[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; policyu
    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
```

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

Permanent link:
https://knoppia.net/doku.php?id=master_cs:fortificacion:tm6&rev=1740418729

Last update: **2025/02/24 17:38**