

Lab 8. Dynamic Analysis

Dan Bruce, David Clark and Hector D. Menendez

Department of Computer Science
University College London

November 27, 2017

Network Analysis

Using the information of the network traffic, we can perform different kind of analysis:

- Conversation Analysis.
- Content Analysis.
- Identify the Malware origin.
- Data Mining Analysis

Wireshark

Wireshark is the world's foremost network protocol analyzer.

It lets you see what's happening on your network at a microscopic level.

It is the de facto (and often de jure) standard across many industries and educational institutions.

Working with Wireshark

Sniffing§

Filtering

Following

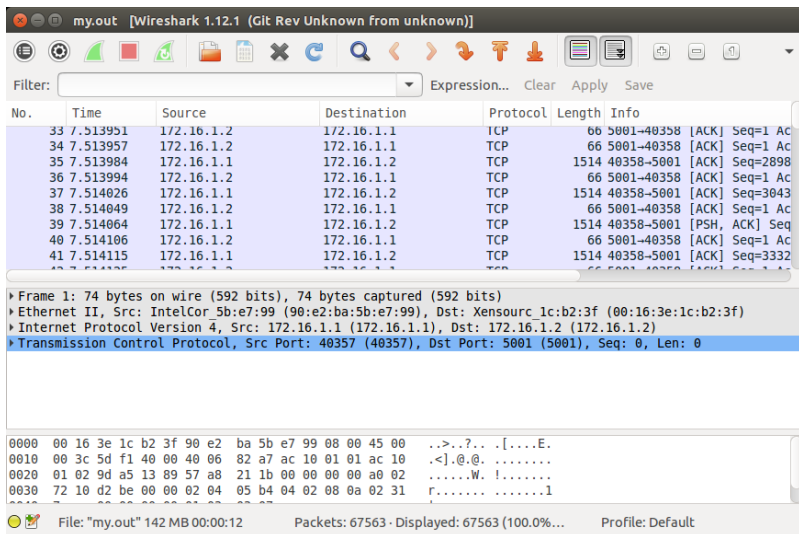
Analysing

Packer Sniffer

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer.

A packet sniffer receives a copy of packets that are sent / received from/by application and protocols executing on your machine.

Wireshark Interface



my.out [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------|-------------|----------|--------|---------------------------|
| 33 | 7.513951 | 172.16.1.2 | 172.16.1.1 | TCP | 66 | 5001→40358 [ACK] Seq=1 Ac |
| 34 | 7.513957 | 172.16.1.2 | 172.16.1.1 | TCP | 66 | 5001→40358 [ACK] Seq=1 Ac |
| 35 | 7.513984 | 172.16.1.1 | 172.16.1.2 | TCP | 1514 | 40358→5001 [ACK] Seq=2898 |
| 36 | 7.513994 | 172.16.1.2 | 172.16.1.1 | TCP | 66 | 5001→40358 [ACK] Seq=1 Ac |
| 37 | 7.514026 | 172.16.1.1 | 172.16.1.2 | TCP | 1514 | 40358→5001 [ACK] Seq=3043 |
| 38 | 7.514049 | 172.16.1.2 | 172.16.1.1 | TCP | 66 | 5001→40358 [ACK] Seq=1 Ac |
| 39 | 7.514064 | 172.16.1.1 | 172.16.1.2 | TCP | 1514 | 40358→5001 [PSH, ACK] Seq |
| 40 | 7.514106 | 172.16.1.2 | 172.16.1.1 | TCP | 66 | 5001→40358 [ACK] Seq=1 Ac |
| 41 | 7.514115 | 172.16.1.1 | 172.16.1.2 | TCP | 1514 | 40358→5001 [ACK] Seq=3332 |

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ▶ Ethernet II, Src: IntelCor 5b:e7:99 (90:e2:ba:5b:e7:99), Dst: Xensourc 1c:b2:3f (00:16:3e:1c:b2:3f)
 ▶ Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.1.2 (172.16.1.2)
 ▶ Transmission Control Protocol, Src Port: 40357 (40357), Dst Port: 5001 (5001), Seq: 0, Len: 0

```

0000  00 16 3e 1c b2 3f 90 e2  ba 5b e7 99 08 00 45 00  ..>..?.. [....E.
0010  00 3c 5d f1 40 00 40 06  82 a7 ac 10 01 01 ac 10  .<|.@.@. ....
0020  01 02 9d a5 13 89 57 a8  21 1b 00 00 00 00 a0 02  .....W. !.....
0030  72 10 d2 be 00 00 02 04  05 b4 04 02 08 0a 02 31  r.....1
  
```

File: "my.out" 142 MB 00:00:12 Packets: 67563 - Displayed: 67563 (100.0%... Profile: Default

Capturing Packets

Run wireshark as an admin user.

Choose the capturing interface.

Run it until you want to stop.

Filtering

You can filter data according to the IP, Protocol.

You can follow a specific data stream.

You can analyse the information of the different protocol packages.

You can save the data in pcap files.

Following

Related to the Filtering process you can follow a specific stream.

With this you can follow specific conversations.

Also, it provides a good interfaces to see protocol exchanges.

Analysing

You can use the statistical tools from Wireshark

They provide different information about the packets such as timing, sender, receiver, etc.

It is interesting for having a general idea of the network.

Network Data

<http://panda.gtisc.gatech.edu/malrec/>

Exercise

- 1 Provide the statistics of the file (Packets, Time Span, Average pps, Average Packet size, Bytes, Average Bytes per second).
- 2 What percentage of packets are IRC packets?
- 3 What is the victim IP?
- 4 How many IRC conversations are? Who are the agents?
- 5 How many packets have been sent in every conversation?
- 6 Show a graph of packets per second for all packets in the pcap file.
- 7 Show an example of a conversation
- 8 Describe the information that can be extracted from the IRC conversations.