# PRÁCTICA 1.5. POLICÍAS Y LADRONES (parte II)

*NORMAS DE ENTREGA.*
La práctica se entregará dentro del plazo indicado en la plataforma "aules". En la práctica se debe indicar el nombre, apellidos y curso del alumno. La entrega de la práctica será en formato .pdf, NO SE ADMITIRÁ otro formato. Si la práctica se entrega fuera de plazo o no cumple las normas que aquí se indican se considerará NO APTA.

La siguiente práctica consiste en jugar a ladrones y policías. Hay 2 tipos de alumnos, unos que son policías y otros que son ladrones. Y cada uno deberá realizar un fin en concreto, **sin saber que es el otro compañero.**

## El ladrón

Este alumno deberá de entrar al ordenador del compañero que se le haya asignado. Y dejar un fichero en una cierta carpeta en su ordenador, como muestra que ha entrado al sistema del compañero. Una vez haya conseguido hacer esto, el policía deberá investigar quien ha sido, en caso de encontrar al responsable, este será descubierto y encarcelado (menos nota).

## El policía

El policía deberá supervisar que nadie entra al sistema, en caso de detectar un intruso deberá investigar quién es y descubrirlo. En caso de que entren en su ordenador y no sepa quien ha sido, este habrá perdido su apuesta con el ladrón (menos nota).

Pistas que usar:

- El SSH usa el puerto 22, ¿Se puede cambiar este puerto?
- Se puede usar el *nmap*
- Para editar los ficheros se usará el comando nano
- PENSAD QUE COSAS HACER ANTES DE HACERLAS PARA NO DEJAR PISTAS. Pensar el ataque antes de atacar
- PREPARAD LAS POSIBLES COSAS PARA DETECTAR EL ATAQUE

Cosas que hacer **OBLIGATORIAS:**

- Todos los alumnos deberán tener instalado el servidor ssh
- Todos los alumnos deberán crear un usuario **alumno** con permisos de administrador (¿os acordáis cómo hacerlo?), la contraseña para este usuario será **12345**
- No se puede cambiar ninguna dirección IP ni nombre de la máquina y estas serán públicas por todos los participantes.
- **No se debe borrar ni hacer daño en el ordenador del compañero. Solo se podrán modificar ficheros de tipo texto.**

Entrega de la práctica

Una vez que el ladrón ha entrado al sistema, deberá de notificárselo al profesor para que este tome nota.

**Deberá de ser entregado un documento a través de la web del curso**, (aules) de la estrategia usada para el ataque y la defensa, según el alumno sea ladrón o policía respectivamente.
Detallar pasos seguidos, y resultados obtenidos, si es posible haced capturas de pantalla para pegarlas en el documento.

## *Instalación del servicio ssh en CentOS 7*

*Nota: La tarjeta de red de la MV debe estar en bridge para obtener el DCHP y DNS del aula.*

1. Vamos a instalar el servidor con el siguiente comando:

```
sudo yum install openssh-server
```

### *Configurar SSH*

Antes de nada, hacemos un backup del archivo original.

*sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak*

Abrimos el fichero y configuramos las directivas necesarias para la conexión.
Se recomienda no permitir conexión remota, como usuario root, pero para nuestra práctica todos los usurarios serán root.

*PermitRootLogin yes*

Se puede cambiar el puerto por defecto de ssh, por otro. ¿tenemos que cambiarlo en nuestra práctica? ¿será una medida de protección contra el ataque?

*Port 2224*

Reiniciamos el servidor OpenSSH

*sudo systemctl reload sshd*

Forzar que el servidor OpenSSH arranque automáticamente al inicio de CentOS 7

*sudo systemctl enable ssh*
*sudo sytemctl start ssh*

### *Crear usuario para SSH*

Para conectarnos de forma remota vamos a crear un nuevo usuario.

*sudo adduser un-usuario*
*sudo passwd una-contraseña*

Vamos a abrir el puerto mediante iptables.
En Centos 7 han sustituido *iptables* por *firewalld,* pero lo curioso es que Firewalld se basa en *iptables*. En principio este cambio lo han realizado para facilitar la existencia a los administradores.

- Instalamos el servicio de *iptables*
  *yum install iptables-services*
- Enmascaramos el servicio de *firewalld*:
  *systemctl mask firewalld*
- Habilitamos el servicio de *iptables*
  *systemctl enable iptables*
- Paramos el servicio de firewalld
  *systemctl stop firewalld*
- Iniciamos el servicio de *iptables*
  *systemctl start iptables*

*Regla iptables para abrir el puerto por defecto del ssh (22).* Se puede hacer de dos maneras, o bien directamente desde línea de comandos (ejemplo1) o bien editando el fichero de iptables. En ambos casos recordar guardar los cambios.

1. *iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT*
2. *nano /etc/sysconfig/iptables*

   y aquí editaríamos el fichero introduciendo la misma línea.

Siempre guardar después de editar:

*iptables-save*

Después reiniciar el servicio

*systemctl restart iptables*
*systemctl enable iptables*
*systenctl start iptables*

*Prueba de conexión SSH*

Desde el anfitrión u otro pc ejecutaremos este comando, para conectar remotamente, donde tendréis que poner la IP del servidor OpenSSH.

*ssh -p puerto un-usuario@ip-del-servidor*