apache2 escolta pel port 80/tcp** i que el **servidor SSH escolta pel port 22/tcp**. Executa:

```
sudo netstat -atupn | grep -E '(apache2|ssh)'
```

i comprova que el resultat és:

```
dacomo@inf1-dacomo:~$ sudo netstat -atupn | grep -E '(apache2|ssh)'
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      517/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN      518/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      517/sshd: /usr/sbin
```

d) Comprova l'**adreça ip** del teu equip executant:

```
ip -4 -br add show dev enp0s3
```

e) Demana al teu company de grup que faci un **ping** al teu equip i comproveu que hi ha resposta per part del teu equip.

f) Demana al teu company que es connecti a la pàgina principal del servidor web del teu equip amb el seu navegador i escrivint a la barra d'adreces l'adreça IP del teu equip.

g) Demana al teu company que es connecti al teu servidor SSH tal i com ho vas fer a la pràctica m11uf1pr2d.

5- Treballant amb el firewall UWF de Linux - Part 1

a) Actualitza la llista de paquets del sistema i a continuació instal·la el firewall UFW. Executa:
sudo aptitude update
sudo aptitude install ufw

i ara comprova que ufw s'ha instal·lat correctament. Executa:

aptitude search ^ufw$

El resultat hauria de ser aquest:

```
dacomo@inf1-dacomo:~$ sudo aptitude search ^ufw$
i   ufw                                                    - program for managing a Netfilter firewall
```

b) Activa el firewall del teu equip i comprova el seu estat. Executa:

sudo ufw enable
sudo ufw status verbose

Comprova:
- que les **connexions entrants** estan **denegades per defecte**.
- que des de l'ordinador d'un company que **no** hi ha accés al servei web i SSH del teu equip.

c) **Permet** que el teu equip **accepti** connexions al port **80/tcp** (el port del servei web). A continuació comprova l'estat del firewall. Executa:

sudo ufw allow 80/tcp
sudo ufw status verbose

Comprova des de l'ordinador d'un company que **sí** hi ha accés al servei web del teu equip. Abans, haurà de netejar l'historial del seu navegador.

d) **Permet** que el teu equip **accepti** connexions al **servei SSH** a partir del nom del servei (**ssh**). A continuació comprova l'estat del firewall. Executa:

sudo ufw allow ssh
sudo ufw status verbose

Comprova des de l'ordinador d'un company que **sí** hi ha accés al servei SSH del teu equip.

e) Intenta fer un **ping** des de l'ordinador del teu company al teu equip i comprova que hi ha resposta. A continuació denega el funcionament del **ping**. El programa **ping** necessita que el **protocol icmp** de **tipus echo-request** estigui **permés**. Per tant, s'ha de denegar. Fes les següent accions:
- Executa: **sudo nano -c /etc/ufw/before.rules**
- A la línia **37**, canvia **ACCEPT** per **DROP**. Salva el fitxer.
- Deshabilita i torna a habilitar el firewall UFW:
  - **sudo ufw disable**
  - **sudo ufw enable**

Comprova que no es pot fer un ping des de l'equip d'un company al teu equip.

6- Treballant amb el firewall UWF de Linux - Part 2

a) Si vols denegar l'accés al teu equip si la petició arriba des d'una adreça IP en concret, com per exemple **192.168.1.37**, llavors s'hauria d'executar aquesta ordre:

```
sudo ufw deny from 192.168.1.37
```

Ara, troba l'adreça IP de l'equip del teu company. A continuació, denega l'accés al teu equip de l'ordinador del teu company de grup a partir de la seva adreça IP, i després comprova l'estat del teu filtre. Assegura't que:

- L'accés al servei web i SSH està permés.
- Que l'adreça IP del teu company té denegat l'accés al teu equip. Si executes:

```
sudo ufw status numbered
```

Ha de sortir una nova regla d'aquest estil:

	To	Action	From
[3]	Anywhere	DENY	192.168.1.37

Evidentment, l'adreça IP de la columna **From** serà realment l'adreça IP de l'ordinador del teu company.

b) Ara, intenta realitzar una connexió des de l'ordinador del teu company:

- Al servei web del teu ordinador. Abans haurà de netejar l'historial del seu navegador. Pot accedir-hi?. Per què?.
- Al servei SSH del teu ordinador. Pot accedir-hi?. Per què?.

c) No hi ha prou amb afegir la regla per denegar l'accés a l'ordinador del teu company, perquè si ho comproves, veuràs que la nova regla és la número [3]. Això vol dir que abans s'han comprovat les regles [1] i [2], i aquestes regles permeten la connexió al serveis web i SSH sense comprovar l'adreça IP. Per tant hem de fer que la regla per denegar accés a l'adreça IP del teu company sigui la primera. Exectuta:

sudo ufw delete 3 → és la posició de la regla que hem creat a l'apartat **a)**
sudo ufw insert 1 deny from 192.168.1.37 → És la nova regla que estarà a la primera posició i l'adreça IP hauria de ser la del teu company.

d) Ara, intenta realitzar una connexió des de l'ordinador del teu company:

- Al servei web del teu ordinador. Abans haurà de netejar l'historial del seu navegador. Comprova que no pot accedir-hi.
- Al servei SSH del teu ordinador. Comprova que no pot accedir-hi.

7- Treballant amb el firewall UWF de Linux- part 3

a) Esborra totes les regles i desactiva el firewall UFW. Executa:

```
sudo ufw reset
```

b) Comprova:

- L'estat del firewall. Hauria d'estat amb el Status igual a **inactive**.
- Si actives el firewall i tornes a comprovar l'estat, veuràs que les regles han estat esborrades.

Lliurament de l'activitat

1- Activitat en grups de 2 persones o individual.

2- S'ha de mostrar el funcionament de:

* Part 1:
  - Mostra que el firewall està actiu i les seves regles de filtratge.
  - Mostra que el teu company no pot fer pings al teu ordinador
  - Mostra que el teu company **sí** pot connectar-se al servei web i ssh.
* Part 2:
  - Mostra que el firewall està actiu i les seves regles de filtratge.
  - Comprova l'adreça IP del teu company d'equip.
  - Mostra que els serveis SSH i web del teu equip estan actius.
  - Mostra que el teu company **no** pot connectar-se al servei web i ssh.
* Part 3:
  - Mostra que has esborrat totes les regles del firewall.
  - Torna a desactivar el firewall

3- Dates de lliurament: Setmana del **24-1-22** al **28-11-22** dins de l'horari escolar per aconseguir el **100%** de la nota. Setmana del **31-1-22** al **4-2-22** dins de l'horari escolar per aconseguir el **100%** de la nota. La setmana del **7-11-22** al **12-2-22** per aconseguir el **70%** de la nota. Després d'aquesta setmana, no s'acceptarà aquesta pràctica.