1. **Averigua qué son y qué uso tienen las herramientas Blackeye y Ngrok.**

**Blackeye** es una herramienta de código abierto utilizada para realizar ataques de phishing, ya que permite clonar sitios web populares y engañar a las víctimas para que ingresen sus credenciales en las páginas falsas.

**Ngrok** es una herramienta que permite exponer un servidor local a Internet creando un túnel seguro, lo que facilita la distribución de páginas de phishing fuera de la red local, haciéndolas accesibles desde cualquier parte del mundo.

<https://cybersecuritynews.es/recurso-hacking-como-crear-una-pagina-de-phishing-y-sacarla-fuera-de-nuestra-red-con-ngrok/>

<https://kevinmelgarejo.com/black-eye-una-herramienta-gratuita-para-hackear-phishing/>

1. **Échale un vistazo a los pasos indicados. Pon ejemplos de cinco webs que Blackeye puede imitar.**

Blackeye puede imitar varias páginas web populares, haciéndolas parecer reales para las víctimas. Algunos ejemplos de sitios web que puede clonar incluyen:

* **Facebook**
* **Instagram**
* **Netflix**
* **Twitter**
* **Google**

Estos sitios son objetivos comunes de los ataques de phishing porque los usuarios suelen estar acostumbrados a introducir sus credenciales en ellos sin sospechar que puedan ser falsos.

1. **Busca herramientas relacionadas con los ataques sniffing. Menciona al menos dos.**

Varias de las **herramientas relacionadas con ataques de sniffing**, que se utilizan para interceptar y analizar el tráfico de red con el fin de capturar datos sensibles, algunas de las más conocidas son:

* **Wireshark**: Un analizador de protocolos que permite capturar y analizar el tráfico de red en tiempo real, proporcionando detalles sobre las comunicaciones.
* **IDS (Sistema de Detección de Intrusiones)**: Un sistema que monitorea el tráfico de red en busca de patrones de tráfico sospechosos y emite alertas cuando se detecta una actividad anómala. Algunos IDS pueden tomar medidas preventivas, como bloquear el tráfico de una dirección IP específica.
* **Ettercap**: Herramienta especializada en ataques "man-in-the-middle" (MitM) que intercepta y modifica el tráfico de red, útil para el sniffing de contraseñas y otra información crítica

<https://impulso06.com/ataques-sniffer-que-son-y-como-protegerte/>