

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández	13/12/2025
	GRUPO 7	

Actividad grupal. Vectores de ataque

Con esta práctica conseguiremos documentar un ciberdelito, analizándolo al máximo en su funcionamiento, bien a través de código, vídeos, artículos científicos, prensa, etc.

Un vector de ataque es el camino que usa un ciberdelincuente para acceder al activo objetivo del ataque.

Sobre la práctica

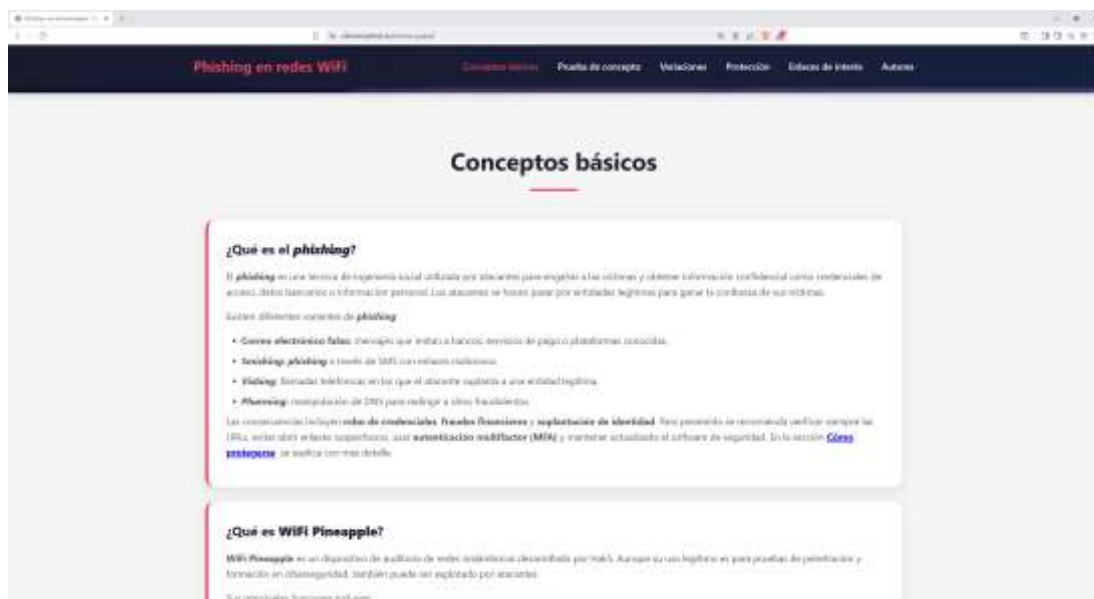
El objetivo es documentar un **ataque de phishing en redes inalámbricas usando WiFi Pineapple con portal cautivo**. En el proyecto, se detallan los conceptos básicos que más relevantes, se realiza una prueba de concepto, analizado posibles variaciones y documentado cómo protegerse de este tipo de ataques.

Toda la información recopilada está disponible en esta página web:
<https://ciberunir.github.io/practica-grupal/>

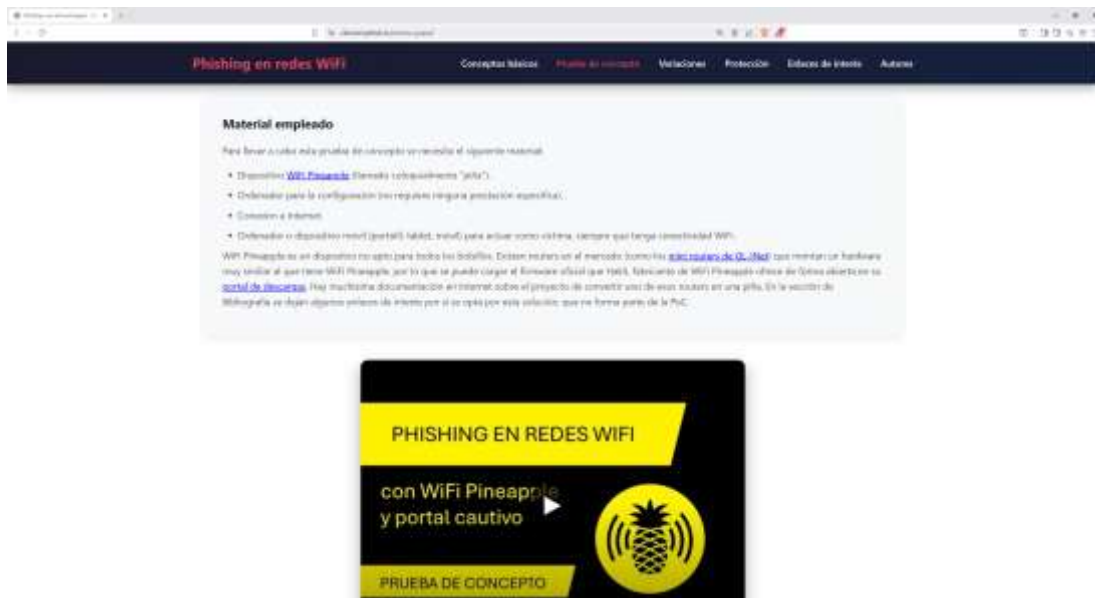
La web está alojada en Github. Junto a este documento se incluye el ZIP del proyecto, con toda la documentación, que también es accesible a través del repositorio (<https://github.com/ciberunir/practica-grupal>). Ejecutando el index.html podemos visualizar la página web de forma local.

No obstante, en el presente documento, se adjuntan imágenes del trabajo realizado:

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández	13/12/2025
	GRUPO 7	



Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández	13/12/2025
	GRUPO 7	



Phishing en redes WIFI

Conceptos básicos | **Prueba de concepto** | Variaciones | Protección | Enlaces de interés | Auténtica

Material empleado

Para llevar a cabo este tipo de ataques se necesitan el siguiente material:

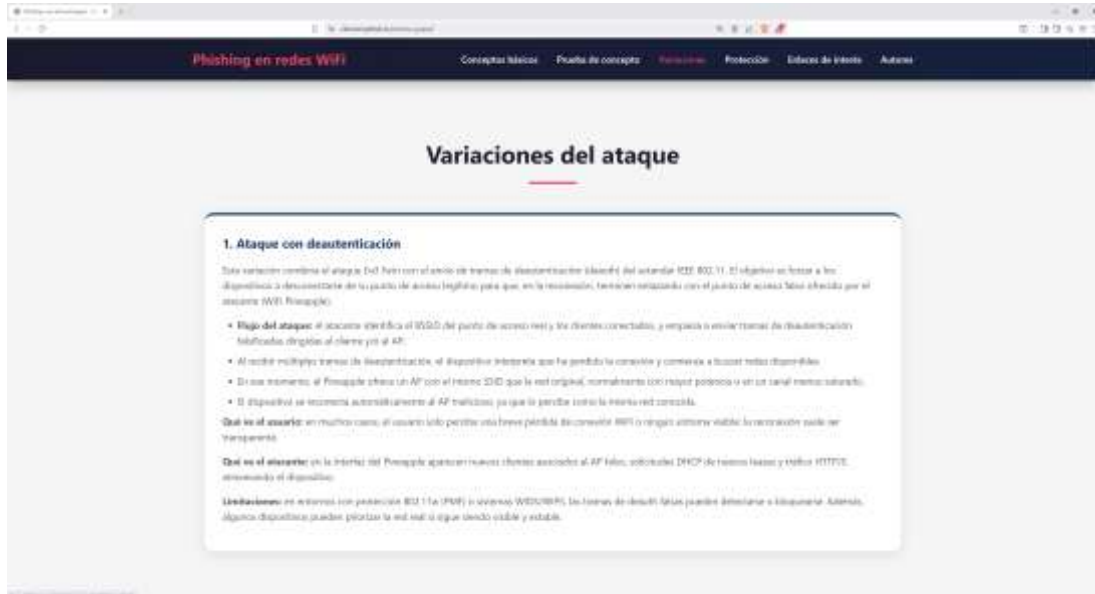
- Dispositivo **WiFi Pineapple** (también se puede usar un "ratón").
- Ordenador para la configuración (no requiere ninguna protección especial).
- Conexión a Internet.
- Ordenador o dispositivo móvil (smartphone, tablet, etc.) para actuar como víctima, siempre que tenga conectividad WiFi.

WiFi Pineapple es un dispositivo no apto para todos los detalles. Existen muchos en el mercado, como los [hackers de Q. U. I. N. I. A.](#) que montan un hardware muy similar al que tiene WiFi Pineapple pero lo que se puede cargar el firmware oficial que tiene, fabricando de WiFi Pineapple clones de otros dispositivos en su [portal de descargas](#). Hay mucha documentación en internet sobre el proyecto de convertir uno de estos routers en una pila. En la sección de Mitigación se describen algunas técnicas de defensa por si se está por esta solución que no forma parte de la PoC.

PHISHING EN REDES WIFI

con WiFi Pineapple y portal cautivo

PRUEBA DE CONCEPTO



Phishing en redes WIFI

Conceptos básicos | Prueba de concepto | **Variaciones** | Protección | Enlaces de interés | Auténtica

Variaciones del ataque

1. Ataque con deautenticación

Esta variación consiste en atacar el protocolo de autenticación basado en el estándar IEEE 802.11. El objetivo es forzar a los dispositivos a desconectarse de la pila de acceso legítima para que, en la reconexión, tengan que conectarse con el punto de acceso falso creado por el atacante (WiFi Pineapple).

- **Flujo del ataque:** el atacante ejecuta el WPS del punto de acceso real y los clientes conectados, y empieza a enviar tramas de deautenticación falsificadas dirigidas al cliente y al AP.
- Al recibir múltiples tramas de deautenticación, el dispositivo interpreta que ha perdido la conexión y comienza a buscar redes disponibles.
- En ese momento, el Pineapple ofrece un AP con el mismo SSID que la red original, normalmente con mayor potencia o en un canal menos saturado.
- El dispositivo se reconecta automáticamente al AP malicioso, ya que le parece como la red más cercana.

Qué se le ofrece: en muchos casos, al usuario solo se le ofrece una breve pantalla de conexión WiFi o ninguna pantalla visible. La reconexión puede ser transparente.

Qué se le ofrece: en la interfaz del Pineapple aparecen nuevos clientes asociados al AP falso, solicitudes DHCP de nuevos hosts y tráfico HTTP, simulando el dispositivo.

Limitaciones: en routers con protección 802.11e (PMF) o routers WDS/BR/RS, los ataques de deautenticación pueden detenerse o bloquearse. Además, algunos dispositivos pueden priorizar la red real si sigue siendo visible y estable.

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández	13/12/2025
	GRUPO 7	

