Domain: Defensive Security

Question 2: HIDS vs NIDS
"What is the difference between a HIDS and a NIDS? When would Blue Team operatives use one over the other?"

Both HIDS and NIDS are intrusion detection systems. HIDS (Host-based intrusion detection system) runs locally - server, workstation, host-based system - while NIDS (Network intrusion detection system) runs an entire subnet on a network.
In other words, NIDS is broader and the first line of defense and HIDS is more focused and acts as a second line of defense against malicious traffic.

In project 2:
NIDS → ELK stack was a network monitoring machine holding Kibana dashboards
HIDS → Filebeat and Metricbeat

NIDS and HIDS complement each other, so it is advised to use both. From a Blue Team perspective of defending against attacks, NIDS provides real-time monitoring and flag issues as they happen. This way the blue-team has time to act ASAP. On the other hand, HIDS examines historical data that may not be caught during real-time scanning.

There was no alarm to indicate that a port scan was happening, or that port 22 and 80 were opened exposing company data to attackers.

Searching for data using Kibana Query Language showed several instances of what happened, for example, bar graphs indicating when and the number of hits port scan, brute-force attacks, request of hidden directory, and webdav connection occurred.

Proposed alarms and mitigation strategies to harden the system were indicated in the PPT presentation. Maintaining the system up to date afterwards is crucial to minimizing future attacks.