Case Study 04

David Murillo Santiago
Professor Pugh
IS-3513
12 November 2023

1. What are the two categories of Intrusion Detection Systems?

Intrusion Detection Systems (IDS) can be categorized into two types: Host-based and Network-based IDS. HIDS and NIDS differ by the scope of the IDS. For example, HIDS focuses on individual hosts, analyzing the activities of a single system. On the other hand, NIDS monitors network-wide traffic, analyzing data from multiple hosts within the network. Both IDS categories have their pros and cons. A notable advantage of HIDS is its ability to provide detailed and host-specific information. For instance, while Anti-virus monitors all activities inside the system, it may not be sufficient to detect and analyze certain system-specific attacks, such as buffer overflow attacks in memory, memory leakage, or malfunctioning of operating system processes. In contrast, HIDS collects and analyzes system data and patterns, to detect any anomalies that may have occurred. Additionally, HIDS aids in safeguarding against insider threats.

2. What are the differences between a signature-based and anomaly-based IDS? Give

examples of each.

A signature-based IDS relies on a predefined collection of attack signatures. One advantage of signature-based IDS is its high effectiveness in detecting known attacks. However, because signature-based systems operate by specifically identifying predefined patterns, they may struggle with new or unknown threats such as zero-days. On the other hand, an anomaly-based IDS references a baseline pattern of normal system activity to identify active intrusion attempts. While signature-based systems excel in recognizing established threats, anomaly-based IDS adds another layer of defense, adapting to evolving cyber threats and providing a dynamic response to emerging attack techniques. Because anomaly-based IDS compares host or network activity to a pre-defined baseline, it is able to identify intrusions whose exploits have not been discovered yet. This adaptability enhances the overall robustness of intrusion detection capabilities.

3. What are the different Anomaly-Detection approaches? Give details on each.

There are three main approaches to anomaly detection: Statistical-Based, Data Mining-Based, and Knowledge-Based Anomaly Detection. Statistical-Based Anomaly Detection relies on statistical analysis to assess user or system behavior, using properties like mean and variance to distinguish normal from malicious activities. Data Mining-Based Anomaly Detection utilizes data mining techniques, involving clustering and classification models to extract patterns and reduce false alarms by removing normal activity from alarm data. Knowledge-Based Anomaly Detection relies on accumulated knowledge about attacks, using methodologies like state transition analysis to detect anomalies with fewer false alarms.

4. According to the article, what devices present a “major research challenge?” Do you

agree?

The article states that developing intrusion detection systems (IDS) for smartphones and tablets constitutes a significant research challenge, particularly due to the challenge of achieving a high intrusion detection rate within the constraints of compromised operating systems in mobile devices. The challenge is underscored by the unique characteristics of smartphones and tablets, which operate in shared system environments, necessitating the IDS to function as an independent module to mitigate potential attacks arising from shared parameters. I agree with this as securing these devices is crucial due to the widespread use of mobile devices and their daily access to sensitive information.