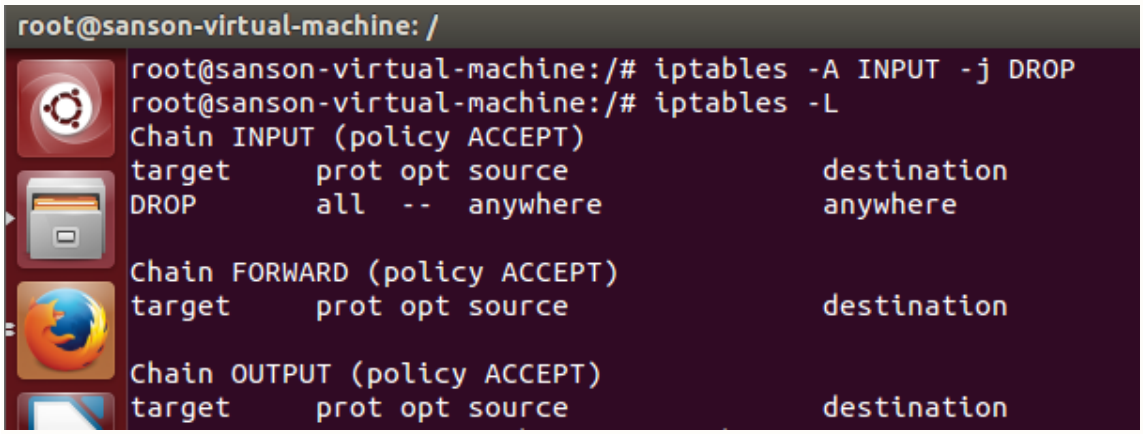
# SWAP: EJERCICIOS TEMA 6

Mónica Jiménez Montañés

- **Ejercicio T6.1**: Aplicar con iptables una política de **denegar** todo el tráfico en una de las máquinas de prácticas. Comprobar el funcionamiento.

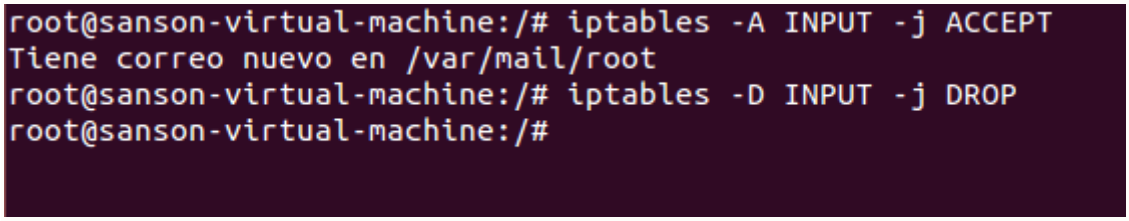
Aplicar con iptables una política de **permitir** todo el tráfico en una de las máquinas de prácticas. Comprobar el funcionamiento.

Para bloquear el trafico introducimos en el terminal el siguiente comando:




Para comprobar el trafico lo hacemos con iptables –L.

Para aceptar el tráfico cambiamos la orden a ACCEPT y borramos la tabla creada con DROP.



```
root@sanson-virtual-machine:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@sanson-virtual-machine:/#
```

- **Ejercicio T6.2:** Comprobar qué puertos tienen abiertos nuestras máquinas, su estado, y qué programa o demonio lo ocupa.

  Usamos el comando *netstat -tulpn*

```
root@sanson-virtual-machine:/# sudo netstat -tulpn
```

```
root@sanson-virtual-machine: /
tcp        0      0 0.0.0.0:8652            0.0.0.0:*               ESCUCHAR
1382/gmetad
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               ESCUCHAR
9557/php
tcp6       0      0 ::1:631                 :::*                    ESCUCHAR
5755/cupsd
tcp6       0      0 :::25                   :::*                    ESCUCHAR
1812/master
tcp6       0      0 :::80                   :::*                    ESCUCHAR
5322/apache2
udp        0      0 239.2.11.71:8649        0.0.0.0:*
1299/gmond
udp        0      0 0.0.0.0:59884           0.0.0.0:*
640/avahi-daemon: r
udp        0      0 0.0.0.0:24585           0.0.0.0:*
966/dhclient
udp        0      0 0.0.0.0:48156           0.0.0.0:*
1960/snmpd
udp        0      0 127.0.1.1:53            0.0.0.0:*
1096/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*
12273/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*
966/dhclient
udp        0      0 0.0.0.0:631             0.0.0.0:*
1231/cups-browsed
udp        0      0 127.0.0.1:161           0.0.0.0:*
1960/snmpd
udp        0      0 0.0.0.0:5353            0.0.0.0:*
640/avahi-daemon: r
```

- **Ejercicio T6.3**: Buscar información acerca de los tipos de ataques más comunes en servidores web, en qué consisten, y cómo se pueden evitar.

Keyloggers y Spyware. Dichos ataques permiten instalarse silenciosamente en la PC con el fin de enviar datos sobre la información que la víctima teclea o almacena en el sistema, incluso, sobre sus hábitos en Internet.

Backdoor o puerta trasera. Mediante herramientas que dan acceso remoto para controlar los sistemas infectados.

Modificando una cadena de consulta de base de datos mediante la inyección de código en la consulta. Es de los ataques más fáciles de llevar a cabo. Esto permite acceder a toda la información de una empresa la cual se almacena en su base de datos.

DDoS. Lo que hace la denegación de servicio es imposibilitar el acceso a una página web. Se generan multitud de peticiones hacia el servidor con la finalidad de desbordar el ancho de banda o consumir todos los recursos de red. De esta forma la web queda inaccesible para cualquier usuario normal que intente acceder al contenido.

Fuerza bruta. Se basa en obtener el usuario y contraseña probando todas las posibilidades posibles de claves alfanuméricas. Generalmente se consiguen obtener contraseñas sencillas debido a que se necesita un menor tiempo al ser normalmente fechas o palabras comunes.

Cross Site Scripting. Es la inyección de scripts maliciosos en webs de confianzas para que los visitantes lo ejecuten creyendo que es de confianza y así los hackers tengan acceso a las cookies o tokens generados por la web presuntamente confiable.

Abuso al sistema vía acceso privilegiado. Es el abuso deliberado de recursos, accesos o privilegios concedidos a una persona por una organización.

Acceso no autorizado con credenciales predeterminadas. Son los métodos a través de los cuales los atacantes obtienen acceso a un dispositivo o sistema protegido con contraseñas y nombres de usuario predeterminados o estandarizados.

Violación de usos aceptables y otras políticas. En realidad, este ataque no distingue si fue cometido de manera accidental o premeditada, la violación a una política fue tener graves consecuencias.

Acceso no autorizado mediante listas de control de accesos débiles o mal configuradas (ACL). Cuando hay las condiciones el atacante puede acceder a recursos y llevar a cabo acciones sin que la víctima se dé por enterada.

Acceso no autorizado vía credenciales robadas. Para llegar a este punto, el atacante se valió de otros métodos para ganar acceso válido a sistemas protegidos sin ser detectado.

RAM scraper. Una nueva forma de diseño de malware para capturar información en la memoria RAM.

Phishing y sus variantes. Una técnica en la cual un atacante utiliza comunicaciones electrónicas fraudulentas para provocar que el destinatario facilite información.