



**Tp4 Programación de Servidores**

**Nombre y apellido del alumno: Matias Hernan Braga**

**Turno: noche**

**Año lectivo: 2021**

**1- De todos los ataques vistos en las ultimas 2 clases y de cómo afectan y explotan ciertas vulnerabilidades, proponga solo 2 acciones a tomar para mitigar las posibilidades de que se hagan efectivos la mayoría de ellos, ser lo más detallado posible dentro de sus conocimientos.**

Hay muchas acciones que se puede y en lo posible se deben tomar para evitar ser victimas de ataques. Dentro de las mas importantes yo pondría la “Autenticación”, es decir verificar que realmente se tiene la comunicación con la persona que se cree. Un ejemplo clásico es al recibir un mail, si se ve algo extraño comprobar la procedencia del mismo.

Otra acción que se debe tomar es monitorear conexiones sospechosas a bases de datos. Ejemplo: muchas consultas hacia un mismo sector o desde una misma ip

**2- Explique Telnet, hay que seguir usándolo?**

Telnet es una herramienta que ha sido utilizada durante décadas por los administradores de sistema informáticos en el ámbito de las redes. Las conexiones remotas no son algo precisamente nuevo, ya desde las primeras redes y con sistemas sin escritorio se utilizaban herramientas como Telnet para conectarnos a servidores y equipos conectados a una red, tanto de forma remota como interna.

A pesar de que actualmente ha sido sustituido por herramientas más seguras, como SSH, Telnet aún sigue teniendo cierta utilidad en entornos seguros por administradores de sistemas.

El nombre de Telnet proviene del acrónimo Telecomunication Network, y básicamente un protocolo de red TCP/IP que es utilizado desde 1960 para establecer conexiones remotas con otros ordenadores, servidores, y dispositivos con un sistema compatible en el acceso mediante este sistema de comunicación. De forma predeterminada se utiliza el puerto de conexión 23.

Además del propio protocolo, también recibe este nombre el programa que lo utiliza para establecer la propia conexión. Para acceder a la otra máquina de forma remota, debemos utilizar un terminal, por ejemplo, Símbolo del sistema de Windows, o el Terminal de Linux. De esta forma podremos interactuar en la máquina remota navegando por sus archivos, ejecutando otros comandos internos, si tenemos permiso, y monitorizar el estado de la propia máquina sin la necesidad de ir físicamente al lugar en donde se encuentra.

Además de ser utilizado en sistemas MSDOS y Windows, también es compatible con sistemas Basados en UNIX, como Mac y Linux, y FreeBSD. Con este protocolo, también seremos capaces de comprobar la conectividad de otras máquinas y comprobar si tienen determinados puertos abiertos al exterior.

Para que podamos establecer una conexión entre dos ordenadores con Telnet, primero necesitaremos tener un cliente en el terminar que estamos nosotros, y un servidor en la máquina a la que pretendemos acceder. Si además lo hacemos fuera de una intranet, o red LAN, necesitaremos tener el puerto 23 abierto en la máquina de destino.

Lo siguiente que vamos a necesitar, es abrir una sesión en la máquina de destino en la que exista una o varias cuentas de usuarios que tengan permitido el acceso. En definitiva, para acceder con un cliente a una máquina destino esta deberá contener una cuenta de usuario habilitada para el acceso, y nosotros necesitaremos conocer tanto el nombre como la contraseña de usuario para establecer la comunicación.

**3- Como funciona a grandes rasgos un servidor de correo**

El emisor del email utiliza un programa de correo electrónico para redactar el mensaje y, al dar clic en “Enviar”

contacta con el servidor SMTP (1). Una vez que éste recibe la orden de entregar un correo, consulta con el servidor DNS (2) para conocer el nombre de dominio (@ del receptor) del servidor donde tiene que entregarlo (3). Luego, el servidor SMTP contactará al servidor del receptor, que utilizará los protocolos POP o IMAP (4) para entregar el correo y, finalmente, el receptor utiliza también un programa de correo electrónico para acceder al email (5).

