

Prueba de Evaluación Continua 2

Curso 2024-2025. Versión: 1.0

Objetivos

El objetivo de esta práctica es comprender un poco mejor cómo se protegen los equipos utilizando firewalls. Para ello trabajaremos en un entorno dividido en dos redes: una red interna dónde encontraremos equipos cliente y una red DMZ dónde se encuentran los servicios de la organización. Como punto de unión entre ambas redes nos encontraremos un enrutador llamado router.

Comprenderemos las diferencias entre un cortafuegos que protege directamente un nodo frente a un cortafuegos orientado a proteger una red. Para ello configuraremos tanto el cortafuegos IPTables en uno de los nodos de la DMZ como en el nodo router para manejar el tráfico de red entre las dos redes existentes.

Se utiliza el cortafuegos IPTables descrito tanto en el texto base de la asignatura como en diversos recursos adicionales del curso.

Antes de abordar la siguiente práctica revisa con cuidado la documentación relacionada con la puesta en marcha del entorno de prácticas.

El equipo docente ha habilitado un foro específico para cualquier duda relacionada con este caso práctico.

Evaluación

El equipo docente evaluará:

- El/la estudiante ha ejecutado el entorno de prácticas y ha realizado los supuestos detallados en esta guía. La práctica estará disponible desde el **5 de marzo 2025 hasta el 18 de mayo 2025**.
- Tras el análisis el estudiante debe entregar una breve memoria de la actividad donde conste:
 - Su nombre, apellidos, correo electrónico de contacto y DNI en la primera hoja del trabajo.
 - La respuesta a todas las preguntas propuestas a lo largo del desarrollo de la práctica, así como cualquier justificación que deba desarrollar, agrupadas en secciones. Deberá existir una sección para cada apartado de la práctica.
 - Conclusiones del ejercicio, donde puede hacer constar sus reflexiones respecto al supuesto, así como cualquier otro comentario que quieran hacer llegar al equipo docente.
- Esta memoria no debe superar las 8 caras (páginas en un editor de textos).

Este documento debe subirse a la plataforma de aprendizaje del curso antes del **18 de mayo 2025**.

Desarrollo de la práctica

Conocemos el entorno de la práctica

Según podemos ver en el esquema de la práctica contamos con dos redes: DMZ e Interna. Vamos a comenzar a trabajar en la red DMZ.

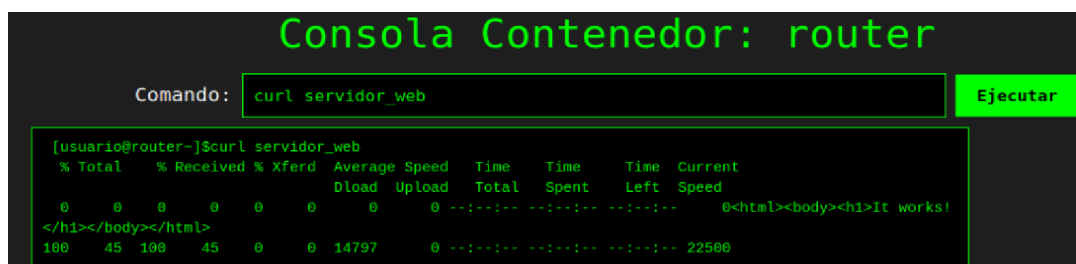
1. Conéctate a todos los nodos de la red para averiguar sus direcciones IP. Usa el comando **ip addr** para averiguarlo y rellena el siguiente cuadro. La excepción es el contenedor Wireshark.

Nodo	Red	Dirección IP	Interfaz de red
servidor_web			
router			
router			
cliente1			
cliente2			

2. Vamos a conectarnos al nodo del **router**. Usaremos la herramienta **nmap** para hacernos una idea de los servicios que están disponibles en las redes así cómo para saber algo más sobre cada uno de los equipos en las redes: que posibles puertos tienen abiertos y qué sistema operativo ejecutan. Con dicha información completa la siguiente tabla:

Nodo	Red	Dirección IP	Puertos	Sistema Operativo
servidor_web				
router				
router				
cliente1				
cliente2				

3. Vamos a comprobar la conectividad de la red DMZ, dónde vamos a comenzar a trabajar. Conéctate al contenedor router y desde su consola prueba si puedes acceder al servidor web con la orden **curl servidor_web**.



```

Consola Contenedor: router

Comando: curl servidor_web [Ejecutar]

[usuario@router-]$ curl servidor_web
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0<html><body><h1>It works!
</h1></body></html>
100 45 100 45 0 0 14797 0 --:--:-- --:--:-- --:--:-- 22500

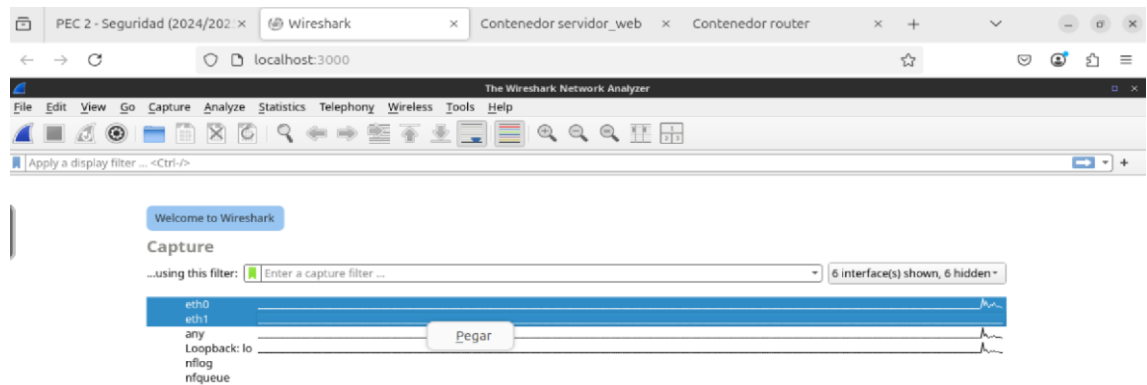
```


También puedes comprobar que la petición ha llegado al servidor web consultando sus logs.

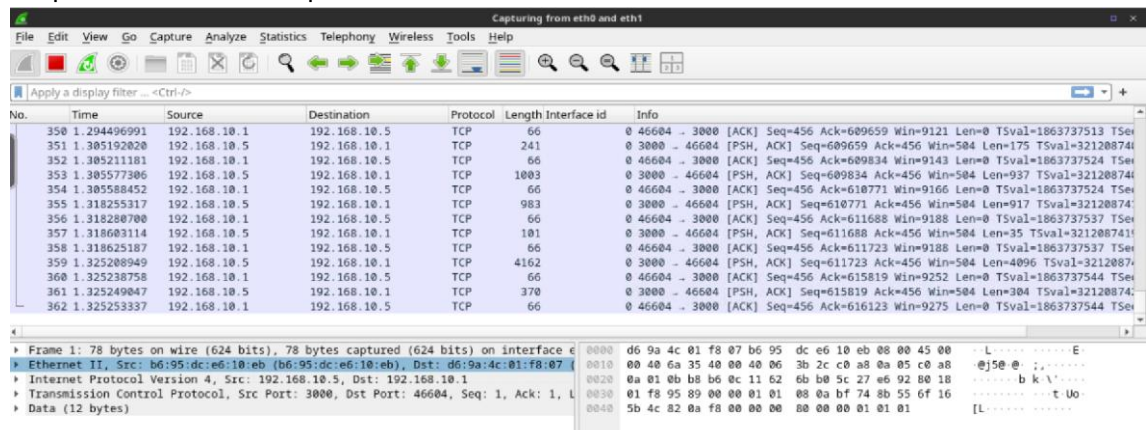



4. En la práctica contamos con un contenedor llamado Wireshark. Este contenedor contiene una instancia del sniffer Wireshark conectado a las dos redes disponibles en el entorno de prácticas. Mediante este contenedor podremos ver el tráfico de red que circula en ambas redes.

Al abrir su pestaña se nos muestran las interfaces dónde podemos capturar el tráfico. Es importante seleccionar tanto eth0 cómo eth1 para poder ver el tráfico de ambas redes.



Una vez seleccionadas ambas redes podemos hacer clic en el icono de la aleta azul  para comenzar la captura de tráfico.



Contamos con una columna llamada Interface id para poder identificar en qué interfaz de red se produce la comunicación. En cualquier momento podemos detener la captura de información con el icono cuadrado rojo  y analizar el tráfico capturado.

Cortafuegos a nivel equipo

Cuando trabajamos un cortafuegos desde la perspectiva de la protección de un equipo individual debemos configurar los filtros orientados a controlar tanto el tráfico entrante al equipo (usando la cadena *INPUT*) y del tráfico saliente del equipo (con la cadena *OUTPUT*).

1. Instalamos IPTables en el nodo `servidor_web`. Para ello vamos a usar el comando **`apk add iptables`**.
2. Tras instalarlo podemos comprobar el estado de IPTables usando el comando **`iptables -L`**.
3. Una vez instalado, vamos a establecer la política por defecto del cortafuegos. Usaremos como política por defecto el bloquear tanto el tráfico de entrada como de salida. ¿Qué reglas debemos usar?. Comprueba las reglas usando la regla **`iptables -L`** para ver el resultado de la configuración.
4. Usa **`nmap`** para comprobar el estado de los puertos del servidor web. ¿Aparecen los puertos? ¿Cuál es su estado?
5. Usar la orden **`curl -m 20 http://servidor_web`** para ver si podemos acceder al servidor web. La opción `-m 20` reduce el tiempo de espera a 20 segundos si el servidor no contesta. Verifica que la petición de la página web no ha llegado al servidor web mirando en los logs de este contenedor.
6. Conforme vemos *no podemos acceder al servidor web*. De esta manera no cumple con su función. Crea una regla que permita que cualquier equipo consulte sólo al servidor web en el puerto 80. El servidor web debe contestar a las conexiones establecidas para poder servir las páginas web por lo tanto necesitaremos una segunda regla. ¿Qué reglas debemos crear?. Comprueba las reglas usando la regla **`iptables -L`** para ver el resultado de la configuración. Añade una captura de pantalla (imagen) de la salida de este comando a tu memoria de prácticas.
7. Comprueba que se ha restablecido correctamente el acceso al servidor web desde el nodo router tanto con la orden `curl` como con `nmap`. Ten paciencia con los comandos, pueden tardar un poco en ejecutarse.
8. El servicio SSH es un servicio de administración de la máquina. Por tanto, no debe estar disponible para ningún equipo. ¿Sería necesario agregar reglas al cortafuegos IPTables para evitar el acceso a dicho puerto por terceros? Justifica tu respuesta y en caso afirmativo indica las reglas que serían necesarias implementar.

Cortafuegos a nivel de red

En nuestro ejemplo contamos con dos redes: una red DMZ compuesta por nuestro servidor web y una red interna. Ambas redes se interconectan mediante el contenedor router y el contenedor Wireshark, que nos permite ver el tráfico de red.

Ahora debemos interconectar ambas redes con ayuda de IPTables para que los contenedores de los clientes puedan acceder al sitio web de nuestra DMZ.

1. Abre la consola del contenedor *cliente1*. Usa el comando **`curl -m 15 servidor_web`**. Seguramente nos diga que no puede resolver el nombre `servidor_web`. Prueba sustituyendo `servidor_web` por la dirección IP del servidor web.
2. Vamos a probar con otra herramienta. Usa el comando **`ping -w 3 <dirección_ip_servidor_web>`**.
3. Abre la consola del contenedor *cliente2*. Usa el comando **`ping -w 3 <dirección_ip_cliente1>`**. De esta manera descartamos que la red interna no tenga conectividad. También prueba con la dirección IP del router en la red interna. Y entre los contenedores clientes.
4. Si todos los paquetes del comando `ping` anterior han sido recibidos podemos concluir que hay conectividad dentro de la red interna. Pero los contenedores de

esta red no pueden acceder a la red DMZ. Debemos permitirlo enrutando su tráfico de red desde la red interna hacia la red DMZ.

5. Vamos a la consola del router y vamos a ver su configuración de IPTables con la orden **iptables -L**. Su política por defecto debe ser de aceptar todo tipo de tráfico. Así que lo primero es crear una política por defecto más restrictiva bloqueando todo tipo de tráfico de red. ¿Qué reglas debemos usar?
6. Para que nuestro contenedor router se comporte como tal debemos permitir el direccionamiento de paquetes para ello debemos ejecutar el siguiente comando:
echo 1 > /proc/sys/net/ipv4/ip_forward
7. Además, los contenedores cliente1 y cliente2 deben usar a nuestro router como su puerta de enlace (Gateway). Para ello en ambos contenedores debemos modificar su enrutamiento creando una nueva ruta por defecto hacia el contenedor router. Esto lo conseguimos con los siguientes comandos, donde debemos sustituir **dirección_IP_router** por la dirección IP del contenedor router:
ip route del
ip route add default via <dirección_IP_router>
8. Lo siguiente que queremos hacer es que el tráfico que nos llega de la interfaz correspondiente a la red interna sea redirigidos a la interfaz de red conectada a la red DMZ. Para ello hemos de crear las correspondientes reglas utilizando la cadena de reenvío de tráfico (FORWARD). ¿Qué reglas usaríamos?. En este punto se valorará la solución más restrictiva desde el punto de vista de la seguridad. Realiza una captura de pantalla mostrando la configuración de IPTables en el contenedor router con la orden **iptables -L** en este punto.
9. Además de usar las reglas de reenvío de tráfico es necesario utilizar otro mecanismo del firewall IPTables: enmascaramiento. Los paquetes que atraviesan el router desde la red interna y llegan a la red DMZ no tienen el mismo rango de direcciones IP. Por ello pueden ser descartados. Por ello debemos utilizar tanto la tabla de enmascaramiento (nat) como su función de POSTROUTING. ¿Qué reglas necesitamos en este caso?
10. Probamos si hemos tenido éxito en nuestra configuración. Utiliza el comando **curl** tanto desde el contenedor cliente1 como el contenedor cliente2 y comprueba si sus peticiones llegan al servidor web. También revisa los logs del contenedor servidor web para comprobarlo.
11. Usa el comando **ping -w 3 <dirección_IP_servidor_web>** desde los contenedores cliente1 y cliente2. ¿Qué ocurre? ¿Por qué?
12. Supongamos que el contenedor **cliente2** es el administrador del servidor web, y por tanto debe poder acceder al servicio SSH instalado en el servidor. ¿Qué reglas deberíamos utilizar para darle permiso de acceso SOLO al contenedor **cliente2**? ¿Dónde aplicaríamos dichas reglas: en el cortafuegos del contenedor router, en el contenedor del servidor web? Comprueba que tu respuesta. En el contenedor cliente2 está instalado el cliente dropbear **dbclient** y el comando de conexión ssh será **dbclient -y <dirección_IP_servidor_web>**.

Por cuestiones de compatibilidad entre el contenedor del servidor web y el contenedor cliente2 cuando inicies la sesión ssh se interrumpirá la sesión. De manera que la manera de saber si se puede o no establecer sesión es por el error timeout.

Anexos

Uso de nmap

En el nodo router ya nos encontramos instalada la herramienta nmap. Sus principales usos son:

- **Localizar sistemas activos.** El primer paso será localizar aquellos equipos que están encendidos y conectados a la red. Podemos averiguar la red a la que nos encontramos conectados utilizando los comandos `ip addr` (Linux) o `ipconfig` (Windows). Una vez sabemos la red objetivo el comando `nmap -sP <dirección IP red>` nos dará información al respecto.
- **Descubrir puertos abiertos.** Tras saber que equipos están activos en la red deseamos saber que posibles puntos de acceso podemos tener a esos equipos. Por ello centramos nuestra atención en los puertos abiertos existentes. Lo primero como ya sabemos que equipos existen en la red podemos ir uno a uno escaneando, en lugar de escanear toda la red. Esto nos permitirá trabajar más rápido. Además, no queremos escanear nuestra propia máquina, sólo aquellos ordenadores descubiertos. Utilizaremos en ese caso la opción `nmap -sS <lista direcciones ip>`. Si además deseamos explorar los puertos UDP debemos usar la opción `-sU`. De acuerdo con la documentación de nmap, los principales estados de los puertos son:
 - *open (abierto)*, indica que en ese puerto hay una aplicación aceptando conexiones con TCP/UDP.
 - *closed (cerrado)*, significa que es un puerto accesible (recibe y responde a los paquetes Nmap) pero que no hay una aplicación ejecutándose tras ese puerto.
 - *filtered (filtrado)*, es un puerto que Nmap no puede saber su estado porque existe algún mecanismo de filtrado (generalmente un firewall) que evita que las peticiones alcancen el puerto.
 - *unfiltered (sin filtrar)*, indica que el puerto es accesible, pero Nmap no es capaz de determinar si está abierto o cerrado. Sólo aparece cuando usamos un escáner basado en peticiones ACK. Otro tipo de escáner podría resolver este estado.
- **Enumerar.** En el proceso de lograr más información sobre los posibles objetivos incluyendo sistema operativo, usuarios, nombre de equipos y cualquier información que podamos localizar. Una primera aproximación es utilizar el comando `nmap -O <dirección IP>` para localizar el sistema operativo de la máquina. Este comando suele llevar tiempo y genera grandes cantidades de tráfico. Además, produce una salida extensa.