

|  |  |
| --- | --- |
| herramienta | Descripción |
| NMap | Escáner de red que identifica host activos, puerto abiertos servicios y sistemas operativos ideal para la fase de reconocimiento. |
| OpenVAS | Plataforma completa que se utiliza para escaneo de vulnerabilidades.detecta fallos conocidos en el software, configuraciones inseguras y errores comunes. |
| Nikto | Analiza servidores web en busca de configuraciones inseguras, archivos peligrosos y vulnerabilidades comunes. |

Anexos

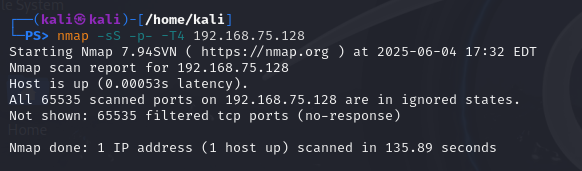
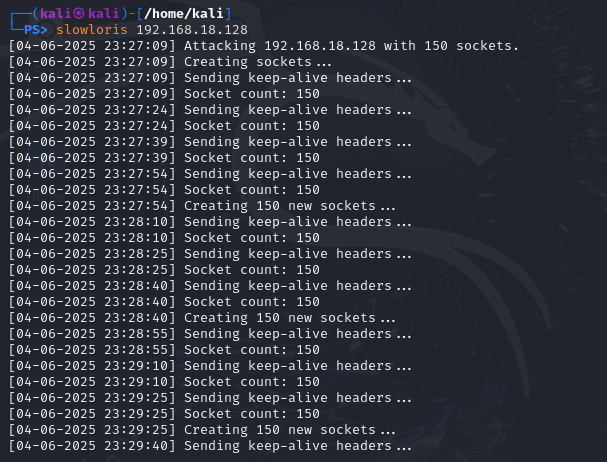


Ilustración 2 La imagen muestra un ataque de tipo **Slowloris** ejecutado desde Kali Linux contra el host 192.168.18.128. Este ataque se caracteriza por abrir múltiples conexiones HTTP (en este caso, 150 sockets) y mantenerlas abiertas el mayor tiempo posible enviando encabezados **keep-alive** de forma periódica. El objetivo del ataque es saturar los recursos del servidor objetivo, impidiendo que atienda conexiones legítimas. Este tipo de ataque es especialmente efectivo contra servidores web mal configurados o sin protección contra conexiones lentas y persistentes.

Figure 1 La imagen muestra el resultado de un escaneo de puertos realizado con la herramienta **Nmap** desde un sistema Kali Linux. El comando usado (nmap -sS -p- -T4 192.168.75.128) indica un escaneo SYN de todos los puertos TCP (-p-) con velocidad moderada (-T4) hacia la IP 192.168.75.128. El resultado informa que el host está activo, pero todos los 65,535 puertos escaneados están en estados "ignorados" o filtrados, lo que significa que no respondieron, probablemente debido a un firewall que bloquea las conexiones.

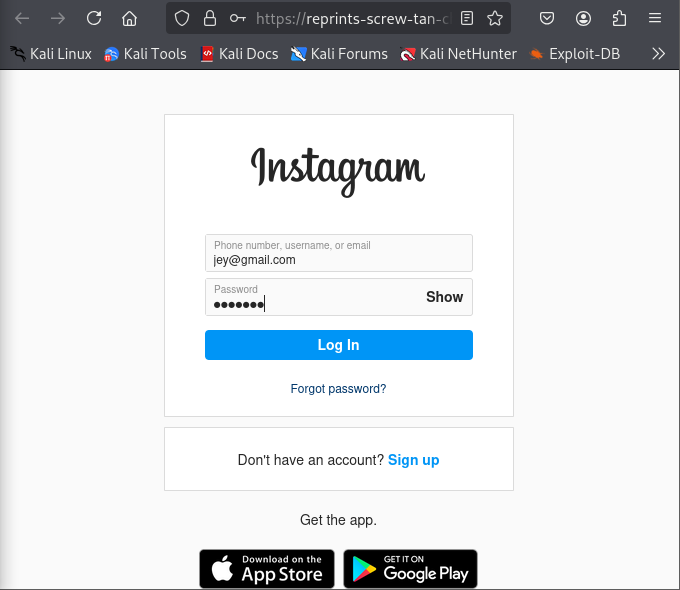


Ilustración 3

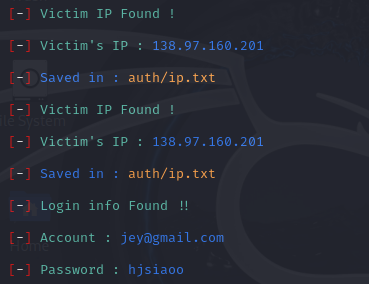


Ilustración 4 muestra los resultados de una posible recolección de credenciales a través de una técnica de **phishing o captura de tráfico malicioso** en Kali Linux. El sistema ha detectado la dirección IP de la víctima (138.97.160.201) y ha guardado esta información en el archivo auth/ip.txt. Además, se ha capturado información de inicio de sesión que se muestra en la Ilustración 3, incluyendo una cuenta de correo electrónico (jey@gmail.com) y una contraseña (hjsiaoo). Este tipo de actividad refleja un entorno de pruebas ofensivas o de simulación de ataques con fines educativos o de auditoría de seguridad, pero debe realizarse siempre con autorización, ya que en contextos reales es ilegal y éticamente inaceptable.

**Recomendaciones**

Se recomienda tener un certificado web, una herramienta anti denegación de servicios, la instalación de un cortafuego y un detector de intruso.

También se recomienda la constante actualización de pluggins y del CMS, la realización de cambios periódicos en la base de datos.