

# SAD - U3 Seguridad Lógica

[Descargar estas actividades](#)

## Índice

### ▼ Actividades Seguridad Lógica

- [Actividad 1. Ataques a contraseñas](#)
- [Actividad 2. Contraseñas de Sistemas Operativos](#)
- [Actividad 3. Defensa ibérica](#)

## Actividades Seguridad Lógica

### Actividad 1. Ataques a contraseñas

Una buena opción para acortar los tiempos de los ataques a las contraseñas es tener algún indicio del formato de las mismas.

Partiendo del archivo **hashes\_practicas.txt** que contiene los hashes de las contraseñas de los usuarios `user1.x`, `user2.x` y `user3.x`, intenta obtener sus contraseñas.

Realiza un ataque a las contraseñas, teniendo en cuenta que las contraseñas tienen las siguientes propiedades:

- **user1.x** se obtiene con un ataque de diccionario
- **user2.x** se obtiene con un ataque por fuerza bruta con máscaras, sabiendo que están formadas por 3 minúsculas seguidas de 3 dígitos, por ejemplo "abc123"
- **user3.x** se obtiene con un ataque por diccionario con máscaras, sabiendo que las contraseñas están formadas por una palabra del diccionario (500\_passwords.txt) seguidas de un año comprendido entre 2000 y 2019.

Documentalo todo con capturas de pantalla en las que se vea el comando y los resultados producidos.

### Actividad 2. Contraseñas de Sistemas Operativos

Hemos conseguido sacar esta información del archivo SAM de Windows

```
100:AE4D4025B89026B533A46849C79CEE3D:7FFB9A84B18B17F66DA382F2C2FEC342:::
```

y esta contraseña de diccionario sacada de un sistema Linux

```
600.zqUv8$nAOCHqjtXJ8QjPIFIXdZes604kCXGIPqypNh5ON/McDRxHn7Mip3dx3gaSLlaE9ieRJaPvjUpq9KD5bmUkRue/
```

¿De qué formas podemos romper estas contraseñas?

Para obtener las contraseñas de Windows puedes usar Ophcrack o John the Ripper. Para las contraseñas de Linux, puedes usar John the Ripper o Hashcat. **Es importante que te fijes en el tipo de hash que se está utilizando para cada contraseña.**

Con Ophcrack, puedes usar las tablas de Rainbow para obtener la contraseña de Windows.

[Tablas rainbow](#)

## Actividad 3. Defensa ibérica

Tomando el hash que se encuentra en el archivo `defensa_iberica.txt`, intenta obtener la contraseña del usuario con alguna de las herramientas vistas en clase.