Introduction To IDS/IPS

In network security monitoring (NSM) operations, the use of `Intrusion Detection Systems (IDS)` and `Intrusion Prevention Systems (IPS)` is paramount. The purpose of these systems is not only to identify potential threats but also to mitigate their impact.

An `IDS` is a device or application that monitors network or system activities for malicious activities or policy violations and produces reports primarily to a management station. Such a system gives us a clear sense of what's happening within our network, ensuring we have visibility on any potentially harmful actions. It should be noted that an IDS doesn't prevent an intrusion but alerts us when one occurs.

- The IDS operates in two main modes: signature-based detection and anomaly-based detection. In `signature-based detection`, the IDS recognizes bad patterns, such as malware signatures and previously identified attack patterns. However, this method is limited to only known threats. For this reason, we also implement `anomaly-based detection`, which establishes a baseline of normal behavior and sends an alert when it detects behavior deviating from this baseline. It's a more proactive approach but is susceptible to false positives, hence why we use both methods to balance each other out.

On the other hand, an `IPS` sits directly behind the firewall and provides an additional layer of protection. It does not just passively monitor the network traffic, but actively prevents any detected potential threats. Such a system doesn't just alert us of intruders, but also actively stops them from entering.

- An IPS also operates in a similar mode to IDS, offering both signature-based and anomaly-based detection. Once a potential threat is detected, it takes actions such as dropping malicious packets, blocking network traffic, and resetting the connection. The goal is to interrupt or halt activities that are deemed dangerous to our network or against our policy.

When deploying IDS and IPS, they are typically integrated into the network at different points, each having its optimal place depending on its function and the overall network design. Both IDS and IPS devices are generally positioned behind the firewall, closer to the resources they protect. As they both work by examining network traffic, it makes sense to place them where they can see as much of the relevant traffic as possible, which is typically on the internal network side of the firewall.

- Intrusion Detection Systems (IDS) passively monitor network traffic, detecting potential threats and generating alerts. By placing them behind the firewall, we can ensure they're analyzing traffic that has already passed the first line of defense, allowing us to focus on potentially more subtle or complex threats that have bypassed the firewall.
- Intrusion Prevention Systems (IPS), on the other hand, actively intervene to stop detected threats. This means they need to be placed at a point in the network where they can not only see potentially malicious traffic but also have the authority to stop it. This is usually achieved by placing them inline on the network, often directly behind the firewall.

The deployment may vary based on the network's specific requirements and the kind of traffic we need to monitor. IDS/IPS can also be implemented on the host level, known as Host-based Intrusion Detection Systems (HIDS) and Host-based Intrusion Prevention Systems (HIPS), which monitor the individual host's inbound and outbound traffic for any suspicious activity.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Please note that the placement of these systems is an integral part of a defense-in-depth strategy, where multiple layers of security measures are used to protect the network. The exact architecture will depend on various factors, including the nature of the network, the sensitivity of the data, and the threat landscape.

IDS/IPS Updates

Moreover, to ensure these systems perform at their best, we consistently update them with the latest threat signatures and fine-tune their anomaly detection algorithms. This requires a diligent, ongoing effort from our security team, but it's absolutely essential given the continually evolving threat landscape.

It's also important to mention the role of Security Information and Event Management (SIEM) systems in our network security monitoring operations. By collecting and aggregating logs from IDS and IPS along with other devices in our network, we can correlate events (analyzing the relationships) from different sources and use advanced analytics to detect complex, coordinated attacks. This way, we have a complete, unified view of our network's security, enabling us to respond quickly to threats.

Coming Up

In this module, we will explore the fundamentals of `Suricata`, `Snort`, and `Zeek`, along with providing insights into signature development and intrusion detection for each of these systems.

Next ➜

Mark Complete & Next

Powered by HACKTHEBOX