Seguridad en TI (TICS413)
Laboratorio n°3

Matías García
matiasgarcia@alumnos.uai.cl

2 de septiembre 2025

1. Servicios Comunes en Linux y sus Puertos de Red Predeterminados

En los sistemas operativos basados en Linux, un servicio es una aplicación o proceso que se ejecuta en segundo plano (también llamados daemons) y que proporciona funcionalidades específicas al sistema o a los usuarios, como la navegación web, el acceso remoto, la gestión de correos electrónicos, entre otros. Cada servicio que requiere comunicación a través de la red, donde se utiliza un número de puerto, que actúa como un punto lógico de conexión en una dirección IP. Una dirección IP (Internet Protocol) es un identificador único que se asigna a un dispositivo en una red. Así, cuando un cliente desea conectarse a un servicio en un servidor, necesita conocer su dirección IP y el número de puerto en el que dicho servicio está escuchando.

Cada servicio que requiere comunicación a través de la red utiliza un número de puerto, que actúa como punto lógico de conexión en una dirección IP. El uso adecuado de puertos y servicios es fundamental tanto para el funcionamiento del sistema como para su seguridad.

Puertos y servicios comunes

Servicio	**Descripción**	**Puerto(s)**
SSH	Acceso remoto seguro	22/TCP
HTTP	Navegación web	80/TCP
HTTPS	Navegación web cifrada	443/TCP
Apache	Servidor web muy utilizado	80, 8080, 443/TCP
FTP	Transferencia de archivos	20, 21/TCP
SMTP	Envío de correos	25, 465, 587/TCP
IMAP	Acceso a correos	143, 993/TCP
MySQL/MariaDB	Bases de datos relacionales	3306/TCP
PostgreSQL	Bases de datos relacionales	5432/TCP

2. Network Mapper (Nmap)

Es una herramienta de código abierto utilizada para exploración de redes y auditorías de seguridad.Su propósito principal es escanear dispositivos conectados a una red con el fin de identificar:

- Hosts activos (dispositivos encendidos y accesibles).
- Puertos abiertos en cada host.
- Servicios en ejecución y sus versiones.
- Sistema operativo de los dispositivos.

Es ampliamente utilizada por administradores de red y profesionales de ciberseguridad para detectar vulnerabilidades, descubrir dispositivos ocultos y mapear la infraestructura de una red.

Ejemplo de uso

Un ejemplo común para escanear un host y ver qué puertos tiene abiertos es:

```
nmap 192.168.1.10
```

Este comando realiza un escaneo básico a la dirección IP 192.168.1.10 e identifica los puertos abiertos y servicios asociados

```
Nmap scan report for 192.168.1.10
Host is up (0.17s latency).
Not shown: 97 closed tcp ports (reset)
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https
MAC Address: DE:AD:BE:EF:12:34 (Fictitious Corp)
```

También existe esta variante para descubrir los host en una red.

```
nmap -sS -T4 -F <interfaz-ip>/24
```

Reemplazar <interfaz-ip>con la interfaz de la ip correcta y asegurarse de estar en la misma red.

3. Secure Shell (SSH)

Es un protocolo de red que permite el acceso remoto seguro a otro equipo a trav´es de una red. Utiliza cifrado para proteger la confidencialidad e integridad de los datos transmitidos.

- Acceder a servidores de forma remota.
- Ejecutar comandos en sistemas remotos.
- Transferir archivos de manera segura (mediante scp o sftp).
- Crear túneles cifrados para redirigir tráfico de red.

Puerto por defecto: 22.

Ejemplo de uso

Para conectarse de forma remota a un servidor dentro de una misma red utilizando SSH, se puede usar el siguiente comando:

```
ssh <usuario>@<IP>
```

```
scp usuario@IP:/ruta/remota/archivo.txt /ruta/local/
```

Reemplazar <usuario>por el usuario del servidor e <IP>por su IP correspondiente.

Este comando establece una conexión segura con el host usando el nombre de usuario más su IP especificado. Si es la primera vez que se conecta, se pedirá aceptar la clave del servidor y luego se solicitará la contraseña del usuario.

4. File Transfer Protocol (FTP)

Es un protocolo de red utilizado para la transferencia de archivos entre un cliente y un servidor a través de una red TCP/IP, como Internet. FTP permite que los usuarios suban o descarguen archivos desde y hacia un servidor remoto.

Aunque FTP no cifra las transmisiones por defecto, existen variantes como FTPS (FTP Secure) y SFTP (SSH File Transfer Protocol) que proporcionan cifrado para garantizar la seguridad de los datos transmitidos.

Puerto por defecto: 21.

Comandos principales

- `get` → Descargar archivos
- `put` → Subir archivos al servidor
- `ls` → Listar archivos en el servidor
- `cd` → Cambiar directorio

Ejemplo de uso

Para conectarse a un servidor FTP, se puede utilizar el siguiente comando:

```
ftp 192.168.1.10
```

Este comando abre una sesión FTP con el servidor en la dirección IP 192.168.1.10. A continuación, se solicitará el nombre de usuario y la contraseña.

```
Connected to 192.168.1.10 (192.168.1.10).
220 (vsFTPd 3.0.5)
Name (192.168.1.10:usuario): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Una vez conectado, puedes usar comandos como:
→ ls para listar los archivos en el servidor.
→ get archivo.txt para descargar un archivo llamado archivo.txt.

```
ftp> ls
227 Entering Passive Mode (192,168,1,10,199,74).
150 Here comes the directory listing.
-rwxr-xr-x 1 65534 65534 102 Apr 23 18:18 backup_creds.txt
```

Para cerrar la sesión FTP, utiliza el comando:

```
bye
```

5. Práctico

El objetivo de este práctico es aplicar nociones de redes y servicios en Linux para identificar y explotar un servicio FTP mal configurado en un entorno de red aislado. Se deberá obtener credenciales mediante FTP anónimo y usarlas para acceder al servidor vía SSH y recuperar un archivo.

1. Detectar con `nmap` el servidor con servicio FTP.
2. Conectarse mediante FTP anónimo.
3. Revisar el archivo con credenciales descargado.
4. Acceder vía SSH al servidor.
5. Encontrar el archivo dentro del servidor.
6. diviertete en el proceso c: