

9900283

مصطفی دریس پور

بخش اول:

1.

با استفاده از wireshark می توانیم بسته ها را بر روی interface های مختلف بررسی کنیم آن ها را فیلتر کنیم و در صورت نیاز به صورت hex یا با یک abstract جزئیات بسته ها را ببینیم.

مثلا می توانیم بسته های drop شده یا مشکلات تاخیر ارسال بسته ها را متوجه شویم. همچنین اگر فعالیت خرابکارانه در سطح شبکه رخ داده باشد آن را می بینیم.

برای مثال با استفاده از این ابزار می توانیم زمان های network burst را تشخیص دهیم. مثال دیگر اگر بر روی یک سرور بسته ها را مشاهده می کنیم می توانیم در صورت بروز حمله DOS تعداد زیادی بسته tcp syn که متناظرا از سمت کلاینت دریافت نمی شود را مشاهده کنیم. همه این موارد با استفاده از این ابزار قابل حصول است.

بخش دوم:

توپولوژی ساخته شده در بخش دوم یک توپولوژی minimal است.

2.1

دو پروتکل tcp و openflow. می دانیم openflow از tcp استفاده می کند.

25	1.059566610	127.0.0.1	127.0.0.1	TCP
26	1.059547015	127.0.0.1	127.0.0.1	TCP
27	1.059575388	127.0.0.1	127.0.0.1	TCP
28	1.059805006	127.0.0.1	127.0.0.1	OpenFlow
29	1.059820714	127.0.0.1	127.0.0.1	TCP
30	1.059936560	127.0.0.1	127.0.0.1	TCP
31	1.059953610	127.0.0.1	127.0.0.1	TCP

2.2

The screenshot shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets on the left, with packet 4293 selected. The packet details pane on the right shows the structure of the selected packet, which is an OpenFlow 1.0 message. The packet is 74 bytes long and contains an OFPT_HELLO message. The packet list pane shows the following details for packet 4293:

No.	Time	Source	Destination	Protocol	Length	Info
4293	35.773220447	127.0.0.1	127.0.0.1	OpenFlow	74	Type: OFPT_HELLO

The packet details pane shows the following structure:

- Frame 4293: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 0
- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 6653, Dst Port: 48856, Seq: 1, Ack: 8, Len: 8
- OpenFlow 1.0
 - 000 0001 = Version: 1.0 (0x01)
 - Type: OFPT_HELLO (0)
 - Length: 8
 - Transaction ID: 2362875664

The packet bytes pane shows the raw data of the packet in hexadecimal and ASCII format.

2.3

41	1.060167119	127.0.0.1	127.0.0.1	TCP	66 6653 → 56334 [ACK] Seq=1 Ac
42	1.060208524	127.0.0.1	127.0.0.1	OpenFlow	74 Type: <u>OFPT_FEATURES_REQUEST</u>
43	1.060218655	127.0.0.1	127.0.0.1	TCP	66 56330 → 6653 [ACK] Seq=9 Ac
44	1.060238301	127.0.0.1	127.0.0.1	OpenFlow	78 Type: OFPT_SET_CONFIG
45	1.060246876	127.0.0.1	127.0.0.1	TCP	66 56330 → 6653 [ACK] Seq=9 Ac
46	1.060359198	127.0.0.1	127.0.0.1	OpenFlow	146 Type: OFPT_FLOW_MOD
47	1.060369665	127.0.0.1	127.0.0.1	TCP	66 56330 → 6653 [ACK] Seq=9 Ac
48	1.060463331	127.0.0.1	127.0.0.1	OpenFlow	74 Type: OFPT_HELLO
49	1.060473612	127.0.0.1	127.0.0.1	TCP	66 56332 → 6653 [ACK] Seq=9 Ac
50	1.060507997	127.0.0.1	127.0.0.1	OpenFlow	74 Type: OFPT_FEATURES_REQUEST
51	1.060516427	127.0.0.1	127.0.0.1	TCP	66 56332 → 6653 [ACK] Seq=9 Ac
52	1.060533199	127.0.0.1	127.0.0.1	OpenFlow	78 Type: OFPT_SET_CONFIG
53	1.060541313	127.0.0.1	127.0.0.1	TCP	66 56332 → 6653 [ACK] Seq=9 Ac
54	1.060563275	127.0.0.1	127.0.0.1	OpenFlow	146 Type: OFPT_FLOW_MOD
55	1.060571656	127.0.0.1	127.0.0.1	TCP	66 56332 → 6653 [ACK] Seq=9 Ac
56	1.060630217	127.0.0.1	127.0.0.1	OpenFlow	74 Type: OFPT_HELLO
57	1.060640019	127.0.0.1	127.0.0.1	TCP	66 56334 → 6653 [ACK] Seq=9 Ac
58	1.060665187	127.0.0.1	127.0.0.1	OpenFlow	74 Type: <u>OFPT_FEATURES_REQUEST</u>
59	1.060673799	127.0.0.1	127.0.0.1	TCP	66 56334 → 6653 [ACK] Seq=9 Ac
60	1.060689934	127.0.0.1	127.0.0.1	OpenFlow	78 Type: OFPT_SET_CONFIG
61	1.060698288	127.0.0.1	127.0.0.1	TCP	66 56334 → 6653 [ACK] Seq=9 Ac
62	1.060717141	127.0.0.1	127.0.0.1	OpenFlow	146 Type: OFPT_FLOW_MOD
63	1.060725424	127.0.0.1	127.0.0.1	TCP	66 56334 → 6653 [ACK] Seq=9 Ac
64	1.560522039	127.0.0.1	127.0.0.1	OpenFlow	98 Type: OFPT_FEATURES_REPLY
65	1.560552025	127.0.0.1	127.0.0.1	TCP	66 6653 → 56330 [ACK] Seq=109

ابتدا کنترلر درخواست feature request را برای سویچ ها می فرستد تا Data path ID را به دست آورد. سپس سویچ در پاسخ بسته های feature reply می فرستد که شامل اطلاعاتی نظیر Capabilities , Data path ID می باشد.

2.4

21482	234.350991593	10.0.0.1	10.0.0.2	OpenFl...	182 Type: <u>OFPT_PACKET_IN</u>
21485	234.351124689	10.0.0.1	10.0.0.2	OpenFl...	188 Type: OFPT_PACKET_OUT
21487	234.351926872	10.0.0.2	10.0.0.1	OpenFl...	182 Type: <u>OFPT_PACKET_IN</u>
21490	234.352056348	10.0.0.2	10.0.0.1	OpenFl...	188 Type: OFPT_PACKET_OUT

این پکت ها با زیر خط صورتی مشخص شده اند.
نمونه ای دیگر از این پکت ها:

```

> Frame 2135: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 48812, Dst Port: 6653, Seq: 205, Ack: 383, Len: 60
▼ OpenFlow 1.0
  .000 0001 = Version: 1.0 (0x01)
  Type: OFPT_PACKET_IN (10)
  Length: 60
  Transaction ID: 0
  Buffer Id: 0xffffffff
  Total length: 42
  In port: 2
  Reason: No matching flow (table-miss flow entry) (0)
  Pad: 00
  > Ethernet II, Src: a6:d4:6f:5b:cf:df (a6:d4:6f:5b:cf:df), Dst: c2:51:c1:f9:9f:0d (c2:51:c1:f9:9f:0d)
  > Address Resolution Protocol (reply)

```

2.5

بسته در دو حالت: Reverse connection, Missing flow control ارسال می شود.
در این پکت ها دستور کار به کنترلر سپرده می شود که می تواند در بخش action ذکر شده باشد (send to controller) یا برای پکت مورد نظر هیچ match وجود نداشته باشد در صورت وجود بافر به مقدار کافی در سوییچ این پیام حاوی بخشی از هدر بسته که 128 بایت است و یک شناسه بافر می باشد که کنترلر در زمان آماده سازی از آن استفاده می کند.
سوییچ هنگام ارسال بسته سوییچ های که بافر داخلی را ساپورت نمی کنند باید بسته کامل را به عنوان بخشی از پیام به کنترلرکننده ارسال کنند. پس وقتی match برای پکت پیدا نشد در openflow sdn بسته برای پردازش دقیق تر به کنترلر فرستاده می شود.

2.6

بسته های ICMP:

No.	Time	Source	Destination	Protocol	Length	Info
21482	234.350991593	10.0.0.1	10.0.0.2	OpenFL...	182	Type: OFPT_PACKET_IN
21485	234.351124689	10.0.0.1	10.0.0.2	OpenFL...	188	Type: OFPT_PACKET_OUT
21487	234.351926872	10.0.0.2	10.0.0.1	OpenFL...	182	Type: OFPT_PACKET_IN
21490	234.352056348	10.0.0.2	10.0.0.1	OpenFL...	188	Type: OFPT_PACKET_OUT

از h1 ping h2

بخش سوم:

3.

```

mininet> iperf
*** Iperf: testing TCP bandwidth between h1 and h2
*** Results: ['11.6 Gbits/sec', '11.7 Gbits/sec']

```

در این توپولوژی minimal ما دو host داریم که با این دستور همدیگر را ping می کنند مقدار bandwidth در اینترفیس که این دو host را به هم وصل می کند متناظرا برای h1,h2 را نشان می دهد.

بخش چهارم:

4.

1.

مثلا در حملات DOS در صورتی که تعداد زیادی بسته SYN دریافت کردیم ولی کلاینت ها متناظرا ACK نفرستادند یعنی ترافیک غیر عادی است و احتمالا حمله DOS است.

2.

در صورتی که client آی پی دامنه را با استفاده از پروتکل dns درخواست کند ولی پس از آن با یک ip دیگری ارتباط برقرار کند (ای پی که با آن کانکت می شود با آی پی دامنه متفاوت است) این یک رفتار غیر عادی (در سطح اینترنت ایران) می باشد و نشان می دهد که client دارد از یک proxy برای رفع فیلترینگ استفاده می کند. به این پدیده dns leaking نیز گفته می شود.