Pràctica 1: Tallafocs bàsics de Windows i Linux

Els objectius de la pràctica **m11uf2pr1** són:
a) Treballar amb el **tallafocs integrat** de **Windows**
b) Treballar amb el **tallafocs ufw** de **Linux**

DOCUMENTACIÓ

a) Firewall de Windows amb seguretat avançada
1- Prioritat de les regles
2- Afegint o editant regles
3- Treballant amb regles de seguretat

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

c) Documentació de l'IOC
Documentació IOC

PRÀCTICA

a) Treballant amb ufw

1- Instal·la i activa sobre Debian o Kali Lunux els servidors ssh, vsftpd, apache2. Comprova el funcionament dels serveis. Habilita l'opció d'escriptura pels usuaris locals utilitzant vsftpd.

2- Preparació de les màquines virtual:

a) Fes treballar la teva màquina virtual Debian o Kali Lunux amb xarxa interna i configura-la amb l'adreça IP 192.168.1.2 i màscara 255.255.255.0.

b) Posa en marxa una màquina Ubuntu treballant amb xarxa interna i configura-la amb l'adreça IP 192.168.1.3 i màscara 255.255.255.0.

c) Posa en marxa una màquina Windows treballant amb xarxa interna i configura-la amb l'adreça IP 192.168.1.4 i màscara 255.255.255.0.

3- Comprova que pots fer pings des d'Ubuntu i Windows a Debian. Amb l'ajut que trobaràs a la secció ENABLE PING del primer enllaç de la documentació sobre UFW, deshabilita el ping de Debian i comprova que ja no pots fer pings al servidor des de Windows i Ubuntu.

4- Torna a permetre els pings cap el servidor. Amb l'ajut de la documentació, fes que a partir de l'adreça IP d'Ubuntu, aquest ordinador no pugui accedir a cap servei del sistema Debian.

5- Habilita l'accés novament d'Ubuntu. Comprova que pots connectar-te des de Windows i Ubuntu al servidor SSH de Debian. Amb l'ajut que trobaràs al enllaços, troba com permetre a l'ordinador windows accedir al servidor SSH i denegar l'accés a l'Ubuntu a partir de la seva adreça IP.

6- Fes que el servidor apache2 utilitzi HTTPS (port 443) i HTTP (80). Fes que el directori arrel per la connexió segura sigui /var/www/htm/secure i crea a dins un document de nom index.html amb el següent codi HTML:

```
<html>
      <title>
            Pàgina segura del lloc web
      </title>
      <body>
            Aquesta és la pàgina inicial del lloc web segur del servidor<br>
      </body>
</html>
```

Comprova que pots connectar-te des Windows i Ubuntu via HTTP i HTTPS a Debian. Amb l'ajut de la documentació denega l'accés al port de la connexió segura des de l'ordinador Windows.

7- Deshabilita la connexió al port 80 pel Windows i comprova que tampoc pot accedir a la pàgina inicial de lloc via HTTP.

8- Esborra l'anterior opció. Crea una opció que permet a Windows accedir al port 80 del servidor Debian i després una que no ho permet. Comprova que passa.

9- Esborra les dues darreres opcions. Ara posa les mateixes regles a l'inrevés. Comprova que passa.

10- Esborra totes les regles però deixa actiu el tallafocs ufw. Obre el navegador des d'Ubuntu o Windows i intenta connectar-te al servidor web de Debian/Kalli. Pots connectar-te?. Què passa?.

11- Obre el fitxer /etc/syslog i comprova quins missatges escriu el sistema quan el client ha intentat connectar-te al servidor.

12- Ara fes les següents tasques:

a) Crea un usuari de sistema de nom **asix2** al servidor Kali/Debian. La resta de paràmetres de l'usuari són els que creguis oportuns.

c) Modifica el firewall per permetre les connexions entrants al port 21.

d) Comprova que des de Windows o Ubuntu amb Filezilla pots connectar-te com usuari asix2 al servidor i pujar un fitxer a la seva carpeta personal. Comprova, executant immediatament l'ordre netstat -atupn que s'ha fet servir el port 20 per la transmissió de dades.

13- Fes les següents tasques:

a) Connecta el servidor Debian/Kali a la xarxa de l'escola i comprova que pot navegar per internet

b) Denega al servidor Debian/Kali el trànsit de de sortida al port 80 de quasevoll ordinador extern.

c) Comprova si pots navegar per internet.

14- Esborra la regla anterior i ara crea una regla per no permetre trànsit de sortida al port 80 només del servidor **www.clot.fje.edu**.

b) Firewall de Windows amb seguretat avança

1- Crea una regla anterior per permetre a Windows tenir trànsit de sortida cap al port **80** de cap servidor a internet. Crea una segona regla que denegui l'anterior. Què passa i per què?

2- Esborra les regles anteriors. Crea una regla anterior per permetre a Windows tenir trànsit de sortida cap al port **80** del servidor **www.clot.fje.edu**. Crea una segona regla que denegui l'anterior. Què passa i per què?

3- Realitza les següents tasques:

a) Instal·la el servidor SSH per Windows FreeSSHd. No s'ha d'instal·lar com un servei.

b) Com usuari Administrador posa en marxa el servei SSH escoltant pel port 2222.

c) Crea un usuari del servidor SSH associat a un usuari de sistema Windows (Opció NT authentication)

d) Des d'un altre sistema connecta't al servidor SSH amb l'usuari creat.

4- Comprova que dins del Firewall de Windows s'ha creat automàticament una regla per servidor SSHd. Comprova que és de tipus **Allow** sobre **TCP** i **UDP.**

5- Bloqueja la connexió del servidor F**reeSSHd**. Comprova ara si es pot realitzar una connexió.

6- Fes que el teu ordinador client tingui l'adreça **192.168.1.20/24**. Fes que Windows tingui l'adreça IP **192.168.1.10/24**. Fes que el marge d'adreces IP acceptades pel sigui des de l'adreça IP **192.168.1.30/24** a **192.168.1.50/24**. Comprova ara si pots establir una connexió.

7- Fes que el teu ordinador tingui ara l'adreça IP 192.168.1.30/24 i comprova ara si pots establir la connexió.

Forma de lliurament

1- Data: **21-1-17/24-2-17**

a) Mostra'm que el servidor Apache2 de Kali/Debian Linux escolta i treballa amb el port 443 i s'accedeix a la pàgina indicada a l'apartat des d'Ubuntu i Windows.

b) Fes que des d'Ubuntu i Windows no es pugui accedir al port 443 del servidor Apache2 de Kali/Debian Linux.

c) Fes que el servidor Kali/Debian no puguir accedir la web de www.collados.org però si a qualsevol altra adreça URL.

d) Comprova que des d'Ubuntu es pot accedir al port 2222 del servidor FreeSSHd de Windows. Bloqueja ara la connexió al port 2222 de Windows i comprova que no es pot accedir des d'Ubuntu.

e) Fes que Windows no pugui accedir a la web de www.collados.org però si a qualsevol altra adreça URL.