Como ler o registro do tcpdump

Esta leitura explica como identificar o ataque de força bruta usando o 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)
```

A primeira seção do arquivo de log de tráfego DNS e HTTP mostra o computador de origem (**your.machine.52444**) usando porta **52444** para enviar uma solicitação de resolução de DNS parao servidor DNS (**dns.google.domain**) para o URL de destino (**yummyrecipesforme.com**). Em seguida, a resposta retorna do servidor DNS para o computador de origem com o endereço IP do 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
```

A próxima seção mostra o computador de origem enviando uma solicitação de conexão (**Flags [S]**) do computador de origem (**your.machine.36086**) usando porta**36086**diretamente ao destino (**yummyrecipesforme.com.http**). O **.http** sufixo é o número da porta; **http** é comumente associado à porta 80. A resposta mostra o destino confirmando que recebeu a solicitação de conexão (**Flags [S.]**). A comunicação entre a origem e o destino pretendido continua por cerca de 2 minutos, de acordo com os carimbos de data/hora entre este bloco (**14:18**) e a próxima solicitação de resolução de DNS (veja abaixo para o**14:20** carimbo de data/hora)..

Os códigos de sinalização TCP incluem:

Flags [S] - Connection **S**tart
Flags [F] - Connection **F**inish
Flags [P] - Data **P**ush
Flags [R] - Connection **R**eset

Flags [.] - Acknowledgment

```
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
```

A entrada de log com o código **HTTP: GET / HTTP/1.1**mostra que o navegador está solicitando dados de **yummyrecipesforme.com** com o **HTTP: GET**método usando **HTTP** versão do protocolo **1.1**. Esta pode ser a solicitação de download do arquivo 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
```

Então, ocorre uma mudança repentina nos logs. O tráfego é roteado do computador de origem para o servidor DNS novamente usando a porta**.52444**(**your.machine.52444 > dns.google.domain**) para fazer outra solicitação de resolução de DNS. Desta vez, o servidor DNS encaminha o tráfego para um novo endereço IP (**192.0.2.172)**e seu URL associado (**greatrecipesforme.com.http**). O tráfego muda para uma rota entre o computador de origem e o site falsificado (tráfego de saída:**IP your.machine.56378 > greatrecipesforme.com.http** e tráfego de entrada: **greatrecipesforme.com.http > IP your.machine.56378**). Observe que o número da porta (**.56378**) no computador de origem mudou novamente quando redirecionado para um novo site.

Fontes e recursos para pesquisa:

- Uma introdução ao uso do tcpdump na linha de comando do Linux: Lista vários comandos tcpdump com exemplos de saída. O artigo descreve os dados na saída e explica por que ela é útil.

- Folha de dicas do tcpdump: Lista comandos tcpdump, opções de captura de pacotes, opções de saída, códigos de protocolo e opções de filtro
- O que é uma porta de computador? | Portas em redes:Fornece uma breve lista das portas mais comuns para tráfego de rede e seus protocolos associados. O artigo também fornece informações sobre portas em geral e o uso de firewalls para bloqueá-las.
- Registro de nome de serviço e número de porta do protocolo de transporte:Fornece um banco de dados de números de porta com seus nomes de serviço, protocolos de transporte e descrições
- Como capturar e analisar tráfego de rede com o tcpdump?:Fornece vários comandos tcpdump com exemplos de saída. Em seguida, o artigo descreve cada elemento de dados com exemplos de saída do tcpdump.
- Masterclass – Tcpdump – Interpretando a Saída: Fornece um guia de referência codificado por cores para a saída do tcpdump