**SEGUNDA PARTE**

**2a. Utilizando un cliente telnet, realiza conexiones al puerto por defecto y a otros puertos y analizar las tramas intercambiadas.**

**2b. Activar el fisgón de claves dsniff en mallet y usarlo para atrapar claves de conexiones entre alice y bob.**

Para ello activo en mallet el dsniff con dos argumentos -m (detección automática de protocolos) y -i (indicar la red que queremos monitorizar):

Texto

Descripción generada automáticamente

Ahora abrimos otra terminal en mallet, donde iniciamos una conexión telnet con bob y alice, primero lo haremos para alice, donde introduciremos las credenciales de bob para loguearse acceder al modo super usuario etc, y después cerramos la conexión telnet con exit.

Texto

Descripción generada automáticamente

alice

Finalizamos la conexión telnet con exit, y en la terminal donde realizamos el dsniff hemos capturado las contraseñas, así como los comandos que han sido introducidos en la conexión telnet, debido a que no es seguro, envía todas las comunicaciones (incluido contraseñas) en texto sin formato.

Texto

Descripción generada automáticamente

Ahora realizamos para bob, primero en una terminal ejecutamos el dsniff y en la otra la conexión telnet a bob:

Texto

Descripción generada automáticamente

bob

Una vez finalizada la conexión telnet, con exit, vemos que hemos obtenido en la terminal donde hemos ejecutado el dsniff.

Texto

Descripción generada automáticamente

**2c. Discutir las debilidades de telnet en términos de seguridad**

La principal vulnerabilidad que tiene este protocolo (telnet) es que no usa ningún mecanismo de encriptación, por tanto, en cualquier sesión telnet, toda la información, así como las credenciales, usuarios etc., se envían en texto plano y pueden ser fácilmente capturadas o interceptadas por un usuario no deseado y esto puede causar numerosos problemas de seguridad.

Aunque esto permitiría pensar que hoy en día está en desuso o que es inútil, el protocolo telnet permite una comunicación bidireccional y se utiliza muchas veces para administrar sistemas de forma remota. A pesar de esto existe SSH protocolo que permite el acceso remoto a un servidor al igual que telnet, pero es un canal seguro, puesto que toda la información está cifrada.

**3. Acceso remoto usando ssh.**

Ahora de la misma forma que en el apartado 2b) pero en vez de utilizando telnet, usaremos ssh de esta forma veremos que la información circula por un canal seguro puesto que va encriptada (conexión segura), puesto que no vamos a ser capaces de obtener la información únicamente voy a realizar la prueba con alice, ya que con bob seria exactamente igual.

Como antes iniciamos un dsniff de la red eth4:

Texto

Descripción generada automáticamente