Assignment: Using Wireshark

# Protocol Analyzer

This is a hands-on assignment using the tool Wireshark.

# Learning objectives

* Learn how to use a protocol analyzer tool.
* Understand the TCP/IP protocol stack using hands-on activities
* Perform simple protocol investigation
* Identify network traffic patterns

## Tools

* Wireshark - See installation instructions [here.](https://github.com/joaoceron/assignments/blob/master/pdf/wireshark-install-basics.pdf)

## Exercise

The **mm-malware.pcap** registers Mirai/Miori Malware exploitation IoT devices using a list of default factory password. As several IoT operating system devices use Android, BusyBox or another Linux variant, a huge quantity of devices had been affected by this Malware variant.

**OBS**: Please, submit the answers in a pdf file. Note, you must submit the Wireshark screenshot to support your answers.

Download **Mirai-Miori-malware.pcap** and use Wireshark to inspect packets and answer the questions:

1. **Which day this capture was realized?**

**TIP:** Look at the statistics menu

1. **Which PROTOCOL did Malware use to test Users/Passwords?**

**TIP**: start your investigation using “Statistics 🡪 Protocol Hierarchy”. After a look at some "strange" protocols closer – use the right button on a specific protocol to select all content (apply filer 🡪 selected) and then select a line and (follow TCP stream) to see the entire dialog, until you get your conclusion choosing between them.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

1. **Identify the comprom­­ised device (IP ADRESS).**

**TIP**: Look for the string “Success!” in all packets using (Edit 🡪 Find Packet). Normally after a correct login, we receive an "Authentication Success!" message.

A screenshot of a cell phone

Description automatically generated

1. **What was the USER/PASSWORD used to get access? (print the result of “follow TCP stream") showing the pair user/password.**

**TIP**: select the right packet first. You can search for a "busybox” string as an indication of a successful login.

1. **Use the menu “Statistics 🡪 IO Graph” to generate a graph including all of these items:**
   1. Real date and time in X-AXIS
   2. Total number of packets by second
   3. Number of DNS packets/s
   4. Number of Telnet packets/s

**TIP**: Remember use very distinctive colors in each line

Additional information:

If you are interested you should compare your results with a packettotal malware analysis:

<https://packettotal.com/app/analytics?id=f03c4f0bad51bf46116c9e6ec8a88945&name=signature_alerts>

# Answers

1. **Which day this capture was realized?**



1. **Which PROTOCOL did Malware use to test Users/Passwords?**

**R:** TELNET/23

1. **Identify the comprom­­ised device (IP ADRESS).**

**R:** 192.168.10.1

A screenshot of a cell phone

Description automatically generated

1. **What was the USER/PASSWORD used to get access? (print the result of “follow TCP stream”) showing the pair user/password.**

**R:** admin/admin

A screenshot of a social media post

Description automatically generated

1. **Use the menu “Statistics** 🡪 **IO Graph” to generate a graph including all of these items:**

A screenshot of a cell phone

Description automatically generated