GrassMarlin

1 Overview

This lab provides an introduction to GrassMarlin, a software tool that provides a method for discovering and cataloging Supervisory Control & Data Acquisition (SCADA) and Industrial Control System (ICS) hosts on IP-based networks.

1.1 Background

The student is expected to have some familiarity with the Linux command line. And some experience with the Wireshark tool is expected (e.g., the wireshark-intro lab).

2 Lab Environment

This lab runs in the Labtainer framework, available at http://my.nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

```
labtainer grassmarlin
```

A link to this lab manual will be displayed, along with a link to the GrassMarlin User Guide.

3 Network Configuration

The lab consists of a single computer that contains the GrassMarlin tool, and a PCAP file.

4 Lab Tasks

Start the GrassMarlin application using this command on the terminal titled "analyst@grassmarlin:

```
grassmarlin
```

Refer to the GrassMarlin User Guide for information about the tool.

From the "File" menu, select "Import Files" and use the "Add Files" button and the file browser to add the PCAP file found at "analysist/ics-trace.pcap". Then use the "Import Selected" button on the "Import" dialog to import that file. It may take a minute to complete the import. When the import completes, close the "Import" dialog.

You should then see the "Logical Graph" of system components that the GrassMarlin tool discovered from the PCAP file.

Right click on components and select "View Details" to learn what the tool has discovered about each component. On the left hand panel, expand the node lists to locate summeries of packet traffic sent and received by each node. Right click on one having substantial traffic, and select "View Frames" to view the captured packets. If you find interesting traffic, you can right click on a frame and select "Open in Wireshark".

5 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.