Reto SSH

6 marzo 2022

línea corta

# Objetivo

Un CTF es una competición que consiste en capturar una bandera escondida en una máquina expuesta en Internet. Vuestro objetivo será alcanzar un fichero (bandera 1) donde tendréis que escribir vuestro nombre y un servidor web (bandera 2) donde tendréis que subir el archivo *index.html* que queráis.

Con este reto se pretende que los alumnos adquieran algunos conocimientos de seguridad y, más concretamente, de SSH, así como conocimientos de otras ramas mientras superan una serie de pruebas que se han establecido en distintas máquinas virtuales del centro.

# Descripción

El reto consiste en realizar una serie de conexiones SSH en máquinas sucesivas hasta llegar a una máquina final donde poder grabar vuestro nombre y subir el fichero *index.html.* Para conseguirlo tendréis que superar una serie de pruebas que os permitirán acceder a cada máquina. Al final de este documento disponéis de una serie de pistas sobre como utilizar algunas de las herramientas necesarias para superar este reto. Además, disponéis de un [github](https://github.com/navasdamas/CTF-SSH) con material que os puede ser de ayuda.

Para comenzar el reto necesitaréis crear una araña en Java que consiga descifrar el usuario y contraseña de la primera máquina, en ella encontraréis las instrucciones para acceder a la siguiente.

El primer alumno que grabe su nombre y suba el fichero index.html será el ganador del reto. Cuando consideréis que habéis terminado el reto, poneros en contacto con algunos de los profesores para que verifique que se ha superado correctamente.

# Instrucciones

En la primera prueba tendréis que acceder mediante SSH a una máquina del centro. El usuario de la máquina es el nombre de uno de los profesores que os imparte clase: Eladio, Ana, Loli, Guillermo, Antonio, Carlos. La contraseña de este usuario se encuentra entre las 200 contraseñas más utilizadas en España en el año 2020: <https://nordpass.com/es/most-common-passwords-list/>

En [github](https://github.com/navasdamas/CTF-SSH) tenéis un fichero llamado *pass\_csv.csv* donde se encuentra este listado de contraseñas en formato csv.

Para superar esta prueba deberéis de crear una araña en Java que realice un ataque de diccionario probando con cada usuario y cada contraseña hasta que consigáis la combinación correcta. Este programa os imprimirá por pantalla cuáles son las credenciales correctas y deberéis de realizar la conexión SSH desde el terminal de vuestro equipo. Una vez dentro de la máquina, podéis abrir o descargarlos el fichero *instrucciones\_maquina\_2.txt* para conocer las instrucciones de la siguiente prueba.

# Material necesario

* [IDE Java](https://www.jetbrains.com/es-es/idea/download/#section=windows)
* [Java JDK](https://www.oracle.com/java/technologies/downloads/)
* Librería SSH de Java: [JSch](https://mvnrepository.com/artifact/com.jcraft/jsch/0.1.55)
* Cliente SSH
* [NMap](https://nmap.org/download)

# Pistas