### **Domain: Defensive Security**

Click to expand.

#### **Question 1: Intrusion Detection Systems**

An IDS, or intruder detection system, will monitor your network and systems for any suspicious and unwanted activity. It does this either based on known signatures (signature-based or by collecting data, establishing a base-line of ‘normal activity’ and notifying you when it detects any abnormal or suspicious behavior.

During our project we had an ELK server set up to monitor our Capstone web server. This ELK server had filebeat, metricbeat, and packetbeat installed. These modules collected data related to our filesystems, network and system metrics, and network traffic packets.This allowed us to see what our traffic looked like during our attack; when it occurred, where it came from, which systems/ directories/files were targeted and how many requests were made to the server at any specific time.

On Day 1, Kibana monitored our network that our target machine is on and collected data on incoming/outgoing network traffic and any and all requests made to the server through the filebeat, metricbeat, and packetbeat modules. We then used this information on Day 2 to map out the attack over time and visualize the different events which occurred. This allowed us to see the play by play of when, where and how our system was attacked and which steps we could take to mitigate/prevent this attack from happening in the future. Kibana monitored our whole network, including all of the nodes which are on it. Kibana does not provide host-specific information such as if a host contains malware, if the files on it were corrupted, if it has any suspicious or malicious applications on it, etc.

In order to find the answers I was looking for, I made use of Kibana’s “discover” feature. This feature allowed me to use a variety of filters to single out specific types of traffic, related to particular machines and presented them to me chronologically. It allowed me to get a clear picture of what occurred and enabled me to dig deeper, when necessary. I believe this type of monitoring is important for public facing servers and for any machines on a network which might contain sensitive information.

#### **Question 2: HIDS vs NIDS**

A HIDS or host-based intrusion detection system which monitors a local machine or host, and monitors specific host-based actions such as which applications are being used, which files are being accessed or modified, etc. A NIDS, on the other hand, monitors traffic on the whole network and its main function is to log and analyze the traffic between nodes, and traffic coming in and out of the network. Both have their benefits and limitations.

A blue team would use a NIDS when they are trying to prevent or mitigate attacks which utilize network traffic and/or which are coming from outside of the internal network such as brute-force attacks, DDoS, worms, analyzing suspicious HTTP requests, remote code injections, etc. Kibana is a NIDS because it provides us with logs from all machines on the network and monitors the traffic coming in and out of the network. It does not, however, provide us with data on which files were accessed on which machine, if they were modified or not, if any machine has malicious applications on it, etc. In order to get this data we would have to configure a HIDS which would allow us to monitor all of those metrics.

A blue team could use a HIDS as a “last line of defense”, when a node has already been infected or intruded and someone is trying to access or modify files on the node, or use a malicious application to damage/steal, etc. I believe a network should have both HIDS and NIDS on their systems to provide the most comprehensive security protection for their servers and users.

#### **Question 3: Dashboards**

Dashboards are extremely important for log analysis because they provide you with one place where you have a clear and immediate overview of the different metrics you’re trying to track and monitor and filter them by given time. During Project 2 we were able to create a dashboard and monitor all of our incoming network traffic and activity from Kibana’s dashboard page.

This allowed us to immediately spot several anomalies during the same time frame and use the discover feature to further investigate. Dashboards are very valuable tools and not having them at my disposal would certainly create more hassle and work. I suppose I could go and use the discover feature to manually filter out the desired metrics I want to analyze. I could also use a packet capture program to manually go through the network traffic myself. However, the dashboard would be greatly missed.

Some of the dashboards we set up where:

* HTTP status codes for the top queries
  + This dashboard applet gives us an overview of which status codes were returned for the top queries made to our server. It’s presented as one pie chart per request, with different colors for each response code.
* Top 10 HTTP requests
  + This gives us an overview of the top 10 urls which were requested and a count of how many requests each url received within a certain time frame.
* Connections over time
  + This presents us with a graphic overview of connections made to our machine over a certain time span. The x-axis has the date and time, while the y-axis contains the number of requests.