CHARLA KALI LINUX: INTRODUCCIÓN AL HACKING ÉTICO

1. Bienvenida y objetivos de la charla

2. ¿Qué es el hacking ético?

- Definición y diferencias con el hacking malicioso.

El hacking ético, también conocido como piratería ética o hacking de sombrero blanco, es una práctica mediante la cual especialistas en seguridad informática simulan ciberataques para detectar y corregir vulnerabilidades en los sistemas de una organización [1][2][3]. A diferencia de los hackers maliciosos (sombrero negro), los hackers éticos actúan con autorización, siguiendo un contrato que garantiza la confidencialidad, el alcance limitado y el respeto a la legalidad vigente [2][3][4].

Su propósito es proteger la infraestructura digital de las empresas, prevenir ataques reales y reforzar las políticas de seguridad. Para lograrlo, emplean los mismos conocimientos, técnicas y herramientas que los ciberdelincuentes, pero con fines preventivos y constructivos [1][4].

Los procesos que siguen suelen estructurarse en fases [3]:

1. Recolección de información
2. Escaneo de vulnerabilidades
3. Acceso y explotación controlada
4. Informe de hallazgos y recomendaciones

Este tipo de prácticas ofrece múltiples beneficios a las empresas [1][3][4]:

- Identificación y corrección de fallos de seguridad antes de que sean explotados.
- Prevención de pérdidas económicas, daños reputacionales y fugas de información.
- Mejora del cumplimiento normativo (como el RGPD).
- Optimización de inversiones en ciberseguridad.

El hacking ético ha ganado protagonismo en un entorno digital cada vez más interconectado, donde los datos personales y corporativos se almacenan en plataformas expuestas a riesgos constantes [2][3]. Empresas tecnológicas, financieras y otras organizaciones digitalizadas recurren cada vez más a estos expertos, bien como personal interno o a través de consultoras externas especializadas [1][3][4].

Existen tres tipos principales de hackers según su ética y propósito [4]:

- Sombrero negro: piratas informáticos con fines delictivos.
- Sombrero blanco: hackers éticos que buscan proteger.
- Sombrero gris: actúan entre ambos extremos, a veces sin permiso, pero sin fines maliciosos.

Además de las auditorías técnicas, los hackers éticos también promueven la educación del personal en buenas prácticas de seguridad, como el uso de contraseñas robustas o la detección de intentos de ingeniería social [1][2].

El perfil del hacker ético combina conocimientos profundos de redes, sistemas, normativas y comportamiento humano, lo que le convierte en un profesional cada vez más demandado y valorado en el mercado laboral [2][4]. También pueden participar en programas de recompensas por detección de errores ("bug bounty"), ofrecidos por grandes empresas tecnológicas [4].

3. Introducción a Kali Linux

Kali Linux es una distribución de GNU/Linux, sucesora de BackTrack Linux, diseñada específicamente para pruebas de penetración y auditoría de seguridad. Desarrollada y mantenida por Offensive Security, se ha convertido en una herramienta esencial para profesionales de la ciberseguridad. [5]

- **Origen y Evolución:** Nació en marzo de 2013 como una reestructuración de BackTrack, buscando mayor estabilidad y un ciclo de actualización continuo ("rolling release"). Se basa en Debian, lo que le proporciona una base sólida y confiable. [6]
- **Características Clave:** Se destaca por su vasta colección de más de 600 herramientas preinstaladas para diversas tareas de seguridad (escaneo de redes, análisis de vulnerabilidades, forense digital, etc.). Es gratuito, de código abierto, soporta múltiples plataformas (escritorio, ARM con NetHunter) y es altamente personalizable. Implementa un modelo de usuario no root por defecto para mejorar la seguridad y permite arrancar en modo "live" desde USB.
- **Comparativa:** Aunque existen otras distribuciones de pentesting como Parrot Security OS (también basado en Debian, con enfoque en privacidad), BackBox (basado en Ubuntu, más ligero) y BlackArch Linux (basado en Arch, con un repositorio masivo de herramientas), Kali Linux es la más reconocida y ampliamente utilizada, considerada por muchos como el estándar de la industria por su comprensividad y el respaldo de Offensive Security.

4. Instalación y configuración inicial

La instalación de Kali Linux ofrece flexibilidad para adaptarse a diferentes necesidades y entornos de trabajo.

Requisitos de Sistema y Modos de Instalación:

Los requisitos mínimos básicos para Kali Linux son bastante modestos, permitiendo su ejecución en hardware antiguo o con recursos limitados. Generalmente, se recomienda al menos:

- **Espacio en Disco:** 10 GB (aunque se sugieren 20-30 GB para instalaciones completas o con herramientas adicionales).
- **RAM:** 512 MB para arquitecturas i386 y amd64 (se recomiendan 2 GB o más, especialmente para herramientas como Metasploit).
- **Procesador:** Un procesador compatible.

Existen varios modos de instalación comunes:

- **Live USB:** Permite ejecutar Kali directamente desde una unidad USB sin instalarlo en el disco duro. Es ideal para pruebas rápidas, análisis forenses sin dejar rastro en el sistema anfitrión, o para probar Kali antes de instalarlo. Se puede crear con herramientas como Etcher o Rufus (en Windows) o el comando dd (en Linux).
- **Máquina Virtual:** Una de las formas más populares y recomendadas de usar Kali. Se instala sobre un hipervisor como VirtualBox o VMware. Esto aísla el entorno de pruebas del sistema operativo principal, ofreciendo seguridad y facilidad para gestionar diferentes configuraciones o volver a estados anteriores. Los requisitos de hardware asignados dependen de los recursos disponibles en la máquina anfitriona.
- **WSL (Windows Subsystem for Linux):** Permite ejecutar un entorno Kali Linux integrado en Windows 10 o 11. Es una opción conveniente para usuarios de Windows que necesitan acceder a las herramientas de Kali sin una máquina virtual completa. La instalación se realiza a través de la Microsoft Store o comandos WSL.

Configuración de Red y Actualizaciones:

Tras la instalación, es crucial configurar la red para obtener conectividad a Internet o a redes locales. Esto puede hacerse mediante DHCP (obtención automática de IP) o configuración manual editando archivos de configuración. En entornos gráficos, también se puede gestionar a través del administrador de red.

Mantener el sistema actualizado es fundamental por seguridad y para tener acceso a las últimas herramientas y funcionalidades. Las actualizaciones se realizan principalmente a través de la terminal utilizando los comandos:

- `sudo apt update`: Actualiza la lista de paquetes disponibles en los repositorios.
- `sudo apt upgrade` o `sudo apt full-upgrade`: Actualiza los paquetes instalados a sus últimas versiones. `full-upgrade` gestiona mejor los cambios de dependencias.

Creación de Instantáneas (Snapshots) para Entornos Virtuales:

Las instantáneas son una característica muy valiosa al ejecutar Kali Linux en máquinas virtuales. Permiten guardar el estado actual de la máquina virtual en un momento dado. Esto es extremadamente útil antes de realizar cambios significativos o potencialmente inestables (como instalaciones de software o configuraciones complejas), ya que permite revertir fácilmente al estado guardado si algo sale mal, sin necesidad de reinstalar el sistema operativo.

Configuración del UI:

Con kali podemos configurar completamente la interfaz de usuario a nuestro gusto y necesidades ya que soporta multitud de entornos. Para la demo práctica hemos utilizado este entorno autoconfigurado: <https://github.com/r1vs3c/auto-bspwm>. Aunque puedes usar el de tu preferencia.

5. Estructura y organización de herramientas en Kali

- Categorías principales (reconocimiento, escaneo, explotación, post-explotación, forense, etc.)
- Navegación y búsqueda de herramientas (“kali-menu”, apt, searchsploit)
- Personalización del entorno (alias, scripts, plugins)

Kali Linux incluye más de 600 herramientas preinstaladas como:

- **Metasploit**: Framework completo para desarrollo y ejecución de exploits.
- **Wireshark y Nmap**: Para análisis de tráfico y escaneo avanzado de redes.
- **Hydra**: Cracker de inicios de sesión con capacidad de multithreading.
- **Aircrack-ng**: Para auditorías de redes inalámbricas.
- **Autopsy**: Herramienta de análisis forense digital.
- **Hashcat**: Potente cracker de hashes con soporte GPU y mas de 350 algoritmos de hashing.
- **SQLmap**: Para detectar y explotar vulnerabilidades SQL injection.
- **Social Engineering Toolkit (SET)**: Para estrategias de ingeniería social.

6. Demo práctica (breve)

Vamos a realizar una demo práctica de auditoría de redes inalámbricas:

https://github.com/Adriansolier322/Aircrack-ng_Tuto

7. Recursos de aprendizaje y certificaciones

Recursos de aprendizaje:

- [TryHackMe](#): Plataforma interactiva con laboratorios prácticos.
- [VulnHub](#): Máquinas virtuales preparadas para practicar.
- [Hack The Box](#): Entorno para practicar penetration testing.
- [YouTube](#): Gran cantidad de tutoriales y recursos.
- [A-to-Z-Vulnerabilitie](#): Repositorio que explica y recopila +100 tipos de vulnerabilidades
- [HackSplaining](#): Vulnerabilidades web con explicación interactiva.
- [Exploit Database](#): Base de datos de exploits organizada.
- [VulDB](#): La mayor base de datos de vulnerabilidades.

Certificaciones relevantes:

- **eJPT** (Junior Penetration Tester) - INE Security (~200€)
- **CEH** (Certified Ethical Hacker) - EC-Council (~1,496€)
- **CISSP** (Certified Information Systems Security Professional) - ISC2 (650-665€)
- **OSCP** (Offensive Security Certified Professional) - Offensive Security (\$1,749)
- **OSWE** (Offensive Security Web Expert) - Offensive Security (\$1,749)
- **OSEP** (Offensive Security Experienced Penetration) - Offensive Security (\$1,749)

Otros recursos:

- **DeepHacking**: Blog sobre ciberseguridad 100% español
- **Incibe**: Instituto nacional de ciberseguridad
- **Awesome-Hacking-Resources**: Repositorio que recopila muchísimos recursos de hacking

8. Conclusiones y preguntas

[Referencias]

- [1] <https://www.telefonica.com/es/sala-comunicacion/blog/hacking-etico-que-es/>
- [2] <https://www.incibe.es/cd2026/talento-hacker/blog/descubre-que-es-el-hacking-etico>
- [3] <https://www.incibe.es/empresas/blog/el-hacking-etico-y-sus-beneficios-el-mundo-empresarial>
- [4] <https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/>
- [5] <https://www.kali.org/>
- [6] <https://datascientest.com/es/kali-linux-todo-lo-que-necesitas-saber>