**Tools for designing and detecting attack scenarios in CPS (Cyber Physical System)**

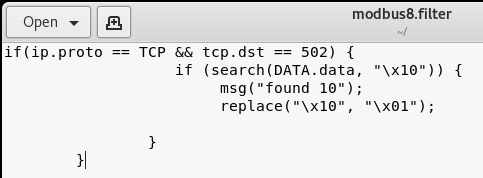


Fig. 1 An example of Ettercap filter

This document is shortly demonstrating the use of Ettercap filters, Metasploit, and Snort. First, the Ettercap generally use for the ARP spoofing attack and scanning hosts. It also has another feature name; Ettercap filter’ to inject a random value in a packet. Figure 1 shows an example of Ettercap cap filter, which first detects the function code 10 in Modbus responses and replaces it with function code 01. Refer the uploaded file **‘ettercap.filters’** to explore more filters.

Now the critical task is how to use this filter in Ettercap. Before uploading the filter in figure 1, it needs to be compatible with Ettercap. To do this, refer the command in figure 2. It converts the filter into the ‘.**ef** ’ format that Ettercap understands.

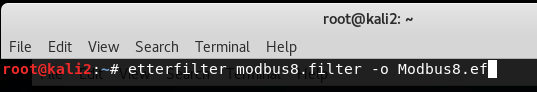


Fig.2 Make the filter compatible to Ettercap

Here the filter is ready. Refer the figures 3 and 4 to know how to upload the filter in Ettercap. Note that, a filter should be uploaded when MITM attack is ongoing.

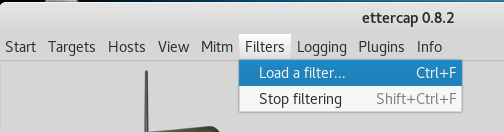


Fig.3 Locate the filter uploading option in Ettercap

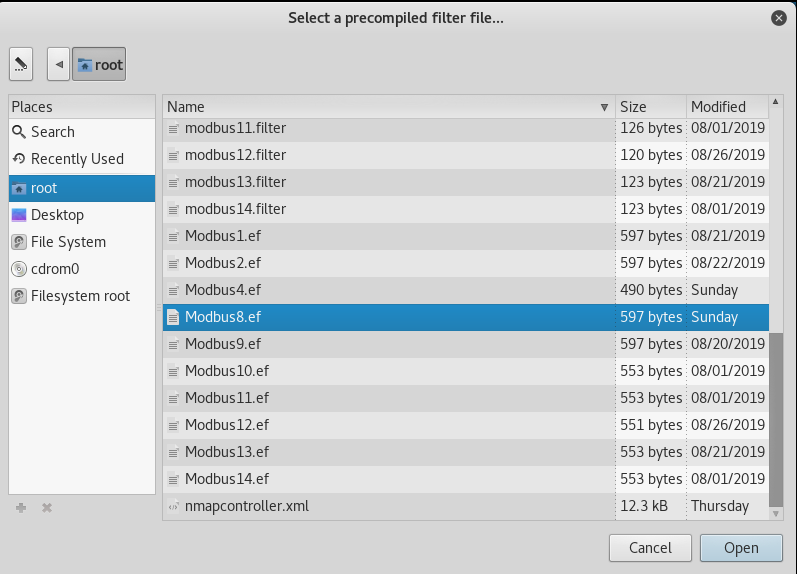


Fig.4 Select the precompiled filter

The second tool is Metasploit which is a top-rated tool for pen-testing. It has some SCADA related modules to exploit security controls. Start the Metasploit using the **‘msfconsole’** command.

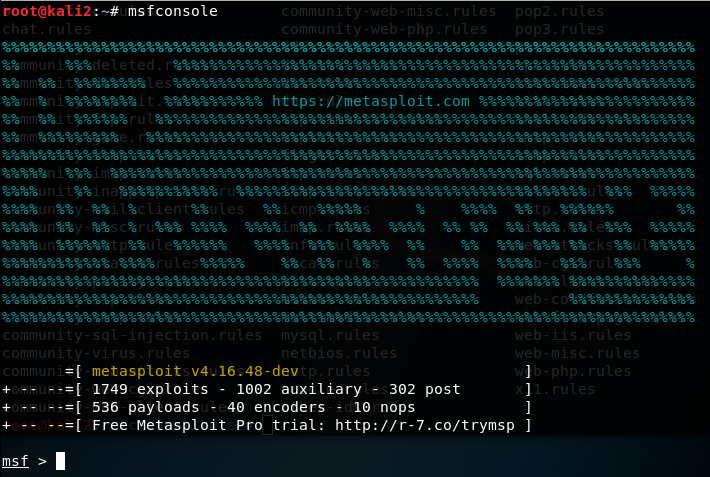


Fig.5 Start Metasploit

Figure 6 shows the implementation of Modbus client module. This module changes the specified register value and reads any register value. Read its description using **info** and **options** commands.

In the following figure, we first set our target, which is the controller using its IP address. Then, we set the write action, address of the register, and the malicious value, i.e., 16473. To run the module, we can use **exploit** or **run** command.

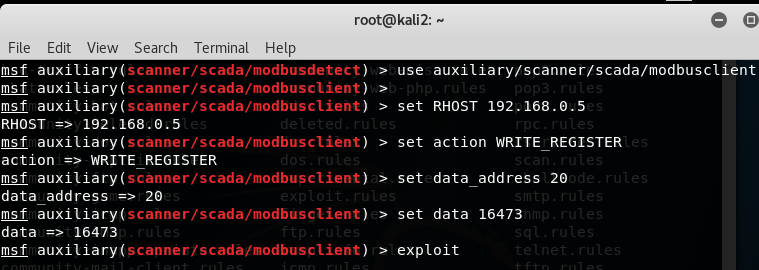


Fig. 6 Modbus client module to change the register values

The third tool is Snort. It is an open source Network Intrusion Detection System (NIDS). It uses rules or signatures of known attacks to detect an intrusion. It is compatible with all the operating systems. We can download it from <https://www.snort.org/downloads>.

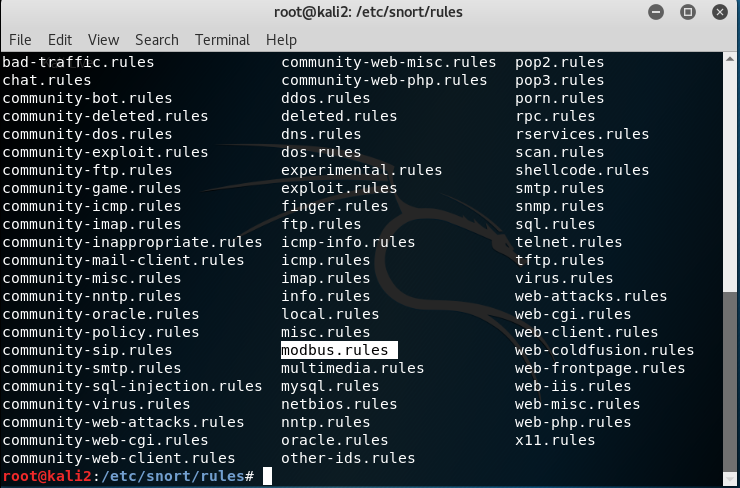


Fig. 7 Snort rules

Figure 7 shows the database of snort rules. It includes a variety of rules. For SCADA system, we may create our own rule, or we can use the rules available [here](https://github.com/digitalbond/Quickdraw-Snort/blob/master/modbus.rules).

To run the snort, first, create a folder name**log** so all the alerts will be available in that folder. Then configure the **snort.conf** file according to the requirement. Now run the following command to start the snort.

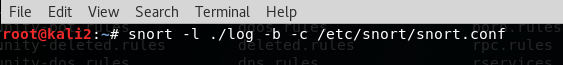


Fig. 8: Run snort

If we have a captured pcap file of an attack, then we can run snort on that file to collect alerts. Refer to the command in figure 9.

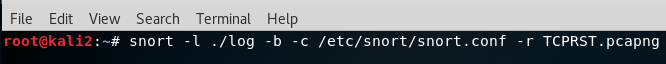


Fig.9: Run snort on pcap file

Note – run the Snort before performing any attack. This way, the snort inspects the packets in a flow using its database of rules. Use **Ctrl + c** tostop the snort.