Detection tools and techniques

In this reading, you'll examine the different types of intrusion detection system (IDS) technologies and the alerts they produce. You'll also explore the two common detection techniques used by detection systems. Understanding the capabilities and limitations of IDS technologies and their detection techniques will help you interpret security information to identify, analyze, and respond to security events.

As you've learned, an **intrusion detection system (IDS)** is an application that monitors system activity and alerts on possible intrusions. IDS technologies help organizations monitor the activity that happens on their systems and networks to identify indications of malicious activity. Depending on the location you choose to set up an IDS, it can be either host-based or network-based.

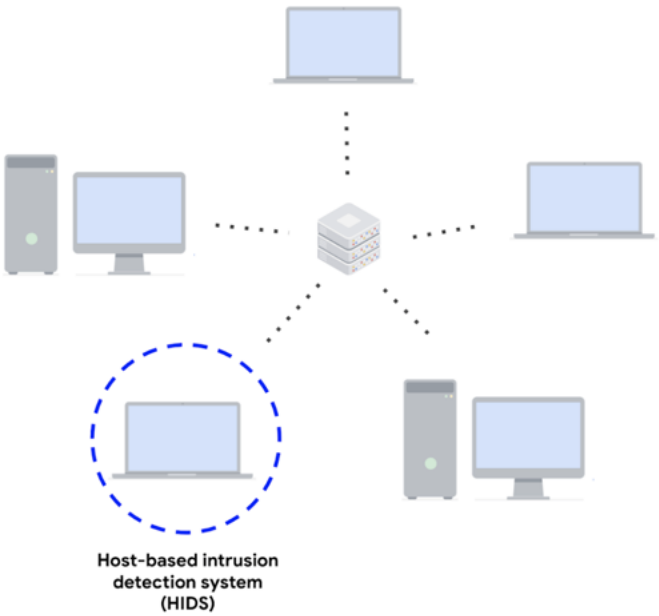
Host-based intrusion detection system

A **host-based intrusion detection system (HIDS)** is an application that monitors the activity of the host on which it's installed. A HIDS is installed as an agent on a host. A host is also known as an **endpoint**, which is any device connected to a network like a computer or a server.

Typically, HIDS agents are installed on all endpoints and used to monitor and detect security threats. A HIDS monitors internal activity happening on the host to identify any unauthorized or abnormal behavior. If anything unusual is detected, such as the installation of an unauthorized application, the HIDS logs it and sends out an alert.

In addition to monitoring inbound and outbound traffic flows, HIDS can have additional capabilities, such as monitoring file systems, system resource usage, user activity, and more.

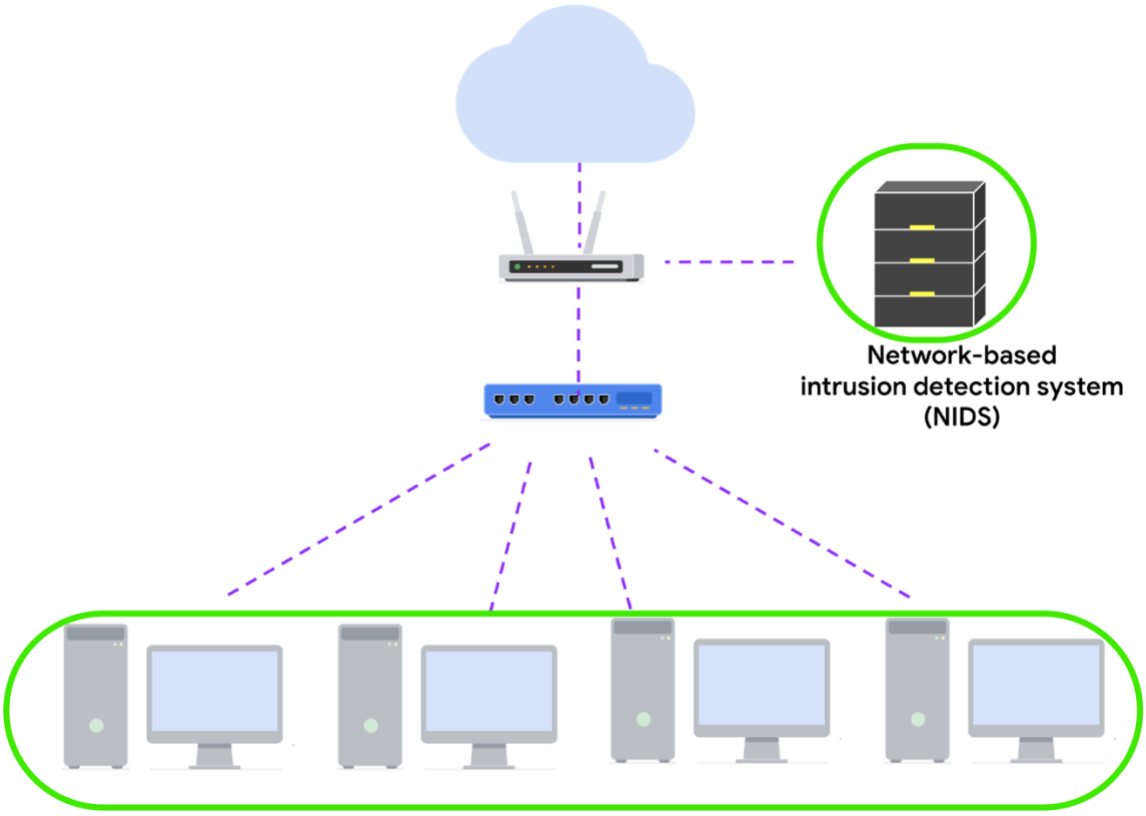
This diagram shows a HIDS tool installed on a computer. The dotted circle around the host indicates that it is only monitoring the local activity on the single computer on which it's installed.



Network-based intrusion detection system

A **network-based intrusion detection system (NIDS)** is an application that collects and monitors network traffic and network data. NIDS software is installed on devices located at specific parts of the network that you want to monitor. The NIDS application inspects network traffic from different devices on the network. If any malicious network traffic is detected, the NIDS logs it and generates an alert.

This diagram shows a NIDS that is installed on a network. The highlighted circle around the server and computers indicates that the NIDS is installed on the server and is monitoring the activity of the computers.



Using a combination of HIDS and NIDS to monitor an environment can provide a multi-layered approach to intrusion detection and response. HIDS and NIDS tools provide a different perspective on the activity occurring on a network and the individual hosts that are connected to it. This helps provide a comprehensive view of the activity happening in an environment.

Detection techniques

Detection systems can use different techniques to detect threats and attacks. The two types of detection techniques that are commonly used by IDS technologies are signature-based analysis and anomaly-based analysis.

Signature-based analysis

Signature analysis, or signature-based analysis, is a detection method that is used to find events of interest. A **signature** is a pattern that is associated with malicious activity. Signatures can contain specific patterns like a sequence of binary numbers, bytes, or even specific data like an IP address.

Previously, you explored the Pyramid of Pain, which is a concept that prioritizes the different types of **indicators of compromise** (IoCs) associated with an attack or threat, such as IP addresses, tools, tactics, techniques, and more. IoCs and other indicators of attack can be useful for creating targeted signatures to detect and block attacks.

Different types of signatures can be used depending on which type of threat or attack you want to detect. For example, an anti-malware signature contains patterns associated with malware. This can include malicious scripts that are used by the malware. IDS tools will monitor an environment for events that match the patterns defined in this malware signature. If an event matches the signature, the event gets logged and an alert is generated.

Advantages

- **Low rate of false positives:** Signature-based analysis is very efficient at detecting known threats because it is simply comparing activity to signatures. This leads to fewer false positives. Remember that a **false positive** is an alert that incorrectly detects the presence of a threat.

Disadvantages

- **Signatures can be evaded:** Signatures are unique, and attackers can modify their attack behaviors to bypass the signatures. For example, attackers can make slight modifications to malware code to alter its signature and avoid detection.
- **Signatures require updates:** Signature-based analysis relies on a database of signatures to detect threats. Each time a new exploit or attack is discovered, new signatures must be created and added to the signature database.
- **Inability to detect unknown threats:** Signature-based analysis relies on detecting known threats through signatures. Unknown threats can't be detected, such as new malware families or **zero-day** attacks, which are exploits that were previously unknown.

Anomaly-based analysis

Anomaly-based analysis is a detection method that identifies abnormal behavior. There are two phases to anomaly-based analysis: a training phase and a detection phase. In the training phase, a baseline of normal or expected behavior must be established. Baselines are developed by collecting data that corresponds to normal system behavior. In the detection phase, the current system activity is compared against this baseline. Activity that happens outside of the baseline gets logged, and an alert is generated.

Advantages

- **Ability to detect new and evolving threats:** Unlike signature-based analysis, which uses known patterns to detect threats, anomaly-based analysis *can* detect unknown threats.

Disadvantages

- **High rate of false positives:** Any behavior that deviates from the baseline can be flagged as abnormal, including non-malicious behaviors. This leads to a high rate of false positives.
- **Pre-existing compromise:** The existence of an attacker during the training phase will include malicious behavior in the baseline. This can lead to missing a pre-existing attacker.

Key takeaways

IDS technologies are an essential security tool that you will encounter in your security journey. To recap, a NIDS monitors an entire network, whereas a HIDS monitors individual endpoints. IDS technologies generate different types of alerts. Lastly, IDS technologies use different detection techniques like signature-based or anomaly-based analysis to identify malicious activity.

Mark as completed