Network IDS Analysis – Instructions

Introduction

- Estimated time to complete this lab - 30 minutes

Objectives

After completing this lab, you will be able to use Squil and Wireshark to:

- Analyze malicious incidents using the Snort network IDS backend
- Pivot between tools for more detailed network traffic analysis

Prerequisites

Before working on this lab, you must have:

- Reviewed the CDA-F Network IDSs training module

Overview of the Lab

Students will apply their existing analysis knowledge and tool skills (e.g., Wireshark) along with additional concepts and solutions (i.e., Squil) from this module to analyze an incident. An Ubuntu desktop is provided for tool access and analysis. The lab mimics analysis scenarios often performed in the real world. While other tools may be used in operational environments, the same analysis concepts can be applied to them.

Computers in this Lab

This lab uses computers as described in the following table.

Computer	Role	Configuration
student-desktop-NN	Analysis Host	Ubuntu OS with Sguil & Wireshark

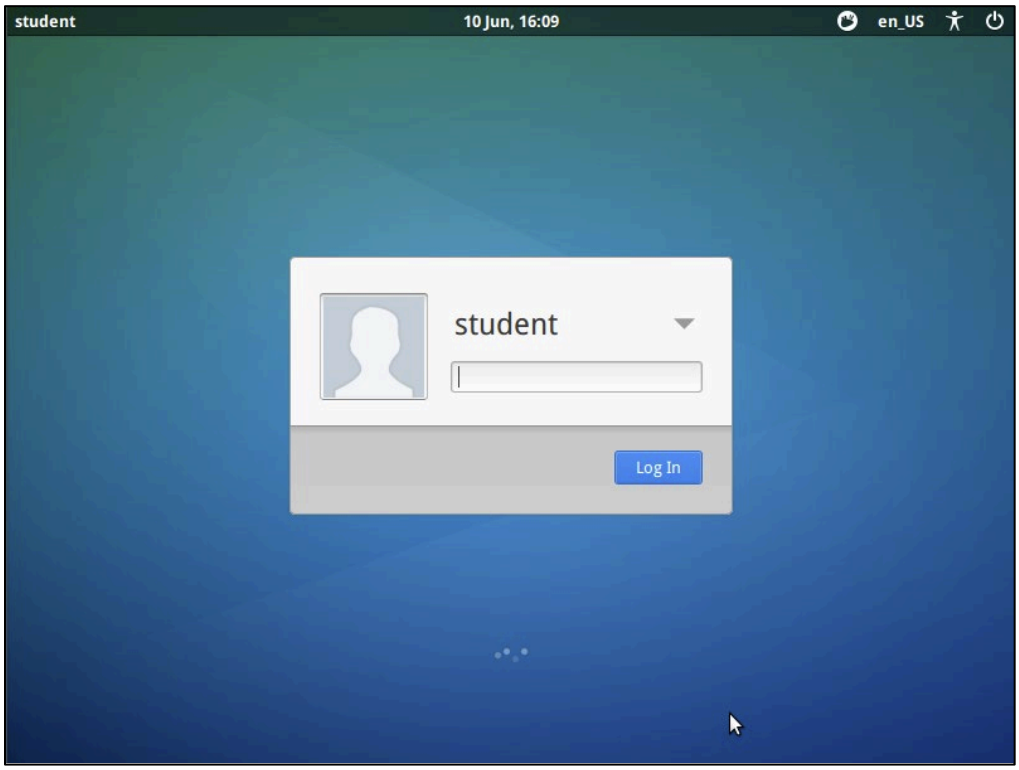
NN in the table is an instructor assigned student number from 01 to 20. Login to the Ubuntu desktop as "**student**" using the password "**12qwaszx!@QWASZX**".

Table of Contents

Instructions

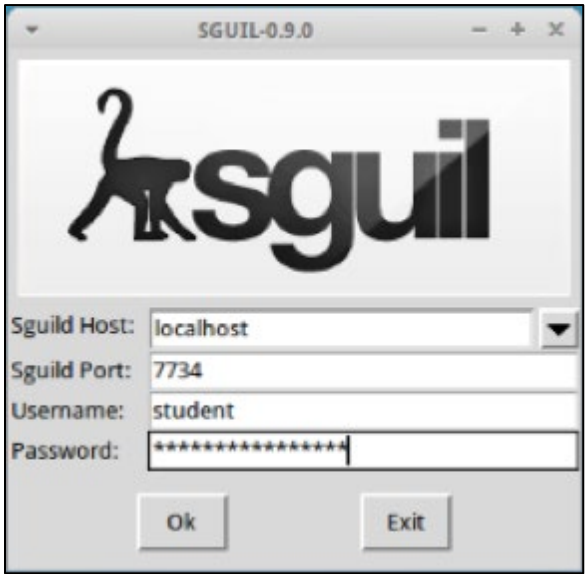
Opening Squil

1. Enter “student” for the username if prompted and “12qwaszx!@QWASZX” as the password. Press the **Log In** button to continue.

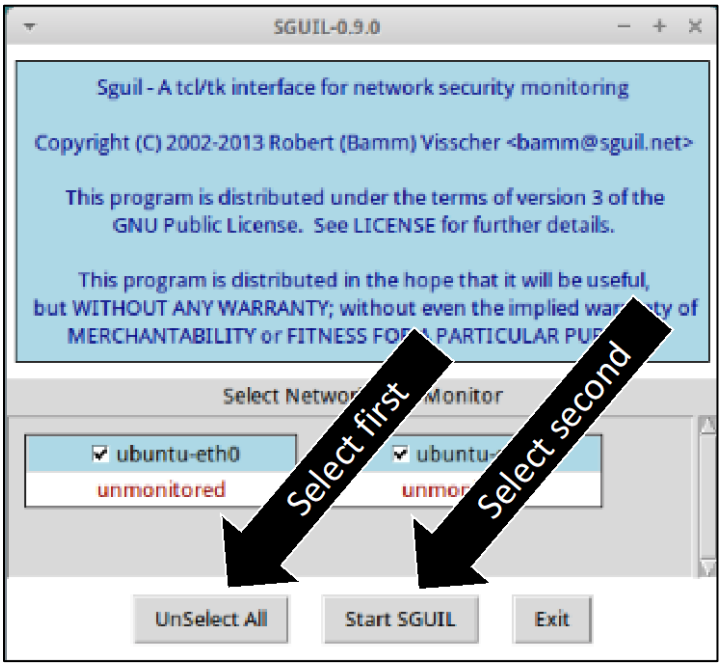


2. Open Sguil by starting the application and logging in. Start by pressing the **Sguil** icon.

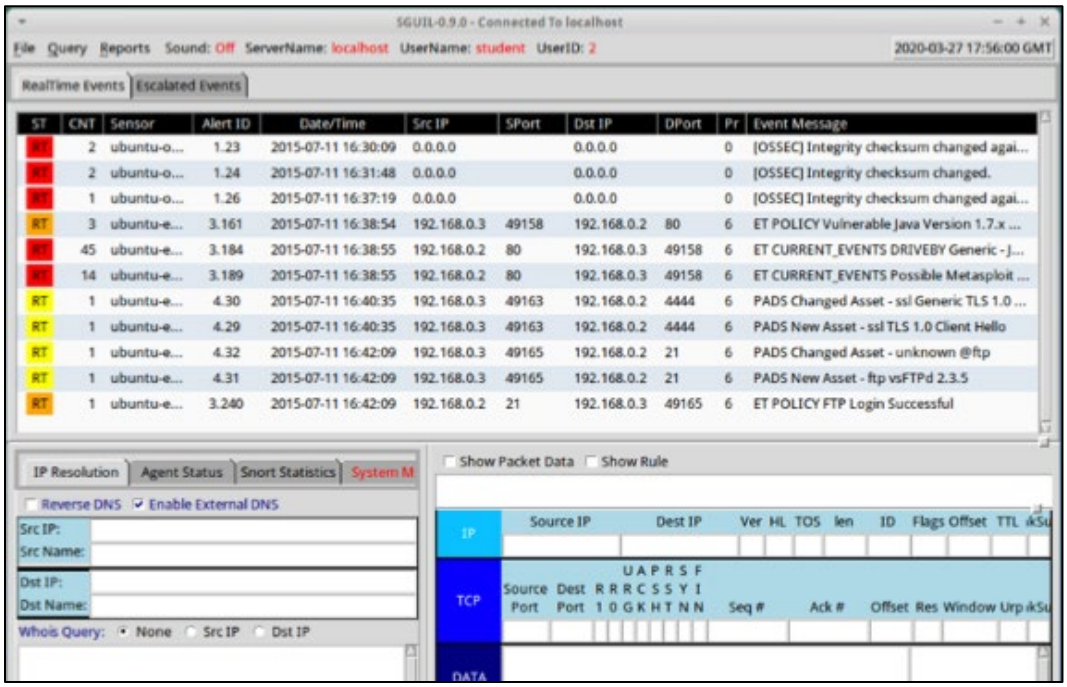
In the login prompt, enter "student" for the username and "12qwaszx!@QWASZX" for the password. Press **OK** when finished.



3. Select the sensors to attach and open the main Sguil interface. In the startup window that appears after logging in, press the **Select All** button to automatically enable any attached sensors. In this lab, the sensors are ubuntu-eth0 and ubuntu-ossec.



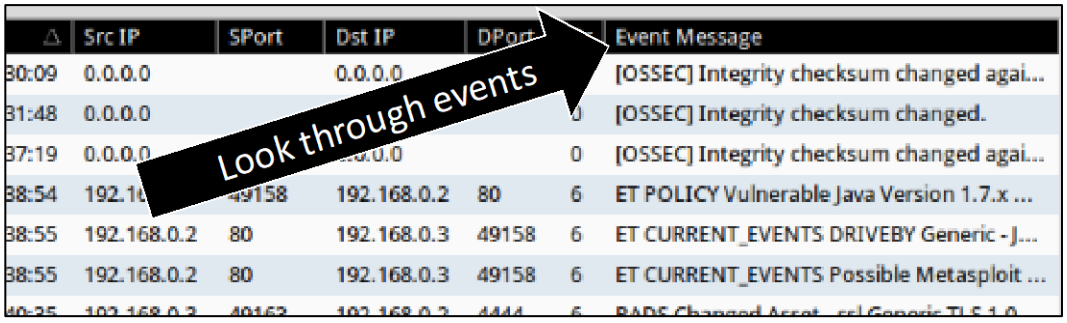
Press the **Start SGUIL** button to bring up the Sguil front end.



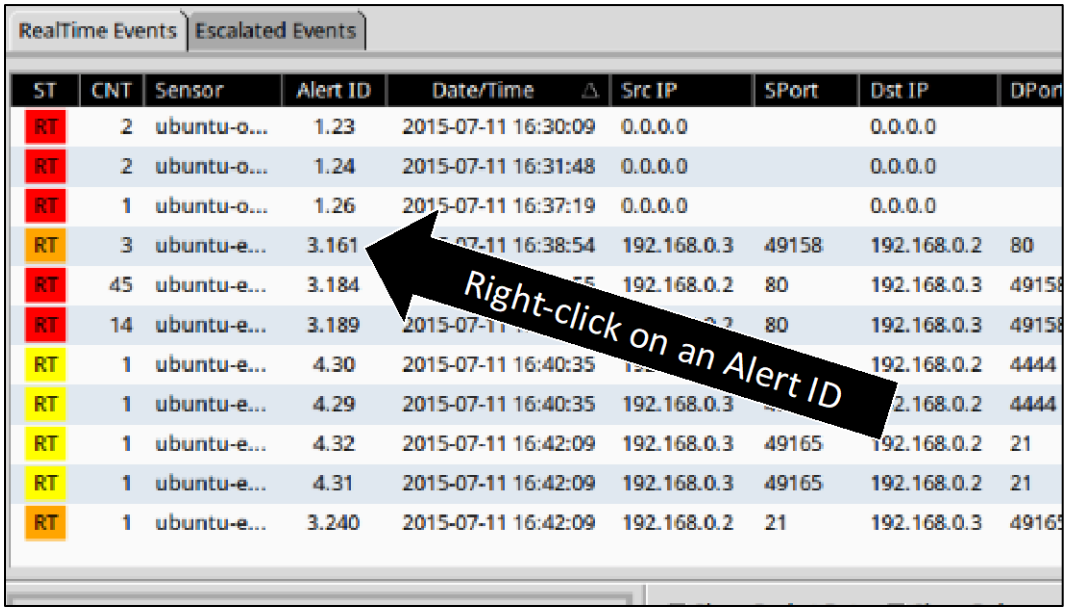
NOTE: If you receive an "Unable to connect" message, wait a minute and try again. Sguil's backend may not have fully started yet.

Using Sguil's Basic Features

1. Become familiar with the alerts displayed in Squil by looking through them.

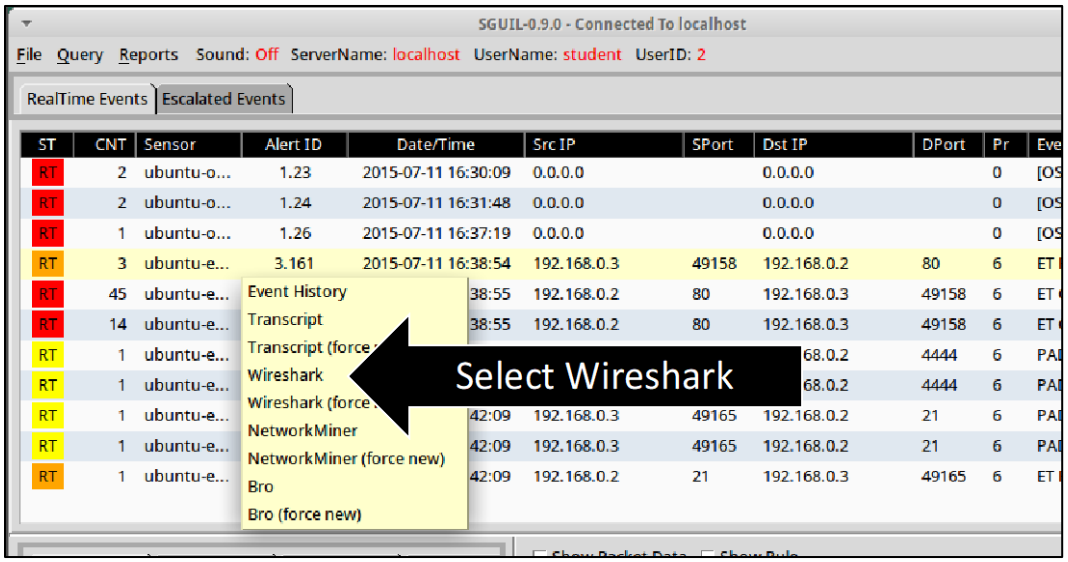


2. Explore Sguil's integration with Wireshark. Start by **right-clicking** on an Alert ID field to open a context menu of tool integrations.



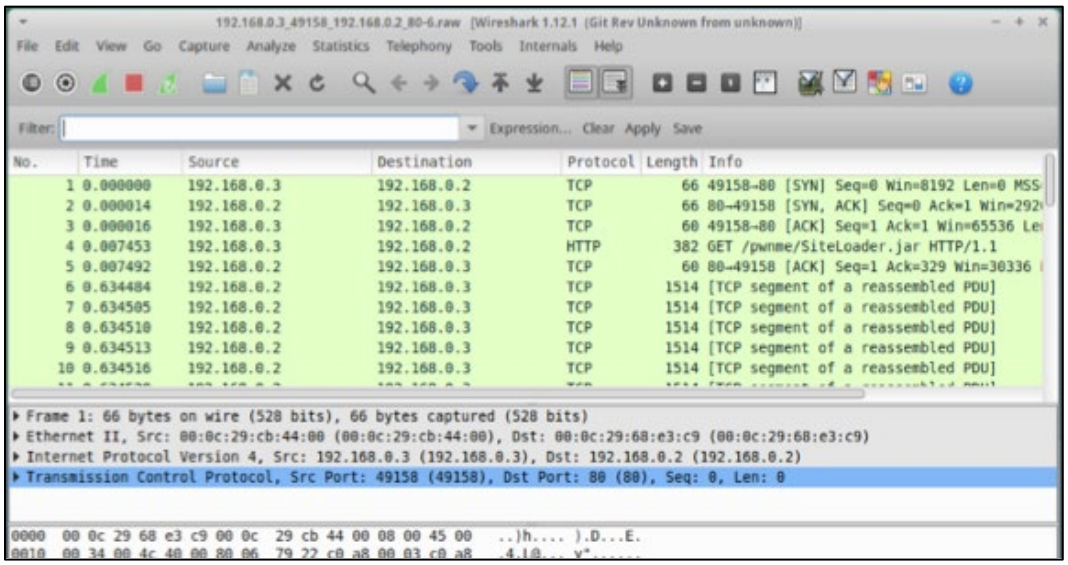
NOTE: You MUST right-click on an Alert ID field. Right-clicking other fields offers different options. In some cases you have to hold the right-click down to keep the menu open.

3. Select **Wireshark** from the list of tools integrated with Sguil.

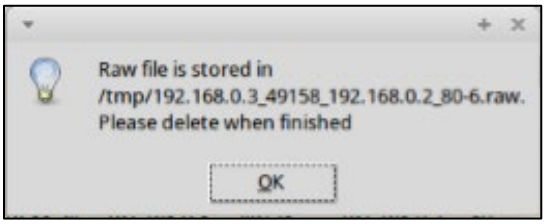


NOTE: If you had to hold the right-click down above, select an option by moving the mouse over Wireshark and releasing the right-click.

4. Analyze the network traffic as covered in the previous labs after Sguil locates the associated network conversion stream and opens it in Wireshark. For example, apply display filters to isolate traffic of interest or select “Follow TCP Stream” to analyze text content transferred.



5. Close Wireshark when finished. You may notice a message box indicating the temporary location of the raw PCAP file. If you chose to pivot to Wireshark from an alert, Sguil creates files like these for a session’s PCAP before loading it into Wireshark. Press **OK** to close this message.



Questions

Your enterprise maintains a set of older workstations for running legacy applications no longer supported by modern day OSs. Due to the outdated OS, they must use an old version of Java. One of these hosts was compromised with an exploit targeting a vulnerability in this version of Java. The exploit provided shell access to the attacker, who then downloaded an additional tool to the host.

Using Sguil, answer the following questions with the information provided above.

- What was the IP address of the attacker? _____
- What was the IP address of the victim? _____
- What was the name of the file downloaded? _____
- What was this type of attack? _____

Try to determine the answers on your own at first. If you are having trouble, see the next page for some hints. Close Wireshark when finished answering all the questions.

Answers

- What was the IP address of the attacker? **192.168.0.2**
- What was the IP address of the victim? **192.168.0.3**
- What was the name of the file downloaded? **download.7z**
- What was this type of attack? **Client-Side**

Having trouble with this lab? Here are a few hints that might help.

- There are two critical events, one for the initial attack and another for the subsequent file download.
- Events occurred within the past 20 events logged by the sensor.

See the Solution Techniques document for the answers and a method of solving each of the lab questions.

You have now completed this lab.