Red-Vs-Blue Project: Interview Questions: Domain: Defensive Security: Question 1: Intrusion Detection Systems

"What does an intrusion detection system (IDS) do and how does it do it?"

An IDS monitors the events occurring in a computer system or network, analyzes them for signs of possible security incidents, and alerts when such events are discovered. Not to be confused with IPS which actively prevents security incidents. IDS' can be either network (resides on the network) or host (resides on the host) based. It is important to keep your IDS updated to include recent malware signatures to reduce system/network attack surface.
In project 2, Red-Team-Vs Blue team, our goal was to play the role of Red Team and Blue Team. As Red Team, we carried out a successful attack against a vulnerable system (Target1). As Blue Team, we were tasked with defending the vulnerable system (Target1). Before the attack can be carried out, we implemented logging via Kibana, on a third machine (Capstone). Kibana is a is Data visualizing tool that inputs, reads, and outputs logs in a human readable and searchable format. It sits on top of FileBeat, PacketBeat, and MetriBeat. In this situation, Kibana was set to capture network traffic coming only from Target1.
On Day1 Kibana was used to log all traffic coming through the Kali Attack Machine and Target1. I created three alerts to capture memory and CPU usage, log file and system access data, and monitor and log traffic HTTP traffic occurring on the network (error codes and responses). This information is logged through the PacketBeat, MetricBeat, and FileBeat tools. On Day 2, Kibana was used to view the Brute Force Attack that was done on Target1(error codes, number of requests, files requested). I was able to use the following commands to view:

- Source.ip:192.168.1.105 and http.response.status_code: * to view all http response codes sent from Target1.
- url.full:"http://192.168.1.105/company_folders/secret_folder/ and source.ip: 192.168.1.90 to view all http response codes sent from Target1, originating from the Kali Attack Machine, after requesting files from the secret folder.

To mitigate this attack, the Blue Team recommends the implementation of a robust alert and network monitoring system. It is critical that system administrators be alerted if HTTP requests exceed a certain threshold, unknown IP addresses attempt to access servers or resources, and logon requests exceed a certain threshold, to name a few. All machines on the network must be subject to logging and monitoring to reduce attack surface. Metrics that are indicators of an attack or unauthorized access should be implemented and closely monitored, as well.