LAB 3 – TRAFFIC ANALYSIS

1. Packet trace a.pcap

- **What is the most prevalent application protocol in the trace?**
  The most prevalent application protocol in this trace is FTP, with a 34.7% of packets.
- **What are the IP addresses and ports of the client and the server?**
  Client = 192.168.56.1:54017
  Server = 192.168.56.101:21
- **Which server (type and version) is running?**
  The server running is the redmint FTP server version 6.4.
- **Write a filter to display the first TCP packet sent in each flow in the trace**
  The filter to write should be: `tcp.seq==0`
- **Looking at the whole trace, what is the client trying to achieve?**
  It is constantly trying to log into the server, failing to do so by putting an incorrect password, stopping the connection, and retrying to login once again.

2. Packet trace b.pcapng

- **How many TCP and UDP conversations are contained in the trace, and how many hosts are involved?**
  There is a total of 1055 TCP conversations and a total of 1400 UDP conversations.
  There is a total of two hosts involved in the trace, PcsCompu_5e:fe:db and PcsCompu_cb:24:13
- **Looking at the whole trace, what is the host 192.168.5.51 doing?**
  It is scanning the ports that are open at 192.168.5.20.
- **Enumerate all different techniques that 192.168.5.51 is using.**
  It's using the next techniques:
  - TCP SYN scan.
  - TCP Xmas scan.
  - TCP connect scan.
  - UDP scan.
- **Which ports are open at 192.168.5.20?**
  Th only port open at 192.168.5.20 is port 80.

3. Packet trace c.pcapng

- **Write a filter to display all HTTP conversations in the packet trace**
  The filter to display all HTTP conversations should be: `http`
- **What is the server and the user agent?**
  User agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
  Server agent: Apache/2.2.16 (Debian)

- **Get all the passwords (in plaintext) of the HTTP Authorization headers contained in the trace.**
  Correct passwords:
  - profesor: claveprofesor
  - profesor2: facil

  Incorrect passwords:
  - profesor: 234235235
  - profesor2: facilona
  - profesor2: fallo