

Universidad Internacional de La Rioja

Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Ciberseguridad

Análisis y desarrollo de un malware APT

Borrador Inicial

|  |  |
| --- | --- |
| Trabajo fin de estudio presentado por: | Alexander Brun Guajardo  David Fernández Sanz  Javier José Guzmán Rubio |
| Tipo de trabajo: | Trabajo Fin de Máster Grupal |
| Director/a: | Manuel Sánchez Rubio |
| Fecha: |  |

Resumen

Este proyecto tiene como objetivo desarrollar un **troyano modular** con diversas funcionalidades de acceso remoto, enfocado en el análisis de seguridad y pruebas de penetración. Se ha implementado un modelo **Cliente-Servidor** que permite la captura de pulsaciones de teclado, transferencia de archivos y ejecución remota de comandos, utilizando **TCP** y **ngrok** para la comunicación.

La metodología seguida incluye la implementación de **cifrado híbrido** mediante **AES y RSA** para asegurar la confidencialidad de los datos transmitidos. El cliente genera una clave AES y la cifra con la clave pública RSA del servidor, estableciendo una comunicación segura.

Los resultados obtenidos demuestran la viabilidad de establecer una infraestructura de control remoto con cifrado robusto. Como conclusión, este trabajo resalta la importancia del cifrado en herramientas de auditoría de seguridad y la necesidad de implementar mecanismos de protección en sistemas expuestos a este tipo de amenazas.

**Importante:** En el caso de un TFE grupal, la extensión del TFE debe garantizar que cada uno de los integrantes del equipo ha dedicado a la elaboración y defensa del trabajo las competencias previstas en la memoria. A modo orientativo, y para garantizar la calidad y dedicación que requiere un TFE grupal, la extensión mínima ha de ser un 50% superior a lo previsto para un TFE individual. Por lo tanto, la extensión mínima en un TFE grupal es de **75 páginas**.

**Palabras clave:** Seguridad informática, troyano, cifrado híbrido, acceso remoto, pruebas de penetración

Abstract

En este apartado se introducirá un breve resumen en **inglés** del trabajo realizado (extensión máxima 150 palabras).

**Keywords**: Se deben incluir de 3 a 5 palabras claves en inglés

Índice de figuras

[Figura 1. *Ejemplo de figura realizada para nuestro trabajo.* 2](#_Toc150422789)

Índice de tablas

[Tabla 1. *Organización del trabajo en grupo.* VIII](#_Toc150422790)

[Tabla 2. *Ejemplo de tabla con sus principales elementos.* 2](#_Toc150422791)

Organización del trabajo en grupo

En este apartado se detallarán las distintas partes en las que se ha dividido el trabajo entre los componentes del grupo, los objetivos perseguidos en cada una de ellas y los mecanismos de coordinación empleados. Este apartado deberá ser validado por el director para poder comenzar con el trabajo.

Partes que aborda el TFE, distribución y estructura de la memoria

Cada estudiante debe abordar elementos/partes que, individualmente, podrían suponer un TFE por sí mismas.

Complete la siguiente tabla que debe reflejar el reparto de trabajo a la hora de confeccionar la memoria del TFE.

Tabla 1. *Organización del trabajo en grupo.*

|  |  |
| --- | --- |
| Organización del trabajo en grupo - Desarrollo de la memoria | |
| Apartado de la memoria | **Responsables** |
| Introducción | Alumno 1, Alumno 2 y Alumno 3 |
| Estado del arte | Alumno 1, Alumno 2 y Alumno 3 |
| Objetivos y metodología de trabajo | Alumno 1, Alumno 2 y Alumno 3 |
| Desarrollo específico de la contribución: parte individual 1 | Alumno 1 |
| Desarrollo específico de la contribución: parte individual 2 | Alumno 2 |
| Desarrollo específico de la contribución: parte individual 3 | Alumno 3 |
| Desarrollo específico de la contribución: parte 4 | Alumno 1, Alumno 2 y Alumno 3 |
| Conclusiones y trabajo futuro | Alumno 1, Alumno 2 y Alumno 3 |

Fuente: Elaboración propia.

Objetivo del TFE desde el punto de vista de la adquisición de conocimientos

Desde el punto de vista de la adquisición de conocimientos, este TFE, incorpora varios segmentos suficientemente diferenciados que, en sí mismos, podrían haber sido tema para una propuesta de investigación individual; con ello los estudiantes alcanzarían una multidisciplinariedad que trasvasa de lo estrictamente teórico a lo empírico. Lo que le aporta el carácter grupal del trabajo es, por lo tanto, un carácter holístico que le da relevancia no solo académica sino práctica, pues termina siendo un resultado utilizable profesionalmente por los estudiantes en su ámbito de trabajo.

Mecanismos de coordinación empleados

Recordar que nos estamos preparando para un día a día en un mundo laboral cada vez más complejo. Este mundo laboral implica siempre trabajar en conjunto con otras personas y profesionales de diferentes ámbitos. Un TFE grupal te prepara para esa realidad a la que nos enfrentamos en un entorno laboral real.

Describir los mecanismos y herramientas de coordinación y comunicación empleados para el desarrollo del TFE grupal.