Prácticas de la Primera Entrega del Curso de Linux

28 de febrero de 2005

En este fichero se enuncian 3 de las 4 prácticas correspondientes a esta entrega. Las tres prácticas se tienen que subir en ficheros independientes para cada una de las tareas planteadas en Moodle (la plataforma con la que estamos trabajando).

Las características especiales que presenta este curso (hay que adecuar la realización de las prácticas al ritmo de aprendizaje/dificultad en la configuración del ordenador con que se está trabajando) desaconsejan establecer una fecha tope distinta de la establecida en la planificación docente para su realización.

Importante: Esta entrega tiene dos prácticas de Tipo I y dos de Tipo II:

TIPO I

E1-I-1 Realizar correctamente todas las preguntas del cuestionario que para esta entrega se ha habilitado en Moodle.

E1-I-2

- El comando `nmap` es una herramienta de exploración de redes y escáner de seguridad. Mediante ella, podemos ver los puertos que se encuentran abiertos en un sistema, observándolos desde el exterior, es decir, intentando la conexión y comprobando la respuesta. Solamente deberemos ejecutarlo sobre nuestra máquina. Si estamos en una red de una empresa u organismo, puede que la política de seguridad no permita que ejecutemos este comando sobre la red, considerándola un ataque a la seguridad.
- Otro comando, `netstat`, nos permite ver los puertos que están esperando conexiones en nuestra máquina y las conexiones que están establecidas, pero desde dentro de nuestra máquina.

La práctica consiste en lo siguiente:

1. Realizar una conexión ssh a nuestro servidor (`$ssh localhost`). Si no está instalado el paquete de servidor `ssh`, deberemos instalarlo[1].

   Fedora: debería estar instalado y en ejecución. En el caso de que no sea así lo instalaremos con:

   ```
   # apt-get install openssh-server
   ```

   Y para reactivarlo

[1] En entregas posteriores estudiaremos mejor este servicio de red.

```
#/etc/init.d/sshd restart
```

Guadalinex: se instala por defecto, sólo hemos de ejecutar

```
#dpkg-reconfigure ssh
```

y marcar las opción deshabilitada de: **Ejecutar el servidor sshd**.

2. Ejecutar los comandos `nmap -sTU localhost` y `netstat -atu`.
3. Enviar el resultado de su ejecución, comentando el resultado de ambos y sus coincidencias y/o diferencias. Comentar todas las conexiones que aparecen como resultado del comando `netstat`.

El resultado de la ejecución de los comandos y las explicaciones deben estar en un fichero de nombre `E1-I-2.txt`.

Tipo II

E1-II-1 Dado el fichero que podéis bajar del servidor, `captura.dump`, correspondiente a una captura de tráfico en una red, identificar lo siguiente.

1. Una sesión telnet, indicando usuario que ha entrado en el sistema, password y comandos ejecutados.
2. Una sesión de recogida de correo electrónico (POP), viendo el contenido del correo electrónico recuperado.
3. Una sesión ssh, indicando si es posible identificar el usuario que ha entrado en el sistema, direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos de origen y destino.

El resultado de la práctica debéis mandarlo en un fichero de nombre `E1-II-1.txt`

E1-II-2 Instalar un firewall personal en vuestra máquina. La política a implementar será la siguiente:

- Permitir todos los accesos desde las máquinas de nuestra red local.
- Para el resto, solamente permitir conexiones a los servicios http, https y smtp.

El resultado de la implantación de las políticas y las explicaciones debe mandarse en formato OpenOffice un fichero de nombre `E1-II-2.sxw`.