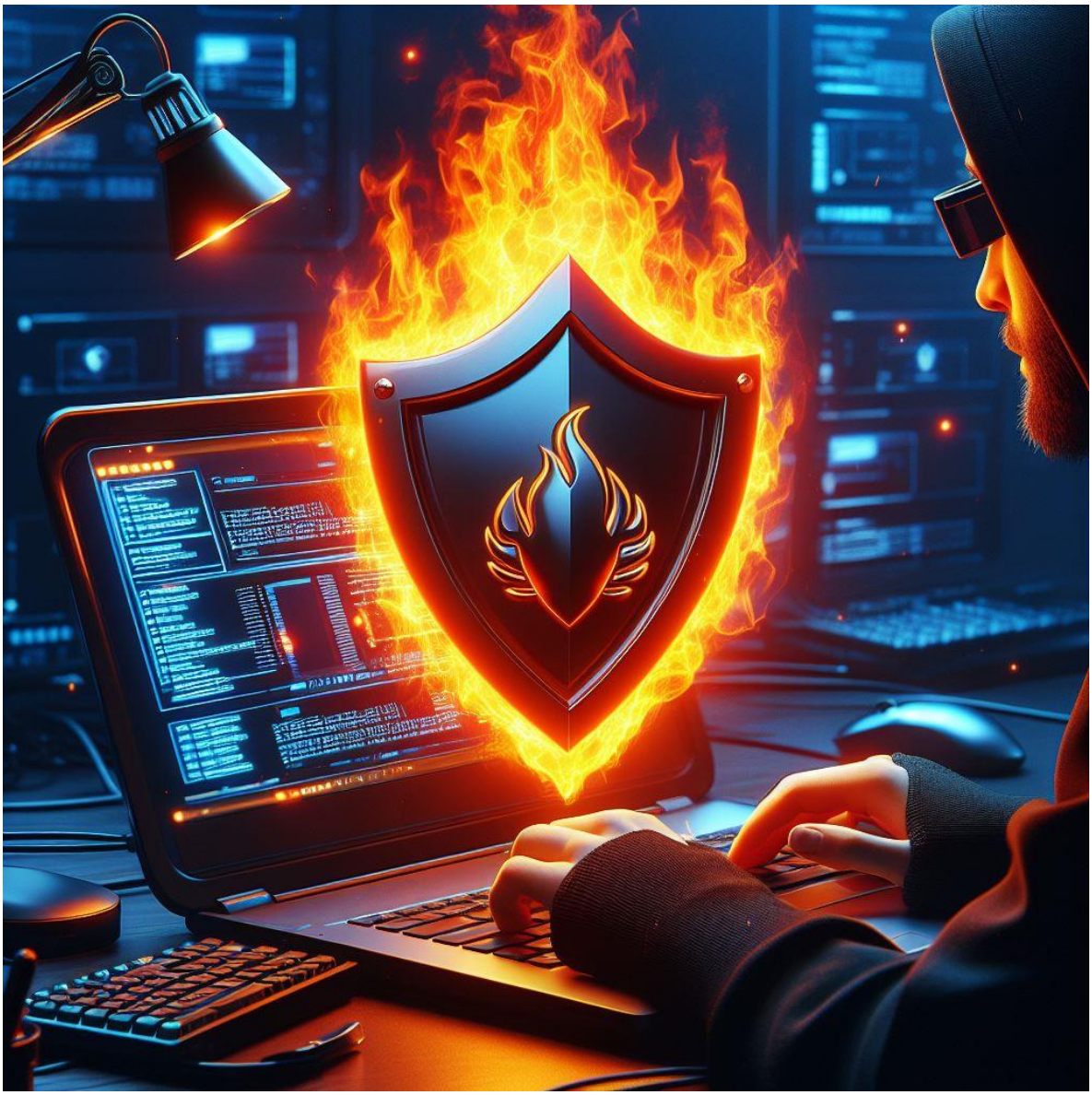
HERRAMIENTAS DE HAKING



Los hackers utilizan una amplia variedad de software y herramientas para llevar a cabo sus actividades, ya sea con fines éticos o maliciosos. Aquí tienes una lista de algunas de las herramientas más comunes:

Sistemas Operativos
1. **Kali Linux**: Una distribución de Linux diseñada específicamente para pruebas de penetración y auditorías de seguridad. Incluye numerosas herramientas preinstaladas para hacking y análisis de seguridad.
2. **Parrot Security OS**: Otra distribución de Linux orientada a la seguridad y el hacking ético, similar a Kali Linux pero con un enfoque en la privacidad y la protección de datos.

Escaneo y Enumeración
1. **Nmap**: Una herramienta de código abierto para el escaneo de puertos y la detección de redes, útil para mapear la red y encontrar dispositivos conectados.
2. **Wireshark**: Un analizador de paquetes de red que permite capturar y examinar datos en tiempo real, útil para diagnosticar problemas de red y análisis de tráfico.

Explotación de Vulnerabilidades
1. **Metasploit Framework**: Una herramienta poderosa para desarrollar y ejecutar exploits

contra máquinas remotas, utilizada tanto por hackers éticos como por hackers maliciosos.
2. **BeEF (Browser Exploitation Framework)**: Una herramienta que permite lanzar ataques dirigidos a navegadores web y explotar vulnerabilidades del lado del cliente.

Criptografía y Fuerza Bruta
1. **John the Ripper**: Una herramienta de cracking de contraseñas que detecta contraseñas débiles en bases de datos de hash.
2. **Hashcat**: Un crackeador de contraseñas avanzado que soporta una amplia variedad de algoritmos de hash y métodos de ataque.

Ingeniería Social y Phishing
1. **SET (Social-Engineer Toolkit)**: Una herramienta diseñada para realizar ataques de ingeniería social, como phishing, spear phishing y ataques basados en USB.
2. **King Phisher**: Una herramienta para simular ataques de phishing y medir la efectividad de los programas de concienciación de seguridad.

Escalamiento de Privilegios y Persistencia
1. **Privilege Escalation Exploits**: Scripts y herramientas específicas para explotar vulnerabilidades que permiten a un atacante obtener privilegios elevados en un sistema.
2. **Rootkits**: Herramientas utilizadas para ocultar la presencia de malware o accesos no autorizados, permitiendo la persistencia en un sistema comprometido.

Análisis y Monitoreo de Vulnerabilidades
1. **OpenVAS**: Un escáner de vulnerabilidades de código abierto que permite identificar fallos de seguridad en sistemas y aplicaciones.
2. **Nessus**: Un escáner de vulnerabilidades comercial ampliamente utilizado para detectar problemas de seguridad en redes y sistemas.

Redes Inalámbricas
1. **Aircrack-ng**: Un conjunto de herramientas para evaluar la seguridad de redes Wi-Fi, incluyendo la captura de paquetes y el crackeo de contraseñas WEP/WPA.

2. **Reaver**: Una herramienta que explota la vulnerabilidad WPS para recuperar la clave WPA/WPA2 de una red Wi-Fi.

Herramientas de Recolección de Información
1. **Maltego**: Una herramienta para el análisis y la recolección de información de código abierto, útil para la inteligencia de amenazas y la investigación forense.
2. **Recon-ng**: Una herramienta de recolección de información diseñada para ser utilizada en el reconocimiento previo a un ataque.

Estas herramientas son esenciales para hackers y profesionales de la seguridad informática para probar, asegurar y, en algunos casos, comprometer sistemas y redes. Sin embargo, es importante recordar que el uso de estas herramientas debe estar dentro de los límites legales y éticos.