**Project Name:  Security Onion, Squil**

**Technology:  IDS / IPS and Related**

**Market:  Security**

**Name / Group: Gagneet Sahota**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Potential Providers:**

Security Onion: Squil

**Intended Activities:**

Analysis

**Design:**

The goal of this lab is to begin to become familiar with one of the primary environments that will be used in this course.  In order to do so, we must become accustomed to using Security Onion tools (such as Squil, Squert, and Kibana). Even if people have been working systems for a long period of time, they will notice changes in the evolution of systems over the years.

**Directions:**

Answer the questions below in preparation for the practical portion of your lab (in Section 3).

**Questions to Answer:**

**Section 0:  Lab Basics**

Explain the following terms / tools:

Security Onion- A linux distro with a suite of tools based for security operations.

Squil- A network security monitoring and event analysis of traffic.

Squert- a web application used to query and view event data stored in sguil.

Kibana- a visualization platform designed to work with Elastic.

**Section 1:  Lab Environment**

How would you define the tools Squil, Squert, and Kibana?

* A combination of linux tools used to monitor and display events that occur on the monitored network.

Said differently, What do each of these tools provide / accomplish?

* Squil allows you to monitor the traffic to see events. Squert works with Sguil to queiry the data. And kibana is used for elastic.

What do Squil, Squert, and Kibana offer our networks and systems in terms of security?

* It allows us to monitor and analyze packets of the networks to see if any threats have occurred. But these tools do not do anything to prevent any attacks from occurring.

Give an example of how each tools is unique / what specific benefit each tool provides.

* Sguil is unique as it gives you real time access of events going on the network. One of the benefits is the ease of the use with the GUI.
* Squert allows data to be filtered and displayed easier in real time, which can be filtered by Ip addresses and countries.
* Kibana- is a visualization tool used for logs. It provides graphs, such as heat maps, line graphs or pie charts.

**Section 2: Practical**

Security Onion

**Exercise 1 - Intro to Squil**

Once you have logged into your VM, open a terminal window by clicking on “Applications”, then “Utilities” and scroll down to and click “Terminal”. Change directory to where you have stored the downloaded Exercise pcaps. If you used the Chromium web browser, those files are stored in the “Downloads” directory.

Extract the files contained in

Ex1-honeynet.org-Scan19.tar.gz

by using the following command:

mkdir ./Exercise1/ && tar fvxz Ex1-honeynet.org-Scan19.tar.gz --directory ./Exercise1

Change directory into the “Exercise1” directory.

Minimize the terminal window and double-click the “Squil” icon on the desktop.

Login to Squil using the credentials that you setup when you built the Security Onion VM; note that these are not the same credentials you use to login to the system. A new window will appear asking which networks to monitor. There should be two options - seconion-ossec and seconion-enxxxx. Ignore the interface labelled “ossec”; make note of what follows the hyphen on the interface starting with “en”. It should be something something similar to enp#s#, where the #-signs are numbers. This is the name of the capture Ethernet interface used for monitoring and it will be needed later. Click “Select All” once you have noted the Ethernet interface name and then “Start SGUIL.” The sguil interface should appear. Make sure that the “RealTime Events” tab is selected and the box under the tab is clear of events. If there are events listed, click one and press F8 to clear it. If there are more than one, keep pressing F8 until they are all cleared.

Bring the terminal back to the foreground. At the command line, enter the following command:\ sudo sleep 15s && sudo tcpreplay -i <Ethernet interface name> -M 100 newdat3.log\ For example, if the name of your capture Ethernet interface is “enp0s8”, the command would be as follows:

sudo sleep 15s && sudo tcpreplay -i enp0s8 -M 100 newdat3.log

When you press enter, you will be prompted for the sudo password; use the password used to login to the VM. Then switch back to the sguil screen and wait.

In about fifteen seconds, long enough to switch back to squil, tcpreplay will replay the newdat3.log pcap file and events will appear in squil. There should be roughly 15 events. Let’s take a look at some of them.

Click on

the event with the Event Message of “GPL TELNET Bad Login”. The fields at the bottom of the window should populate. If they do not, make sure that the checkboxes next to “Reverse DNS”, “Enable External DNS”, “Show Packet Data” and “Show Rule” are all checked.

Let’s find out where this failed login attempt possibly originated from… Next to “Whois Query” are three radio buttons; select “Src IP” and wait for the field under that to populate. Scroll down in that field until you see “country:”. What two letter country code is present? You can use Google to determine what country this is, or, if you scroll down to the “address:” fields, you can find it there. What country is the possible source of this attack?

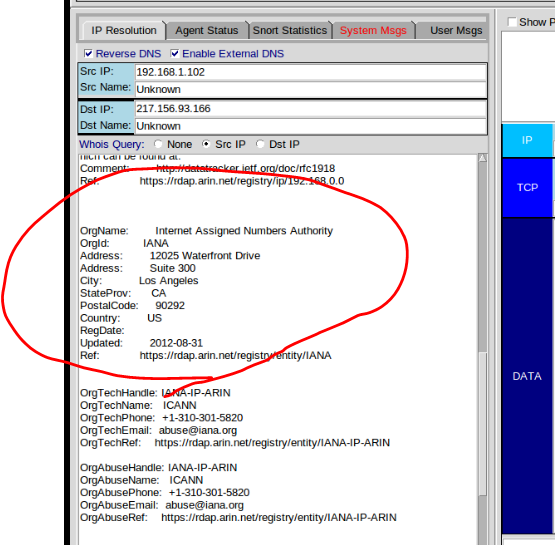
Now that we have determined where the attack IP is likely located, we conclude that this is an unauthorized access attempt since we do not have an office, etc. in the country that would be accessing this system.

Squil allows you to Classify events based on the results of an investigation. To classify this event, right-click on the “RT” on the left of the row for this event. In the pop-up menu, go to “Update Event Status” and then chose “CAT III - Attempted Unauthorized Access (F3)”. You can also select the event and press F3. The event will not disappear from the “RealTime Events” field.

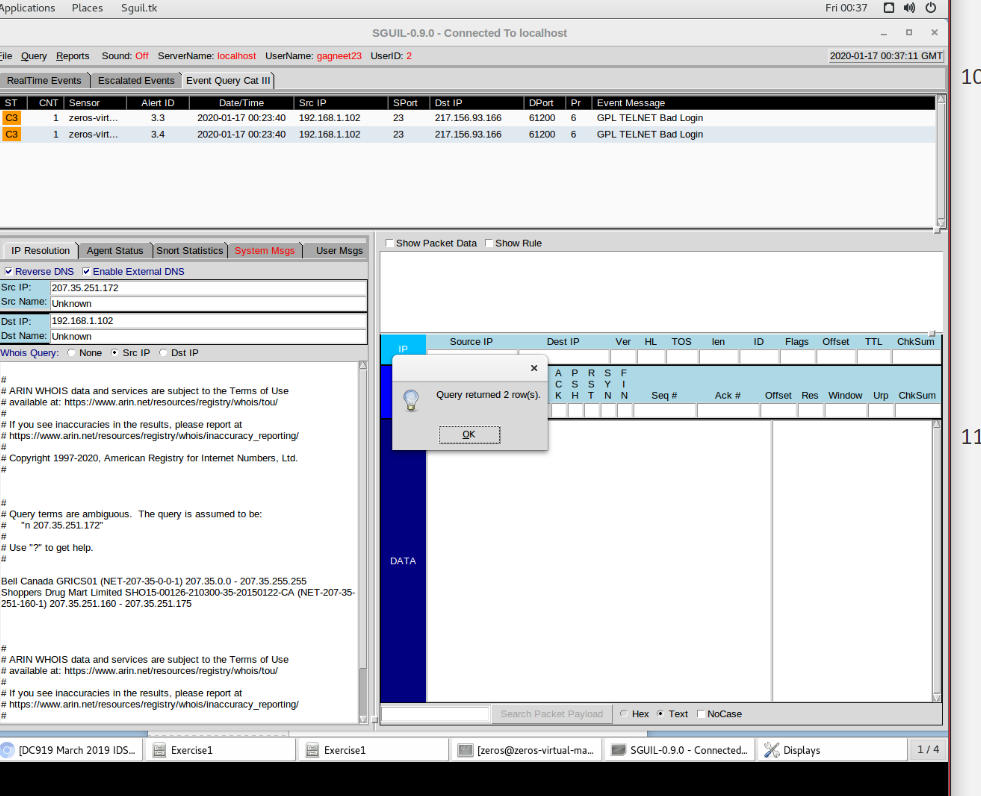
The “RealTime Events” view allows you to see events as they are generated by the IDS. As a SOC analyst monitoring an IDS, this is the event queue from which you would pick and investigate events. Now, say you want to look at all of the events that have been classified as “Attempted Unauthorized Access”. To do this, select “Query” from the squil menu bar, choose “Query by Category” and then the “CAT III: Attempted Unauthorized Access” query. This opens a query builder screen. With the query builder function, you can query the events catalogued by Security Onion. For this exercise, click the “Submit” button. A new tab with the query results will appear and the event you classified in Step 9 should be displayed. When you are ready to continue, close this tab using the “Close” button in the upper left corner.

Squil also allows you to perform packet analysis in the same interface. Select the event labelled “ET ATTACK\_RESPONSE Possible /etc/passwd via SMTP (linux style)”. The fields at the bottom should populate; if they do not, make sure the checkboxes referenced in Step 7 are checked. Using the blue-color coded fields on the bottom right of the screen, we can see the header and payload information for the packet, including source and destination IP and port. The “DATA” field is where we want to dig for information on this attack. According to the event description, someone attempted to email the contents of the /etc/passwd file to someone. Using the information in the “DATA” field, examine the packet payload and determine the recipient of the file. What is the recipient (TO:) email address?

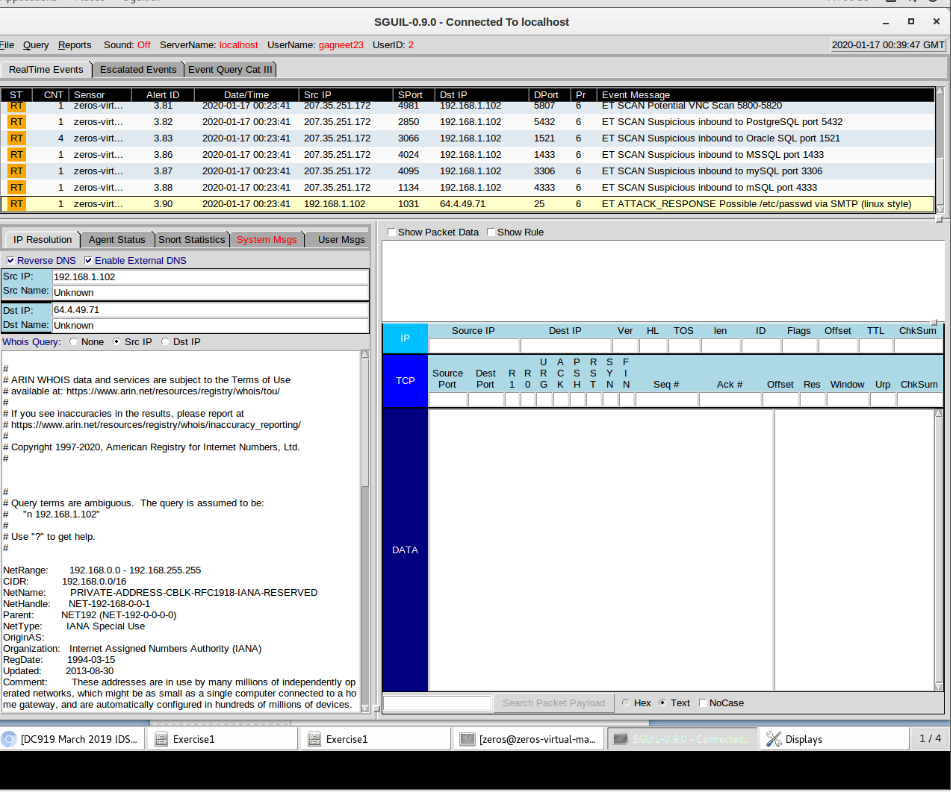
Location of IP



Redefined as events as “login breach”



Looking at the “attack response”



**Useful Sites:**

https://securityonion.net

**Deliverable(s):**

Use this document as a base and include your ideas here.

(1.) Answer Questions

(2.) Document your Installation (with command line examples and screenshots, where relevant).

Remember that the more clear that your documentation is, the better that it will serve you in the long run.

Submit and upload to Canvas in the assignment area for this project.