17.1 Wireshark

This tutorial tries to give you some hands-on experience in using wireshark. Wireshark offers you a lot of assistance when it comes to analyzing sniffed traffic. We encourage you to make use of them.

17.1.1 Warming Up

- Start up wireshark **in the lab VM**
- Start a capture session on your main network interface (`eth0`).
- Open a terminal and issue the command: `curl -q http://www.nt.uni-saarland.de/`

Answer the following questions **using only your packet capture**:

- How many distinct flows of data can you identify?
- What protocols are used to facilitate your web request?
- Do you see any ARP requests or responses? If so why, if not why not?
- How many DNS request do you see? Why is there more than one?
- How many RRs are included in the answers to the DNS queries? What are their record types?
- What was the HTTP status code returned by the server?
- What is the name of the software serving the web page?
- Does the web server set a cookie?
- How long did it take the webserver to answer your request?
- Did the complete website arrive from the server in one IP packet? If not, how many packets were sent?
- What is the MAC address of your host?
- What is the MAC address of the default gateway?
- Can you find the MAC address of the webserver? If so, how? If not, why not?

17.1.2 What the Heck?

Open the file **scan.pcapng** in wireshark.

Background:

This capture file was taken from a very large and long-time established network that had been considered very stable and unchanging. The network administrator has given you this file that contains what he considers “suspicious” behavior and has asked you to evaluate it.

Questions:

- What is the IP address of the scanning host?
- What is the IP address of the target host?
- Which TCP port is open on the target?
- Which ICMP packets contain non-standard Type/Code numbers?

17.1.3 Cursed

Open the file **cursed.pcapng** in wireshark.

Background:

Sure, Scott is one of your best friends at the company, but he's always asking for computer help. No amount of training seems to work. Today he sent you a text message to complain that his computer hard drive light is always blinking - even when he's not touching the keyboard. With a promise of decent drinks after work, you remotely connected to his machine and started capturing traffic. Sure enough - loads of packets were flying around. Just then, Scott arrived in your office.

Hmmm... Scott is here, but his computer seemed to have a lot of network activity going on. You stopped the trace to see what happened in the background on his system.

Questions:

- How many different IP hosts is Scott's machine communicating with?
- What is the average packets-per-second rate seen in this trace file?
- How many HTTP POST requests did Scott's machine send?
- What location information is contained in the POST to scanscout.com?
- What application appears to be generating these GET/POST requests?
- Find export and reassemble *load_small.png*. What shape is displayed in the image?

17.2 GNS3

17.2.1 Trouble in Virtual Paradise

For this exercise you will have to build a small network using GNS3.

a. Start up GNS3 and create a new project. Set up the following network.

```
                     +------------+         +-------------+
+-----------+        |  =======>  |         |  =======>   |         +-----------+
|   VPCS    | ------ |     SW     | ------- |     SW      | ------- |   VPCS    |
+-----------+        |  <=======  |         |  <======    |         +-----------+
                     +------------+         +-------------+


    PC 1                  SW 1                    SW 2                    PC 2
```

b. Set up IP connectivity on the network by configuring `PC1` and `PC2` using IP addresses from the RFC1918-ranges. Verify your configuration by pinging `PC2` from `PC1`

c. A friend of yours is asking you for help with a networking issue he has been having. His network is very similar to the network given above and has an additional computer (`PC3`) attached to a third switch (`SW3`). To make his network more resilient against link failure he thought it would be a good idea to attach `SW3` not only to `SW1` but to `SW2` as well. You decide to help him in diagnosing the problem.

Add the additional components to your network and configure `PC3` with an IP address in the same subnet as `PC1` and `PC2` and verify your configuration as above.

- What is the problem?
- What is the cause? Describe what is happening step by step.
- How can you fix the problem?