[FORT]TEMA 6: Securizando la red

La máquina más segura en la que no está conectada a la red, en el momento en el que se conecta una máquina a la red, cuantos más servicios más proporcione, mayores amenazas.

Limitar accesos a un servicio

Control de acceso a nivel de aplicación

Para denegar acceso a una máquina en especial modificamos /etc/hosts.deny y añadimos su IP de la siguiente forma:

```
nano /etc/hosts.deny #Modificamos el fichero
#Linea que se añade:
ftpd: 192.168.2.15, 192.168.3.15, 192.168.4.4 #Bloqueamos 3 ips
telnetd: ALL #Se bloquea el acceso por telnet
```

A esto se le llama control de acceso a nivel de aplicación ya que se realiza la conexión pero la rechaza la apicación.

se modifica el contendio de nano /etc/unedtd.d cpn los siguiente:

```
telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/telnetd #Una conexión
de telnert llama a tcpd que llama a telnet.
telnet stream tcp nowait root /usr/sbin/telnetd /usr/bin/telnetd
```

Control de acceso a nivel de filtrado de paquetes (IPTables y NFTables)

editamos nano /etc/hosts.deny:

```
cd /root/nftables
nano host-ftpd
#Contenido:
table ip filter{
  chain Input{
    type filter hook input priority filter; policy
    ip daddr (192.168.12.10) tcp dport 21 log reject #Bloqueamos el puerto
21 para la IP indicada
  }
}
#Fin contenido



~/NFTABLES ./host-ftpDrop.conf #Permite configurar que se rechaza en el ftp
```

```
con NFTABLES
```

NFTABLES: Cadenas

Cada regla es siempre una selección de paquetes y cada regla siempre tienen la misma estructura que es la selección de paquetes y luego la acción. Funciona como una especie de AND perezoso. La acción puede ser:

- ACCEPT para aceptar
- REJECT para rechazar
- DROP simplemente ignora el paquete.
- JUMP para saltar a otra cadena y retornar a donde se estaba
- GOTO lo mismo, pero sin retorno

Una cadena base es aquella que se define con el tipo de cadena, tipo de hook, prioridad que tiene y su política por defecto. A una cadena base le llegan los paquetes de un hook. Una vez que un paquete hace un match con una regla, se hace la acción que dice y no se hace más, a menos que tenga la opción log. Ejemplo para uun container en la 10.0.3.200 modificamos \NFTABLES\container-web.conf:

```
table ip filter{
  chain Input{
    type filter hook prerouting priority dstnat; policy accept;
    ip daddr (192.168.2.10) tcp dport 21 log reject #
  }
}
```

NFTABLES\

Configuración SSHD

```
ssh -p 22222 10.0.3.200
```

```
cd /etc/sshd_config
```

</code>