KALI LINUX: INTRODUCCIÓN AL HACKING ÉTICO

ÍNDICE

¿Qué es el Hacking Ético?

Práctica simulada

Ataques controlados para detectar y corregir vulnerabilidades en los sistemas de organización.

Beneficios a las empresas

Tipos de hackers

Sombrero negro, sombrero blanco y sombrero gris.

Metodología del Hacking Ético

Reconocimiento

Recolección de información sobre el objetivo mediante técnicas pasivas y activas.

Escaneo

Análisis técnico para identificar vulnerabilidades potenciales en sistemas.

Explotación

Aprovechamiento controlado de vulnerabilidades sin causar daños reales.

Documentación

Registro detallado de hallazgos y recomendaciones para su corrección.

Introducción a Kali Linux

- Distribución de GNU/Linux basada en Debian.
- Creado en 2013 a partir de BackTrack.
- Más de 600 herramientas, FOSS y altamente personalizable.
- La mejor alternativa a Parrot Security OS, BackBox o BlackArch Linux.

Instalación y Configuración Inicial

1

Requisitos mínimos:

Requisitos mínimos: 10 GB disco, 512 MB RAM, procesador compatible. Más RAM recomendada para herramientas.

2

Modos comunes:

Modos comunes: Live USB para pruebas rápidas; Máquina Virtual para entornos seguros; WSL para integración en Windows.

3

Configuración:

Configuración: Red mediante DHCP o manual. Actualizaciones via terminal con *apt update* y *upgrade*.

4

Instantáneas:

Instantáneas: Guarda estados en máquinas virtuales para revertir cambios fáciles y seguros.

5

Configuración GUI (opcional)

Personalizar el entorno: Kali es totalmente personalizable y se puede ajustar a todo tipo de entornos, en este caso utilizaremos Bspwm (https://github.com/r1vs3c/auto-bspwm).

Herramientas de Kali

Kali Linux

Sistema operativo especializado con más de 600 herramientas preinstaladas.

Metasploit

Framework completo para desarrollo y ejecución de exploits.

Wireshark y Nmap

Para análisis de tráfico y escaneo avanzado de redes y protocolos.

Hydra

Cracker de inicios de sesión con capacidad de multithreading y ataques de diccionario

Aircrack-ng

Para monitorización y auditorias de redes inalámbricas

Autopsy

Realización de análisis forense digital

Hashcat

Potente hash cracker que soporta +350 tipos de hash y capacidad de computo con GPU

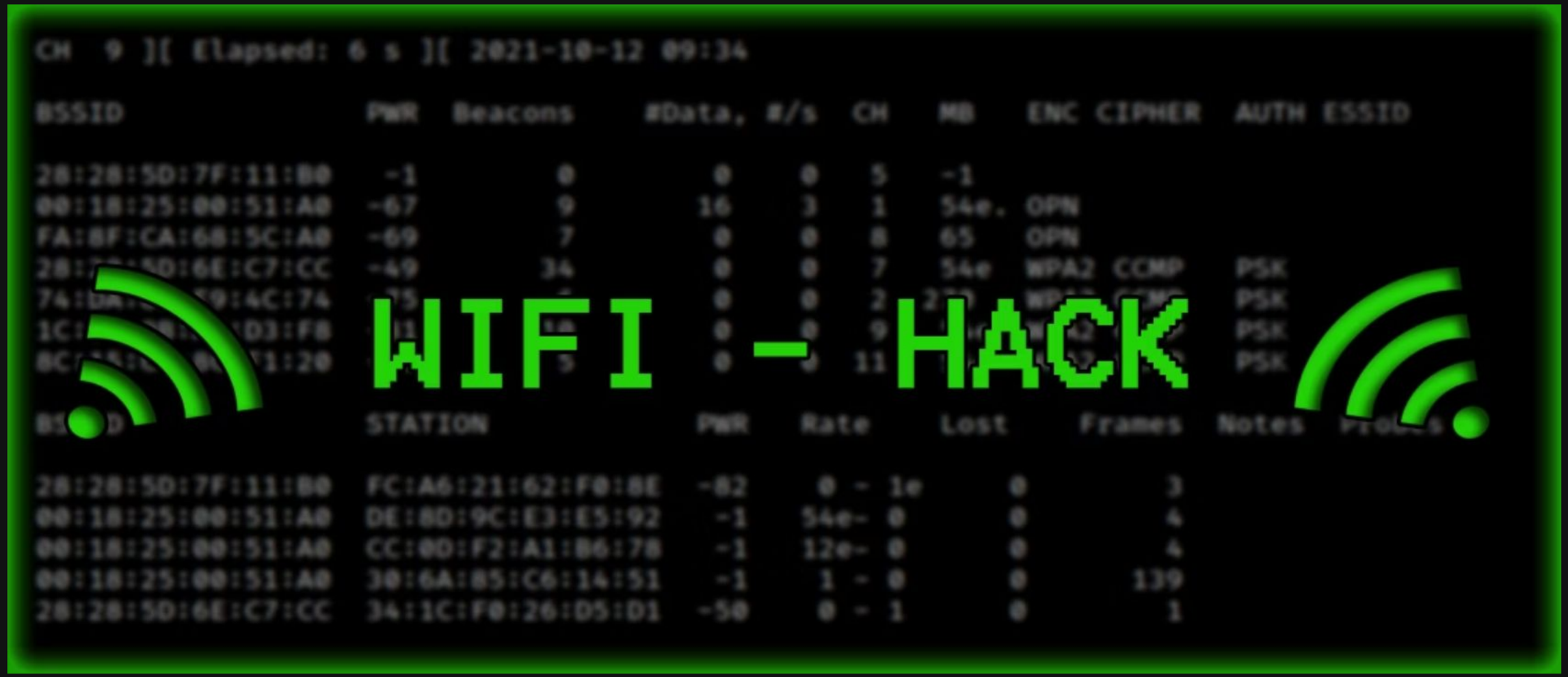
SQLmap

Para detectar y explotar vulnerabilidades SQLinjection

Social Engineering Toolkit (SET)

Kit de herramientas para el desarrollo de estrategias de ingeniería social

Demo Práctica



Recursos de aprendizaje

TryHackMe

Plataforma interactiva con laboratorios prácticos para todos los niveles.

Hack The Box

Entorno para practicar penetration testing con máquinas reales + cursos de especialización + certificaciones.

VulnHub

Plataforma que recopila máquinas virtuales preparadas para importar y explotar.

Youtube

Hay gran cantidad de recursos en youtube de casi todos los niveles, desde el más básico hasta lo más complejo.

A-to-Z-Vulnerabilitie s

Repositorio de GitHub que recopila +100 tipos de vulnerabilidades con su explicación y casos prácticos junto con recursos y herramientas.

HackSplaining

Página web con gran cantidad de vulnerabilidades, sobre todo web, con explicación. Además, es interactiva, lo que permite aprender de forma práctica.

Exploit Database

Una base de datos que recopila miles de exploits de forma organizada y accesible desde una web.

VulDB

La base de datos de vulnerabilidades más grande actualmente.

Certificaciones

Junior Penetration Tester

INE Security - **200€ aprox**

Certified Ethical Hacker

EC-Council - **1496,77€**

Certified Information Systems Security Profesional

ISC2 - **650€ a 665€**

Offensive Security Certified Professional

OffSec - **$1,749**

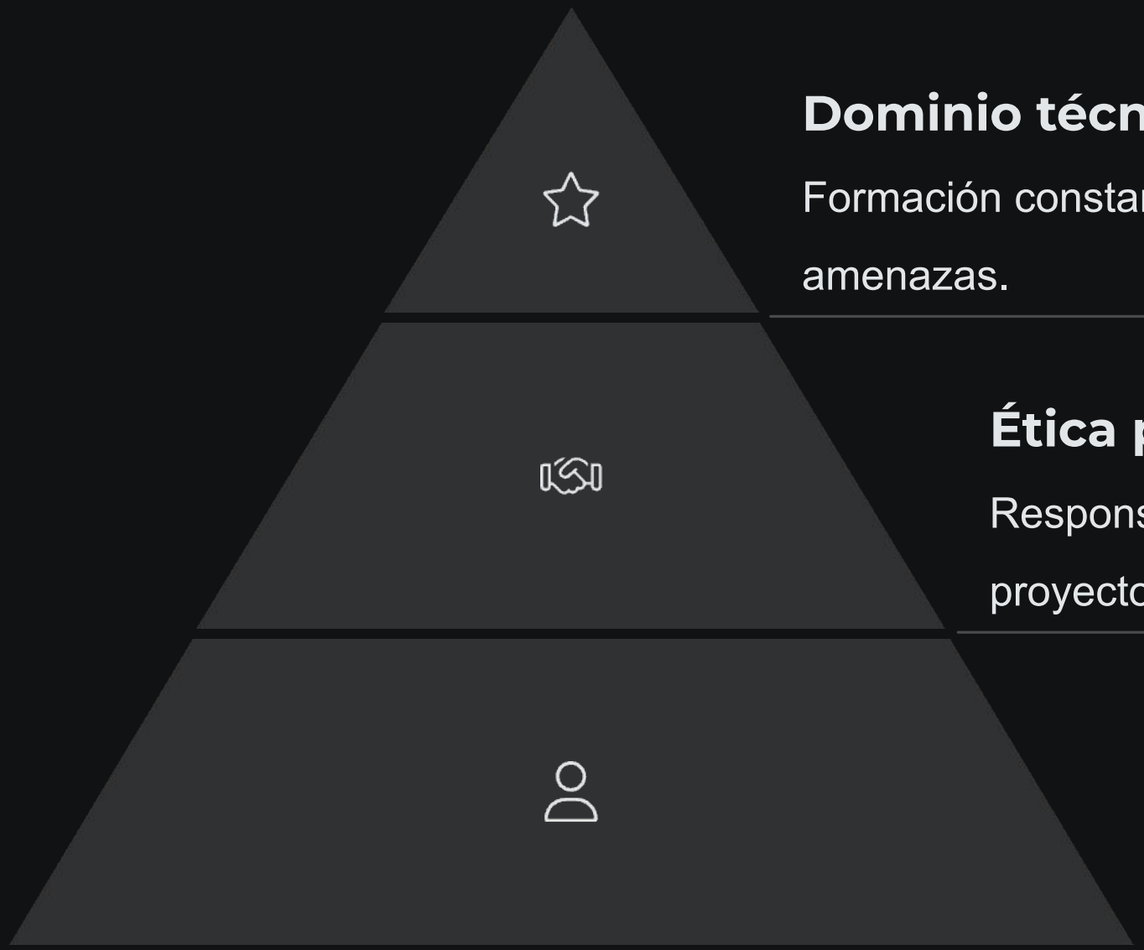
Offensive Security Web Expert

OffSec - **$1,749**

Offensive Security Experienced Penetration

OffSec - **$1,749**

Conclusiones



Dominio técnico

Formación constante en nuevas tecnologías y amenazas.

Ética profesional

Responsabilidad y confidencialidad en cada proyecto.

Comunidad activa

Participación en foros, eventos y plataformas especializadas.