

Chapter 1

Network security

1.1 Protocols and servers

1.1.1 Telnet

El protocolo Telnet es un protocolo de la capa de aplicación usado para conectarse a una terminal virtual u otra computadora. Usando Telnet, un usuario puede conectarse a otra computadora y acceder a su terminal (console) para correr programas, empezar procesos y realizar tareas del administrador de forma remota.

El protocolo Telnet es relativamente sencillo. Cuando un usuario se conecta, se le pregunta por un nombre de usuario y una contraseña. Una vez que el usuario fue autorizado, tendrá acceso a una terminal remota del sistema. Desafortunadamente, toda esta comunicación entre el cliente Telnet y el servidor Telnet no está encriptada, lo que lo hace un objetivo fácil para los hackers.

Un servidor Telnet usa el protocolo Telnet para escuchar conexiones entrantes en el puerto 23. Consideremos un ejemplo:

Un usuario se está conectando a *telnetd*, un servidor Telnet. Los pasos son como siguen:

1. Primero, se le pide un nombre de usuario.
2. Después, se le pide la contraseña (no se muestra).
3. Una vez que inicia sesión es bienvenido con un mensaje.

4. El servidor le da una terminal. El "\$" indica que no es una terminal root.

Aunque telnet nos dio acceso a una terminal en poco tiempo, no es un protocolo confiable para administración remota, pues todos los datos son mandados en texto claro.

Telnet no es considerado una opción segura, especialmente porque cualquiera que esté capturando el tráfico de internet sería capaz de descubrir el nombre de usuario y la contraseña, lo que le daría acceso al sistema remoto. La alternativa segura es SSH.

1.1.2 Hypertext Transfer Protocol (HTTP)

El Hypertext Transfer Protocol (HTTP) es el protocolo usado para transferir páginas web. Tu navegador web se conecta al servidor web y usa HTTP para pedir páginas HTML e imágenes, mandar forms y subir varios archivos. Cada vez que buscamos en la World Wide Web (WWW) usamos el protocolo HTTP.

HTTP manda y recibe los datos en texto claro, entonces podemos usar una herramienta simple como Telenet (o Netcat) para comunicarnos con un servidor web y que actúe como un navegador web. La diferencia fundamental es que necesitamos introducir los comandos relacionados a HTTP en lugar de que el navegador lo haga por nosotros.

En el siguiente ejemplo, veremos como podemos solicitar una página de un servidor, más aún, descubriremos la versión del servidor web. Para conseguir esto, usaremos el cliente Telnet. Lo usamos porque Telnet es un protocolo simple, además, usa texto claro para la comunicación. Usaremos Telnet en lugar de un buscador web para pedir un archivo del servidor web. Los pasos son los siguientes:

1. Primero, nos conectamos al puerto 80 usando *telnet MACHINEIP 80*
2. Después, debemos escribir *GET /index.html HTTP/1.1* para obtener la página index.html o *GET / HTTP/1.1* para obtener la página por defecto.
3. Finalmente, debemos proveer un valor para el host, como *host: telnet* y picar la tecla enter dos veces.

Necesitamos un servidor HTTP (webserver) y un cliente HTTP (web browser) para usar el protocolo HTTP. El servidor web va a "sevir" un conjunto específico de archivos al web browser que pide los recursos.

Tres elecciones populares para servidores HTTP son:

- Apache
- Internet Information Services (IIS)
- nginx

Apache y nginx son gratis y de código abierto. IIS es de código cerrado y requiere una licencia.

1.1.3 File Transfer Protocol (FTP)