MC833 - Tarefa 2

Erik de Godoy Perillo - RA: 135582

31 de março de 2016

1. As interfaces pelas quais pode-se capturar dados podem ser listadas com a *flag* `-list-interfaces`:

```
$ tcpdump --list-interfaces
1.wlp3s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up,
Running]
3.lo [Up, Running, Loopback]
4.enp2s0 [Up]
5.bluetooth-monitor (Bluetooth Linux Monitor)
6.nflog (Linux netfilter log (NFLOG) interface)
7.nfqueue (Linux netfilter queue (NFQUEUE) interface)
8.dbus-system (D-Bus system bus)
9.dbus-session (D-Bus session bus)
10.usbmon1 (USB bus number 1)
11.usbmon2 (USB bus number 2)
12.usbmon3 (USB bus number 3)
```

   São muito mais interfaces que as mostradas como disponíveis pelo `ifconfig`:

```
$ ifconfig -a -s
Iface MTU RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR
Flg
enp2s0 1500 0 0 0 0 0 0 0 0 BMU
lo 65536 4433 0 0 0 4433 0 0 0 LRU
wlp3s0 1500 842849 0 0 0 325951 0 0 0 BMRU
```

2. Usando-se a *flag* `-nn`, consegue-se ver os endereços IP ao invés dos nomes dos domínios dos *hosts*.

```
$ tcpdump -r tcpdump.dat | tail -n1
ding from file tcpdump.dat, link-type EN10MB (Ethernet)
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
```

```
$ tcpdump -nnr tcpdump.dat | tail -n1
ding from file tcpdump.dat, link-type EN10MB (Ethernet)
01:34:44.339015 IP 128.30.4.222.39675 > 128.30.4.223.5001:
Flags [.], ack 2, win 115, options [nop,nop,TS val 282139339
ecr 282204955], length 0
```

Assim, os endereços IP de *willow* e *maple* são, respectivamente, `128.30.4.222` e `128.30.4.223`.

3. –

```
$ tcpdump -e -r tcpdump.dat | tail -n1
ding from file tcpdump.dat, link-type EN10MB (Ethernet)
01:34:44.339015 00:16:ea:8e:28:44 (oui Unknown) >
00:16:ea:8d:e5:8a (oui Unknown), ethertype IPv4
(0x0800), length 66:  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
```

Assim, os endereços MAC de *willow* e *maple* são, respectivamente, `00:16:ea:8e:28:44` e `00:16:ea:8d:e5:8a`.

4. –

```
$ tcpdump -nnr tcpdump.dat | tail -n1
ding from file tcpdump.dat, link-type EN10MB (Ethernet)
01:34:44.339015 IP 128.30.4.222.39675 > 128.30.4.223.5001:
Flags [.], ack 2, win 115, options [nop,nop,TS val 282139339
ecr 282204955], length 0
```

Assim, as portas de *willow* e *maple* são, respectivamente, `39675` e `5001`.

5. –

```
$ tcpdump -r tcpdump.dat | tail -n2
reading from file tcpdump.dat, link-type EN10MB (Ethernet)
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
```

```
$ tcpdump -r tcpdump.dat | head -n1
reading from file tcpdump.dat, link-type EN10MB (Ethernet)
01:34:41.473036 ARP, Request who-has maple.csail.mit.edu tell
willow.csail.mit.edu, length 28
```

```
$ tcpdump -r tcpdump.dat | tail -n1
reading from file tcpdump.dat, link-type EN10MB (Ethernet)
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
```

O último ACK é de número 1572890, assim foram transferidos 1572889 bytes. A conexão começou em 1:34:41.47 e terminou em 1:34:44.34, assim ela durou 2.87 segundos. Deste modo, a vazão foi de $1572.889/2.87 = 548$ Kilobytes por segundo.

6. –

```
$ cat outfile.txt | grep "1473:2921|ack 2921"
01:34:41.474225 IP willow.csail.mit.edu.39675 >
maple.csail.mit.edu.commplex-link:  Flags [.], seq 1473:2921,
ack 1, win 115, options [nop,nop,TS val 282136474 ecr
282202089], length 1448
01:34:41.482047 IP maple.csail.mit.edu.commplex-link >
willow.csail.mit.edu.39675:  Flags [.], ack 2921, win 159,
options [nop,nop,TS val 282202095 ecr 282136474], length 0
```

Entre o envio e o ACK do recebimento, o tempo foi de $41.482 - 41.474 = 0.08$ segundos.

```
$ cat outfile.txt | grep "13057:14505|ack 14505"
01:34:41.474992 IP willow.csail.mit.edu.39675 >
maple.csail.mit.edu.commplex-link:  Flags [.], seq 13057:14505,
ack 1, win 115, options [nop,nop,TS val 282136474 ecr
282202090], length 1448
01:34:41.499373 IP maple.csail.mit.edu.commplex-link >
willow.csail.mit.edu.39675:  Flags [.], ack 14505, win 331,
options [nop,nop,TS val 282202114 ecr 282136474], length 0
```

O tempo foi de $41.499 - 41.475 = 0.24$ segundos. Diversos fatores podem ter causado a diferença de tempo.

7. –

Three-way handshake:

```
 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
```

número	fonte	destino	mensagem
1	willow	maple	SYN, seq=1258159963
2	maple	willow	SYN, ACK=1258159964, seq=2924083256
3	willow	maple	ACK=1

Connection termination:

```
 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
01:34:44.329956 IP maple.csail.mit.edu.commplex-link >
willow.csail.mit.edu.39675:  Flags [.], ack 1572890, win 820,
options [nop,nop,TS val 282204945 ecr 282139320], length 0
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
```

número	fonte	destino	mensagem
1	maple	willow	FYN
2	willow	maple	ACK
3	willow	maple	FYN
4	maple	maple	ACK