

PRÁCTICA 2 - SEGURIDAD INFORMÁTICA

Los objetivos de esta práctica 2 son los siguientes:

I. DISEÑO DE UN DIAGRAMA DE RED Y DE UNA SOLUCIÓN DE SEGURIDAD

1. Usar un software para realizar un diagrama de red donde aparezca el diseño de la arquitectura de la red (equipos, subredes, dispositivos de comunicación, etc.)

II. CONSTRUCCIÓN DE UN FIREWALL MEDIANTE IPTABLES

1. Implementación de una maqueta que simule una red
2. Implementación de un firewall en Linux mediante iptables.

INTRODUCCIÓN

Supongamos que una empresa llamada ISW nos contrata como consultores de seguridad. Nuestro primer cometido es montar la infraestructura de seguridad necesaria por medio de un firewall basado en Linux. Para ello montaremos un equipo con Linux y usaremos reglas con iptables.

Los requisitos de la empresa son:

1. Para la red local (10.0.0.0/8) sólo deberían poder navegar por Internet (tanto http como https). También deben acceder a la web de la intranet de la empresa.
2. En esta DMZ debe haber un servidor Linux que básicamente es un servidor web donde tendremos nuestra página web, además de un servidor SSH para poder administrarlo de forma remota y un servidor DNS que resuelva las direcciones IP locales.

PARTE 1: CREACIÓN DEL DISEÑO DE LA SOLUCIÓN MEDIANTE UN DIAGRAMA DE RED

Se pide:

1. Realizar un diagrama con la arquitectura física de la red. Se deberá usar para ello algún programa de diseño de redes y diagramas como puede ser el Visio (o mejor alguna alternativa de software libre como Calligra, Graphviz o DIA). En cualquier caso el aspecto del diagrama debe ser lo más profesional posible. No valdría usar cuadrados ni rectángulos para ello, sino iconos representativos de los equipos, servidores, routers, etc...

NOTA: Se deberá indicar en el diagrama los equipos, redes, servicios y direcciones IP, que nos será de gran ayuda para después implementarlo.

PARTE 2: CREACIÓN DE FIREWALL CON IPTABLES

Mediante una maqueta en un sólo equipo (con máquinas virtuales) o en varios, realizar la implementación de la situación planteada. Para ello se deberá usar el software de simulación de máquinas virtuales VmWare o Virtual box.

Más concretamente, en el caso de usar un equipo con máquinas virtuales:

En un equipo con VirtualBox instalado (que hará la función de equipo que accede desde Internet) deberé tener además dos instancias o máquinas virtuales con Linux:

1. La primera máquina virtual, llamada SERVDMZ (**es necesario cambiar el hostname: recordad que son dos ficheros, /etc/hostname y /etc/hosts**) será un servidor con los siguientes servicios:

- Servidor web (Apache o Nginx).
- Servidor SSH

Este equipo estará situado en la DMZ.

Este servidor debe ser accesible tanto desde nuestra LAN protegida (lo que sería nuestra Intranet) como desde fuera (nuestro sitio web en Internet). Para ello deberemos redirigir todas las peticiones que vengan de Internet y desde la Intranet, tanto por HTTP como por HTTPS a este servidor.

Además, debe ser accesible desde nuestra Intranet mediante SSH para realizar tareas de administración remota.

NOTA: Esta máquina virtual podría ser la creada en la primera práctica.

2. El equipo host (es decir, el Windows o Mac donde está instalado el VirtualBox) hará las funciones de red local que deberá estar totalmente protegida.

3. La segunda máquina virtual, llamada FW (**es necesario cambiar el hostname**) hará las funciones de firewall. Para ello se pide realizar la tabla con las reglas de filtrado mediante un **script** e **iptables**, con el código debidamente comentado para que sea comprensible.

4. Este firewall debe realizar las siguientes funciones:

1. Permitir el acceso a determinados servicios instalados en un servidor que está situado en la DMZ, tanto desde Internet como desde nuestra LAN
2. Prohibir accesos a servicios no deseados a la DMZ
3. Proteger la LAN
4. Permitir la navegación web a los equipos de la LAN.
5. Permitir el acceso a la web de la Intranet de la empresa de los equipos de la LAN.

En concreto, las cuatro pruebas que hay que conseguir son (ver criterios de evaluación):

PRUEBA 1: Acceso desde la LAN a la DMZ vía SSH: 1.5 puntos

PRUEBA 2: Acceso desde la LAN a la DMZ vía HTTP. Se debería acceder a la página web publicada en el servidor de la DMZ mediante el nombre del dominio creado en la segunda parte de la práctica 1. Es decir, deberíamos poner en nuestro equipo de la LAN www.apellidos_separados_por_guion.com y ver nuestra página web: 1.5 puntos.

- Si accedemos usando la IP y no el nombre la puntuación será de sólo 0.5 puntos en vez de 1.5 puntos.

PRUEBA 3: Acceso desde la LAN a INTERNET vía http y DNS: 3 puntos

PRUEBA 4: Acceso desde INTERNET (puede simularse con un equipo que no esté en la LAN ni en la DMZ) al servidor web de la DMZ vía http: 3 puntos

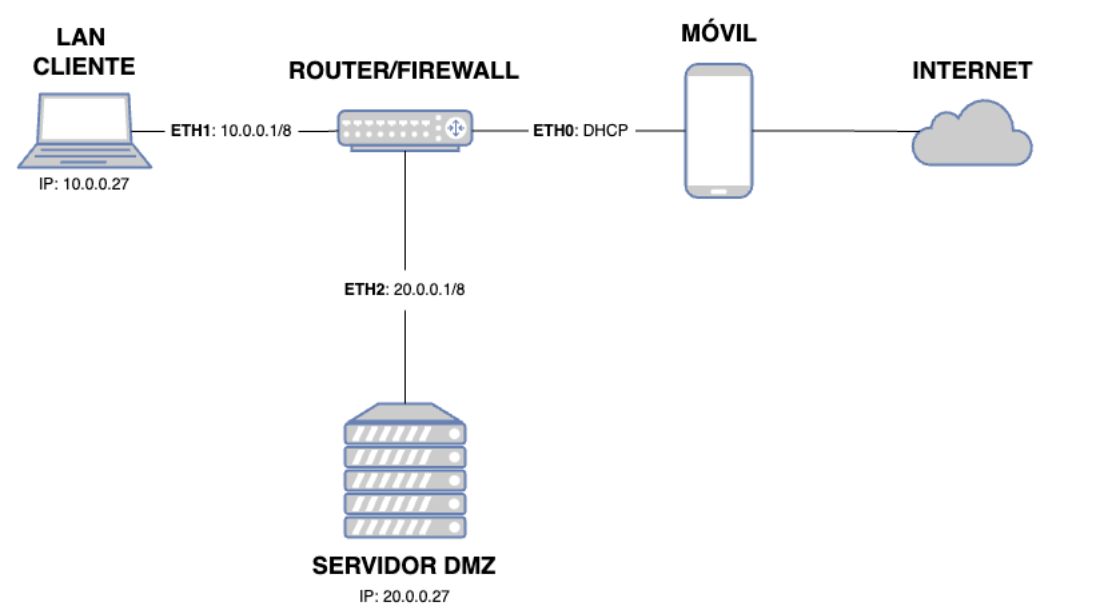
Presentación de la memoria y diseño de la maqueta: 1 punto

NOTA: Recordad que es necesario defender la práctica en el día indicado para aprobarla.

IMPORTANTE: La defensa será únicamente válida si el script que se defiende es exacto al que se ha entregado.

PANTALLAZOS QUE MUESTRAN LAS PRUEBAS CONSEGUIDAS

DISEÑO DE LA RED (1 punto)



PRUEBA 0: Pantallazo con las reglas cargadas en el firewall.

```

diego@firewall: ~
File Actions Edit View Help

(diego@firewall)-[~]
$ sudo iptables -L
[sudo] password for diego:
Sorry, try again.
[sudo] password for diego:
Chain INPUT (policy DROP)
target     prot opt source                destination          state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination          tcp dpt:ssh
ACCEPT     tcp  --  10.0.0.0/8            20.0.0.0/8
ACCEPT     tcp  --  10.0.0.0/8            20.0.0.0/8
ACCEPT     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              20.0.0.27            tcp dpt:http
ACCEPT     udp  --  10.0.0.0/8            20.0.0.0/8            udp dpt:domain
ACCEPT     all  --  anywhere              anywhere              state RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere

```

```

diego@firewall: ~
File Actions Edit View Help

(diego@firewall)-[~]
$ sudo iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination          tcp dpt:http-alt to:20.0.0.27:80
DNAT       tcp  --  anywhere              Server

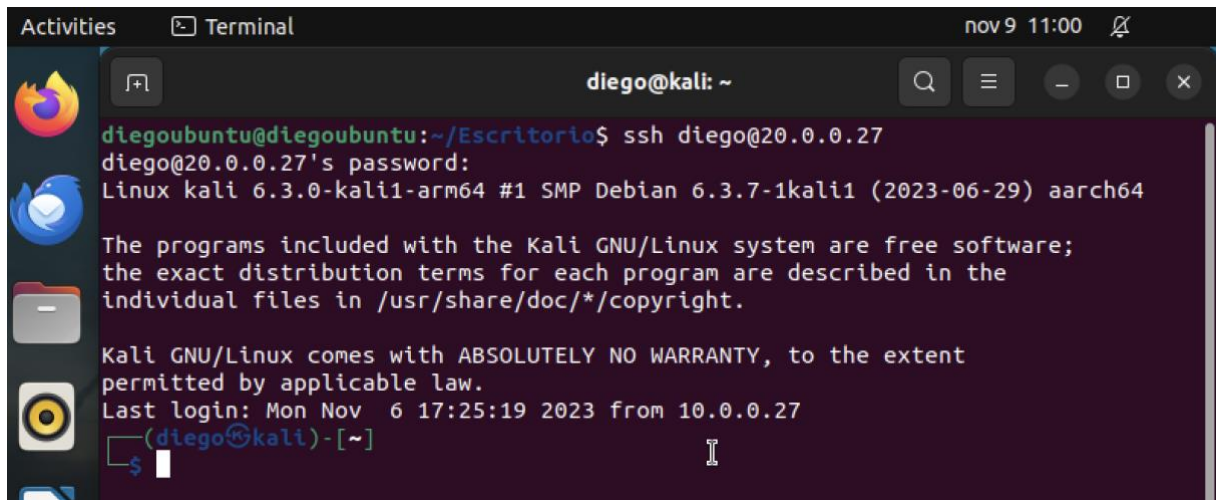
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  10.0.0.0/8            anywhere

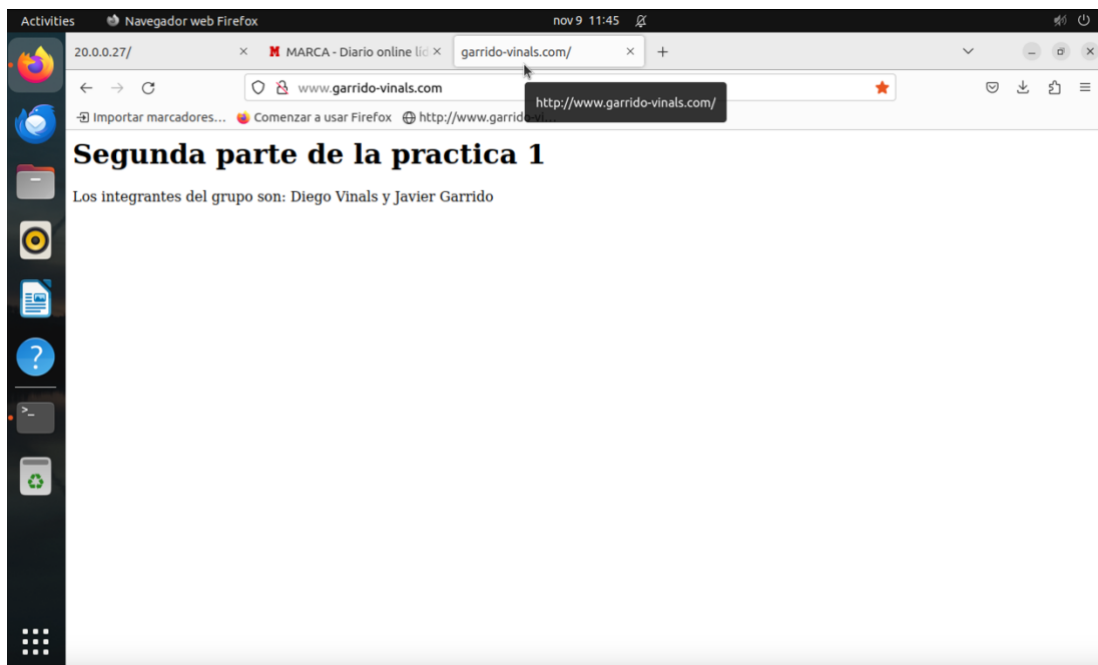
```

PRUEBA 1 (1.5 puntos): Pantallazo donde se vea que desde la LAN se accede al servidor SSH de la DMZ.

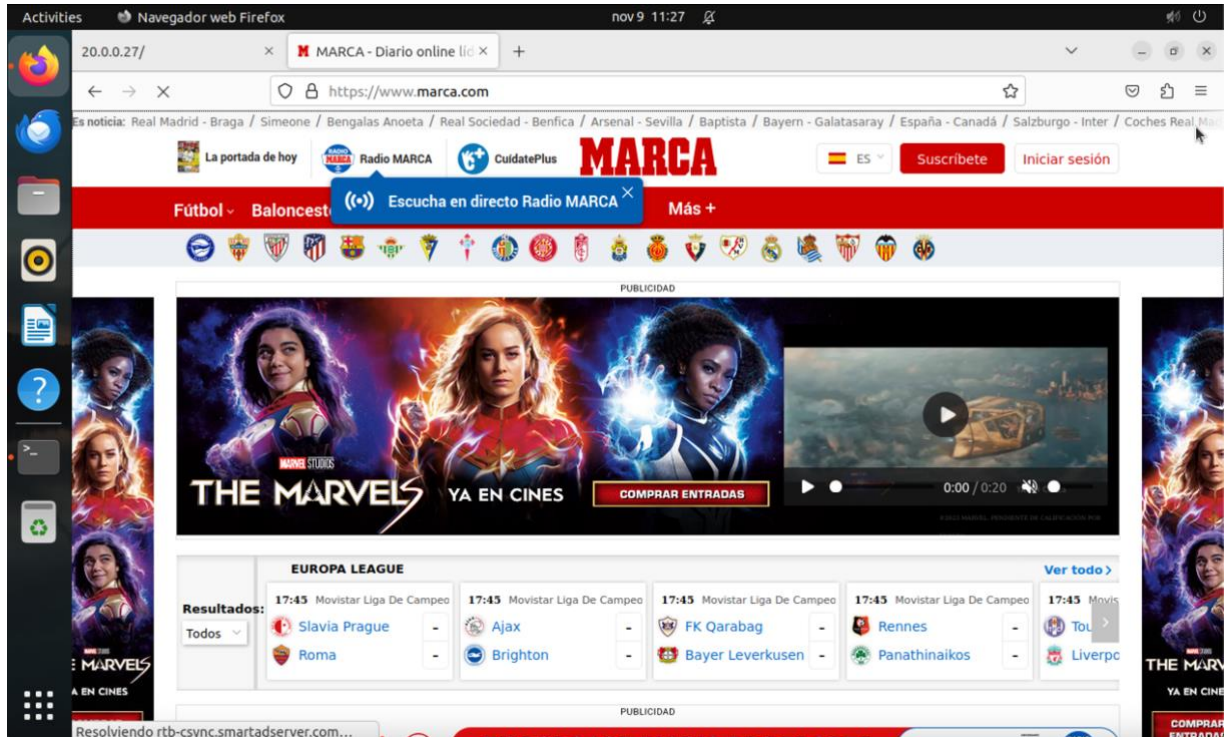


```
diego@kali: ~  
diegoubuntu@diegoubuntu:~/Escritorio$ ssh diego@20.0.0.27  
diego@20.0.0.27's password:  
Linux kali 6.3.0-kali1-arm64 #1 SMP Debian 6.3.7-1kali1 (2023-06-29) aarch64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Mon Nov  6 17:25:19 2023 from 10.0.0.27  
diego@kali)~]  
$
```

PRUEBA 2 (1.5 puntos): Pantallazo donde se vea que desde la LAN se accede a la página web de la DMZ mediante el nombre DNS creado.



PRUEBA 3 (3 puntos): Pantallazo donde se vea que desde la LAN se accede a Internet.



PRUEBA 4 (3 puntos): Pantallazo donde se vea que desde un equipo que no tiene una IP de la LAN ni de la DMZ (puede ser el propio móvil) se accede a la página web de la DMZ por la IP del servidor.



INSTRUCCIONES

1. Entrega: un fichero comprimido que contenga:

- El script usado para implementar las reglas del firewall. **El script deberá contener variables para que sea más general y hacer uso de ellas.**
- Una memoria en PDF con las explicaciones y cualquier captura de pantalla que se considere oportuno para mostrar la resolución de las pruebas. Os recomiendo que lo hagáis resumido a modo de una guía, ya que así os servirá por si os toca hacer algo parecido en el futuro.

2. La extensión de la memoria, en formato pdf, no podrá superar las 20 hojas (siendo la extensión mínima la que se considere oportuna).

3. Esta práctica 2, al igual que la primera, **SÓLO** podrán realizarse en grupos de dos alumnos como máximo o de tres en el caso de que ya se haya hecho así la primera práctica.

4. El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.

5. Cada grupo, además de presentar una memoria, deberá defender la maqueta implementada.

NOTA: La nota de cada componente del grupo puede ser diferente en función del trabajo realizado y de la defensa.

1. La fecha límite de entrega será el domingo 12 de noviembre a las 23 horas.

No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.

IMPORTANTE:

2. No pueden aparecer en el script puertos innecesarios y que no estén en el enunciado. Si aparecen puertos y en la defensa no se sabe explicar su aparición, la práctica no se considerará bien hecha, aunque funcione. Esa aparición de puertos inexplicables es un indicio claro de que la práctica ha sido copiada.
3. Si el script es igual en dos grupos (mismos puertos, mismo orden de reglas, mismas direcciones IP, etc...) la práctica estará suspensa por copia, y se aplicará el reglamento que rige sobre los casos de plagio.
4. Si no se defiende la maqueta con éxito la práctica no estará aprobada, aunque el script sea correcto.