**Project Name:  Security Onion: Architecture and Performance Considerations for Production**

**Technology:  Security Onion**

**Market:  Security**

**Name / Group: Gagneet Sahota**

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

**Potential Providers:**

Security Onion

**Intended Activities:**

Design: Architecture and Performance Considerations for Production

**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 delve into the design and architectural considerations that are relevant to medium to large organization in efforts to be able to capture packets and events in order to gain greater threat awareness and ultimately aid in response.  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 2).

**Questions to Answer:**

**Section 0:  Lab Basics**

Explain the following terms:

Port Mirror- able to mirror a certain port to monitor traffic

Tap- to monitor traffic without interrupting normal traffic of the network

Sensor- A sensor is placed closed to traffic to gather information about a network, such as placing a security onion distro within an organization between traffic.

**Section 1:  Lab Environment**

Where within your organization is it best to locate Security Onion (SO) and similar technologies?

* It would be best to place a security onion within the network, or in between the outgoing traffic of the organization. I would make sure there is atleast one at each branch of the organization to get all accurate information of current networks.

When we think about performance considerations, what performance aspects do you consider when placing Security Onion within your organization?

* To ensure that if is between the outgoing traffic of the organization to ensure that the hardware is atleast gigabit so its not creating bottlenecks and slowing down the network. It would be ideal to put the SO within the organization to monitor traffic flow rather then all traffic going into the onion which could slow down the throughput to the web.

In what ways do performance considerations intersect with security considerations?  Said differently, are there any ways that performance issues can hinder security?  If so, indicate such and make note of how your design(s) address these issues.

* Things tend to be faster without security as whether it be security OS as security onions or security software such as Mcafee antivirus, these software’s have to analyze the data before it goes through the network or scan computers while users are working. If performance gets hung up it could cause a virus to get through as the hardware isn’t as fast to catch it or analyze what’s going on the network. If I were to design a network that focused on performance and security with the budget to buy the hardware, I would ensure to have gigabit switches, with honeypots through out the network to ensure my network isn’t compromised without my knowledge. These features would ensure that my hardware doesn’t get caught up when a threat is on the network allowing the threat to bypass through to the network or to a user.

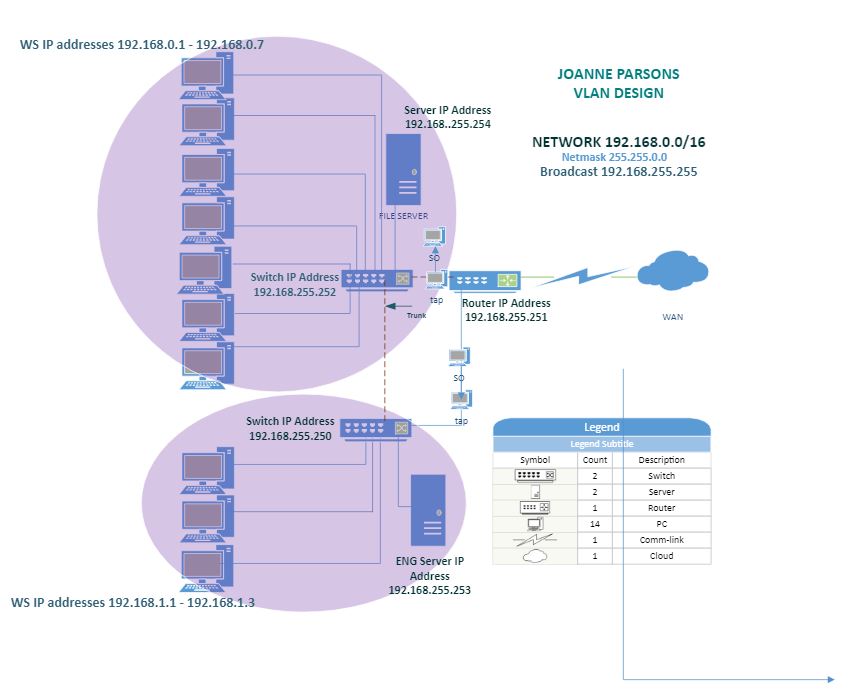
**Important:**  Within your answer, consider that your organization has a corporate headquarters and several (i.e. 5 to 10 or more) branch locations.

Within your response(s), make note of specifics (i.e. When you are indicating the use of a particular component / network gear.   Also make note of what networking gear you are using within your design and its overall features and configuration).

Where relevant, indicate the benefits and in addition to any drawbacks of your design.  Be sure to clearly make note of any unstated assumptions that are incorporated within your design.

**Section 2: Practical**

Create a design that illustrates your security and network architecture.  Within your write-up, include visual depictions of your design so the details.  This means that your submission for this lab should include ***BOTH a write-up*** that provides a narrative and background for your design ***as well as diagrams*** (using any tool that you prefer: Visio, dia, Google Docs Draw, 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.

Submit your document(s).

***As with all labs, your writeup should be entirely your own.***

**Useful Sites:**

[https://securityonion.net (Links to an external site.)](https://securityonion.net/)

[https://sourceforge.net/projects/dia-installer (Links to an external site.)](https://sourceforge.net/projects/dia-installer)

**Deliverable(s):**

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

(1.) Answer Questions

(2.) Document your Design (with appropriate narrative and graphical documentation / modeling, 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.