[FORT] Práctica 6: Mantenimiento

Se mantiene la configuración de red de la práctica 5.

Preparación

La MAQUINA1 tiene un container corriendo SSH en el puerto 222. El puerto 222 se redirige al container

Primero creamos un script con el código que se nos ha proporcionado:

```
  GNU nano 7.2                                          script.sh *
#!/usr/sbin/nft -f
#en esta maquina la direccion del container es 10.0.3.200
table ip nat {
        chain PREROUTING { #redirigimos conexiones externas alssh al container
                type nat hook prerouting priority dstnat; policy accept;
                ip daddr {192.168.2.10, 192.168.3.10, 192.168.4.10} tcp dport {222} log
                ip daddr {192.168.12.10, 192.168.13.10, 192.168.14.10} tcp dport {222} log
                ip daddr {192.168.2.10, 192.168.3.10, 192.168.4.10} tcp dport {222} dnat to 10.0.3.2
                ip daddr {192.168.12.10, 192.168.13.10, 192.168.14.10} tcp dport {222} dnat to 10.0.
        }
}
```

y lo hacemos ejecutable con el siguiente comando:

```
sudo chmod +x /etc/nftables/script.sh
```

Instala Syslogd en el container

Primero debemos revisar el nombre del container con el comando:

```
lxc-ls
```

```
root@fso2025:~# lxc-ls
deb
```

En este caso el container se llama deb y podemos arrancarlo (en caso de que esté apagado) con el con el siguiente comando:

```
lxc-start -f -n deb
```

Una vez levantado el container nos podemos conectar a este con:

```
lxc-attach -n deb
```

```
root@fso2025:~# lxc-attach -n deb
root@deb:~#
```

una vez dentro del container instalamos syslogd:

```
root@deb:~# apt install inetutils-syslogd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  inetutils-syslogd
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 84.2 kB of archives.
After this operation, 171 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian stable/main amd64 inetutils-syslogd amd64 2:2.4-2+deb12u1 [84.2 kB]
Fetched 84.2 kB in 0s (533 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package inetutils-syslogd.
(Reading database ... 12198 files and directories currently installed.)
Preparing to unpack .../inetutils-syslogd_2%3a2.4-2+deb12u1_amd64.deb ...
Unpacking inetutils-syslogd (2:2.4-2+deb12u1) ...
Setting up inetutils-syslogd (2:2.4-2+deb12u1) ...
```

1. Crea claves RSA para los usuarios user001, user002 y user003 en Maquina2. user003 debe estar protegido por una passphrase

Para crear las claves RSA para los usuarios usamos el siguiente comando logueados desde sus cuentas:

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa
```

```
user001@fso2025:~$ ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa
Generating public/private rsa key pair.
Created directory '/home/user001/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user001/.ssh/id_rsa
Your public key has been saved in /home/user001/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:jpxSbVuCOevsFVzeBW0cc4GZIOFNJBkxazmP65gGdFM user001@fso2025
The key's randomart image is:
+---[RSA 4096]----+
|         B*+oo*oo|
|        .EO  =+o |
|        .*.. ..  |
|     . B.o+. .   |
|    . * S.o..    |
|     + B =.      |
|    . * +.       |
|     + o+        |
|     .=o .       |
+----[SHA256]-----+
```

```
root@fso2025:~# su - user002
user002@fso2025:~$ ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa
Generating public/private rsa key pair.
Created directory '/home/user002/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user002/.ssh/id_rsa
Your public key has been saved in /home/user002/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:oPQw1wFtjVBqLg5RVPZshC0yp3Tghba9Vcu45WndzSw user002@fso2025
The key's randomart image is:
+---[RSA 4096]----+
|    .++*B+o      |
|   o*o=*=.o      |
|  .o=O=o=+ .     |
|   ooO.oo +      |
|  . o ooS+ o . + |
|   o .. . + . E +|
|     .    .     . |
|                 |
|                 |
+----[SHA256]-----+
```

En el caso de user003, a diferencia que con los anteriores usuarios, no dejaremos la passphrase vacía:

```
user003@fso2025:~$ ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa
Generating public/private rsa key pair.
Created directory '/home/user003/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user003/.ssh/id_rsa
Your public key has been saved in /home/user003/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:B6MjijtbLJsBSVEHimfm/waqx4JhNlBf2Zuoxq8RqKc user003@fso2025
The key's randomart image is:
+---[RSA 4096]----+
| ..o.. o         |
|. + . o .        |
|.++. . .oo       |
|o* .. ..oo       |
|+ o.o.o S .      |
|oB o=o . .       |
|Oo*ooo           |
|+X+  oo          |
|E*  .o.          |
+----[SHA256]-----+
```

2. Habilita el acceso a MAQUINA1 desde MAQUINA2 para los usuarios del 001 al 003

Para habilitar el acceso a la máquina 1 desde la máquina 2 debemos conectarnos a la máquina 2 desde la 1 y copiar las claves RSA de cada usuario

Notas para ejercicio 5: syslogd: para aceptar los logs ay que poner -r, para que los reenvíe hay que ponerle -h. Archivos importantes a modificar:

```
cd /etc/init.d/
sudo nano inetutils-syslogd
sudo nano /etc/default/inetutils-syslogd
```

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:fortificacion:p6&rev=1742307932

Last update: **2025/03/18 14:25**