



Hacking Ético

Topic	Control de Dispositivos IR: Controlar dispositivos que usan señales infrarrojas.
Module	IT - Ciberseguridad
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Gonzalo Antonio Ortiz Fernandez Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@July 8, 2024
Wochentage	Montag
Deadline	@July 8, 2024
Status	Sended
Attached files	<u>Unidad_50_Hacking Ético.pdf</u>

Objetivo

Tema

Herramienta Utilizada: Flipper

Explicación Técnica del Proceso de Control del Aire Acondicionado con Señales Infrarrojas

Proceso Paso a Paso

Consideraciones Técnicas

Conclusión

Anexo



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.

Tema

Control de Dispositivos IR: Controlar dispositivos que usan señales infrarrojas.

Encender y apagar un aire acondicionado

Controlar un proyector

Herramienta Utilizada: Flipper

El Flipper es un dispositivo versátil que permite la captura, almacenamiento y reproducción de señales infrarrojas (IR), entre otras funcionalidades. En este caso, ha sido utilizado para hackear el control del aire acondicionado.

Explicación Técnica del Proceso de Control del Aire Acondicionado con Señales Infrarrojas

Proceso Paso a Paso

1. Captura de Señales IR:

- **Frecuencia de Encendido:**

Utilizando el Flipper, se capturó la señal infrarroja emitida por el control remoto original del aire acondicionado cuando se presiona el botón de encendido. Esta señal contiene la información específica codificada que el aire acondicionado reconoce para iniciar su funcionamiento.

- **Guardado como "Encender_aire":**

La señal capturada fue almacenada en la memoria del Flipper bajo el nombre "Encender_aire". Esto facilita su identificación y uso posterior.

- **Frecuencia de Apagado:**

De manera similar, se capturó la señal infrarroja emitida por el control remoto original cuando se presiona el botón de apagado del aire acondicionado. Esta señal contiene la información que el aire acondicionado reconoce para detener su funcionamiento.

- **Guardado como "Apagar_aire":**

La señal capturada fue almacenada en la memoria del Flipper bajo el nombre "Apagar_aire".

2. Almacenamiento de Señales:

- **Formato de Almacenamiento:**

Las señales IR fueron guardadas en un formato que el Flipper puede reproducir fácilmente. Esto generalmente implica el almacenamiento de

los datos de la señal, incluyendo la frecuencia y la duración de cada pulso de la señal IR.

3. Reproducción de Señales IR:

- **Emisión de la Señal "Encender_aire":**

Cuando se quiere encender el aire acondicionado, el Flipper reproduce la señal almacenada como "Encender_aire". El aire acondicionado recibe esta señal, la decodifica y realiza la acción de encenderse.

- **Emisión de la Señal "Apagar_aire":**

Para apagar el aire acondicionado, el Flipper reproduce la señal almacenada como "Apagar_aire". El dispositivo receptor (aire acondicionado) recibe la señal, la decodifica y se apaga.

Consideraciones Técnicas

- **Protocolos IR:**

Las señales IR suelen seguir protocolos específicos como NEC, Sony, RC5, entre otros. Cada protocolo tiene su propia estructura de codificación de datos. En este caso, es probable que el Flipper haya detectado y utilizado el protocolo adecuado para el aire acondicionado específico.

- **Integridad de la Señal:**

Es esencial que la señal reproducida por el Flipper sea una réplica exacta de la señal original capturada. Cualquier distorsión podría resultar en la falla del comando enviado.

Conclusión

Utilizando el Flipper, se capturaron y almacenaron las señales IR de encendido y apagado del aire acondicionado. Estas señales fueron guardadas bajo los nombres "Encender_aire" y "Apagar_aire", respectivamente. El Flipper puede reproducir estas señales para controlar el aire acondicionado de manera efectiva, replicando los comandos del control remoto original.

Este proceso demuestra cómo la tecnología de señales IR puede ser utilizada en el contexto de hacking ético para entender y controlar dispositivos electrónicos, subrayando la importancia de la precisión y el conocimiento de los protocolos IR.

Anexo



El Flipper con los archivos guardados



Los aires acondicionados utilizados



Para recordar @July 8, 2025



Probando

```
Filetype: IR library file
Version: 1
name: POWER_ON
type: parsed
protocol: NECext
address: 83 55 00 00
command: 90 6F 00 00

name: POWER_OFF
type: parsed
protocol: NECext
address: 83 55 00 00
command: 31 CE 00 00
```

https://prod-files-secure.s3.us-west-2.amazonaws.com/5e382540-cfec-4f0e-8fed-111ef4874400/709367a1-89be-4132-8430-c7bfe3451d89/WhatsApp_Video_2024-07-09_at_09.23.01_bf1e90c5.mp4

https://prod-files-secure.s3.us-west-2.amazonaws.com/5e382540-cfec-4f0e-8fed-111ef4874400/808ce049-cf9c-402b-bc03-5da9fecd40c7/video_flipper.mp4



SCRIPT de prueba para el IR del proyector de la clase