How to read the tcpdump traffic log

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 la computadora de origen (tu.máquina.52444) que usa el puerto 52444 para enviar una solicitud de resolución de DNS al servidor DNS (dns.google.domain) para la URL de destino (yummyrecipesforme.com). A continuación, la respuesta vuelve 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
```

En la siguiente sección se muestra el equipo de origen que envía una solicitud de conexión (Flags [S]) desde el equipo de origen (su.máquina.36086) mediante 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 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, de acuerdo con las marcas de tiempo entre este bloque (14:18) y la siguiente solicitud de resolución DNS (consulte a continuación la marca de tiempo 14:20).

Flags	Significado en TCP	Explicación en español
[S]	SYN	Solicita iniciar una conexión
[S.]	SYN + ACK	Respuesta aceptando inicio de conexión
[.]	ACK	Reconocimiento (acknowledgment)
[P.]	PSH + ACK	Empuje de datos y reconocimiento
[F]	FIN	Solicita terminar la conexión
[F.]	FIN + ACK	Finaliza conexión con reconocimiento
[R]	RST	Restablece una conexión (por error o rechazo)
[R.]	RST + ACK	Restablece con reconocimiento (menos común)
[FP.]	FIN + PSH + ACK	Finaliza la conexión empujando los últimos datos
[SFP.]	SYN + FIN + PSH + ACK	Raro; múltiples flags combinados
[P]	PSH	Empuje de datos sin ACK (inusual/anómalo)
[F,P.]	FIN + PSH + ACK	Finaliza y empuja datos
[S,R]	SYN + RST	Conflicto lógico (no debería ocurrir)
[U.]	URG + ACK	Dato urgente con reconocimiento
[E.]	ECE + ACK	Notificación de congestión con ACK
[W.]	CWR + ACK	Reducción de ventana por congestión + ACK

```
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 utilizando la versión 1.1 del protocolo HTTP. 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
```

Entonces, se produce un cambio repentino en los registros. El tráfico se enruta desde el ordenador de origen al servidor DNS de nuevo mediante el puerto .52444 (tu.máquina.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 su URL asociada (greatrecipesforme.com.http). El tráfico cambia a una ruta entre el equipo de origen y el sitio web falsificado (tráfico salie nte: IP tu.máquina.56378 > greatrecipesforme.com.http y tráfico entrante: greatrecipesforme.com.http > IP tu.máquina.56378). Tenga en cuenta que el número de puerto (.56378) en el equipo de origen ha cambiado de nuevo cuando se redirige a un nuevo sitio web.

Resources for more information

- An introduction to using tcpdump at the Linux command line: Enumera varios comandos tcpdump con una salida de ejemplo. En el artículo se describen los datos de la salida y se explica por qué son útiles.
- tcpdump Cheat Sheet: Enumera los comandos tcpdump, las opciones de captura de paquetes, las opciones de salida, los códigos de protocolo y las opciones de filtro
- What is a computer port? | Ports in networking: 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 bloquear puertos.
- Service Name and Transport Protocol Port Number Registry: Proporciona una base de datos de números de puerto con sus nombres de servicio, protocolos de transporte y descripciones
- How to Capture and Analyze Network Traffic with tcpdump?: Proporciona varios comandos tcpdump con salida de ejemplo. A continuación, en el artículo se describe cada elemento de datos en ejemplos de salida tcpdump.
- Masterclass – Tcpdump – Interpreting Output: Proporciona una guía de referencia codificada por colores para la salida tcpdump