**Análisis de vulnerabilidades (tipo Nessus)**

# LAS 15 MEJORES HERRAMIENTAS PARA REALIZAR ANÁLISIS DE VULNERABILIDADES INTERNAS Y HACKEAR REDES CORPORATIVAS

El pentesting es uno de los procesos más importantes en ciberseguridad, ya que permite realizar un correcto análisis de vulnerabilidades internas para determinar cuál es la mejor forma de abordar las fallas encontradas. Esta es una labor esencial para los especialistas, por lo que es necesario reflexionar sobre cuáles son las mejores herramientas disponibles.

En esta ocasión, los especialistas en análisis de vulnerabilidades internas del Instituto Internacional de Seguridad Cibernética [(IICS)](https://www.iicybersecurity.com/ciberseguridad-ciberdefensa-servicios.html) le mostrarán las 15 mejores herramientas para realizar este tipo de escaneo en redes corporativas. Las herramientas mostradas a continuación son utilizadas activamente por una amplia gama de especialistas, por lo que será útil para todos los interesados conocer sus capacidades y dominarlas a la perfección.

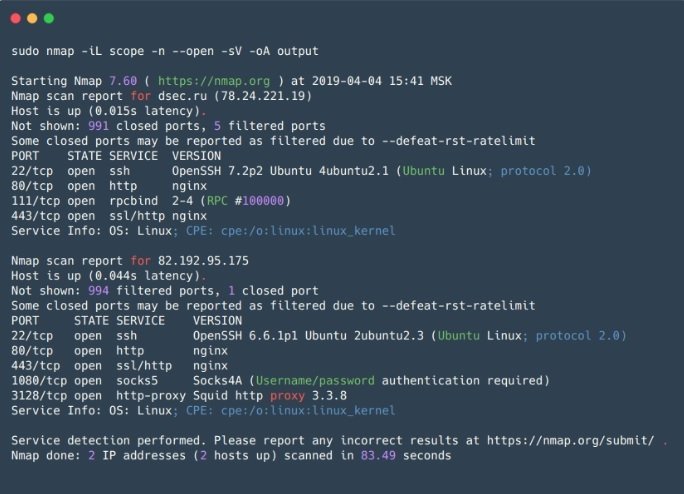
## **NMAP**

Esta es una utilidad de escaneo de red de código abierto y una de las herramientas de análisis de vulnerabilidades internas más populares en el mundo de la ciberseguridad. Nmap se usa principalmente para el escaneo de puertos, aunque tiene muchas otras características muy útiles para los investigadores, incluyendo el servicio de escucha de puertos abiertos e identificación de vulnerabilidades de seguridad.

Nmap permite a los investigadores elaborar un mapa de red detallado, obtener la mayor cantidad de información sobre la ejecución de servicios en los hosts de la red y verificar de manera proactiva algunas vulnerabilidades conocidas.

***Ventajas:*** La herramienta funciona rápidamente con una pequeña variedad de hosts, además cuenta con una configuración flexible para sacar explotar al máximo todas sus capacidades. Nmap también cuenta con conjuntos predefinidos de scripts para diferentes tareas y arroja sus resultados en cinco formatos diferentes, incluyendo XML.

***Desventajas:*** La principal desventaja de Nmap es que la información sobre hosts en particular no estará disponible hasta que se complete el escaneo de todo el grupo. Además, durante los escaneos se envían paquetes SYN al puerto objetivo, lo que impacta directamente en el rendimiento del escaneo general en comparación con otras soluciones para el análisis de vulnerabilidades internas.

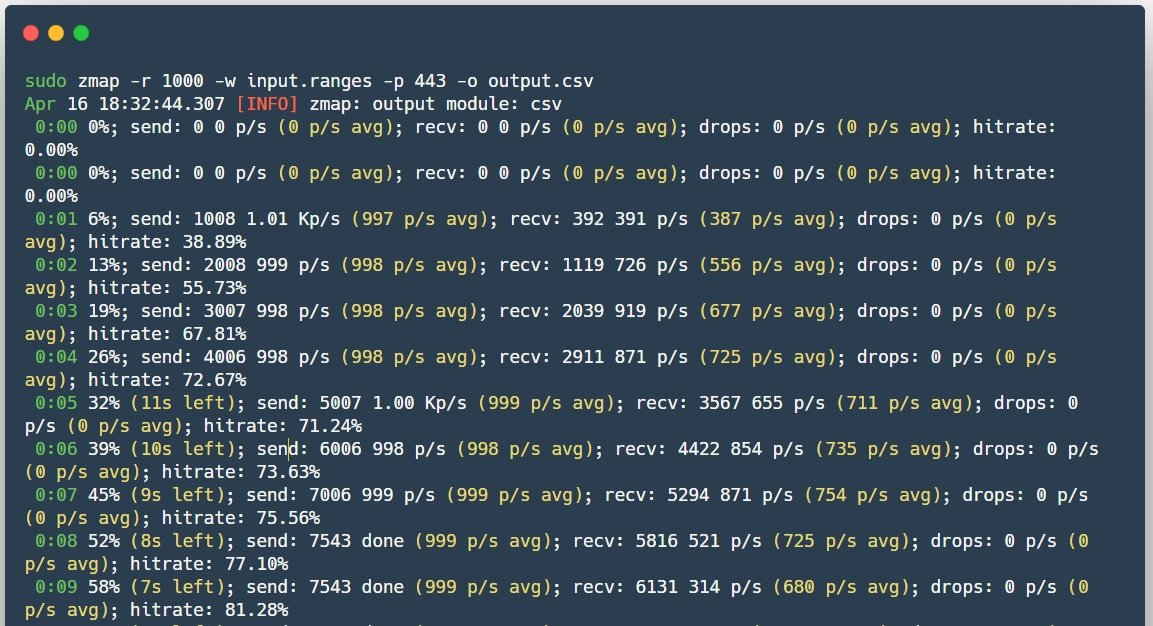


## **ZMAP**

Zmap (no confundir con ZenMap) también es un escáner de código abierto creado como una alternativa más rápida a Nmap. A diferencia de su contraparte, Zmap no espera hasta que se devuelva una respuesta al enviar paquetes SYN, sino que continúa escaneando, esperando en paralelo las respuestas de todos los hosts, por lo que en realidad no mantiene el estado de la conexión.

***Ventajas:*** Entre las mejores características de Zmap se encuentran su velocidad de escaneo, la generación de tramas Ethernet sin pasar por la pila del sistema.

***Desventajas:*** La principal desventaja es que el uso de esta herramienta puede causar una denegación de servicio (DoS) al equipo de red, por ejemplo, para deshabilitar enrutadores intermedios, a pesar de la carga distribuida, ya que todos los paquetes pasarán por un enrutador.

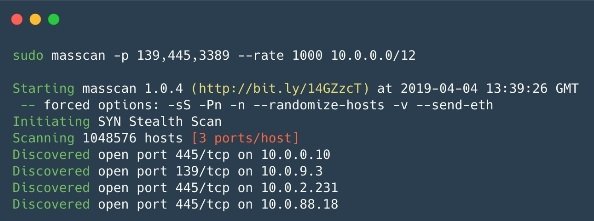


## **MASSCAN**

Masscan es un escáner de código abierto que fue creado con un objetivo en mente: escanear Internet aún más rápido (en menos de 6 minutos a una velocidad de cerca 10 millones de paquetes por segundo). Acorde a los expertos en análisis de vulnerabilidades internas, esta herramienta funciona casi igual que Zmap, solo que a una mejor velocidad.

***Ventajas:*** La sintaxis de Masscan es similar a Nmap y el programa también admite algunas opciones compatibles con Nmap, además de su destacada velocidad de operación que lo convierte en uno de los escáneres asincrónicos más rápidos.

***Desventajas:*** De forma similar a Zmap, la carga en la red es demasiado alta, lo que podría conducir a una condición DoS.



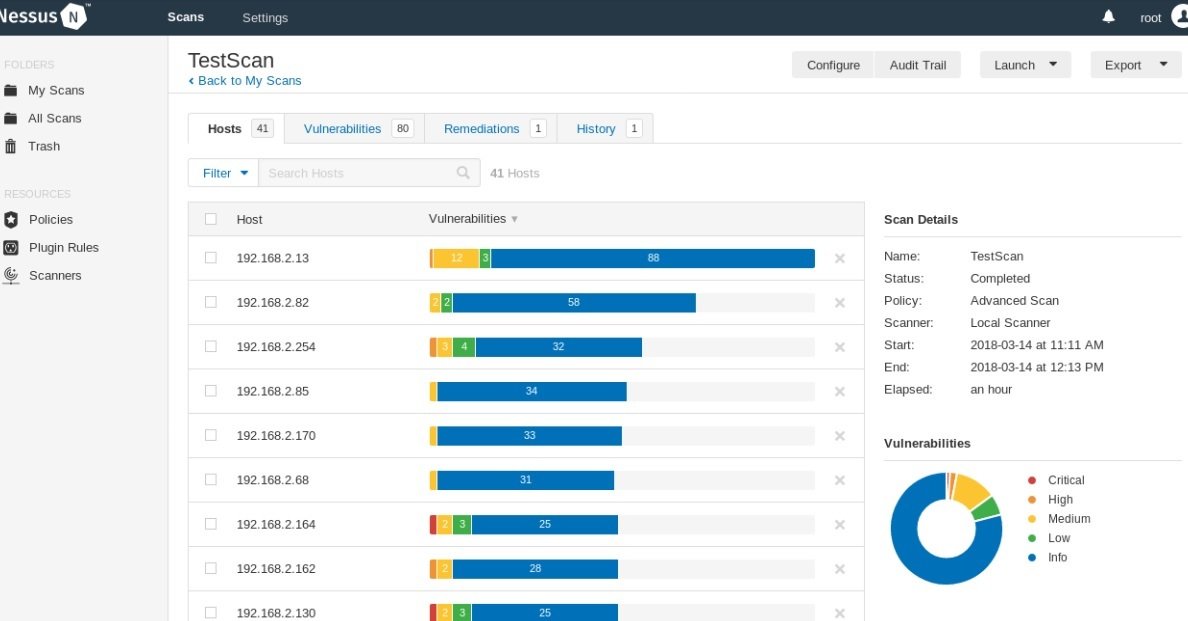
## **NESSUS**

Nessus es un escáner para automatizar la verificación y detección de vulnerabilidades conocidas en el sistema escaneado. Acorde a los expertos en análisis de vulnerabilidades internas, existe una versión gratuita de Nessus Home que permite escanear hasta 16 direcciones IP con la misma velocidad y análisis detallado que la versión de pago.

La herramienta es capaz de identificar versiones vulnerables de servicios o servidores, detectar errores en la configuración del sistema y contraseñas de diccionario de fuerza bruta. Se puede utilizar para determinar la corrección de la configuración del servicio, así como en preparación para la auditoría de PCI DSS.

***Ventajas:*** La herramienta cuenta con scripts separados para cada vulnerabilidad gracias a su base de datos constantemente actualizada. Nessus también arroja resultados en formatos como texto plano, XML, HTML y LaTeX; API Nessus y permite el escaneo de credenciales de Windows o Linux para buscar nuevas actualizaciones.

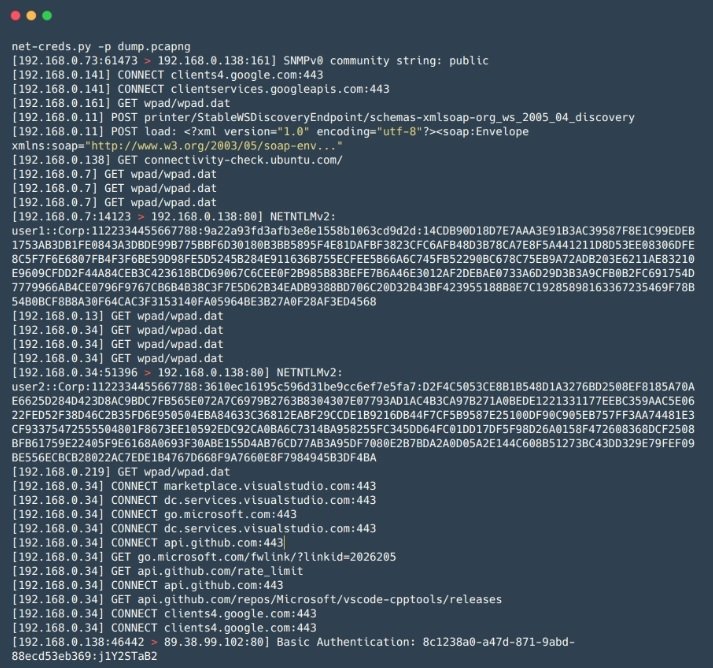
***Desventajas:*** Es posible que se produzcan fallos en el funcionamiento de los sistemas escaneados, sin mencionar que la versión completa de esta herramienta requiere una suscripción.



## **NET-CREDS**

Esta es una herramienta de Python para la recopilación de contraseñas y hashes, así como otros datos relevantes para el análisis de vulnerabilidades internas. Net-Creds es ideal para un rápido análisis de grandes volúmenes de tráfico durante ataques Man-in-The-Middle (MiTM), por ejemplo. (qué son los ataques MiTM -> [Qué es un ataque de Man‑in‑the‑Middle y cómo funciona | WeLiveSecurity](https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/) y ejemplo de ello -> <https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html>

***Ventajas:*** La identificación del servicio se basa en el análisis de paquetes en lugar de identificar un servicio según el puerto utilizado, además de que en realidad es bastante fácil de usar.

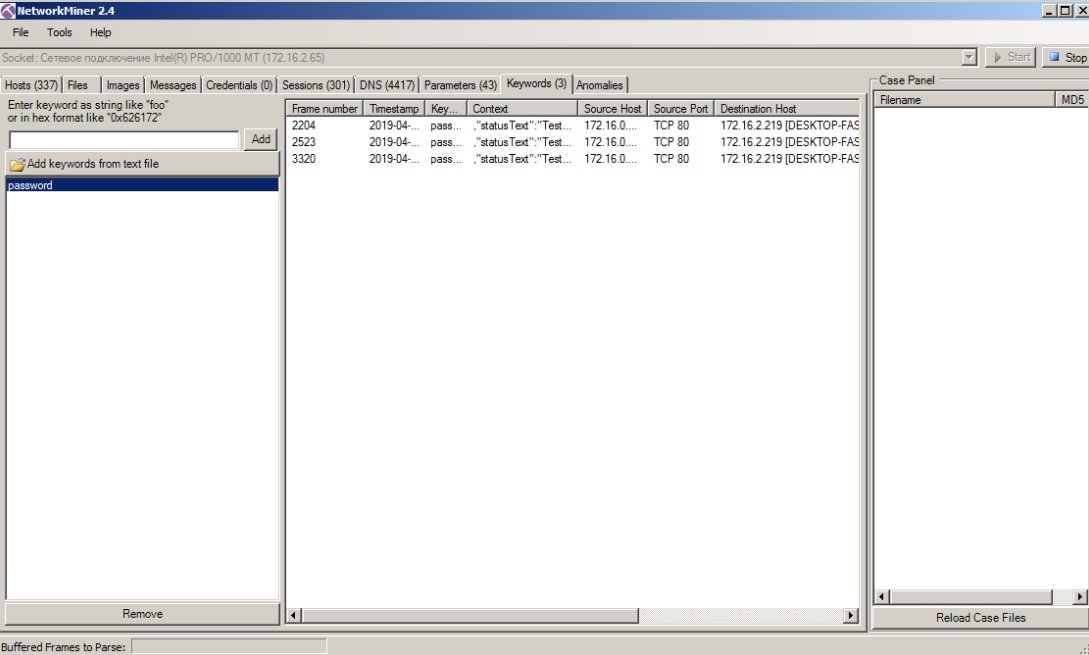


## **NETWORK-MINER**

Este es un análogo de Net-Creds en su principio de funcionamiento, pero tiene una gran variedad de funcionalidades adicionales. Al igual que Net-Creds, Network-miner es ideal para analizar grandes cantidades de tráfico en poco tiempo.

***Ventajas:*** Esta herramienta cuenta con una sofisticada interfaz gráfica y opciones para la visualización y clasificación de datos por grupos, simplificando el análisis de tráfico.

***Desventajas:*** Al igual que Net-Creds, esta herramienta cuenta con una versión gratuita con funciones limitadas, por lo que los investigadores deberán pagar para acceder a una versión completa.



## **MITM6**

Esta es una herramienta para realizar ataques apuntando contra IPv6. En sistemas Windows, la interfaz IPv6 está habilitada por defecto, lo que permite a los analistas configurar el servidor DNS del sistema objetivo empleando paquetes Router Advertisement, lo que permite falsificar el DNS del sistema objetivo.

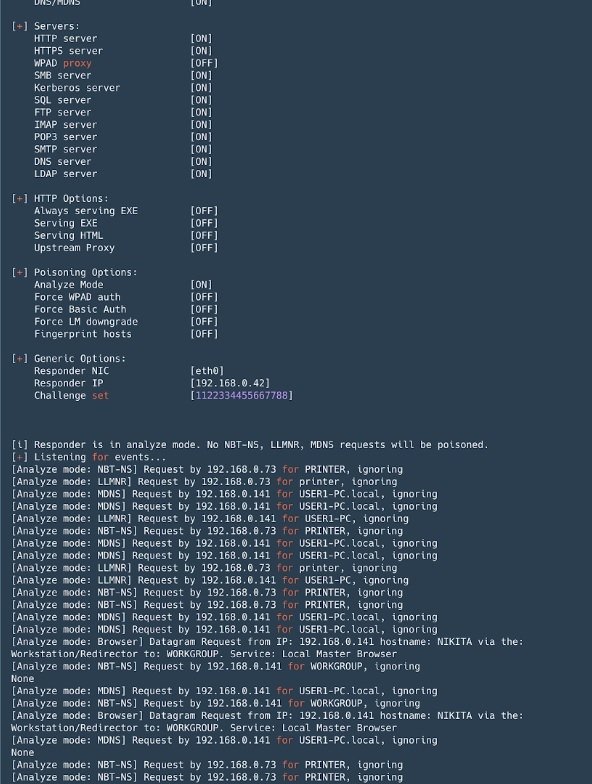
***Ventajas:*** Funciona muy bien en muchas redes debido a la configuración predeterminada de los hosts y las redes de Windows.

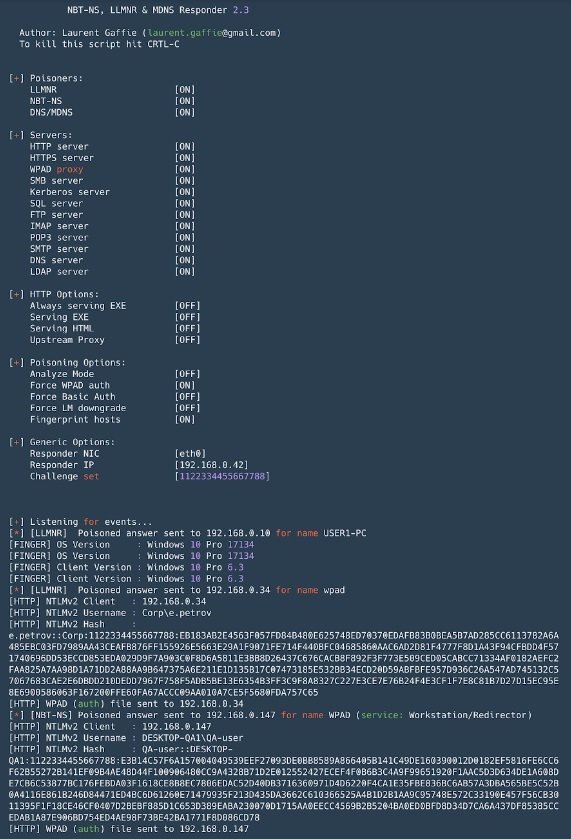
## **RESPONDER**

Esta es una herramienta para la falsificación de protocolos de resolución de nombres (como LLMNR, NetBIOS o MDNS) indispensable para cualquier red de Active Directory. Además de realizar ataques de falsificación, la herramienta puede interceptar la autenticación NTLM e incluye un conjunto de herramientas para recopilar información e implementar ataques NTLM-Relay (más información sobre estos ataques y expiación de vulnerabilidades relacionadas en: [Vulnerabilidad NLTM Relay en MS Windows es ampliamente explotada (cci-entel.cl)](https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1247/)).

***Ventajas:*** Por defecto, la herramienta levanta muchos servidores con soporte de autenticación NTLM: SMB, MSSQL, HTTP, HTTPS, LDAP, FTP, POP3, IMAP y SMTP, además de que permite suplantar DNS en caso de ataques MiTM.

***Desventajas:*** Cuando se ejecuta en sistemas Windows, el enlace del puerto 445 (SMB) presenta algunas dificultades, señalan los especialistas en análisis de vulnerabilidades internas.



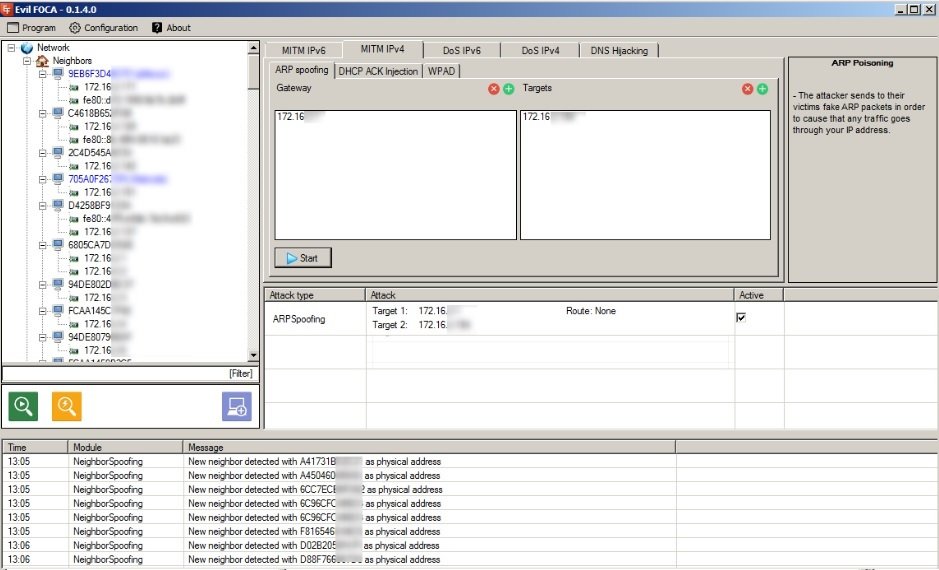


## **EVIL FOCA**

Evil Foca es una herramienta para probar múltiples variantes de ataques contra redes IPv4 e IPv6. La herramienta puede escanear la red local, identificar dispositivos, enrutadores y sus interfaces de red y realizar varios ataques contra los dispositivos conectados.

***Ventajas:*** Esta herramienta es muy útil para ataques DoS y variantes de ataque MiTM (suplantación de ARP, inyección DHCP ACK, ataques SLAAC, suplantación DHCP). Además, se puede realizar un secuestro de DNS y cuenta con una interfaz gráfica muy fácil de usar.

***Desventajas:*** A diferencia de la mayoría de las herramientas, Evil Foca solo funciona en sistemas Windows.

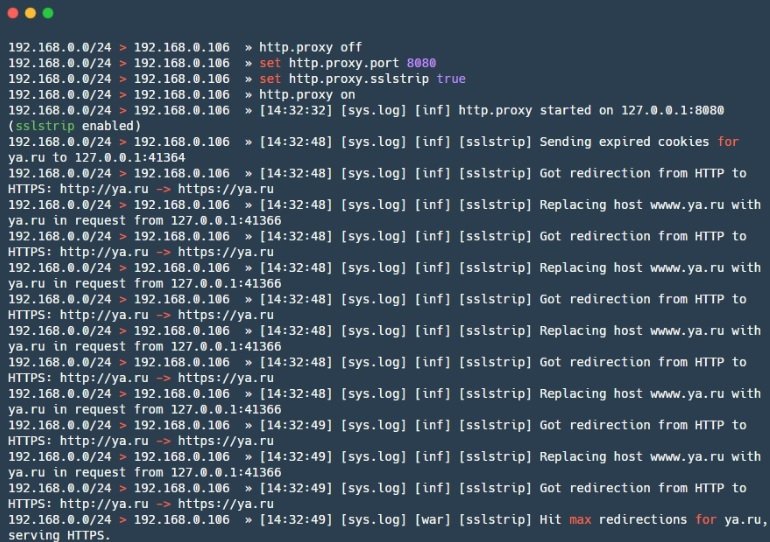


## **BETTERCAP**

Este es un poderoso marco para analizar y atacar redes, y aquí también estamos hablando de ataques a redes inalámbricas, BLE (bluetooth low energy) e incluso ataques MouseJack en dispositivos HID (interfaz humana) inalámbricos. Bettercap también contiene una funcionalidad para recopilar información del tráfico.

***Ventajas:*** La herramienta puede capturar las URLs visitadas y hosts HTTPS, además de que hace posible desplegar ataques MiTM y administrar el tráfico según las necesidades de los investigadores. La herramienta también tiene soporte para caplets, que son archivos que permiten describir ataques complejos y automatizados en un lenguaje de secuencias de comandos.

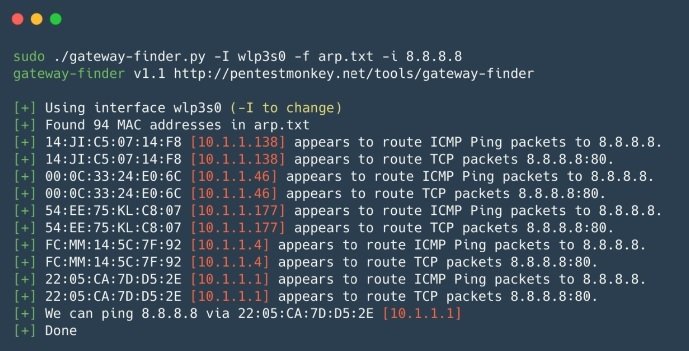
***Desventajas:*** Algunos módulos (por ejemplo, ble.enum) no son parcialmente compatibles con macOS y Windows, además de que algunos están diseñados solo para Linux (packet.proxy, por ejemplo).



## **GATEWAY\_FINDER**

Este es un script de Python que ayuda a identificar posibles gateways en la red. Acorde a los expertos en análisis de vulnerabilidades internas, esta herramienta es ideal para verificar la segmentación o encontrar hosts que puedan enrutar a una subred o Internet deseada. Gateway\_finder también es muy adecuado para pruebas de penetración interna cuando necesita verificar rápidamente rutas no autorizadas o rutas a otras redes locales internas.

***Ventajas:*** La principal ventaja de Gateway\_finder es que es muy fácil de usar y tiene gran capacidad de personalización.



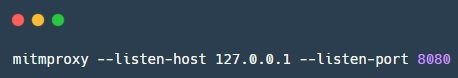
## **MITMPROXY**

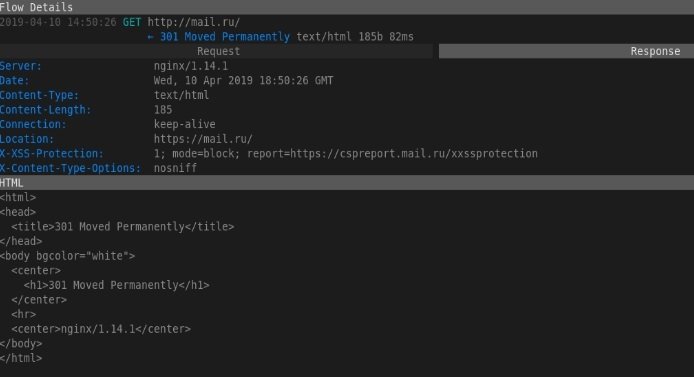
Esta es una herramienta de código abierto para analizar el tráfico protegido por SSL/TLS. Los expertos en análisis de vulnerabilidades internas pueden emplear Mitmproxy para interceptar y modificar el tráfico seguro, aunque esta herramienta no permite realizar ataques de descifrado SSL/TLS.

Un ataque consta de Mitmproxy, para el tráfico de proxy, mitmdump, similar a tcpdump, pero para el tráfico HTTP (S), y mitmweb, una interfaz web para Mitmproxy.

***Ventajas:*** La herramienta funciona con múltiples protocolos y también admite la modificación de diversos formatos, desde HTML hasta Protobuf. La herramienta también tiene una API para Python, que permite a los usuarios escribir scripts para tareas no estándar.

***Desventajas:*** El formato de volcado no es compatible con nada, es difícil usar grep y el usuario tiene que escribir scripts.





## **SIET**

SIET es una herramienta para aprovechar las capacidades del protocolo Cisco Smart Install. Es posible obtener y modificar una configuración, así como tomar el control de un dispositivo Cisco, mencionan los expertos en análisis de vulnerabilidades internas.

***Ventajas:*** El uso del protocolo Cisco Smart Install permite realizar toda clase de acciones, incluyendo:

* Cambiar la dirección del servidor tftp en el dispositivo cliente enviando un paquete TCP con formato incorrecto
* Copiar el archivo de configuración del dispositivo
* Reemplazar la configuración del dispositivo, por ejemplo, agregando un nuevo usuario
* Actualizar la imagen de iOS en el dispositivo

***Desventajas:*** SIET funciona con un conjunto limitado de dispositivos Cisco, además de que necesita una IP blanca para obtener una respuesta del dispositivo o debe estar en la misma red con el dispositivo.

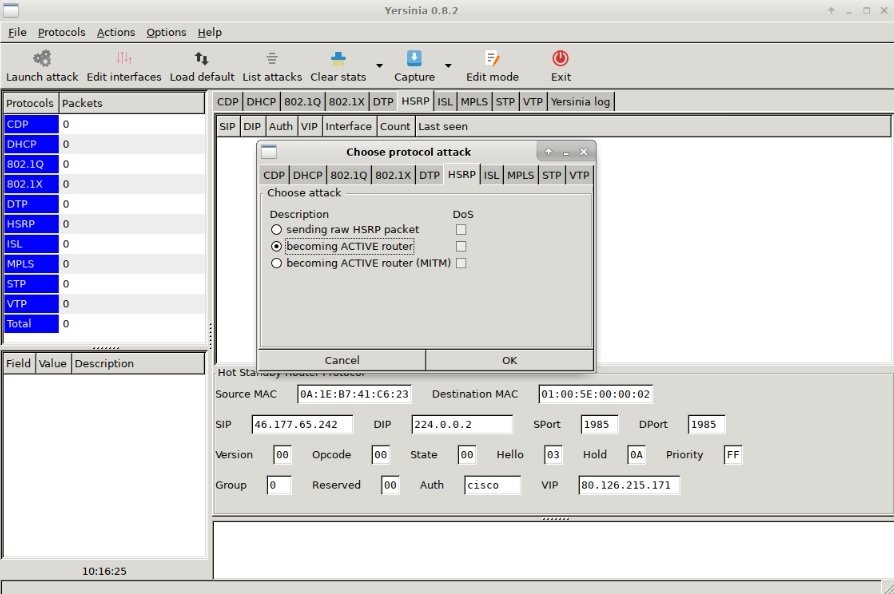


## **YERSINIA**

Yersinia es un marco de ataque L2 diseñado para explotar fallas de seguridad en varios protocolos de red L2. (ampliación temario capas de redes L2 y L3 -> [Switch Cisco - Enlaces L2 vs L3 - Blog MaxNeTI](https://blog.maxneti.com/cisco-routing-switching/sw-cisco-configuracion/#:~:text=Una%20Red%20LAN%20esta%20compuesta,configuraciones%20para%20compartir%20las%20VLANs.))

***Ventajas:*** Permite ataques a STP, CDP, DTP, DHCP, HSRP, VTP y otros.

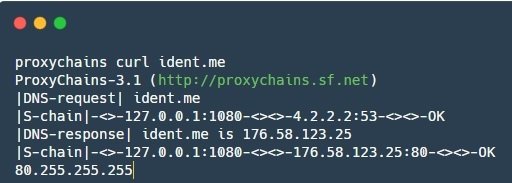
***Desventajas:*** Los expertos creen que la interfaz de Yersinia es muy difícil de utilizar para la mayoría de los investigadores.



## **PROXYCHAINS**

Proxychains es una herramienta que permite a los usuarios redirigir el tráfico de aplicaciones a través de un proxy SOCKS específico.

***Ventajas:*** Proxychains ayuda a redirigir el tráfico de algunas aplicaciones, que por defecto no saben trabajar con un proxy.



Recuerde que este artículo fue elaborado con fines exclusivamente informativos, por lo que IICS no es responsable del mal uso que pueda darse a esta información. Para conocer más sobre riesgos de seguridad informática, malware, análisis de vulnerabilidades internas y tecnologías de la información, no dude en ingresar al sitio web del Instituto Internacional de Seguridad Cibernética (IICS).