# ISEC 325 Homework 07

Answer the following questions based on your reading of the text books, the module key points, and the instructor’s presentation this week.

1. [2 points] What are some of the considerations to be taken into account when capturing network traffic?

Some considerations to take into account are that capturing network traffic can be illegal if not give permission by the network owner to use a sniffer, the computer needs to be connected on the network part so the firewall doe not stop it, the sniffer needs to be able to connect to the network segment, and a sniffer can not be used to decipher encrypted traffic.

1. [3 points] Define intrusion detection, intrusion prevention, and incident response. How are the three ideas related to one another?

Intrusion detection is the means of identifying when an attacker is attempting to either gain entry or disturb the normal operations of the system. The intrusion prevention are means of deterring intrusions such as setting up firewalls. Intrusion response is how an organization will react to the intrusion and go about securing and getting rid of the problem. The three ideas are related to one another as they all deal with intrusions and can be seen sort of as steps like how first you make deterrents, next you detect intrusion, finally you handle them.

1. [2 points] How does a network-based IDPS differ from a host-based IDPS?

The network IDPS will be connected to a segment of the network where it can monitor traffic and find patterns. It helps to find different attacks to the network. The host IDPS is on a specific computer or server and will monitor activity on the host system and find intrusions that are trying to go through the host rather than straight through the network.

1. [2 points] How does a signature-based IDPS differ from a behavior-based IDPS?

The signature IDPS will look for known signature patterns as many attackers will have their own distinct signatures. The behavior IDPS will instead look at the traffic and the normal behaviors to find anomalies within the traffic.

1. [2 points] What is a monitoring (or SPAN [switched port analyzer]) port? What is it used for?

The monitoring port is a connection on a network device. The port is configured so it can view all traffic that moves through the device.

1. [2 points] What is active intrusion prevention, and how does it differ from passive?

Active intrusion prevention is where an organization will implement active countermeasures that are used to stop attacks such as using the LaBrea tool. It differs from passive as it is actively checking incoming data and running countermeasures to prevent attacks before they happen.

1. [2 points] From a security perspective, which is least desirable, a false positive or a false negative alarm? Why?

A false negative is the least desirable as it means that an attack was able to get pass the system without being reported while the false positive will send an alert without there being an actual attack. Knowing whether there is an attack or not is very important which is why even if the alarm occurs without an actual attack, people will be able to take the time to check to see if there is one while not reporting the attack can cause a lot of damage before someone is able to spot it.

1. [10 points] Research the open-source IDPS called “Snort.” Write a summary of how Snort fits within the concepts presented this week (e.g. network vs. host, signature vs. behavior, detection vs. prevention, etc.) If a small office wanted to configure Snort for its use, how would you suggest implementing it? Where would it be on the network? How would you configure alerts or responses? I expect several detailed paragraphs and perhaps a diagram for this answer. Cite your sources.

Snort is used to provide real-time network traffic and log data packets. It uses signature inspection as we discussed earlier along with behavior which checks for anomalies. Snort also acts as a packet sniffer so it can check packets within the network traffic, I would suggest implementing snort on people’s personal systems and the business system as it can be used for both personal and business needs. This way people can get used to it on their own systems and it will help people who work from home or check work information like email at home.

Snort can be placed on the inside of the firewall to detect the internal traffic or placed outside the firewall to check incoming traffic. The alerts can be configured to determine what Snort sees as unusual activity or even risks of vulnerability. It generates the reports directly to the users. I would set up different rules for Snort as to how it should handle some different attacks and send alerts when there are attacks or threats.

*Snort 3 is available!* Snort. (n.d.). Retrieved July 3, 2022, from https://www.snort.org/

*Snort-network intrusion detection and prevention system*. Fortinet. (n.d.). Retrieved July 3, 2022, from https://www.fortinet.com/resources/cyberglossary/snort#:~:text=SNORT%20is%20a%20powerful%20open,to%20detect%20potentially%20malicious%20activity.

1. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about.  In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This week we looked at intrusions and how to handle them. A lot of what we look at seems to involve sniffers and packet/ traffic tracking. I know that capturing network traffic is a topic that we cover a lot so I was surprised that it brought up how it is illegal when its unauthorized. I thought that was more obvious as we can compare it to shadowing a person. Back in high school we would job shadow someone and we would follow them as they work to learn about what they do. They gave us forms to fill out and made sure that the person we are shadowing signed the form so the school knew where the students were and the person being shadowed could be in charge of the student at that time. Now taking this and turning it into unauthorized shadowing would be illegal as that leans more on stalking a person since you are following them, understanding their routine, and what they do during the day. I look at the capturing of network traffic in a similar way as the authorization lets the person capture and check the traffic for anomalies and take note of the normal traffic patterns. Without authorization, a person is doing the network equivalent of stalking as they are tracking the traffic, determining what its pattern is and finding anomalies.