Immagine che contiene testo

Descrizione generata automaticamente 

*Grado en Ingeniería Informática-Ingeniería del Software*

*2021-2022*

*Curso de Seguridad en Sistemas Informáticos y en Internet*

**PAI 3.**

**BYODSEC**

**BRING YOUR OWN DEVICE SEGURO PARA UNA UNIVERSIDAD PÚBLICA USANDO ROAD WARRIOR VPN**

**SECURITY TEAM 11**

*Matilde Ghidini*

*Matteo Halilaga*

*Gabriele Petroni*

**INDICE**

[**INTRODUCCIÓN** 3](#_Toc100150561)

[Objetivos del proyecto 3](#_Toc100150562)

[**TECNOLOGIAS Y LIBRERÍAS UTILIZADAS** 3](#_Toc100150563)

[Lenguaje de programación: Python 3](#_Toc100150564)

[Socket 3](#_Toc100150565)

[SSL 3](#_Toc100150566)

[Sqlite3 3](#_Toc100150567)

[Algoritmo SHA256 3](#_Toc100150568)

[JSON 3](#_Toc100150569)

[Logging 3](#_Toc100150570)

[Uuid 4](#_Toc100150571)

[Hamachi 4](#_Toc100150572)

[**SOLUCION** 4](#_Toc100150573)

[TAREA 1 : Arquitectura Cliente-Servidor Segura con SSL 4](#_Toc100150574)

[TAREA 2: Análisis de tráfico de red en comunicaciones – Wireshark 4](#_Toc100150575)

[TAREA 3: Selección e implementación del conjunto de cipher suite más adecuado para la seguridad con SSL/TLS 4](#_Toc100150576)

# **INTRODUCCIÓN**

En este proyecto se píde la realización de un sistema que pueda implementar de la Política de Seguridad Bring your Own Device (BYOD), que consiste en que los empleados utilicen sus propios dispositivos para realizar sus trabajos, pudiendo tener acceso a recursos de la Universidad tales como correos electrónicos, bases de datos y archivos en servidores corporativos usando una VPN SSL. Para la transmisión de todos estos elementos es fundamental la implementación de canales de comunicación seguros.

## **Objetivos del proyecto**

1. Desarrollar/seleccionar cómo llevar a la práctica de forma lo más eficiente posible los canales de comunicación segura para la transmisión de credenciales (usuario, contraseñas) y un mensaje con el Protocolo SSL/TLS (autenticidad, confidencialidad e integridad). Tener en cuenta que el número de empleados que usarán la aplicación son aproximadamente 300.

2. Utilizar alguna herramienta de análisis de tráfico que permita comprobar la confidencialidad e integridad de los canales de comunicaciones seguros.

3. Establecer los Cipher Suites que serán usados en la versión TLS 1.3. Además, el cliente nos solicita pruebas sobre la capacidad para soportar a los 300 empleados por la VPN SSL desarrollada. Nota: Es muy importante para el cliente que la implementación de la VPN que se implemente sea los más eficiente posible. Considerando eficiente aquella solución con bajo overhead, baja

# **TECNOLOGIAS Y LIBRERÍAS UTILIZADAS**

## **Lenguaje de programación: Python**

Hemos decidido desarrollar nuestro proyecto utilizando el lenguaje Python.

## **Socket**

Hemos utilizado la librería Python socket, para implementar construir nuestra arquitectura cliente-servidor.

## **SSL**

## **Sqlite3**

Para crear una base de datos donde almacenar XXXXXXXXXXXXXXXXXXXXXXX hemos utilizado la librería Python Sqlite3, que es un base de datos SQL self-contained y file-based.

## **JSON**

Hemos utilizado la librería Python json, para la serialización y deserialización e los datos enviados del client hasta el server.

## **Logging**

Hemos utilizado la librería Python logging, para XXXXXXXXXX

## **Hamachi**

Hamachi es un software de virtualización de redes que permite emular una red local (LAN) a los dispositivos conectados por WAN. Con Hamachi se puede generar una red local aunque los dispositivos se encuentren en distintos lugares repartidos por el mundo. Para ello, Hamachi hace uso de redes privadas virtuales ([VPN](https://www.geeknetic.es/VPN/que-es-y-para-que-sirve)). Hemos utilizado. Hamachi para simular el funcionamiento de nuestro programa en diferentes dispositivos.

# **SOLUCION**

## **TAREA 1 : Arquitectura Cliente-Servidor Segura con SSL**

El primer paso para poder implementar el protocolo SSL es la generación de claves y certificados auto firmados. Para eso, se instala openssl, se generan primero una clave privada, luego un CSR y finalmente un certificado.

El siguiente paso es la construcción de una arquitectura cliente-servidor, utilizando socket ssl.

## **TAREA 2: Análisis de tráfico de red en comunicaciones – Wireshark**

## **TAREA 3: Selección e implementación del conjunto de cipher suite más adecuado para la seguridad con SSL/TLS**