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

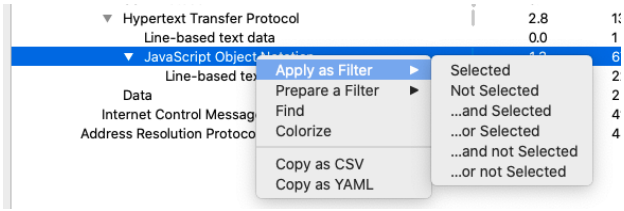
The **mm-malware.pcap** registers Mirai/Miori Malware exploitation IoT devices using a list of default factory password. As several IoT operating system devices use Android, BusyBox or another Linux variant, a huge quantity of devices had been affected by this Malware variant.

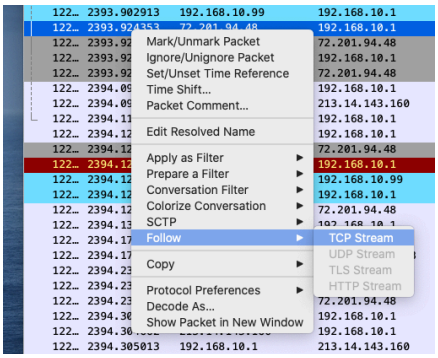
OBS: Please, submit the answers in a pdf file. Note, you must submit the Wireshark screenshot to support your answers.

- Install Wireshark (https://www.wireshark.org/download.html)
- Download **mm-malware.pcap** (https://github.com/LMBertholdo/classes/blob/master/wireshark/mm-malware.pcap)
- Answer the questions

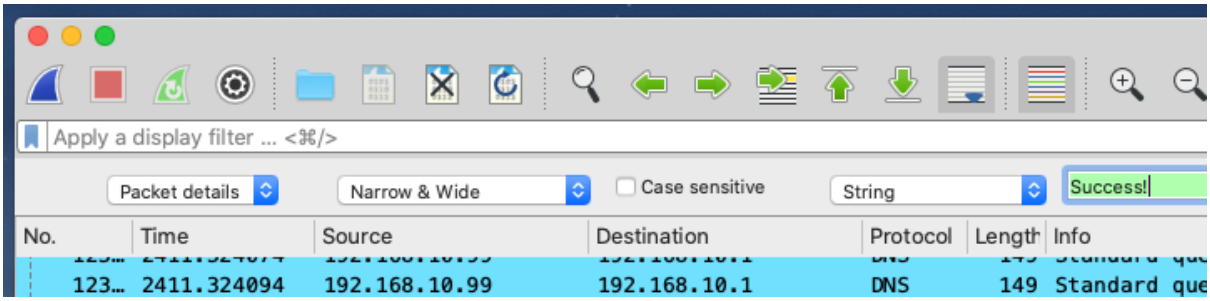
1) **Which day this capture was realized?**
TIP: Look at the statistics menu

2) **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.





3) **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.



4) **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.

5) **Use the menu "Statistics → IO Graph" to generate a graph including all of these items:**
   a. Real date and time in X-AXIS
   b. Total number of packets by second
   c. Number of DNS packets/s
   d. 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