**Project Name:  Packet Replay Lab**

**Technology:  Security Onion**

**Market:  Security**

**Name / Group: Gagneet Sahota**

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

**Directions:**

Answer the questions below in preparation for the practical portion of your lab (in Section B).  All responses are individual / no group work.

**Section A: Questions to Answer**

**Part 01:  Security Onion for SME (Small to Medium Enterprise) vs. Large Enterprise**

Identify and illustrate the differences between designing a security onion deployment for a SME vs a Large Enterprise.

Be sure to make note of any architectural differences that you may consider for a particular organization based on either its overall geographic footprint or scale.

When considering a large enterprise, consider that you own a large retailer with somewhere between 100 to 400 sites across the nation / world.

Be sure to highlight the benefits as well as any drawbacks that a given design offers.

SME:

* Can place in locations in different departments around the organization where the traffic is the most
* Because of the small size everything can be connected to the main network with a tap connected to the onion so it won’t degrade traffic speed or cause bottle necks.

Large Enterprise:

* Can place in different locations if in a SD-wan to report back to the central headquarters with the data
* If not in a SD-wan, I would place one per a location with a tap and when a security audit happens the auditor can gather the information from the Security onion.

**Part 02:  Architecture and Performance**

Make note where performance considerations could lead to certain network security architectural decisions.

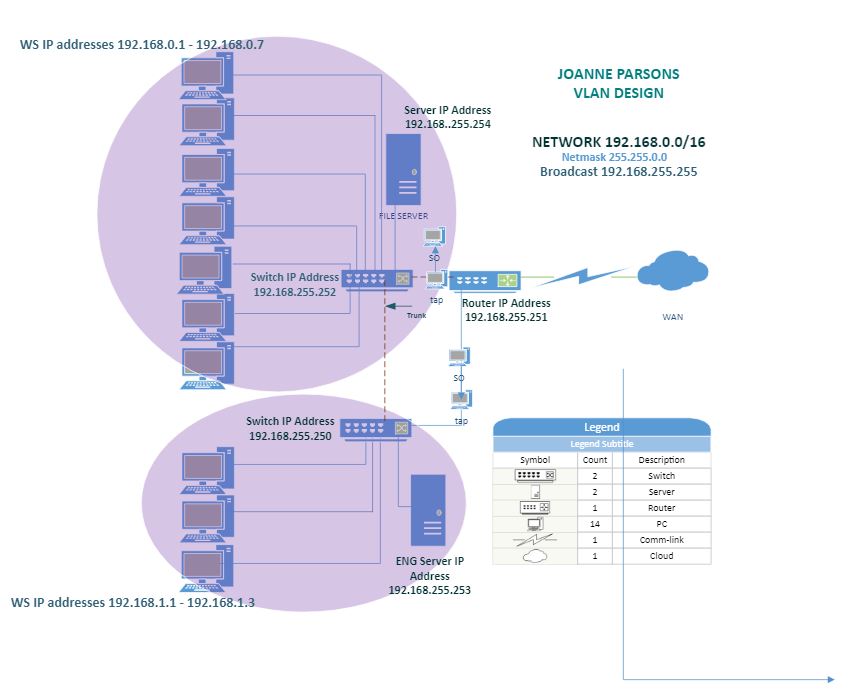
Give examples of how one could incorrectly place security onion within their infrastructure that could lead to a large(r) scale compromise.

Be clear to indicate relevant details.

* By placing a security onion at the end of the network and having all the traffic funnel through the one onion can cause performance flaws and be a risk to network security. Because the onion gathers information from the traffic it will slow it down to process packets before allowing them to pass. Which would make a delay when the report of a attack on the network is passed back to the network administrator.

**Part 03:  Management and Orchestration**

Indicate your overall network infrastructure and flow of data from your security onion systems that you have placed throughout your organization.  Within your example show how you would architect security onion within a smaller organization vs. larger enterprise. In this part (Part 03), include a network diagram of your network flows (i.e. from home office to branch, etc.).



With the concept of having a corporate location with multiple branch locations, I would design my network with the following. For all my surveillance, IP cameras and teller cameras, I would route these to its own router and firewall. With it connected to a server where it can be stored and accessed by using a secure login that is projected on that small network. This first firewall would block all traffic outgoing/incoming besides an AWS cloud connection to prevent any hijacking or data manipulation for the traffic.

My next 10 gigabit switch would have printers, local users and IP phones connected. This switch would be attached to its own firewall that would have sandboxing with a UTM for fast detection of unusual network activity and endpoints on each user’s computer. Depending on what the day to day activities, the ports on the network would be closed all expect those needed. Through this switch I would have a VLAN for the internal wireless network that would disallow sharing of any files or network drives that could be accessed through desktop computers. Rules applied in the network through both switches would disallow remote access between locations or shared network drives between branch locations. If resources were unlimited, I would also have this in a SD-WAN to ensure that main organization can see all threats can be seen and network can be monitored in the main location with a instant response team monitoring the traffic through all the branches of the company.

We would have security nodes in front of storage servers with security nodes plugged into a TAP to not sacrifice performance of analyzation that the Security onion does on the network. Then on a different network switch isolated we would have users with the same layout of having the switch plugged into a TAP that is connected to a sensor in a SD\_WAN.

**Part 04:  Packet Replay**

Describe the process of packet capture replay using security onion.

* In security onion packet capture is useful as it can analyze the traffic to see If any malware or bad actors are on the network. This can be done by using the trcpreply command in Security onion with a combination of sguil.

What is the benefit of packet replay and how is it accomplished?

Illustrate using command line example(s).

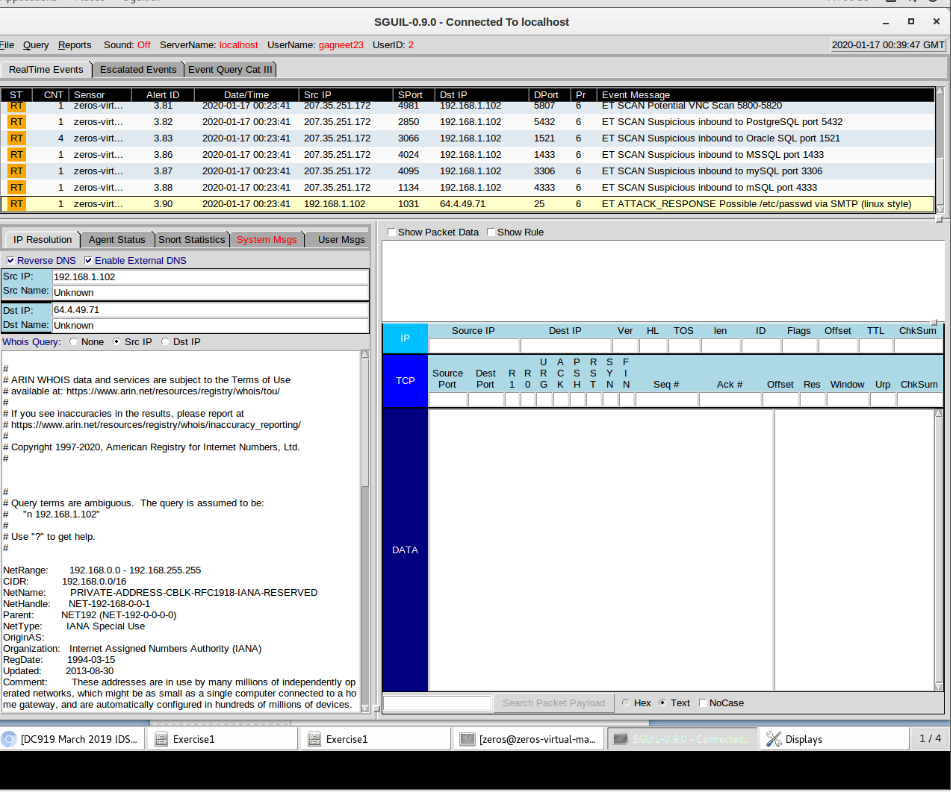
* At the command line, enter the following command: sudo sleep 15s && sudo tcpreplay -i <Ethernet interface name> -M 100 newdat3.log. When you press enter, you will be prompted for the sudo password. Once the password is accepted head back to squil to see the analysis of the packet

**Section B: Practical**

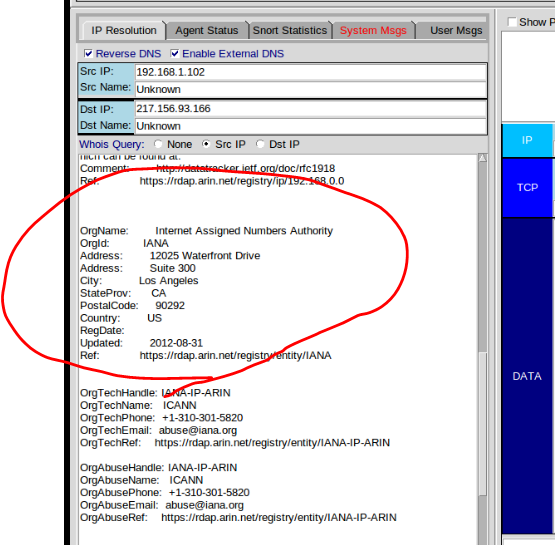
Utilize a package capture from a previous lab.

Indicate what things Squil can assist you in determining.

Provide a 1 page writeup on the process of using Squil and the understanding that you gleaned from the package capture that you selected.



Once packets are captured in sguil, this will be the page seen. From here you can continue to look in each packet by reading the information in the 8th column. For the example in this lab I choose an event of a attack shown below.



This is useful to see information of the location of the originating IP address along with other information if trying to track down a bad actor. Sguil can also assist you for seeing if there has been an intrusion into your network by looking at application packets that shouldn’t be on your network or traffic outgoing to a foreign country.

**Useful Sites:**

https://securityonion.net

https://securityonion.readthedocs.io/en/latest

https://en.wikipedia.org/wiki/Sguil

**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.