Cómo leer el registro de tráfico de tcpdump

Esta lectura explica cómo identificar el ataque de fuerza bruta utilizando tcpdump.

|  |
| --- |
| 14:18:32.192571 IP**tu.máquina.52444 > dns.google.dominio**:35084+ ¿A?**recetasdeliciosasparami.com**. (24)  14:18:32.204388 IP**dns.google.dominio**>**tu.máquina.52444**:35084 1/0/0 A**203.0.113.22**(40) |

La primera sección del archivo de registro de tráfico DNS y HTTP muestra la computadora de origen (**tu.máquina.52444**) usando el puerto**52444**para enviar una solicitud de resolución de DNS ael servidor DNS (**dns.google.dominio**) para la URL de destino (**recetasdeliciosasparami.com**). Luego, la respuesta regresa del servidor DNS a la computadora de origen con la dirección IP de la URL de destino.**(203.0.113.22**).

|  |
| --- |
| 14:18:36.786501 IP**tu.maquina.36086**>**recetasdeliciosasparami.com.http**:**Banderas [S]**, seq 2873951608, win 65495, opciones [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], longitud 0  14:18:36.786517 IP yummyrecipesforme.com.http > su.máquina.36086:**Banderas** **[S.]**, seq 3984334959,ack2873951609, victoria 65483, opciones [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], longitud 0 |

La siguiente sección muestra la computadora de origen enviando una solicitud de conexión (**Banderas [S]**) desde el ordenador de origen (**tu.máquina.36086**) usando el puerto**36086**directamente al destino (**recetasdeliciosasparami.com.http**). El **.http**el sufijo es el número de puerto;**http**se asocia comúnmente con el puerto 80. La respuesta muestra el destino reconociendo que recibió la solicitud de conexión (**Banderas [S.]**). La comunicación entre el origen y el destino previsto continúa durante aproximadamente 2 minutos, según las marcas de tiempo entre este bloque (**14:18**) y la siguiente solicitud de resolución de DNS (ver más abajo para**14:20**marca de tiempo).

**Los códigos de bandera TCP incluyen:**

**Banderas [S]**- Conexión**S**tarta

**Banderas [F]**- Conexión**F**bajar

**Banderas [P]** - Datos **PAG**Ush

**Banderas [R]**- Conexión**R**caso

**Banderas [.]**- Agradecimiento

|  |
| --- |
| 14:18:36.786589 IP su.máquina.36086 >**recetasdeliciosasparami.com.http**: Banderas [P.], seq 1:74, ack 1, win 512, opciones [nop,nop,TS val 3302576859 ecr 3302576859], longitud 73:**HTTP: OBTENER / HTTP/1.1** |

La entrada de registro con el código**HTTP: OBTENER / HTTP/1.1**muestra que el navegador está solicitando datos de**recetasdeliciosasparami.com**con el**HTTP: OBTENER**método que utiliza**HTTP**versión del protocolo**1.1**Esta podría ser la solicitud de descarga del archivo malicioso.

|  |
| --- |
| **14:20**:32.192571 IP**tu.máquina.52444 > dns.google.dominio**: 21899+ A? greatrecipesforme.com. (24)  14:20:32.204388 IP**dns.google.domain > tu.máquina.52444**: 21899 1/0/0 A**192.0.2.172**(40)  14:25:29.576493**IP your.machine.56378 > greatrecipesforme.com.http**: Banderas [S], seq 1020702883, win 65495, opciones [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], longitud 0  14:25:29.576510 IP**greatrecipesforme.com.http > your.machine.56378**: Banderas [S.], seq 1993648018, ack 1020702884, win 65483, opciones [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], longitud 0 |

Luego, se produce un cambio repentino en los registros. El tráfico se enruta desde el equipo de origen al servidor DNS nuevamente mediante el puerto.**.52444**(**tu.máquina.52444 > dns.google.dominio**) para realizar otra solicitud de resolución DNS. Esta vez, el servidor DNS enruta el tráfico a una nueva dirección IP (**192.0.2.172)**y su URL asociada (**grandesrecetasparami.com.http**). El tráfico cambia a una ruta entre el ordenador de origen y el sitio web falsificado (tráfico saliente:**IP your.machine.56378 > greatrecipesforme.com.http**y tráfico entrante:**greatrecipesforme.com.http >** **IP tu.máquina.56378**). Tenga en cuenta que el número de puerto (**.56378**) en la computadora de origen ha cambiado nuevamente cuando se redirige a un nuevo sitio web.

Recursos para más información

* [Una introducción al uso de tcpdump en la línea de comandos de Linux](https://opensource.com/article/18/10/introduction-tcpdump): Enumera varios comandos tcpdump con un ejemplo de salida. El artículo describe los datos de la salida y explica su utilidad.
* [Hoja de trucos de tcpdump](https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/):Enumera comandos tcpdump, opciones de captura de paquetes, opciones de salida, códigos de protocolo y opciones de filtro
* [¿Qué es un puerto de computadora? | Puertos en redes](https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/):Proporciona una breve lista de los puertos más comunes para el tráfico de red y sus protocolos asociados. El artículo también proporciona información sobre los puertos en general y el uso de firewalls para bloquearlos.
* [Registro de nombre de servicio y número de puerto del protocolo de transporte](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml):Proporciona una base de datos de números de puerto con sus nombres de servicio, protocolos de transporte y descripciones.
* [¿Cómo capturar y analizar el tráfico de red con tcpdump?](https://geekflare.com/tcpdump-examples/):Proporciona varios comandos tcpdump con ejemplos de salida. A continuación, el artículo describe cada elemento de datos en ejemplos de salida de tcpdump.
* [Clase magistral: Tcpdump: Interpretación de la salida](https://packetpushers.net/masterclass-tcpdump-interpreting-output/):Proporciona una guía de referencia codificada por colores para la salida de tcpdump