Pauta del Proyecto de Seguridad Informática
Unidad 2
Desarrollo de Software para Seguridad

Ricardo Pérez
riperez@utalca.cl

Descripción general

El proyecto consiste en desarrollar un keylogger que capture información ingresada por teclado en un dispositivo de "víctima", cifrar y transmitir estos datos de forma segura, y realizar un ataque MITM (Man-in-the-Middle) para evaluar la resistencia de la comunicación a interceptaciones.

Ejercicio 1: Desarrollo de Keylogger (35 puntos)

Objetivo: Desarrollar un keylogger funcional que capture todas las pulsaciones de teclado en el dispositivo de la víctima, independientemente del sistema operativo (Android, Linux, macOS o Windows).
Requisitos específicos:

- Implementar el keylogger en el lenguaje de programación de preferencia, sin reutilizar fragmentos de código de otros equipos.
- Documentar detalladamente el código fuente, explicando cada sección.
- Proporcionar evidencia del funcionamiento del keylogger.

Criterios de evaluación:

- **Funcionalidad del Keylogger (15 puntos)**: Evaluar si el keylogger captura efectivamente las pulsaciones de teclado en el sistema operativo elegido.
- **Originalidad y documentación del código (10 puntos)**: Calidad y claridad de la documentación, incluyendo explicaciones detalladas del código.
- **Evidencia de funcionamiento (10 puntos)**: Proporcionar capturas de pantalla, videos, o pruebas que demuestren que el keylogger funciona correctamente en el dispositivo de la víctima.

Ejercicio 2: Cifrado y transmisión de datos (35 puntos)

Objetivo: Cifrar la información capturada y enviarla periódicamente a un dispositivo controlado por el estudiante.
Requisitos específicos:

- Seleccionar e implementar un algoritmo de cifrado seguro y justificar la elección.
- Transmitir los datos cifrados periódicamente al dispositivo del estudiante y almacenarlos para su análisis.
- Desencriptar los datos recibidos para mostrar el contenido capturado por el keylogger.
- Proveer evidencia en cada paso de este ejercicio.

Criterios de evaluación:

- **Justificación del algoritmo de cifrado (10 puntos)**: Argumentos sólidos y fundamentados sobre la elección del algoritmo de cifrado.
- **Transmisión de datos cifrados (10 puntos)**: Efectividad de la transmisión y periodicidad adecuada en el envío de datos.
- **Desencriptación y almacenamiento (10 puntos)**: Precisión en el desencriptado de datos y adecuado almacenamiento para análisis.
- **Evidencia documentada (5 puntos)**: Capturas de pantalla, videos, o pruebas de cada etapa del proceso.

Ejercicio 3: Ataque MITM y seguridad del keylogger (30 puntos)

Objetivo: Realizar un ataque MITM al dispositivo de la víctima y demostrar que, aunque la información es interceptada, no puede ser descifrada.
Requisitos específicos:

- Implementar un ataque MITM que capture la comunicación entre el keylogger y el dispositivo del estudiante.
- Asegurarse de que el malware no sea detectado por sistemas de detección de intrusos o antivirus.
- Justificar las alternativas de mitigación que pueden emplear los usuarios o especialistas de TI contra este tipo de amenazas.

Criterios de evaluación:

- **Implementación del ataque MITM (15 puntos)**: Calidad y efectividad en la captura de datos y la configuración del ataque MITM.
- **Evasión de detección (10 puntos)**: Evaluar si el keylogger es capaz de evitar la detección por sistemas de seguridad.
- **Justificación de medidas de mitigación (5 puntos)**: Explicación clara de las estrategias que los usuarios o administradores de TI pueden emplear para contrarrestar esta amenaza.

Evidencias del proyecto

Documentación completa:

- Explicación detallada de cada ejercicio, incluyendo los pasos y la lógica empleada.
- Incluir referencias y fundamentaciones teóricas que respalden las decisiones técnicas.

Video Demostrativo:

- **Duración**: El video debe cubrir todos los pasos del proyecto, permitiendo que ambos integrantes expliquen sus aportes.
- **Contenido**: Mostrar el funcionamiento de cada ejercicio, desde la captura de datos hasta la transmisión y el ataque MITM.
- **Participación**: Ambos integrantes deben participar en la explicación y presentación de las evidencias.
- **Subida del video**: El video debe estar disponible al menos un día antes de la defensa, con el enlace compartido en la plataforma indicada.

Presentación y defensa

Contenido:

- Explicación breve del proyecto, sus objetivos y el enfoque en seguridad informática.
- Demostración y explicación de los resultados de cada ejercicio.
- Responder preguntas del profesor o evaluador sobre los procedimientos y decisiones técnicas empleadas.

Criterios de evaluación:

- **Claridad en la explicación**: Capacidad para explicar cada etapa técnica del proyecto de manera precisa y comprensible.
- **Conocimiento de conceptos**: Demostrar comprensión de los conceptos de seguridad aplicados y cómo afectan la protección de datos.
- **Trabajo en equipo**: Equilibrio en la participación de ambos integrantes y coherencia en la presentación.

Calificación Total

Total: 100 puntos