Atividade 3 - TCPDump

September 1, 2015

Contents

1 Interfaces disponíveis e permissões de usuário

Estão disponíveis as interfaces `lo, wlp2s0 e enp0s25`, o TCPDump não pode capturar em nenhuma delas como usuário comum, mas pode capturar dados na interface bluetooth0. Ele também não tem permissão para capturar nas interfaces usb ou nas usadas pelo dbus. Ele não consegue usar nenhuma interface que exija o uso de $\text{raw}_{\text{sockets}}$ pois meu usuário não está em nenhum grupo que tenha a permissão para isso. E nem as interfaces usbmon pois elas dependem de arquivos que meu usuário não tem permissão de leitura (`/sys/kernel/debug/usb/usbmon/1t`)

2 IP address dos hosts envolvidos

Basta rodar tcpdump -nn para obter os ips no lugar dos hostnames resolvidos
`maple: - 128.30.4.223`
`willow: - 128.30.4.222`

3 MAC address dos hosts envolvidos

`maple: - 00:16:ea:8d:e5:8a`
`willow:` - Não foi possivel obter o MAC de willow, um motivo para isso é que maple não requisita o MAC de willow, pois o aprende ao receber a primeira mensagem (testei com tcpdump -XX mas realmente não há esse dado no log)

4 Portas envolvidas na sessão

Assim como na 3 foi necessário rodar o comando com opção `-nn` para obter o numero da porta onde roda o serviço commplex-link
`maple: - commplex-link (5001)`
`willow: - 39675`

5 Total transmitido e velocidade média

O primeiro tempo no log é 01:34:41.473036, o ultimo 01:34:44.339015. Aparentemente a sessão durou 2.865979s. Nesse período fomos do seq 1 na linha 6 ao 1567673 na linha 1912, das linhas 1 a 5 temos logs de ARP e de 1913 a 1918 acks Logo tivemos 1567673 bytes, 1.4950Mb, em 2.8659s, ou 534.188kbps Os números não mudam muito descontando o tempo do ARP

6 RTT

O pacote com seq 1473:2921 foi capturado no linha 8 (tempo = 01:34:41.474225), seu ack (2921) foi recebido na linha 22 (tempo = 01:34:41.482047), temos aqui um RTT de 0.00782s (7.82ms)

Já o pacote com seq 13057:14505 está na linha 35 do log, (tempo = 01:34:41.489825) e seu ack na linha 46 (tempo = 01:34:41.499373) O RTT nesse caso foi de 0.00954s (9.54ms)

Os primeiro pacote (mais rápido) foi do host willow para o host maple, o seguinte foi de maple para willow, a diferença de tempo poderia ser atribuída

a vários fatores, dentre eles um dos hosts estar mais carregado ou a um maior uso da rede, 2ms não é um tempo muito significativo (tive diferenças maiores entre o meu host e o roteador ligados por um cabo em uma rede gigabit, pelo dump do aparentemente a conexão entre willow e maple é ethernet de 10mbps)

7 Three way handshake & Connection Termination

Three Way handshake: Um ponto característico do three-way handshake é o pacote com as flags `SYN,ACK`, esse pode ser encontrado com o comando `tcpdump -r tcpdump.dat 'tcp\[13\] = 18'`. Ele foi encontrado na linha em que o tempo = 01:34:41.474055, (linha 4). A linha 3 é o SYN correspondente e a linha 5 o ACK.

Mensagem	Fonte	Destino	Protocolo	Informação relevante (FLAGS)
Linha 3	willow	maple	TCP	SYN
Linha 4	maple	willow	TCP	SYN,ACK
Linha 5	willow	maple	TCP	ACK

```
   01:34:41.473518 IP willow.csail.mit.edu.39675 > maple.csail.mit.edu.commplex-link:
Flags [S], seq 1258159963, win 14600, options [mss 1460,sackOK,TS
val 282136473 ecr 0,nop,wscale 7], length 0
   01:34:41.474055 IP maple.csail.mit.edu.commplex-link > willow.csail.mit.edu.39675:
Flags [S.], seq 2924083256, ack 1258159964, win 14480, options [mss
1460,sackOK,TS val 282202089 ecr 282136473,nop,wscale 7], length
0
   01:34:41.474079 IP willow.csail.mit.edu.39675 > maple.csail.mit.edu.commplex-link:
Flags [.], ack 1, win 115, options [nop,nop,TS val 282136474 ecr
282202089], length 0
```

(ele também poderia ser encontrado por estar no inicio da conexão e esse dump em particular ser bem comportado e conter apenas uma)

O Connection Termination pode ser encontrado de forma similar, graças a flag `FIN`, mais especificamente `FIN-FIN,ACK-ACK` O comando para filtrar pacotes com a flag FIN é `tcpdump -r tcpdump.dat 'tcp[tcpflags] & (tcp-fin) ! = 0'`. Que retorna os pacotes com tempo = 01:34:44.311921 (FIN) (linha 1908) e 01:34:44.339007 `FIN-ACK` (linha 1917), aos 2 se soma o `ACK` final na linha 1918

Mensagem	Fonte	Destino	Protocolo	Informação relevante (FLAGS)
Linha 1908	willow	maple	TCP	FIN
Linha 1917	maple	willow	TCP	FIN,ACK
Linha 1918	willow	maple	TCP	ACK

```
01:34:44.311921 IP willow.csail.mit.edu.39675 > maple.csail.mit.edu.commplex-link:
Flags [FP.], seq 1572017:1572889, ack 1, win 115, options [nop,nop,TS
val 282139311 ecr 282204927], length 872
01:34:44.339007 IP maple.csail.mit.edu.commplex-link > willow.csail.mit.edu.39675:
Flags [F.], seq 1, ack 1572890, win 905, options [nop,nop,TS val
282204955 ecr 282139320], length 0
01:34:44.339015 IP willow.csail.mit.edu.39675 > maple.csail.mit.edu.commplex-link:
Flags [.], ack 2, win 115, options [nop,nop,TS val 282139339 ecr
282204955], length 0
```

Mais uma vez, teria sido possível encontrar esses dados simplesmente porque eles estão no final da conexão