Cómo leer el registro de tráfico DNS y HTTP

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

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)

14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084
1/0/0 A 203.0.113.22 (40)
```

La primera sección del archivo de registro de tráfico DNS y HTTP muestra el equipo de origen (**your.machine.52444**) utilizando el puerto **52444** para enviar una solicitud de resolución DNS al servidor DNS (**dns.google.domain**) para la URL de destino (**yummyrecipesforme.com**). Luego, la respuesta regresa del servidor DNS al equipo de origen con la dirección IP de la URL de destino **(203.0.113.22**).

```
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http:
Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS
val 3302576859 ecr 0,nop,wscale 7], length 0

14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086:
Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss
65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0
```

La siguiente sección muestra a la computadora de origen enviando una solicitud de conexión (**Flags [S]**) desde la computadora de origen (**your.machine.36086**) utilizando el puerto **36086** directamente al destino (**yummyrecipesforme.com.http**). El sufijo **.http** es el número de puerto; **http** se asocia comúnmente con el puerto 80. La respuesta muestra al destino reconociendo que recibió la solicitud de conexión (**Flags [S.]**). La comunicación entre el equipo de origen y el destino previsto continúa durante aproximadamente 2 minutos, de acuerdo con las marcas de tiempo entre este bloque (**14:18**) y la siguiente solicitud de resolución DNS (consulta a continuación la marca de tiempo **14:20**).

Los códigos de indicadores [Flag] TCP incluyen:

Flags [S] - Connection **S**tart (inicio de la conexión)
Flags [F] - Connection **F**inish (fin de la conexión)
Flags [P] - Data **P**ush (inserción de datos)
Flags [R] - Connection **R**eset (Restablecimiento de conexión)
Flags [.] - Reconocimiento

```
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http:
Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val
3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1
```

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

```
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)

14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899
1/0/0 A 192.0.2.172 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http:
Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS
val 3302989649 ecr 0,nop,wscale 7], length 0

14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378:
Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss
65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0
```

Luego, un cambio repentino ocurre en los registros. El tráfico se enruta desde el equipo de origen al servidor DNS utilizando nuevamente el puerto **.52444** (**your.machine.52444 > dns.google.domain**) 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 a su URL asociada (**greatrecipesforme.com.http**). El tráfico cambia a una ruta entre la computadora de origen y el sitio web falso (tráfico saliente: **IP your.machine.56378 > greatrecipesforme.com.http** y tráfico entrante: **greatrecipesforme.com.http > IP your.machine.56378**). Ten en cuenta que en la computadora de origen ha cambiado nuevamente el número de puerto (**.56378**) al redirigirse a un nuevo sitio web.

Recursos para obtener información adicional

- Una introducción al uso de tcpdump en la línea de comandos de Linux: enumera varios comandos de tcpdump con resultados de ejemplo. El artículo describe los datos de los resultados y explica su utilidad.
- Guía de trucos de tcpdump: indica comandos de tcpdump, opciones para capturar paquetes, opciones de salida, códigos de protocolo y opciones de filtro

- ¿Qué es un puerto de una computadora? | Puertos en redes: proporciona una breve lista de los puertos más comunes para el tráfico de red y sus protocolos asociados. El artículo también brinda información acerca de los puertos en general y el uso de firewalls para bloquearlos.
- Nombre del servicio y registro del número de puerto del protocolo de transporte: brinda 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?: enumera varios comandos tcpdump con resultados de ejemplo. Luego, el artículo describe cada uno de los datos en los ejemplos de resultados tcpdump.
- Clase magistral – Tcpdump – Interpretación de resultados: otorga una guía de referencia codificada por colores para los resultados tcpdump