BlackPhish: Suplantación de Sitios Web para Análisis de Vulnerabilidades

Implementación Práctica de Ataques de Phishing con Kali Linux

Edinson Carrascal Reyes

INTRODUCCIÓN

El phishing representa uno de los vectores de ataque más explotados en la historia de la ciberseguridad, siendo responsable del 80% de las vulnerabilidades explotadas por atacantes, principalmente aprovechando debilidades humanas.

PHISHING

El phishing es una técnica de ingeniería social que consiste en la suplantación de identidad de sitios web legítimos para engañar a usuarios y obtener información sensible como credenciales, datos financieros o información corporativa

Principio

Confianza: Crear credibilidad

Reciprocidad; generar obligación

Autoridad: Simular posiciones

Urgencia: presión de tiempo

Escasez: oportunidades limitadas

Tipos

Email phishing

Spear phishing

Whaling

Vishing

Smishing

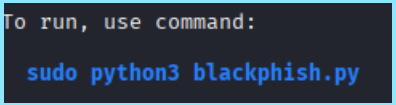
Impacto

Según estudios recientes, el 52.1% de empleados consideran que tienen el conocimiento necesario sobre amenazas cibernéticas, pero el 47.9% restante no se siente preparado. A pesar de que la ciberseguridad es prioritaria, los colaboradores no cuentan con suficiente capacitación para reducir estas amenazas

BLACKPHISH

BlackPhish es una herramienta de código abierto diseñada para realizar pruebas de penetración mediante la clonación de sitios web legítimos. Permite a profesionales de seguridad evaluar la vulnerabilidad de usuarios frente a ataques de phishing en entornos controlados.

INSTALACIÓN



1

ABRIR TERMINAL

Acceder a la terminal del sistema operativo Kali Linux desde el menú de aplicaciones o con el atajo Ctrl + Alt + T.

2

CLONAR REPOSITORIO

Descarga el código fuente de BlackPhish desde el repositorio oficial de GitHub.

3

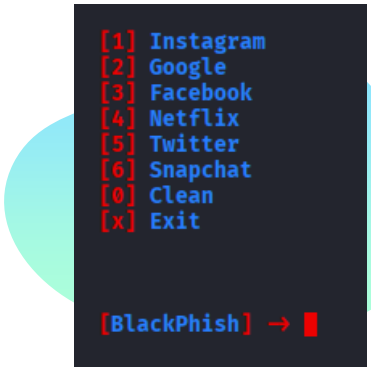
EJECUTAR ESCIPT

Instala todas las dependencias necesarias y configura el entorno de BlackPhish.

INSTALACIÓN COMPLETA

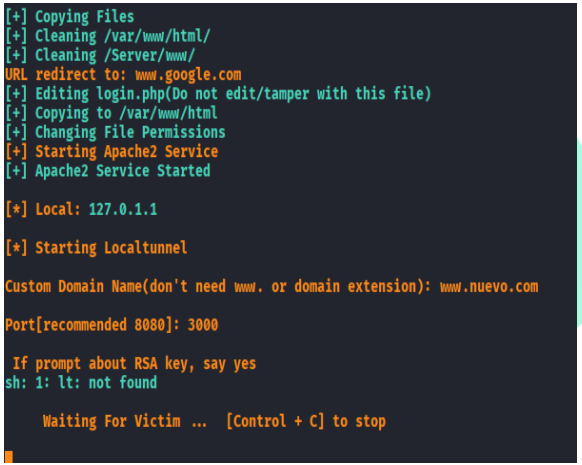
AHORA SE ACEPTA EL
USO DE RESPOSABILIDAD

IMPLEMENTACIÓN DE ATAQUE



ESCOGER SITIO

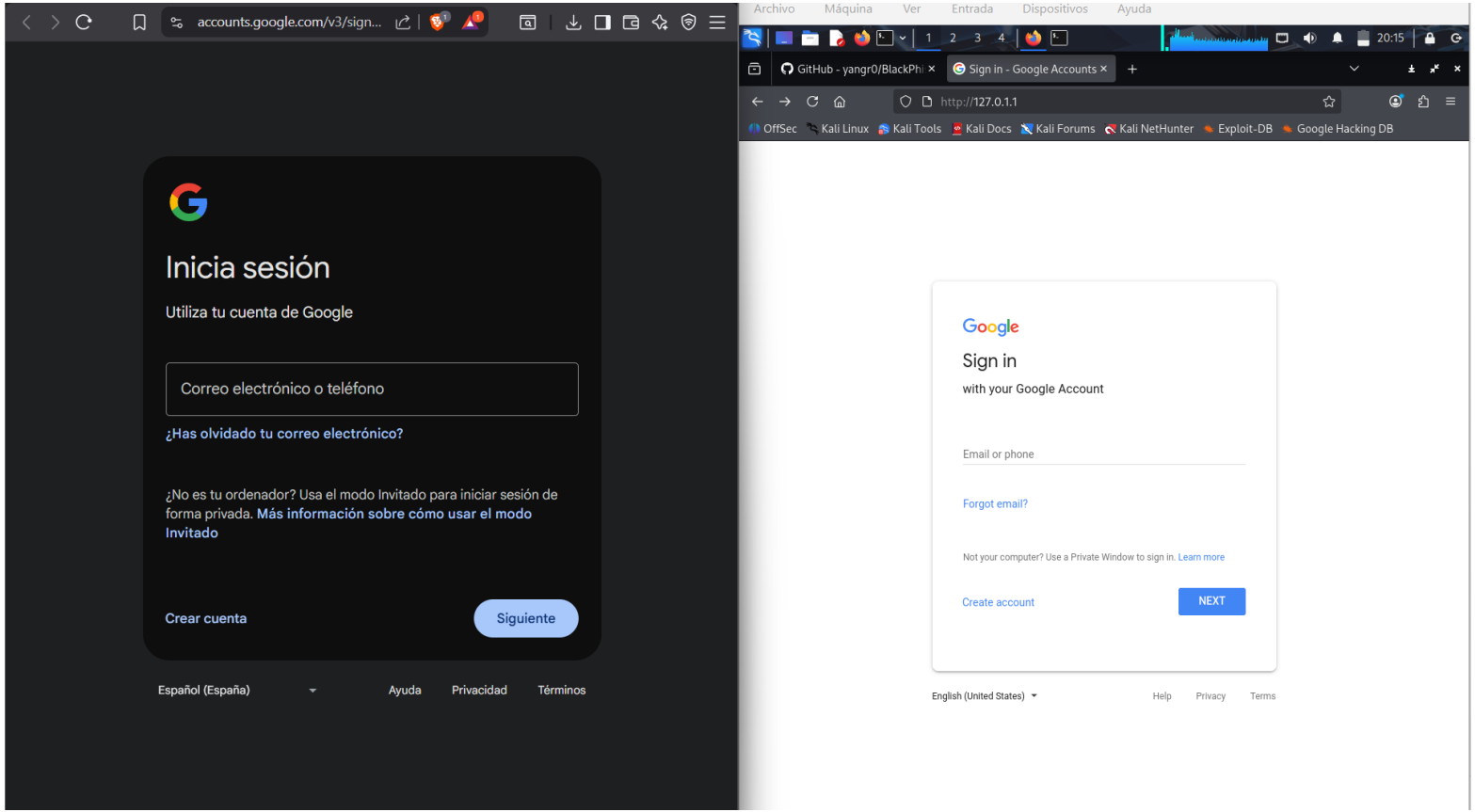
Presionar un numero para seleccionar la pagina a clonar



EJCUCIÓN

Sistema de ejecucicon finalizado y configurado ahora solo debes ir a la url

ATAQUE IMPLEMENTADO



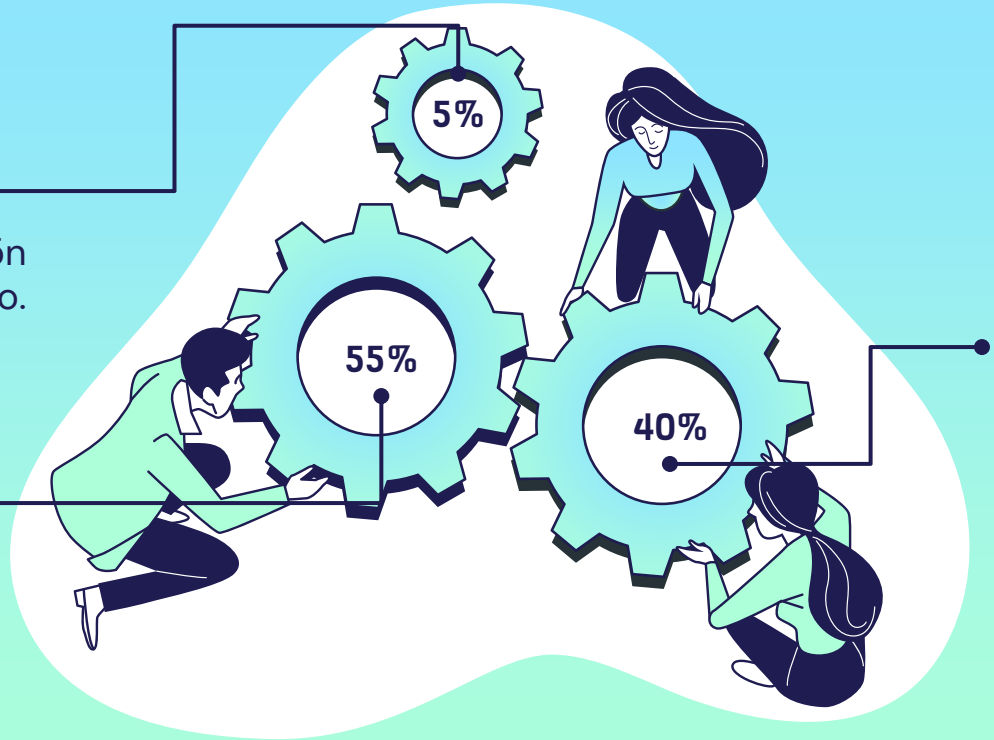
VECTORES DE ATAQUE COMBINADOS

EMAIL SPOOFING

Falsificación de la dirección de correo electronico.

URL MASKING

Enmascaramiento de URLs maliciosas.

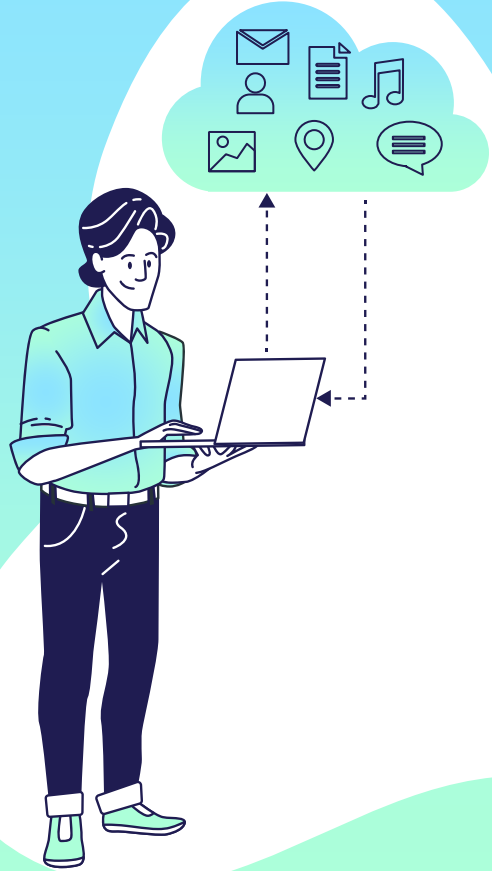


VISHING

Llamadas telefonicas para obtenerinformación

CONCLUSIÓN

1. A pesar de los avances tecnológicos en seguridad, el 80% de las brechas exitosas explotan vulnerabilidades humanas. La tecnología sola no es suficiente sin usuarios capacitados.
2. El 94.4% de empleados reconoce que los programas de capacitación reducen riesgos. Las organizaciones deben implementar simulaciones periódicas, no solo charlas teóricas.
3. Herramientas como BlackPhish demuestran lo fácil que es crear ataques convincentes. Las defensas deben actualizarse continuamente para mantenerse efectivas.



REFERENCIAS

- Guía Actividad Semana 5. (2024). *Uso de la herramienta Blackphish*. Material didáctico del curso.
- IBM. (2013). *The 2013 IBM Cyber Security Intelligence Index*. IBM Security Services.
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100. https://doi.org/10.1145/1290958.1290968
- Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Namin, A. S. (2020). How social engineers use persuasion principles during vishing attacks. *Information & Computer Security*.
- Organización de los Estados Americanos [OEA]. (2019). *Estado de la ciberseguridad en el Sistema Financiero Mexicano*. http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf


GRACIAS