Intrusion detection and prevention system (IDPS)

Overview

An intrusion detection and prevention system (IDPS) is a solution that monitors a network for threats and then takes action to stop any threats that are detected.

An IDPS is closely related to an intrusion detection system (IDS). While both systems detect threats and send alerts about them, an IDPS also attempts to remediate those threats.

An IDPS is sometimes called an intrusion prevention system (IPS). The terms IDPS and IPS are mostly used interchangeably, but when someone mentions an IPS they are often referring to the threat hunting function of an IDPS.

How does an IDPS work?

An IDPS works in several different ways depending on the vendor, the chosen deployment method, and the needs of the organization deploying it.

An intrusion detection system (IDS)

- It is a device or software application that monitors a network or systems for malicious activity or policy violations.
- Any intrusion activity or violation is typically either reported to an administrator or collected centrally using a **security information and event management (SIEM) system.**
- A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Classification of IDS

IDS types range in scope from single computers to large networks.

The most common classifications are **network intrusion detection systems (NIDS)** and **host-based intrusion detection systems (HIDS).**

A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS.

It is also possible to classify IDS by detection approach. The most well-known variants are

- **Signature-based detection** (recognizing bad patterns, such as malware) and
- **Anomaly-based detection** (detecting deviations from a model of "good" traffic, which often relies on machine learning).
- **Reputation-based detection** (recognizing the potential threat according to the reputation scores).

Some IDS products have the ability to respond to detected intrusions. **Systems with response capabilities are typically referred to as an intrusion prevention system**.

Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and characterize malicious traffic.

Comparison with firewalls

- ✓ Although they both relate to network security, an IDS differs from a firewall in that a conventional network firewall (distinct from a next-generation firewall) uses a static set of rules to permit or deny network connections.

- ✓ It implicitly prevents intrusions, assuming an appropriate set of rules have been defined.

- ✓ Essentially, firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network.

- ✓ An IDS describes a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

- ✓ This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators.

- ✓ A system that terminates connections is called an intrusion prevention system, and performs access control like an application layer firewall.

Intrusion detection category

IDS can be classified by where detection takes place (network or host) or the detection method that is employed (signature or anomaly-based).

Analyzed activity

A. Network intrusion detection systems [NIDS]

- Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks.
- Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.
- NIDS function to safeguard every device and the entire network from unauthorized access.
- An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.
- OPNET and NetSim are commonly used tools for simulating network intrusion detection systems.
- NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matchin
- g the records in the NIDS.

- When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS, often referred to as inline and tap mode, respectively.
- On-line NIDS deals with the network in real time.
- It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not.
- Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

Artificial Neural Network (ANN) based IDS

- NIDS can be also combined with other technologies to increase detection and prediction rates.
- Artificial Neural Network (ANN) based IDS are capable of analyzing huge volumes of data due to the hidden layers and non-linear modeling, however this process requires time due its complex structure.
- This allows IDS to more efficiently recognize intrusion patterns.
- Neural networks assist IDS in predicting attacks by learning from mistakes;
- ANN based IDS help develop an early warning system, based on two layers. The first layer accepts single values, while the second layer takes the first's layers output as input; the cycle repeats and allows the system to automatically recognize new unforeseen patterns in the network.
- This system can average 99.9% detection and classification rate, based on research results of 24 network attacks, divided in four categories: DOS, Probe, Remote-to-Local, and user-to-root.

B. Host intrusion detection systems [HIDS]

- Host intrusion detection systems (HIDS) run on individual hosts or devices on the network.
- A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.
- It takes a snapshot of existing system files and matches it to the previous snapshot.
- If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

Detection method

A. Signature-based

- Signature-based IDS is the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.
- This terminology originates from anti-virus software, which refers to these detected patterns as signatures.
- Although signature-based IDS can easily detect known attacks, it is difficult to detect new attacks, for which no pattern is available.
- In signature-based IDS, the signatures are released by a vendor for all its products.
- On-time updating of the IDS with the signature is a key aspect.

B. Anomaly-based

- Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware.
- The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model.
- Since these models can be trained according to the applications and hardware configurations, machine learning based method has a better generalized property in comparison to traditional signature-based IDS.
- Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious.
- Most of the existing IDSs suffer from the time-consuming during detection process that degrades the performance of IDSs.
- Efficient feature selection algorithm makes the classification process used in detection more reliable. New types of what could be called anomaly-based intrusion detection systems are being viewed by Gartner as User and Entity Behavior Analytics (UEBA) (an evolution of the user behavior analytics category) and network traffic analysis (NTA).
- In particular, NTA deals with malicious insiders as well as targeted external attacks that have compromised a user machine or account.
- Gartner has noted that some organizations have opted for NTA over more traditional IDS.

Intrusion prevention System [IPS] and/or Intrusion detection and prevention systems (IDPS)

- Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.
- Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.
- In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.
- IDPS have become a necessary addition to the security infrastructure of nearly every organization.
- IDPS typically record information related to observed events, notify security administrators of important observed events and produce reports.
- Many IDPS can also respond to a detected threat by attempting to prevent it from succeeding.
- They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Thus, Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address. An IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options.

Classification of IPS

Intrusion prevention systems can be classified into four different types:

Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

Wireless intrusion prevention system (WIPS): monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.

Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.

Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Detection methods

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.

Signature-based detection: Signature-based IDS monitors packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures. While it is the simplest and most effective method, it fails to detect unknown attacks and variants of known attacks.[30]

Statistical anomaly-based detection: An IDS which is anomaly-based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network – what sort of bandwidth is generally used and what protocols are used. It may however, raise a False Positive alarm for legitimate use of bandwidth if the baselines are not intelligently configured. Ensemble models that use Matthews correlation co-efficient to identify unauthorized network traffic have obtained 99.73% accuracy.

Stateful protocol analysis detection: This method identifies deviations of protocol states by comparing observed events with "pre-determined profiles of generally accepted definitions of benign activity".While it is capable of knowing and tracing the protocol states, it requires significant resources.

Placement

The correct placement of intrusion detection systems is critical and varies depending on the network. The most common placement is behind the firewall, on the edge of a network.

This practice provides the IDS with high visibility of traffic entering your network and will not receive any traffic between users on the network. The edge of the network is the point in which a network connects to the extranet. Another practice that can be accomplished if more resources are available is a strategy where a technician will place their first IDS at the point of highest visibility and depending on resource availability will place another at the next highest point, continuing that process until all points of the network are covered.

If an IDS is placed beyond a network's firewall, its main purpose would be to defend against noise from the internet but, more importantly, defend against common attacks, such as port scans and network mapper. An IDS in this position would monitor layers 4 through 7 of the OSI model and would be signature-based. This is a very useful practice, because rather than showing actual breaches into the network that made it through the firewall, attempted breaches will be shown which reduces the amount of false positives. The IDS in this position also assists in decreasing the amount of time it takes to discover successful attacks against a network.

Sometimes an IDS with more advanced features will be integrated with a firewall in order to be able to intercept sophisticated attacks entering the network. Examples of advanced features would include multiple security contexts in the routing level and bridging mode. All of this in turn potentially reduces cost and operational complexity.

Another option for IDS placement is within the actual network. These will reveal attacks or suspicious activity within the network. Ignoring the security within a network can cause many problems, it will either allow users to bring about security risks or allow an attacker who has already broken into the network to roam around freely. Intense intranet security makes it difficult for even those hackers within the network to manoeuvre around and escalate their privileges.

Limitations

- Noise can severely limit an intrusion detection system's effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.
- It is not uncommon for the number of real attacks to be far below the number of false-alarms. Number of real attacks is often so far below the number of false-alarms that the real attacks are often missed and ignored.
- Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to newer strategies.
- For signature-based IDS, there will be lag between a new threat discovery and its signature being applied to the IDS. During this lag time, the IDS will be unable to identify the threat.
- It cannot compensate for weak identification and authentication mechanisms or for weaknesses in network protocols. When an attacker gains access due to weak authentication mechanisms then IDS cannot prevent the adversary from any malpractice.
- Encrypted packets are not processed by most intrusion detection devices. Therefore, the encrypted packet can allow an intrusion to the network that is undiscovered until more significant network intrusions have occurred.
- Intrusion detection software provides information based on the network address that is associated with the IP packet that is sent into the network. This rate.

However, the address that is contained in the IP packet could be fais beneficial if the network address contained in the IP packet is accuked or scrambled.

- Due to the nature of NIDS systems, and the need for them to analyse protocols as they are captured, NIDS systems can be susceptible to the same protocol-based attacks to which network hosts may be vulnerable. Invalid data and TCP/IP stack attacks may cause a NIDS to crash.
- The security measures on cloud computing do not consider the variation of user's privacy needs.They provide the same security mechanism for all users no matter if users are companies or an individual person.

Prevention actions

Once the IDPS detects a perceived threat, it can take several courses of action—depending on how it’s set up and the type of threat detected. Common preventative actions against attacks are to:

- **Alert administrators:** In this most basic type of response, the IDPS alerts human security administrators, much like an intrusion detection system would. Alerts like this are created when an automatic action might not be appropriate, or when the system is unsure if there is a false positive.
- **Employ banishment (expulsion) vigilance:** When the IDPS takes this action, it stops incidents before they have a chance to occur by blocking traffic or flagged users from a threatening IP address. A common example is blocking an IP address that has failed a password check too many times.
- **Change the security environment:** Similar to banishment vigilance, this technique has the IDPS change the security setup of the network to prevent the threat from gaining access. An example of this response would be reconfiguring a firewall.
- **Modify the attack content:** This technique involves automatically altering the content of the attack. For example, if a suspicious email is flagged, the IDPS would remove any aspect of the email that might contain content malicious to the network, such as email attachments.

Benefits of an IDPS

An IDPS can be a useful tool for both your enterprise security teams and the wider organization. An IDPS can help you:

- **Scan activity and respond to threats without human intervention:** Although complex threats often require human intervention, an IDPS enables methodical and rapid response to simpler threats, and it can flag complex threats for human intervention more rapidly. As a result, security teams can respond to threats before they do damage, and they are able to handle increasing numbers of threats.
  - **Find threats that might slip through:** An IDPS—especially if it’s using anomaly-based detection—can flag threats that human security experts might miss.
  - **Enforce user and security policies continuously:** The rule-based nature of an IDPS means that threat detection is applied in a consistent way.
  - **Meet compliance requirements:** The use of an IDPS means that fewer humans have to interact with private data—which is a regulatory requirement in many industries.

Evasion techniques

There are a number of techniques which attackers are using, the following are considered 'simple' measures which can be taken to evade IDS:

Fragmentation: by sending fragmented packets, the attacker will be under the radar and can easily bypass the detection system's ability to detect the attack signature.

Avoiding defaults: The TCP port utilised by a protocol does not always provide an indication to the protocol which is being transported. For example, an IDS may expect to detect a trojan on port 12345. If an attacker had reconfigured it to use a different port, the IDS may not be able to detect the presence of the trojan.

Coordinated, low-bandwidth attacks: coordinating a scan among numerous attackers (or agents) and allocating different ports or hosts to different attackers makes it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.

Address spoofing/proxying: attackers can increase the difficulty of the Security Administrators ability to determine the source of the attack by using poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server, it makes it very difficult for IDS to detect the origin of the attack.

Pattern change evasion: IDS generally rely on 'pattern matching' to detect an attack. By changing the data used in the attack slightly, it may be possible to evade detection. For example, an Internet Message Access Protocol (IMAP) server may be vulnerable to a buffer overflow, and an IDS is able to detect the attack signature of 10 common attack tools. By modifying the payload sent by the tool, so that it does not resemble the data that the IDS expect, it may be possible to evade detection.

Case Study 1

Siemens automates communication security with Red Hat Ansible

Siemens, a global technology company, uses public key infrastructure (PKI) technology to secure communications internally and with third-party partners and Internet of Things (IoT) solutions. To simplify and better automate its PKI environment, Siemens worked closely with Red Hat Consulting to replace its legacy automation solution with Red Hat Ansible Automation (ansutomation tool example). Siemens' PKI team is now using Ansible on Windows to automate manual management tasks and improve communications security across the business.

Benefits

- Optimized Ansible for Windows-based security environment
- Improved IT efficiency by automating management tasks and adopting continuous integration and delivery (CI/CD) approach
- Enhanced in-house Ansible expertise with dedicated, expert consulting and training

Simplifying and scaling communications security

Siemens is a global technology company focusing on electrification—from power generation, transmission, and distribution to smart grid solutions and the efficient application of electrical energy—as well as the areas of medical imaging and laboratory diagnostics. The company is the 10th largest software company in the world and a leader in intelligent infrastructure and sustainable energy.

Digitalization is a key component of Siemens' vision for the future. One of the tools that supports this vision is public key infrastructures (PKIs), a collection of processes and policies for creating, using, managing, and storing digital certificates and other secure communications components. PKI technology is used by all of Siemens 372,000 employees, as well as 100,000 users from the company's business partners, to reliably protect access to sensitive information. For example, an email can be encrypted using a PKI and a user's smart card, a physical authorization device.

The company is increasingly using PKIs to also secure Internet of Things (IoT) communications and now maintains two PKI environments for these different use cases. Additionally, communication between a greater variety of service teams is increasing. These changes have created additional complexity, particularly for configuration, increasing workloads for Siemens' PKI team.

To support this growth in PKI use, Siemens sought a more robust automation solution that would help its teams accommodate demand while reducing configuration complexity.

"Siemens does not make money by operating computers. Our focus is selling trains, power plants, or computed tomography [CT] imaging technology," said Rufus Buschart, Head of PKI at Siemens. "Central IT is under time and resource pressure to make the most of its investments."

Optimizing automation with integrated, supported technology

Siemens chose to replace its legacy automation solution for its PKI environment with Red Hat Ansible Automation. This simple, agentless IT automation solution supports configuration management and other IT functions and automates repetitive tasks for complex deployments. Ansible also offers a user friendly management interface that can integrate with other services for full visibility into IT automation.

Red Hat Consulting worked with Siemens' PKI team during a 2-day discovery workshop to draft a strategic project plan for automating its secure, Windows-based environment. Over the following 100 days, Red Hat consultants worked on-site or remotely with the team to quickly implement Ansible Automation with a continuous integration and delivery (CI/CD) pipeline.

"We needed more automation, and for this Red Hat Ansible Automation was the perfect choice, but we were not experts in Ansible," said Buschart. "We wanted Ansible up and running quickly, but the deployment needed to be correct. It's important to maximize our IT investment, so we wanted as much detail as possible from Red Hat's experts."

Improving IT security with help from Ansible experts

Optimized Windows environment automation

Working with Red Hat Consulting helped Siemens optimize its new Ansible Automation deployment to work effectively in its Windows-based PKI environment. For example, Siemens worked closely with Red Hat consultants to learn how to use infrastructure-as-code and CI/CD practices to write and test playbooks, with all hardening measures now scripted in Ansible.

“Our environment is Windows-based, but Ansible comes from the Linux world,” said Buschart. “We had error messages, particularly around connecting to a server, and we wanted to replace basic usernames and passwords with strong authentication. Red Hat consultants made a big difference in reaching these goals.”

Improved management efficiency

Previously, Siemens’ PKI team spent hours manually checking for minor unwanted changes to the configuration of its Windows-based communications environment. With Red Hat Ansible Automation, supported by Red Hat Consulting, Siemens has automated these audits to improve configuration quality while reducing manual effort.

Additionally, developers can now use Ansible Playbooks to independently deploy and dismantle development environments as needed, as well as automatically deploy and test new PKI software versions before release.

“What we really like about Ansible is being able to check our playbooks into a version control system. We have the configuration of our environment stored in Git, which is very convenient,” said Buschart. “We don’t have to go on the server, just our Git repository, to check that the server looks as it should.”

As a result of these improvements, the company anticipates that its time to market will improve.

Enhanced in-house expertise

To make the most of its automation investment, Siemens worked closely with Red Hat to get hands-on experience and best practices guidance for operating and maintaining its new Ansible Automation technology.

Now, in the year since the initial deployment, Siemens’ PKI team can independently create its own playbooks, with Red Hat available to check technical details or troubleshoot if needed

Enhanced in-house expertise

To make the most of its automation investment, Siemens worked closely with Red Hat to get hands-on experience and best practices guidance for operating and maintaining its new Ansible Automation technology.

Now, in the year since the initial deployment, Siemens’ PKI team can independently create its own playbooks, with Red Hat available to check technical details or troubleshoot if needed. “Whenever we need Red Hat, they are there,” said Buschart.

Evolving to Infrastructure-as-Code

In the near future, Siemens plans to work with Red Hat to begin explore using Jenkins, an open source, JavaTM-based automation server, to automate testing processes.

“We need to change our mindset. We’ll stop thinking of computers as boxes and more as just a place where software is running. We need a vision of infrastructure-as-code,” said Buschart. “The role of the typical administrator opening a console, connecting to a server, and starting to configure will disappear in the coming years. It’ll be replaced by someone creating scripts in Ansible that are checked in and implemented automatically. Instead of patching servers, we’ll spin up a new one with the updates and applications we need.”

About Siemens

Siemens AG (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability, and internationality for more than 170 years. The company is active around the globe, focusing on the areas of electrification, automation, and digitalization. One of the largest producers of energy-efficient, resource-saving technologies, Siemens is a leading supplier of efficient power generation and power transmission solutions and a pioneer in infrastructure solutions as well as automation, drive, and software solutions for industry. With its publicly listed subsidiary Siemens Healthineers AG, the company is also a leading provider of medical imaging equipment – such as computed tomography and magnetic resonance imaging systems – and a leader in laboratory diagnostics as well as clinical IT. In fiscal 2018, which ended on September 30, 2018, Siemens generated revenue of €83.0 billion and net income of €6.1 billion.