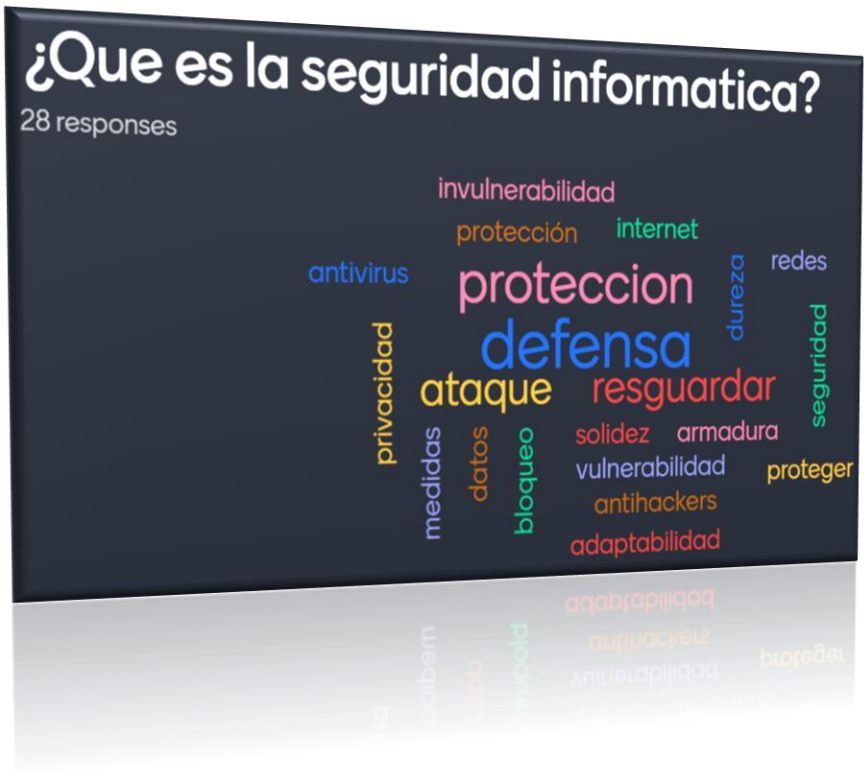
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Hacking Ético

Objetivo:

Realizar y documentar pruebas prácticas utilizando Flipper Zero, un dispositivo multifuncional para pruebas de seguridad y hacking ético. Cada grupo de dos estudiantes realizará demostraciones prácticas de diferentes ataques y grabará un video explicativo de no más de 1.5 minutos.

Materiales Necesarios:

- Un dispositivo Flipper Zero por grupo.
- Computadoras con acceso a Internet.
- Software de edición de video (opcional, para recortar y ajustar videos).
- Teléfonos móviles o cámaras para grabar los videos.

Instrucciones:

Parte 1: Formación de Grupos y Asignación de Tareas

1. **Formación de Grupos:**
   - Dividir a los alumnos en grupos de dos personas, registrar el nombre, grupo y nombre de la tecnología para la demostración
   - https://docs.google.com/spreadsheets/d/16oAEM7CFJyX_RG0W3G3hxIUth5gaWTppN0Pj9mybhaI/edit?gid=2109863044#gid=2109863044

2. **Asignación de Tareas:**
   - Cada persona dentro del grupo debe realizar una demostración práctica diferente utilizando el Flipper Zero.

Parte 2: Investigación y Preparación

1. **Investigación:**
   - Cada grupo debe investigar y seleccionar dos tipos de ataques o pruebas que se pueden realizar con Flipper Zero. Ejemplos incluyen:
     - **Clonación y Emulación de RFID:** Clonar y emular tarjetas RFID.
     - **Control de Dispositivos IR:** Controlar dispositivos que usan señales infrarrojas.
     - **Interacción con Dispositivos NFC:** Interactuar con dispositivos que usan NFC.
     - **Ataques de Fuerza Bruta Bluetooth:** Intentar conectarse a dispositivos Bluetooth no seguros.
     - **Simulación de HID (Human Interface Device):** Actuar como un teclado o ratón USB para enviar comandos a un ordenador.

- **Captura y Reproducción de Señales Sub-GHz:** Escanear, capturar y reproducir señales de dispositivos que operan en el rango de frecuencia sub-GHz.
- **Analizador de Señales Digitales:** Analizar y depurar protocolos digitales mediante la captura de datos en los pines GPIO.
- **Lectura y Escritura de Cartuchos de Juegos:** Leer y escribir datos en cartuchos de juegos.
- **Interacción con Sistemas de Automóviles:** Escanear y reproducir señales de sistemas de entrada sin llave.
- **Comandos GPIO:** Usar los pines GPIO para controlar y recibir datos de dispositivos electrónicos.
- **Analizador de Emisiones Electromagnéticas:** Detectar y analizar emisiones electromagnéticas de dispositivos electrónicos.

2. **Planificación:**
   - Planificar cómo llevarán a cabo las demostraciones prácticas y los pasos necesarios para cada ataque o prueba.

Parte 3: Ejecución de la Prueba y Grabación del Video

1. **Ejecución:**
   - Realizar las demostraciones prácticas utilizando el Flipper Zero.
   - Asegurarse de seguir todos los pasos necesarios y tomar notas sobre el proceso.
2. **Grabación del Video:**
   - Cada estudiante debe grabar un video explicativo de no más de 1.5 minutos que incluya:
     - Introducción del tipo de ataque o prueba.
     - Demostración práctica del ataque o prueba.
     - Explicación del impacto y las implicaciones del ataque o prueba.
   - Asegurarse de que el video sea claro y conciso, mostrando tanto el dispositivo como el proceso en acción.

Ejemplo de Video:

- **Introducción:** "Hola, les voy a mostrar cómo realizar un ataque de clonación RFID con Flipper Zero."
- **Demostración Práctica:** Mostrar cómo escanear una tarjeta RFID y luego emularla usando el Flipper Zero.
- **Explicación del Impacto:** "Este ataque puede ser usado para clonar tarjetas de acceso, lo que puede comprometer la seguridad de lugares restringidos. Es importante asegurarse de que las tarjetas RFID utilicen cifrado seguro para prevenir este tipo de ataques."

Parte 4: Presentación y Evaluación

1. **Subida de Videos:**
   - Subir los videos a una plataforma designada por el instructor antes de la fecha límite.

2. **Presentación en Clase:**
    - Cada grupo presentará sus videos a la clase.
    - Discutir brevemente los ataques o pruebas realizadas y responder preguntas de sus compañeros y el instructor.
3. **Evaluación:**
    - Los videos serán evaluados basándose en:
        - **Claridad y Concisión:** Si el video es claro y se ajusta al tiempo límite.
        - **Exactitud Técnica:** Si la demostración fue realizada correctamente y se explicaron bien los pasos.
        - **Comprensión del Impacto:** Si se explicó adecuadamente el impacto del ataque o prueba.

Conclusión

- **Resumen de la Actividad:**
    - Discutir lo aprendido sobre las capacidades de Flipper Zero y la importancia de la ciberseguridad.
    - Reflexionar sobre cómo estos conocimientos pueden aplicarse para mejorar la seguridad en sistemas reales.

Recomendaciones

- **Seguridad y Ética:**
    - Recordar siempre que las pruebas de seguridad deben realizarse de manera ética y con el consentimiento adecuado.
    - Nunca usar habilidades de hacking para actividades maliciosas.

Ejemplos de Demostraciones con Flipper Zero

1. Clonación y Emulación de RFID:

- **Descripción:** Capturar y emular tarjetas RFID de baja y alta frecuencia.
- **Impacto:** Puede utilizarse para acceder a áreas restringidas que utilizan sistemas de control de acceso basados en RFID.

2. Control de Dispositivos IR:

- **Descripción:** Capturar y reproducir señales infrarrojas para controlar dispositivos como televisores, acondicionadores de aire, etc.
- **Impacto:** Permite el control no autorizado de dispositivos electrónicos a través de señales IR.

3. Interacción con Dispositivos NFC:

- **Descripción:** Leer, escribir y emular tarjetas y etiquetas NFC.
- **Impacto:** Puede usarse para manipular sistemas de pago NFC, tarjetas de transporte y otros dispositivos que utilicen esta tecnología.

4. Ataques de Fuerza Bruta Bluetooth:

- **Descripción:** Intentar conexiones y explorar dispositivos Bluetooth no seguros.
- **Impacto:** Puede comprometer dispositivos Bluetooth que no estén adecuadamente protegidos.

5. Simulación de HID (Human Interface Device):

- **Descripción:** Actuar como un teclado o ratón USB para enviar comandos a un ordenador.
- **Impacto:** Permite la inyección de comandos maliciosos en sistemas vulnerables.

6. Captura y Reproducción de Señales Sub-GHz:

- **Descripción:** Escanear, capturar y reproducir señales de dispositivos que operan en el rango de frecuencia sub-GHz (315 MHz, 433 MHz, etc.).
- **Impacto:** Puede interceptar y reproducir señales de sistemas de apertura de puertas, mandos de garaje, y otros dispositivos de control remoto.

7. Analizador de Señales Digitales:

- **Descripción:** Analizar y depurar protocolos digitales mediante la captura de datos en los pines GPIO del Flipper Zero.
- **Impacto:** Ayuda a comprender y manipular protocolos digitales en dispositivos electrónicos.

8. Lectura y Escritura de Cartuchos de Juegos:

- **Descripción:** Leer y escribir datos en cartuchos de juegos, como los de Game Boy.
- **Impacto:** Permite modificar y hacer copias de seguridad de los datos de los cartuchos de juegos.

9. Interacción con Sistemas de Automóviles:

- **Descripción:** Escanear y reproducir señales de sistemas de entrada sin llave y otros sistemas electrónicos de vehículos.
- **Impacto:** Puede usarse para investigar y auditar la seguridad de sistemas de entrada sin llave.

10. Comandos GPIO: - **Descripción:** Usar los pines GPIO del Flipper Zero para controlar y recibir datos de dispositivos electrónicos. - **Impacto:** Permite la integración y prueba de dispositivos electrónicos personalizados.

11. Analizador de Emisiones Electromagnéticas: - **Descripción:** Detectar y analizar emisiones electromagnéticas de dispositivos electrónicos. - **Impacto:** Puede ayudar en la identificación de posibles fugas de datos y vulnerabilidades en dispositivos.

