Defensive Security – Intrusion Detection Systems

An intrusion detection system, or an IDS, is a very common tool in any enterprise network so it is very important to understand what it does, and how it does it. In the final project for this class the ELK Stack, or Elastic Stack was the network-based intrusion detection system in place. An ELK Stack is composed of three separate open-source projects; Elasticsearch, Logstash, and Kibana. These three systems allow an IT team to monitor, visualize, and collect data from any configured machines on the network. This system collects log data, network data, operating system metrics, as well as performance metrics from deployed applications. Specifically in the project, the intrusion detection system collected syslog data as well as system metrics from the configured hosts. However, this instance of Kibana was not collecting performance metrics of the applications running on the virtual machines.

During the first day of the project, the ELK Stack was not utilized much besides to ensure that it was installed and running. Three alerts were also set up to potentially detect malicious traffic caused by the attack. That does not mean it was not important for the red-team objectives performed on the first day. The intrusion detection system was actively collecting data from the “Target 1” system about the attacks. Any actions done on or to the target machine were recorded and sent to Elasticsearch via two packages, Filebeat for syslog data and Metricbeat for system and service metrics. These “beats" can also be used for many other types of data collection as well. In addition, they can be used to send the data to Logstash for additional processing before it reaches Kibana and Elasticsearch if the environment requires it. On the second day of the engagement, the Elastic Stack was used to study and visualize the traffic created by the attacks to the “Target 1” virtual machine. The different actions taken during the offensive tasks were easily searched and visualized. In conjunction with the monitoring, alerts are a large part of the “detection” in intrusion detection system. These alerts allow for custom notifications or actions based on custom sets of rules. These rules would be designed when traffic varies from a known baseline.

Elastic Stack was not collecting data from all machines on the network. There were only two virtual machines sending metrics and logs to Kibana, “Target 1” and “Target 2”. The ELK Stack instance configured for this project was not collecting performance data from the Apache web server. That would be possible with the Application Performance Monitoring (APM) package that can be installed. This would allow the IDS to collect in depth information and errors of the Wordpress website being hosted. When researching the data collected, many features of Kibana were utilized. The biggest tool used was Elasticsearch, this allows for very granular searching of the data. Like many database engines, extremely complex and detailed searches are possible through Kibana Query Language, or KQL. The visualizations Kibana offers were a great way to quickly find anomalies in the traffic from the first day. When it comes to incident response, it is important to be able to find threats and suspicious activity fast and efficiently. The complex search functionality, and simple visuals make that possible.

When it comes to deploying an IDS in a new environment, many factors must be taken into account. Cost is a large part of how a Elastic Stack will be configured, as it is priced per GB indexed. Because

of this, it may not be cost efficient to monitor every machine on a network through the IDS. Keeping this pricing structure in mind, it would be important to understand what devices, metrics, and events would be integral to the functionality of the organization. For example with this project's topology, the web server machines are the most integral part. They provide a public facing website for customers to utilize, if this goes down, that would mean lost revenue. So a company may decide that certain items or metrics may be less important, and would be willing to live with the consequences if something were to happen. Another thing to keep in mind is "alert fatigue" in the analysts. If every machine and every possible data point is being sent to Kibana, it will become overwhelming and may cause a severe event to go unnoticed. So when it comes to deciding how an IDS is configured, it is very important to look at the baseline traffic of the network and decide what is most important for the organization to monitor, because at the end of the day, an intrusion detection system does not generate money, it only helps prevent more severe losses from occurring.