**Domain: Offensive 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?"

1. **Restate the Problem**

The two most common types of intrusion detection systems are the Network Intrusion Detection Systems (NIDS) and the Host Intrusion Detection System (HIDS). The Network Intrusion Detection System monitors and analyzes network traffic for suspicious behavior and threats in real time on any inbound and outbound traffic. NIDS sensors are placed at critical points in the network such as on the subnet where firewalls are located to detect Denial of Service attacks. The Host Intrusion Detection System monitors and analyzes system configuration and application activity for devices running on the enterprise network. HIDS examines historical data to catch hackers using non-conventional methods that may be difficult to detect analyzing real-time data. Blue Team operatives would use both the NIDS and HIDS. They complement each other and it is ideal to incorporate both systems. NIDS offers a faster response time while HIDS can identify malicious data packets that originate from inside the enterprise network.

1. **Provide a Concrete Example Scenario**

In the project, the ELK Stack log server was in place and the information was monitored in Kibana. These systems collected log files, log events, metrics, statistics, and packets from the network servers. They cannot process encrypted packets. Kibana is a Host Intrusion Detection System as well as a Network Intrusion Detection system as they run on the enterprise hosts to detect host attacks and detect network anomalies by monitoring the inbound and outbound traffic.

1. **Explain the Solution Requirements**

Kibana monitored and logged SSH login attempts for port 22 through the Filebeat System. Also, the exploitation of least privilege using the top sudo commands were logged and monitored. The exploitation of privilege escalation using top sudo commands were logged and monitored as well. Alerts were configured for excessive HTTP errors, HTTP request bytes over 3500, and CPU usage over 50%. This information was collected from the Target 1 virtual machine.

1. **Explain the Solution Details**

It is apparent that Kibana is a NIDS because it monitors and analyzes in real time, as engagements were being performed on day one and day two, events were logged. Kibana also demonstrates HIDS activity as it tracks changes made to the registry settings and critical system configuration, log and content files, and alerting to any unauthorized activity. Alerts, index patterns, a query for ‘result.condition.met’ was also conducted to view all traffic from the designated alerts.

1. **Identify Advantages and Disadvantages of the Solution**

A network can absolutely have both HIDS and NIDS and it is actually preferred, they complement one another. NIDS offer a faster response time while HIDS can identify malicious data packets that originate from inside the enterprise network. HIDS are appropriate to use on mission-critical machines that are not expected to change because they can identify file permission changes and unusual client-server requests. NIDS are appropriate when specific content within a packet which can be used for uncovering intrusions such as exploitation attacks or compromised devices.

**References**

*Hands-on Wazuh Host-based Intrusion Detection System (HIDS) Deployment*. Module 5 - Hands-on Wazuh Host-based Intrusion Detection System (HIDS) Deployment - Blue Teams Academy - Free Training 2021. (n.d.). https://www.blueteamsacademy.com/wazuh/.

*Network Intrusion Detection System: Managed IDS*. Redscan. (2020, November 19). https://www.redscan.com/services/managed-intrusion-detection-system/.

Radichel, T. (2020, November 7). *IDS and IPS in the Cloud*. Medium. https://medium.com/cloud-security/ids-and-ips-in-the-cloud-f07aac110d31.

Rapid7. (2020, October 27). *The Pros & Cons of Intrusion Detection Systems: Rapid7 Blog*. Rapid7. https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-systems/.