# Práctica de FW e IDS

***Objetivos:***

Aprender a establecer políticas de seguridad para proteger la red y sus servicios:

- Definiendo reglas que permitan implementar filtrado de paquetes, firewalls de estados, redirección de paquetes; para satisfacer distintos tipos de requerimientos y en función de las topologías planteadas.
- Configurando distintos tipos de IDSs estudiados (de Red, Host y Filesystem) y analizando los registros que los mismos proveen.

**Parte 1: Firewalls**

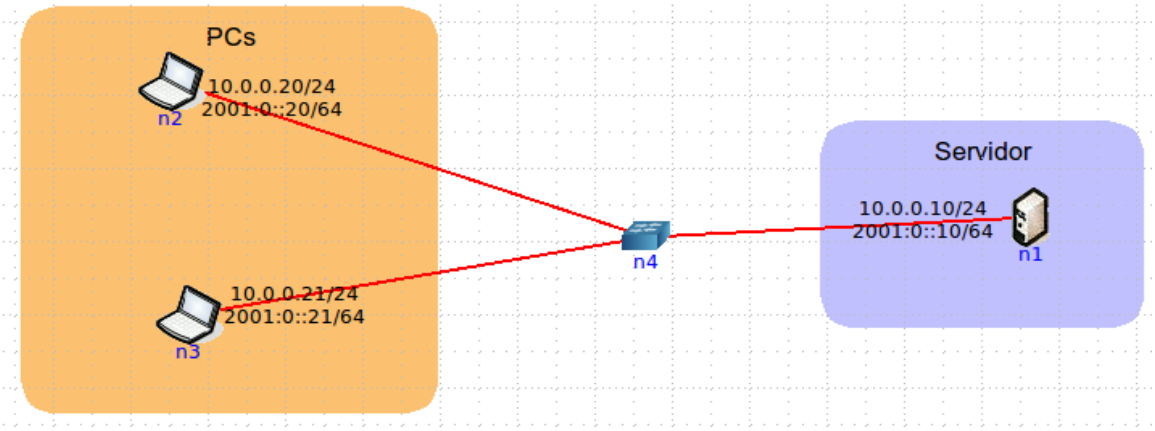
Puede encontrar de utilidad la información publicada en http://www.faqs.org/docs/iptables/

o en http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html. Tenga en cuenta que para la verificación del correcto funcionamiento de las reglas definidas pueden ser útiles los siguientes comandos:

- Desde el lado de quien inicia las comunicaciones, es decir desde cliente, el servidor o ambos dependiendo de la topología; ping, nmap, telnet, netcat, hping3
- En el firewall: tcpdump, iptables

**Sección A - Topología LAN**

Utilizando la herramienta "**core**" arme una topología como la siguiente.




1) Verifique los servicios (TCP/UDP) que brinda el servidor con los comandos ***netstat -nat*** y ***netstat -nau***

2) Configure el firewall del Servidor para aceptar solamente conexiones al puerto 22 utilizando una política restrictiva.
   **VERIFICACION Y BORRADO**
   - Verifique con los comandos: telnet o netcat, hping3, ping, nmap, tcpdump e iptables -nL -v, el correcto funcionamiento de las reglas.

- Una vez finalizado, desconfigure lo hecho, de modo que el firewall acepte todo. Nota: con el comando "iptables -F" se eliminan todas reglas, salvo las políticas configuradas, y con "iptables -Z" se reinicializan los contadores a cero.

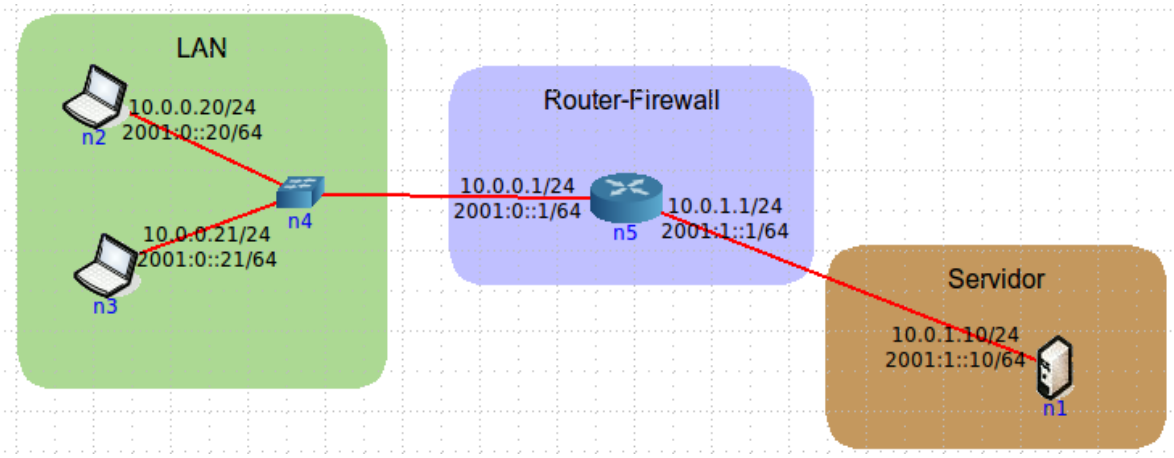
3) Configure el firewall del Servidor para aceptar solamente conexiones al puerto 22 utilizando una política permisiva.
   (a) Proceda a realizar el procedimiento de VERIFICACION Y BORRADO.

4) Configure el firewall del Servidor para redireccionar toda petición que llega al puerto TCP 2222 para que sea dirigida hacia el puerto TCP 22 del mismo equipo, siendo el puerto 2222 el único que puede recibir conexiones desde las PCs. El puerto 22 del servidor, no debería ofrecer servicio directamente.
   (a) Proceda a realizar el procedimiento de VERIFICACION Y BORRADO.

5) Configure el firewall del Servidor para permitir solamente conexiones al puerto 22 solamente. Además configure el firewall de una de las PCs de modo que la misma pueda realizar cualquier tipo de comunicación hacia los demás (siempre y cuando el Servidor se lo permita) pero que los demás no puedan iniciar comunicaciones nuevas hacia ella. **Nota: debe utilizar estados para resolver este ejercicio.**
   (a) Proceda a realizar el procedimiento de VERIFICACION Y BORRADO.

## Sección B - Topología Ruteada

Utilizando la herramienta "core" arme una topología como la siguiente.




2. Verifique que el router-firewall tiene la conmutación de paquetes habilitada. Para ello, visualice el contenido del archivo **/proc/sys/net/ipv4/ip_forward**, con el siguiente comando **"cat /proc/sys/net/ipv4/ip_forward"**. (1 = habilitada. 0 = deshabilitada). Para cambiar dicho valor, utilice los comandos **"echo 1 > /proc/sys/net/ipv4/ip_forward"** o **"echo 0 > /proc/sys/net/ipv4/ip_forward"** respectivamente.

   Verifique que el ruteo funciona ejecutando el comando ***ping*** desde una de las PCs de la LAN al Servidor luego de modificar la mencionada opción en el router/firewall. Puede adicionalmente hacer el seguimiento de los paquetes para debugear hasta donde están llegando los paquetes con el comando ***tcpdump*** aplicado en las distintas interfaces del

router/firewall y del Servidor.

3. Ejecute el siguiente script en el Servidor para simular distintos servicios:

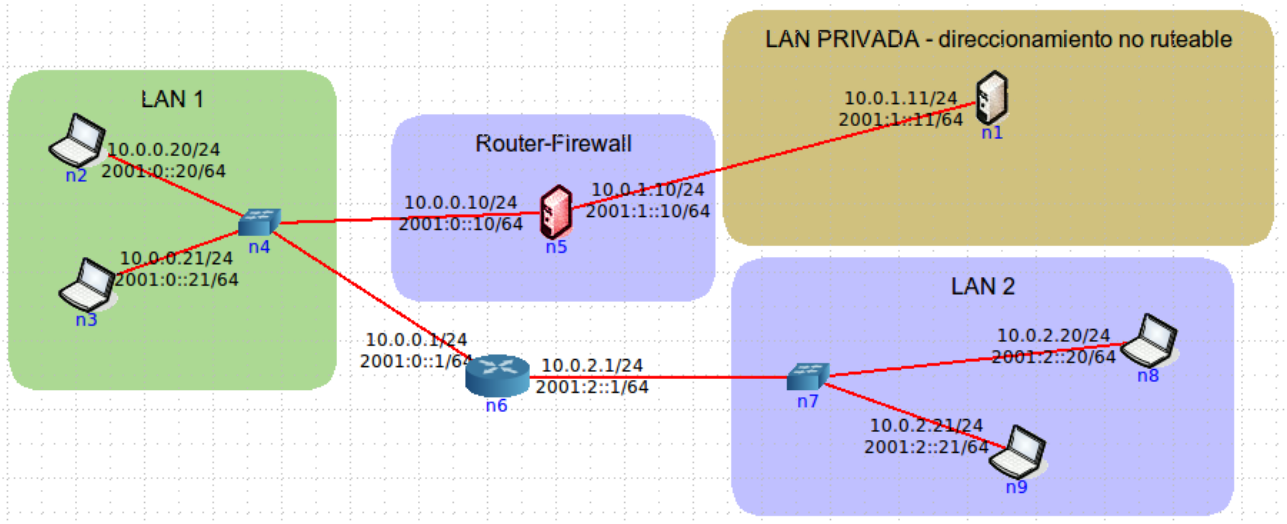
```
# ncat -l 21 -k & ncat -l 25 -k & ncat -l 80 -k &  ncat -l 443 -k &
```

4. Verifique los servicios (TCP/UDP) que brinda el servidor con los comandos ***netstat -nat*** y ***netstat -nau***

5. Configure el firewall del router-firewall, utilizando una política restrictiva y las caracteristicas de STATEFULL del firewall, de modo que:
   (a) Se permita únicamente el acceso desde la LAN a los servicios: FTP, SSH y HTTP que corren en el Servidor.
   (b) Además de las comunicaciones permitidas anteriormente ninguna otra comunicación hacia el router-firewall debe permitirse, ya sea desde la LAN como desde el Servidor.
   (c) Desde el firewall se deben poder iniciar conexiones SSH y HTTPS al Servidor.
   (d) Desde el servidor se debe permitir el acceso al servicio SSH de las PCs de la LAN.
      1. Proceda a realizar el procedimiento de VERIFICACION Y BORRADO.

**Sección C - Topología Nateada**

Utilizando la herramienta "**core**" arme una topología como la siguiente.




Tenga en cuenta que la idea de esta sección es configurar un firewall con redirecciones. Para ello, hay una red que no es ruteable, por lo cual si desde LAN1 o LAN2 se intentan realizar algún tipo de comunicación, la misma no funcionará.

**IMPORTANTE:** Al armar la topología, lo único que no se autoconfigura debidamente es el gateway del servidor, la simulación de algunos servicios y la función de conmutación de paquetes en el router-firewall. Para corregir esto deberá realizar en el Servidor:

```
# route del default
# route add default gw 10.0.1.10
# ncat -l 21 -k & ncat -l 25 -k & ncat -l 80 -k &  ncat -l 443 -k &
```

En tanto en el router-firewall deberá realizar:

```
# echo 1 > /proc/sys/net/ipv4/ip_forwarding
```

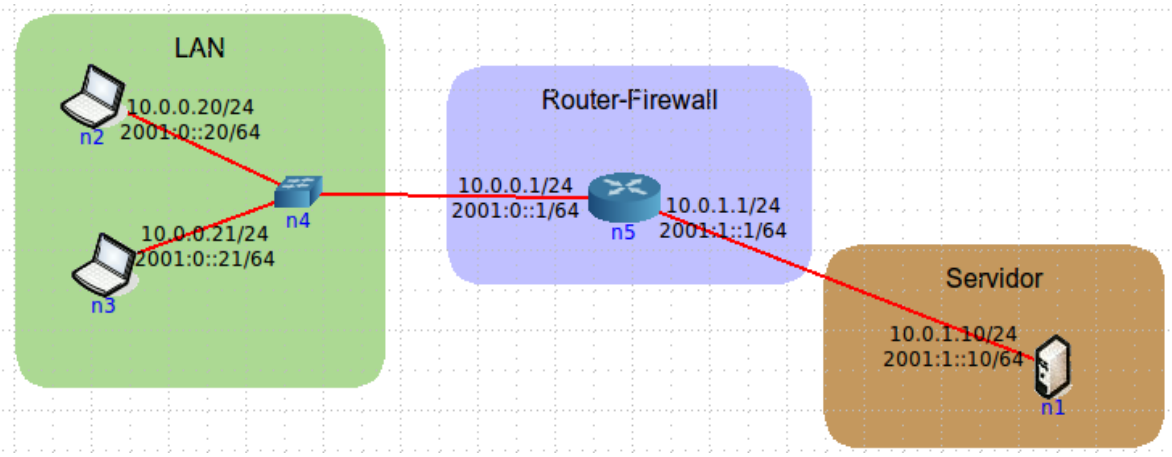
1. Por defecto, desde la LAN 1 o la LAN 2 ¿es posible hacer un ping al servidor? ¿cuál es el problema?
2. Desde el servidor, ¿es posible hacer un ping a las PCs de la LAN 1 o la LAN 2? Utilice **tcpdump** para evaluar si los pings del servidor llegan o no y analice porque.
3. Configure el firewall del router-firewall, utilizando una política restrictiva y las caracteristicas de STATEFULL del firewall, de modo que:
   1. Se permita en el firewall cualquier tipo de comunicación desde el servidor hacia las PCs de la LAN 2 pero no de la LAN 1.
   2. Se permita todo el tráfico proveniente desde la LAN 1 y la LAN 2 dirigido al puerto 80 del firewall, redirigiendolo al puerto 80 del servidor.
   3. Se deniegue cualquier otro tipo de comunicación.

   Verificar el correcto funcionamiento realizando desde la LAN 1 y la LAN 2 con un escaneo de puertos sobre el firewall, el cual deberá informar que el único puerto abierto es el 80.

## Parte 2: IDS de red

### Topología IDS de red

Utilizando la herramienta "**core**" arme una topología como la siguiente.




### Configuración

1. Ejecute el siguiente script en el Servidor para simular distintos servicios:

```
# ncat -l 21 -k & ncat -l 25 -k & ncat -l 80 -k &  ncat -l 443 -k & ncat -l 3376 &
```

2. Ejecute el router/firewall donde correrá el snort:

```
# mkdir /var/log/snort
```

**Pruebas de detección simples**

Se utilizará Snort como un IDS de red en el Router/Firewall para que analice el tráfico que circula entre la red LAN y la red donde está el Servidor.

1. Inicie el Snort en el router-firewall con el siguiente comando, de modo que reporte en la misma consola las alertas que se disparan:

```
# snort -A console -p -S HOME_NET=10.0.0.0/8 -c /etc/snort/snort.conf -i eth0
```

2. Realice un escaneo de puertos desde una de las PCs de la LAN hacia el servidor y responda:

   **DEL LADO DEL ATACANTE**

   1. ¿Que puertos arrojó el escaneo como abiertos?
   2. ¿porqué el puerto 3376 no fue detectado? Y ¿Como ejecutaría nmap para que verifique el estado de todos los puertos?

   **DEL LADO DEL ADMINISTRADOR**

   3. ¿El ataque se detectó con Snort?
   4. ¿Cómo cataloga Snort dicho ataque?

3. Desde una de las PCs de la LAN, ejecute el siguiente comando y responda:

```
# wget http://10.0.1.10/../../cmd.exe
```

   **DEL LADO DEL ADMINISTRADOR**

   1. ¿El ataque se detectó con Snort?
   2. ¿Cómo cataloga Snort dicho ataque?

**Pruebas de armado de reglas**

Desarrollando reglas con Snort.

En el desarrollo de esta parte experimentaremos con Snort y hping3, para probar el funcionamiento de reglas personalizadas.

**DEL LADO DEL ATACANTE**

Utilizando la herramienta hping3 genere las siguientes situaciones:

1. Segmentos TCP con los siguientes valores:
   - Flag de SYN encendido
   - Flag de URG encendido
   - Puerto destino 80
   - IP destino: IP del servidor

2. Paquete IP con los siguientes valores:
   - TTL = 300

- Puerto destino del paquete TCP: 80
- Flag SYN del segmento TCP encendido.
- IP destino: IP del servidor

3. Paquete IP con los siguientes valores:
   - Tamaño del payload = 200
   - Puerto destino del paquete TCP: 80
   - Flag SYN del segmento TCP encendido.
   - IP destino: IP del servidor

**EN EL ROUTER – FIREWALL**:

1. Cree el archivo /etc/snort/rules/reglas.rules con las reglas necesarias para poder detectar las situaciones generadas por el cliente en el inciso anterior. Para ello deberá escribir las reglas de Snort necesarias para detectar los tipos de paquetes que se generan. Para poder realizar este punto puede utilizar el siguiente manual: ftp://petrinet.dvo.ru/pub/Vyatta/build-iso/pkgs/vyatta-snort/debian/my/snort_rules.html

2. Modifique el archivo /etc/snort/snort.conf incluyendo la siguiente directiva al final del mismo:

```
include $RULE_PATH/reglas.rules
```

3. Inicie el Snort en el router-firewall con el siguiente comando, de modo que reporte en la misma consola las alertas que se disparan:

```
# snort -A console -p -S HOME_NET=10.0.0.0/8 -c /etc/snort/snort.conf -i eth0
```

4. Verifique en la consola de Snort las alertas mientras utiliza la herramienta hping3 en el cliente.

## Parte 3: IDS de host e IDS de filesystem

### Topología para IDS de host e IDS de filesystem

Tanto las pruebas de IDS de Host e IDS de filesystem, se trabajará directamente sobre el LiveCD de Lihuen. Es deseable para las pruebas de IDS de Host, que el sistema esté conectado a la red, de forma tal que se puedan establecer comunicaciones desde otras PCs al mismo.

### IDS de Host

Fail2ban es un IDS de host el cual permite reaccionar ante eventos identificados como adversos. Para ello, analiza logs de diferentes servicios en búsqueda de patrones determinados que indiquen la la presencia de dichos eventos. Una vez detecta la situación anómala, Fail2ban agrega reglas de firewall que eviten las comunicaciones desde el origen de los ataques.

### Pruebas

Se utilizará Fail2ban para filtrar ataques de fuerza bruta sobre el servicio de SSH. Para ello, ante una cantidad configurable de intentos, se procederá al fitrado de la IP desde donde provienen dichos intentos.

1. Corrobore que las las reglas de firewall del Lihuen LiveCD permiten el acceso remoto mediante SSH.
2. Inicie el demonio de fail2ban (/etc/init.d/fail2ban start)
3. Verifique el acceso remoto via SSH al Lihuen LiveCD. Tenga en cuenta que el usuario **root** tiene password **lihuen**.
4. Intente ingresar nuevamente utilizando credenciales inválidas en reiteradas ocasiones hasta que el Lihuen deje de responder a las peticiones de acceso.
5. Analice en el Lihuen las reglas de firewall. ¿Qué puede observar?
6. Distinga los accesos fallidos en el archivo /var/log/auth.log
7. Verifique la configuración de fail2ban para SSH en el archivo /etc/fail2ban/jail.conf. Deberá observar:

```
[ssh]

enabled = true
port    = ssh
filter  = sshd
logpath  = /var/log/auth.log
maxretry = 6
```

8. Reduzca la cantidad de intentos fallidos para que a los 3 intentos sin éxito, el servicio sea bloqueado. Para ello deberá:
    1. Editar el archivo /etc/fail2ban/jail.conf
    2. Borrar el archivo /var/log/auth.log
    3. Reiniciar el servicio de logs con el comando /etc/init.d/rsyslog restart
    4. Reiniciar el servicio de fail2ban.
    5. Pruebe nuevamente el intento de conexión SSH.

**IDS de Filesystem**

Tripwire es una herramienta que permite realizar tests de integridad sobre el filesystem de modo de detectar determinadas situaciones que pueden llegar a ser consideradas anormales. Por ejemplo, tripwire podria detectar:

- Modificaciones en un archivo de configuración
- Reemplazo de un binario o librería del sistema
- Presencia de archivos nuevos en el sistema

**Pruebas**

Se utilizará Tripwire para realizar una comprobación inicial del sistema y luego verificar la integridad de elementos del filesystem actualizando cambios que se saben que se deben al mantenimiento del sistema y no a un evento adverso.

(a) Configuración inicial. Abra una terminal de root y ejecute los siguientes comandos:

- Dado que tripwire ya está instalado en el sistema, pero nunca fue configurado, el siguiente comando disparará el proceso de configuración inicial del producto.
  **# dpkg-reconfigure**

  Durante dicho proceso deberá realizar diversas acciones. Entre ellas:
  - Creará una clave de sitio para la firma de archivos de configuración de tripwire.
  - Creará una clave local para la firma de diversos archivos, como por ejemplo la base de datos de tripwire.
  - Reconstruirá el archivo de configuración de Tripwire.
  - Reconstruirá el archivo de directrices de Tripwire.

- Una vez realizado el paso anterior hay que inicializar la base de datos de tripwire, mediante el comando:
  **# tripwire --init**

- Una vez inicializada la base de datos realice una revisión del sistema de archivos mediante el comando:
  **# tripwire --check**

  Esta revisión es la que se va a realizar periódicamente para la verificación de la integridad del filesystem

- Visualice los reportes que se generaron:
  **# cd /var/lib/tripwire/report/**
  **# ls**
  **lihuen-20111021-140211.twr**

- Inspeccionar un reporte de tripwire:
  **# twprint --print-report --twrfile lihuen-20111021-140211.twr**

  Debido a la gran cantidad de elementos que se visualizan, los cuales se deben al hecho que se está trabajando sobre un LiveCD, se procederá a realizar una inspección particular de algún elemento en lugar de trabajar sobre chequeos integrales del filesystem.

- Inspeccionar atributos almacenados en la base de datos de tripwire sobre un elemento del filesystem. Por ejemplo:
  **# twprint --print-dbfile /etc/hosts**

- Modifique el archivo /etc/hosts simulando que la misma se debió a una actualización del sistema.

- Testear la integridad del elemento modificado:
  **# tripwire --check /etc/hosts**

- Evaluar el reporte generado por el test de integridad anterior:
  **# twprint --print-report --twrfile <reporte_test_archivo_etc_hosts>**

- Actualizar la base de datos de tripwire para que guarde los atribitos nuevos para el archivo, puesto que dichos cambios se debieron a una actualización del sistema.
  **# tripwire --update -r <reporte_test_archivo_etc_hosts>**

- Volver a inspeccionar los atributos almacenados en la base de datos de tripwire:
  **# twprint --print-dbfile /etc/hosts**

**Bibliografía**:


- http://www.faqs.org/docs/iptables/
- http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
- http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/
- http://vace.homelinux.com/wiki/uploads/f/f0/Iptables.gif
- ftp://petrinet.dvo.ru/pub/Vyatta/build-iso/pkgs/vyatta-snort/debian/my/snort_rules.html