4.2 HOST-BASED INTRUSION DETECTION SYSTEM

A Host-Based Intrusion Detection System, or HIDS, is a type of cybersecurity solution that monitors IT systems for signs of suspicious activity to detect unusual behaviors or patterns associated either with human users or applications that could be a sign of a security breach or attempted attack.

HIDS systems are so-named because they operate on individual host systems. In this context, a host could be a server, a PC, or any other type of device that produces logs, metrics, and other data that can be monitored for security purposes.

How does Host-Based Intrusion Detection work?

Host-Based Intrusion Detection works by collecting data from servers, computers, and other host systems, then analyzing the data for anomalies or suspicious activity.

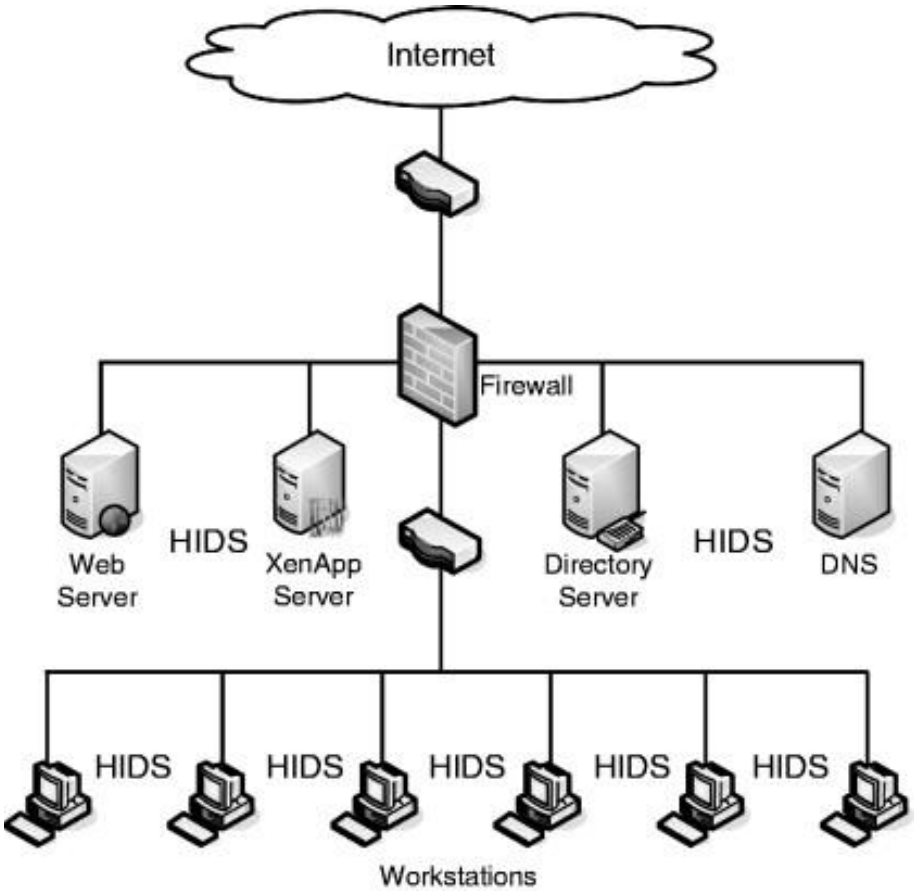
The data that HIDS tools analyze may include security-centric data sources, such as authentication logs (which record login events). However, a HIDS typically also analyzes other types of data, like application and operating system logs. Even though the latter types of data are not related to security specifically, unusual patterns within those data sets could be linked to security issues.

For example, a HIDS could monitor network traffic flows to detect that an application has suddenly begun receiving high volumes of requests from previously unknown external IP addresses. This activity could be the sign of a brute-force login attempt or an effort to probe the application for vulnerabilities that attackers could exploit. With this information, security teams could block the offending IP addresses.

To deliver results that are as accurate as possible, a HIDS should link and correlate different types of data sources, which makes it possible to gain deeper context on potential security events.

For instance, network traffic logs can be analyzed in conjunction with application event logs so that the HIDS can determine whether unusual activity on the network correlates with unusual activity by the application.

In the former case, it’s possible that attackers are trying to find a vulnerability in the application but have not yet succeeded. In the latter, it’s possible that they have breached the application, which is why the HIDS detects anomalous behavior by the application as well as unusual traffic patterns on the network.



Types of HIDS

Host-Based Intrusion Detection Systems can be broken into two main categories based on how they are deployed:

- **Agent-based HIDS**: An agent-based HIDS relies on software agents that are installed on each host to collect information from the host. This is a “heavier-weight” approach because running agents on hosts increases the resource utilization of the hosts.
- **Agentless HIDS**: With an agentless HIDS, information from hosts is collected without relying on agents, such as by streaming the data over the network. This type of HIDS is more complex

to implement, and agentless HIDS sometimes can’t access as much data as agent-based solutions, but the agentless approach offers the benefit of consuming fewer resources.

HIDS components

No matter which type of HIDS you deploy, your HIDS solution will typically include three main components:

- **Data collectors**: Using either agents or an agentless approach, your HIDS deploys sensors that collect data from hosts.
- **Data storage**: After being collected, the data is usually aggregated and stored in a central location. The data is retained at least as long as is necessary to analyze it, although organizations may also choose to keep the data on hand so they can reference it at a later time if desired.
- **Analytics engine**: The HIDS uses an analytics engine to process and evaluate the various data sources that it collects. The purpose of analytics is to look for patterns or anomalies, then assess the likelihood that they are the result of security risks or attacks.

HIDS capabilities

After a HIDS detects potential security problems, it can do three main things.

Alerting

The first is alerting. Alerting is the process of informing IT and/or security teams about a potential security issue.

Ideally, HIDS alerting features should be capable of assessing the severity of each security risk the HIDS identifies, then generating alerts accordingly. For example, low-risk security events should be labeled as such so that engineers are aware that those alerts are not likely to require immediate attention.

Reporting

HIDS platforms can generate reports about the overall state of security within an IT environment. The data included in reports can vary, but it may include the number and types of security risks identified by a HIDS over time, for instance, or how security issues vary across different types of hosts (such as Windows-based hosts versus Linux-based systems).

Reporting is useful for assessing security trends over time, as well as for demonstrating the security posture of an organization.

Response

In some cases, HIDS tools are capable of carrying out certain automated response activities to help remediate risks. For example, if a HIDS determines that a particular external endpoint is trying to probe a company's servers, it could automatically generate firewall rules to block the probes. Automated remediation like this not only saves time and effort on the part of engineers, but also ensures that security risks can be blocked immediately.

HIDS security considerations and best practices

To get the most value out of a HIDS, consider best practices like the following:

- **Monitor all hosts**: A HIDS is of limited value if it only monitors some hosts. To gain the broadest possible context on security risks, your HIDS should monitor all hosts. That way, you'll know whether and how quickly security issues spread among hosts, as well as how many of your hosts are targeted by attacks. You'll also be able to detect attacks that target just one host rather than attempts to reach many hosts at once.
- **Contextualize data**: As noted above, the more data sources your HIDS analyzes collectively, the greater the context it has on potential security risks. Context is critical for distinguishing actual risks from false positives and generating accurate alerts.
- **Configure smart alerts**: To avoid distracting engineers with "alert fatigue," a HIDS should be configured to alert only on events that require a response. Alerts should also be categorized based on severity level so that engineers know which ones to prioritize.
- **Consider agentless HIDS**: While an agent-based HIDS has its advantages (such as easier access to host-based data), agentless HIDS solutions are easier to deploy and manage in many respects because they don't require installing software agents on each host. They are also lighter on resource consumption.
  - As more and more of our professional and personal lives move online, it's increasingly important to keep our networks secure from potential cyber-attacks and reduce your cyber exposure. One tool that is frequently used for this purpose is a Network Intrusion Detection System or NIDS. But what exactly is NIDS, and how does it work?

- NIDS is a security tool designed to detect, monitor, and analyze traffic for suspicious activity or malicious attacks. It is essential to a larger security infrastructure and prevents network breaches and data theft.
- In this article, we will explore NIDS in detail, including its definition, working principle, and types. We will also discuss the advantages and limitations of using NIDS and why it is an essential tool for network security today.