Introduction to intrusion prevention systems

Detect and block attacks in real time

Himanshu Arora

March 19, 2013

This article focuses on intrusion prevention systems (IPS), a technology that can detect and prevent computer systems from intrusions in real time. Learn about the different types of IPSs, how they work, and why they are better than traditional firewalls. This article discusses Snort, OSSEC, and Suricata, three popular free or open-source IPSs.

Introduction

Cyber security is a heated discussion topic in the IT world today. With the exponential increase in cyber crime, individuals as well as corporations are feeling the heat of computer security breaches. Even state governments are being targeted successfully by cyber criminals (see Related topics). Extensive cyber crime creates doubt about the computer defense systems in place today. Although no security mechanism can guarantee 100-percent protection against malicious computer intrusions, deploying the best possible defense systems makes it difficult for cyber intruders to enter computer systems and cause damage.

In the computer defense systems arena, firewalls and anti-virus protection are not enough. You need more proactive, intuitive, and preemptive computer defense technology with the capability to detect and prevent, or block, an attack in real time. One such technology is the intrusion prevention system (IPS) or intrusion detection and prevention system.

In this article, learn the basics of IPSs and how are they different from intrusion detection systems (IDSs) and firewalls. The article also looks at some popular free and open-source software (FOSS) for IPSs.

IBM IPS products

IBM® offers a range of intrusion prevention solutions and other security products. These solutions stop Internet threats before they impact your business. IBM Security Network Intrusion Prevention solutions provide comprehensive protection while reducing the cost and complexity associated with deploying and managing point solutions. See Related topics for more information on these Security Network Intrusion Prevention solutions.

Infrastructure protection solutions
IBM Infrastructure protection solutions provide in-depth security across your network, servers, virtual servers, mainframes, and endpoints. This spans a wide range of critical security needs from identifying and blocking the latest emerging threats to keeping all endpoints in continuous compliance with organizational policies.

Intrusion prevention systems

An IPS is a preemptive network security approach that uses advanced techniques to detect and block (or prevent) possible intrusion attempts into a computer system. An IPS thoroughly scans the traffic flowing to and from a computer system or computer network for security breaches. If a threat is detected, the system is able to take defensive actions such as dropping a particular data packet or dropping the whole connection. The scan captures details, the action report is logged in a file, and an alert is sent to the system or network administrator.

IPSs differ in how they scan the data streams to detect a threat or intrusion. Some of the most popular methods are described below.

**Signature method**

In the signature method, the IPS compares the real-time data stream patterns with a huge database of attack patterns that have already been detected. In this process, each data packet is scanned, byte by byte, for a particular pattern or string that represents complete or partial code associated with a known attack. The pattern or string could be anything, such as a command name or a specific set of characters.

For example, consider a hypothetical situation in which an unsuccessful attempt to log in to a server generates a "Login Failed" response to a user. This response is normal if users forget their login credentials or enter the wrong credentials, but a repetitive login failure could signal a possible intrusion attempt. If there is a rule in the IPS that scans the outgoing packets for the signature "Login failed," after a legitimate number of login retries an alert would be generated to the system or network administrator.

Another example involves the usernames and passwords used in repetitive login attempts. If an IPS is configured to match usernames and passwords with the list of usernames and passwords collected from known attacks, then this type of signature match can also trigger an alert.

When a new attack is detected, the attack pattern or signature for that attack is generated by the IPS vendor and added to the database of signatures used by the IPS in the form of updates or software patches. This process is similar to the way an anti-virus program updates its database of known viruses.

If a match is found, preventive action is taken and an alert is generated. This step ensures that known cyber attacks or intrusion attempt patterns do not cause damage to the computer system.

Following are some examples of signature matching:

- Matching the subject description or attachment name of an email with details of a known or detected malicious email.
• Tracking the denial-of-service attack by counting the number of times a command is executed and matching it with known statistics of a similar kind of attack.
• Matching a user activity prior to authentication or login with a known attack pattern.

The weakness of the signature method is that it's highly likely a new type of attack or intrusion attempt will be undetected by the IPS. If a known intrusion attempt is carried out in steps with a large time gap between each step, there's a chance that such attacks might go unnoticed. And, if an attack signature is slightly modified, it's possible that an IPS might not detect it.

Profile method

In the profile method, the IPS collects a pattern of data stream flowing to and from a computer system (or computer network) in controlled or trusted conditions. This pattern is treated as a baseline profile and compared against the real-time data stream patterns. A real-time data stream pattern that is found to be suspiciously different from the baseline profile is treated as an attack, and preventive action is taken against it. A standard baseline profile can represent normal behavior of things such as network connections, applications, users, and hosts.

For example, if a real-time data stream is observed to be accessing a crucial system file that wasn't accessed when the baseline profile was generated in the controlled environment, this attempt is treated as malicious. The incident is then reported through an alarm.

The IPS can also be taught to recognize normal system behavior through artificial intelligence (see Related topics). Because this method checks for deviations from normal data traffic, it is also known as the anomaly-based method.

The weakness of the profile method is that it can cause false alarms; a valid change in the real-time data stream pattern could be misinterpreted as an attack. Also, it is hard to maintain a standard baseline profile as network topologies change frequently.

Stateful protocol method

Data packets are wrapped with various protocol headers. Each layer of the TCP/IP or Open Systems Interconnection (OSI) model adds the header of the protocol (the protocol being used for that layer, that is) to the received packet. Protocols follow a standard document format known as Requests for Comments (RFCs). An RFC completely explains the protocol and describes how it should be used. The RFC forms the basis of the stateful protocol method. In this method, each protocol header is peeled apart and scanned for its consistency with what its RFC specifies. A deviation from the RFC is considered alarming, and an alert is raised.

For example, a TCP packet with only SYN and FIN flags on is a deviation from what the TCP RFC specifies. If a data packet with the TCP header contains both these flags on, then this needs to be reported.

In addition to monitoring the ideal behavior of a protocol, an IPS also has intelligence about how a particular protocol is implemented in the real world to make sure that a normally practiced RFC violation is not treated as a malicious attempt to breach computer security.
The stateful protocol method is like the profile method. The difference is that the profile method uses network- or host-specific rules while the stateful protocol method uses the protocol-specific rules described in corresponding RFCs. It scans the protocol states and makes sure that the protocol is being used in a proper way and is following valid state transitions.

**Which method is better?**

There is no clear answer to this question, but here are some facts to keep in mind:

- An IPS working on the signature method is able to detect only the attack pattern of a known attack. All other types of attacks, even slight variants of a known attack, are usually not detected. An IPS working on the stateful protocol method checks if the protocols are implemented according to standards. This approach enables an IPS to detect even unknown attacks that violate a protocol RFC rule.
- IPSs with capabilities of both the signature and protocol methods of attack detection are getting popular. Using this hybrid method, an IPS can scan the protocol headers for alarming RFC violations and data packets for known attack signatures. This approach provides enhanced security to a host or computer network.
- Compared to the profile-based method, IPSs working on the signature-based method are more popular among corporations. Profile-based IPSs tend to generate a lot of false alarms that result in undesired data traffic disruptions and extensive monitoring of the alarms generated. The entire computer network setup would be at the mercy of the limited signature rules in a signature-based IPS. The time gap between the detection of a new attack and the release of a software patch or update from the vendor could be large enough to expose the computer network to the new attack.

Researchers and programmers are working to develop a superior IPS model that would incorporate the best features of all three methods and detect known and unknown attacks with equal accuracy.

**Types of IPSs**

Popular IPS types are host, network, or wirelessly based.

**Host IPS**

A host IPS scans the traffic, both outgoing and incoming, at a given host. This type of IPS is installed as software on a host. It runs as a process and scans various characteristics of the host system (executables, connections, and file access) and prevents malicious intrusion attempts. The component of an IPS installed on a host is known as an agent. The agent scans the host characteristics and takes preventive actions. Every agent transmits data or log information to centralized servers used to manage hosts. This way, each host has its own IPS while the information for the complete network can be accessed through the centralized management servers.

Sometimes, the agent running on an individual host is configured in a way that an attack detected by the agent is reported back to the central server. The central server sends the control command
back to the agent to let it know which preventive action needs to be taken. Although there's nothing wrong in this type of configuration, this approach does increase the response time of an IPS and possibly gives an attacker enough time to carry out the damage.

An agent-based design includes a manager and various agents. There are several host IPSs that follow agentless design. In this type of design, the data is fetched by a central entity (manager) through the existing resources available on computer hosts.

**Network IPS**

A network IPS scans the incoming and outgoing traffic on a network. This type of IPS is usually installed at key positions in the network, for example, in proximity to the router, firewall, or hub. A network IPS mostly scans the traffic at the application layer, but some network IPSs are able to scan traffic at the transport and Internet layers. Network IPSs work in promiscuous mode and are used to detect and prevent network attacks.

As in the case of host IPSs, network IPSs are also configured to contact the central management servers for either logging information or a control command that specifies the preventive action to be taken for an attack.

**Wireless IPS**

A wireless IPS scans the wireless data traffic to prevent an unauthorized access or attack on the LANs and other resources that use the wireless Internet connection. A wireless IPS monitors the radio spectrum for the presence of suspicious access points. It also detects the use of wireless attack tools. As soon as a wireless IPS detects an unauthorized wireless access point, it alerts the network or system security administrator.

A wireless IPS is deployed in the form of sensors that contain antennas and radios for scanning the wireless data traffic. A central server then scans the data captured by the sensors.

**IPSs, IDSs, and firewalls**

There are distinct differences between IPSs, IDSs, and firewalls.

**IPS versus IDS**

The major difference between an IPS and an IDS is that an IDS is only capable of detecting an intrusion or attack and reporting it to the appropriate authority. An IDS is not capable of responding to an attack by taking a preventive action such as dropping a packet or closing down a connection. An IPS is capable of detecting an intrusion and also of taking preventive measures. Thus, IPSs are sometimes also known as IDPSs (intrusion detection and prevention systems).

**IPS versus firewall**

A firewall is capable of limiting access to a computer system or a computer network. It controls the data traffic at the level of TCP/IP ports. For example, a firewall can limit access to a port that no standard service uses. However, if an attacker penetrates through a standard port like port 80
(used for HTTP) there is little that a firewall can do. Firewalls usually operate only on the packets that are coming into the network or a host.

An IPS can scan the traffic in real time by scanning the pattern of the data stream against a database of known attack patterns or a standard data pattern. An IPS can also scan both the inbound and outbound data stream traffic.

If you compare an IPS and a firewall to a security system, it could be said that the firewall checks only the ID cards of the data packets, but the IPS checks the baggage, too.

Free, open source IPSs

Many IPSs are being used in the real world today. Three popular free and open source (FOSS) IPSs to consider are Snort, OSSEC, and Suricata.

Snort

Snort, an open source IPS that's used globally (see Related topics), was developed by Martin Roesch, who later founded the company Sourcefire. Though Sourcefire uses the core technology of the Snort IPS with other variants for commercial purposes, the original Snort IPS remains under GPL license and is free to use, edit, and redistribute.

Snort is a network-based intrusion detection and prevention system (NIDS) that uses signature, anomaly, and protocol methods to detect a cyber attack. Snort:

- Can perform protocol analysis and content searching or matching
- Can detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more
- Uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture
- Has a real-time alerting capability that incorporates alerting mechanisms for syslog, a user specified file, a UNIX® socket, or WinPopup messages to Windows clients
- Has three primary uses:
  - A straight packet sniffer, like tcpdump
  - A packet logger, useful for network traffic debugging
  - A full-blown network IPS

The Snort IPS can detect the following attacks:

Buffer overflows

A buffer overflow is when the input provided to a program buffer overruns the buffer's boundaries and spills over to overwrite the data stored at neighboring locations in memory. This is a popular technique used by cyber criminals to alter the behavior of a program. (See Related topics.)

Stealth port scans

This is an advanced port scanning technique through which port scans cannot be detected by the auditing tools. Normal port scanning can be detected by observing frequent connection
attempts with no data. In the case of stealth port scans, port scanning can be done at a very slow rate. The slow rate ensures that auditing tools do not identify the connections request (used by stealth port scanning) as malicious attempts to intrude into computer systems. (See Related topics.)

CGI attacks
Cyber criminals can exploit vulnerabilities in CGI scripts to break into computer systems even without access to any user login accounts on the system. (See Related topics.)

SMB probes
A server message block (SMB) works as an application layer protocol to provide shared access permissions to files, ports, and so on. An SMB probe can check for the shared entities available on the system. A cyber criminal can use an SMB probe to detect which files, ports, and so on are shared on the system. This approach can leave the computer system highly vulnerable to attacks. (See Related topics.)

OS fingerprinting attempts
Operating system (OS) fingerprinting is the science of detecting the OS details of the target computer system. The information includes the vendor name, underlying OS, OS generation, device type, and so on. A cyber criminal can use this technique to know the OS details of the target computer system. (See Related topics.)

Table 1 lists some of the pros and cons of Snort.

### Table 1. Pros and cons of Snort

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is free to download and use.</td>
<td>No GUI for rule manipulation.</td>
</tr>
<tr>
<td>The rules are easy to write.</td>
<td>It is slow in packet processing.</td>
</tr>
<tr>
<td>It has good community support.</td>
<td>It cannot detect a signature split over multiple TCP packets, which occurs when packets are configured in inline mode.</td>
</tr>
<tr>
<td>It is highly flexible in terms of deployment.</td>
<td></td>
</tr>
</tbody>
</table>

Snort is available for the following operating systems:

- Linux®
- FreeBSD
- OpenBSD
- NetBSD
- Solaris
- Microsoft™ Windows™
- MacOS
- IRIX
- AIX®
- HP-UX

The commercial variant of Snort (which uses much of Snort's core), developed by Sourcefire, is among the five top selling IPS solution providers (see Related topics). Hence, Snort is very popular as an open-source alternative.
OSSEC

OSSEC, another open source IPS (see Related topics), was developed by Daniel B. Cid. In 2008, this project and all its copyrights were acquired by the company Third Brigade. In 2009, Third Brigade was acquired by Trend Micro. This project has been through many transitions but it has remained open source.

Unlike Snort, OSSEC is a host-based intrusion detection and prevention system that uses both signature- and profile-based methods to detect cyber attacks.

OSSEC capabilities include:

File integrity checking
   Lets you check important files for changes. It can be used to detect an unauthorized access to a file (mostly system files) by a cyber criminal; a cyber attack usually accesses or makes changes to system files. Software that performs this type of task is known as a file integrity checker. (See Related topics.)

Very strong log monitoring
   Logs can always provide a view of what is happening in the system. OSSEC has a very powerful engine that can collect and scan all application-specific logs—a task that's very cumbersome if done manually. This capability lets administrators know exactly what is going on in the system.

Rootkit detection
   Rootkits are malicious pieces of software designed to hide malicious processes (that hold root or administrative privileges) from being detected by normal detection methods on a computer system. OSSEC provides rootkit detection. (See Related topics.)

Agent and agentless monitoring
   OSSEC provides both agent-based and agentless modes of monitoring.
   - An agent-based design contains a manager that sits at a central position in the network while software agents are deployed on various hosts. Agents scan the data flowing in and out from hosts and send the information to the manager in case something needs to be reported.
   - Agentless design uses existing methods and available software on a system to fetch the information required by the manager.

Table 2 outlines some of the pros and cons of OSSEC.

Table 2. Pros and cons of OSSEC

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses a very powerful log scanning engine.</td>
<td>Sends only a limited number of alerts (12) per hour. This weakness can be exploited by engaging OSSEC in the first step and then launching the actual attack later.</td>
</tr>
<tr>
<td>Incorporates features to meet the requirements of the payment card industry.</td>
<td>Supports syslogs, which can easily be spoofed.</td>
</tr>
<tr>
<td>Contains security information and an event manager to centralize log management on a huge network.</td>
<td></td>
</tr>
</tbody>
</table>
OSSEC is available for the following operating systems:

- GNU/Linux (all distributions, including RHEL, Ubuntu, Slackware, Debian, and so on)
- Microsoft Windows 7, XP, 2000, and Vista
- Microsoft Windows Server 2003 and 2008
- VMWare ESX 3.0, 3.5 (including CIS checks)
- FreeBSD (all versions)
- OpenBSD (all versions)
- NetBSD (all versions)
- Solaris 2.7, 2.8, 2.9, and 10
- AIX 5.3 and 6.1
- HP-UX 10, 11, 11i
- MacOSX 10

OSSEC is widely popular with those who want to deploy a host-based IPS. It has won many awards and positive reviews in the industry.

**Suricata**

Suricata is another open source IPS (see Related topics). It is owned by the non-profit Open Information Security Foundation (OISF). Many other vendors also support the development of Suricata.

Like Snort, Suricata is a network IPS. Suricata uses the signature method to detect a cyber attack.

Suricata operates by fetching one packet at a time from the system. The fetched packet is preprocessed and then fed to the core engine that runs the detection algorithms to check if the packet is normal or malicious. Based on the decision, the packet is either accepted or rejected.

Capabilities of Suricata include:

**High scalability**

With multi-threading, you can run one instance that will balance the load of processing across every processor on a sensor that Suricata is configured to use. This approach allows commodity hardware to achieve 10GB speeds on real-life traffic without sacrificing ruleset coverage.

**Protocol identification**

Because Suricata recognizes the most common protocols automatically as the stream starts, rule writers can write a rule to the protocol—not to the port expected. This approach makes Suricata a malware command and control channel hunter like no other. Off port HTTP CnC channels, which normally slide right by most IDS systems, are child's play for Suricata. With dedicated keywords you can match on protocol fields, which range from HTTP URI to an SSL certificate identifier.

**File identification, MD5 checksums, and file extraction**

Suricata can identify thousands of file types while crossing your network. If you decide you want to look at a file further, you can tag it for extraction and the file will be written to a disk with a meta data file describing the capture situation and flow.
The file's MD5 checksum is calculated on the fly, so if you have a list of MD5 hashes you want to keep in (or out of) your network, Suricata can find the list.

Table 3 shows some of the pros and cons of Suricata.

**Table 3. Pros and cons of Suricata**

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides advanced processing of HTTP streams through an HTTP normalizer and parser.</td>
<td>Expensive on system resources, resulting in slow network connections.</td>
</tr>
<tr>
<td>Highly efficient.</td>
<td>Can cause false alarms in some cases.</td>
</tr>
<tr>
<td>Uses Snort's rulesets.</td>
<td></td>
</tr>
</tbody>
</table>

Suricata is available for the following operating systems:

- Linux
- FreeBSD
- Mac OS X
- Microsoft Windows

Suricata, which has only a couple of releases, is still relatively new.

**Snort, OSSEC, or Suricata?**

Which IPS is best for you depends on your requirements. Each system has advantages and disadvantages that you should explore before making your selection.

It's not logical to compare Snort or Suricata with OSSEC. Snort and Suricata are network intrusion prevention systems (NIPS) while OSSEC is a host intrusion prevention system (HIPS). Though OSSEC has the capacity to detect some types of anomalies, its power lies in log scanning. It is recommended that you use Snort for packet inspection because it's designed to monitor network activity. After Snort is up and active, you can use OSSEC to scan the logs produced by Snort. This way, you can have the best of both products.

If you're comparing Suricata with Snort, keep in mind that Suricata is fairly new. It was forked from Snort to develop a modern alternative with capabilities such as multi-threading. See Related topics for detailed comparisons of Snort and Suricata.

**Conclusion**

Though it's hard to eradicate or permanently stop unauthorized computer system intrusions, you can use superior defense techniques like intrusion detection and prevention systems for the best possible safety. With FOSS IPS the technology is available to everyone today.
Related topics

- **Snort vs Suricata** and **Suricata-vs-snort**: Delve into the discussions.
- **IBM Security Network Intrusion Prevention System**: Learn more about this product.
- **Snort**: Read more about this open source network intrusion and prevention detection system.
- **OSSEC**: Learn about the open source host-based intrusion detection system and its **awards and reviews**.
- **Suricata**: Read about this high performance Network IDS, IPS, and Network Security Monitoring engine.
- "**Lax Security at LinkedIn Is Laid Bare**": Read how the data company didn't protect its data.
- **Anonymous hacks U.S. government websites with anti-ACTA messages**: Visit this blog to read more about the hacking collective Anonymous.
- **Intrusion Detection FAQ: What Are The Top Selling IDS/IPS and What Differentiates Them from Each Other?**: Explore the market leaders and how to compare their offerings.
- **INTRUSION DETECTION AND PREVENTION SYSTEM: CGI ATTACKS**: Read this thesis about the results of research performed on CGI-related web server attacks.
- On Wikipedia, read about:
  - **Intrusion Prevention System**
  - **Artificial intelligence**
  - **Buffer overflow**
  - **Server Message Block**
  - **File integrity monitoring**
  - **Rootkit**
- On Nmap, read about **Port Scanning Techniques** and **OS Detection**.
- **Download the Snort Engine and Snort Rules**.
- **Download OSSEC**.
- **Download Suricata**.

© Copyright IBM Corporation 2013
**Trademarks**
(www.ibm.com/developerworks/ibm/trademarks/)