GUÍA TÉCNICA PRACTICAS INSTRUCTOR

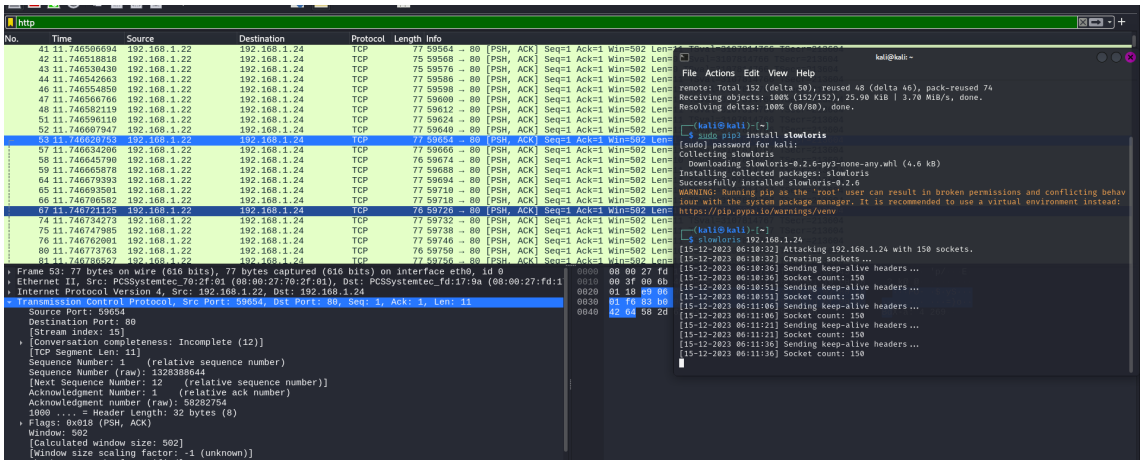
MÓDULO 14. TALLER 2

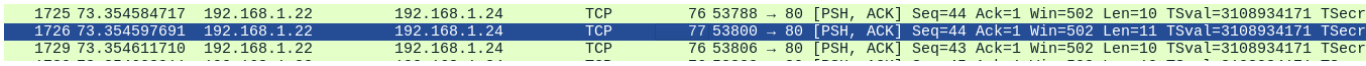
TALLER 2: EJECUTAR UN ATAQUE DOS CON SLOWLORIS

Mediante la herramienta Slowloris realice un ataque DoS, documentar proceso y resultados.

Instalamos el programa con sudo pip3 install slowloris y lo ejecutamos con slowloris 192.168.1.24 (máquina víctima)

Abrimos WIRESHARK para ver si el DoS se está ejecutando y comprobamos que en este caso lo está. Como slowloris funciona a través de HTTP ponemos en el filtro http para localizar con mayor facilidad el ataque.





Podemos ver que usamos el protocolo TCP para comunicarnos con la víctima y el tamaño de cada paquete es de 77 bits a través del puerto 80 usando paquetes PSH y ACK.

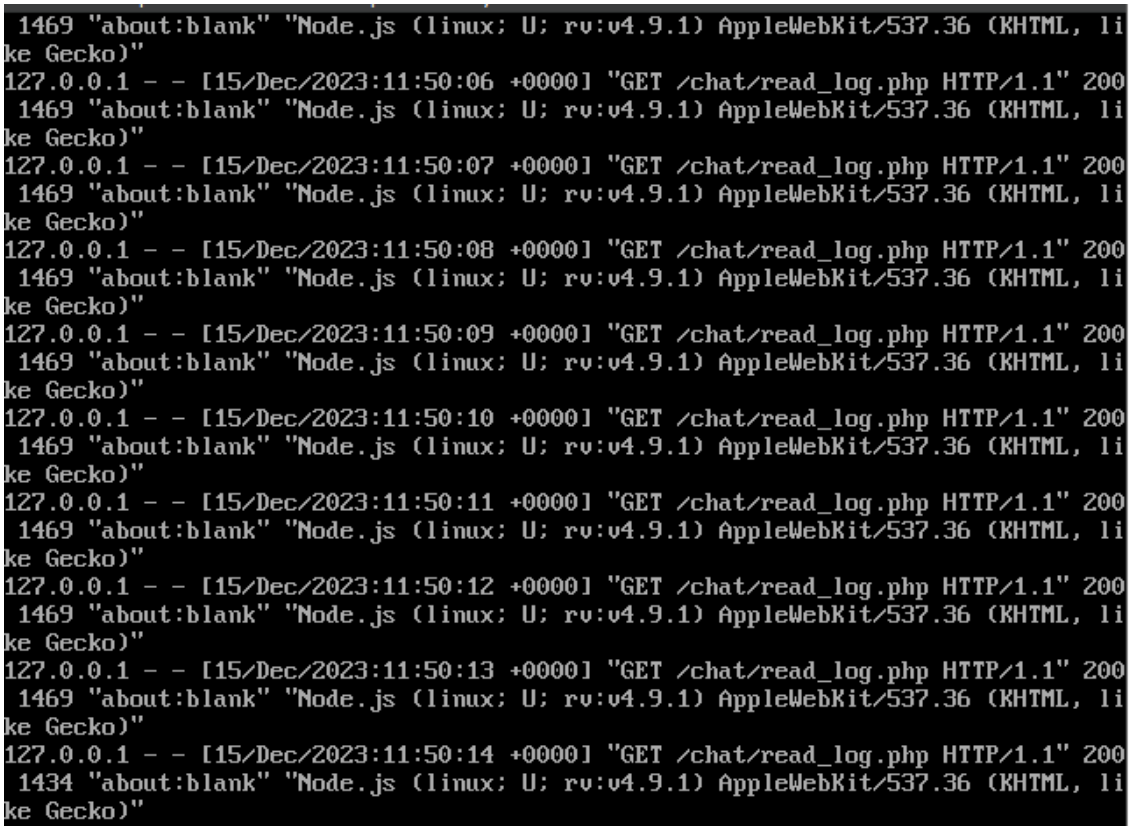
Accedemos a la máquina Metasploitable mediante root a la carpeta de logs:

Sudo su

Cd /var/log/apache2/

Ls

Cat Access.log y observamos el DoS



Slowloris tiene las siguientes opciones:

-p > puertos (normalmente 80)

-s > sockets (número de sockets para usar en el test)

-v > verbose (verbosidad)

-ua > randuseragents (randomiza user-agents con cada petición)

-x > useproxy (usa un SOCKS5 proxy para conectar

--https (usa HTTPS para las peticiones)

--sleeptime (tiempo para dormir entre cada cabecero enviado)