Intrusion detection system (IDS) (Part 1)

IDS (Intrusion Detection Systems) is a device or software that monitors network traffic, suspicious behaviors and alerts for system administrators.

As the Internet and internal networks become more and more popular, the challenge of unauthorized network intrusion problems forces organizations to add systems to check for IT security vulnerabilities. One of the most talked about systems is the intrusion detection system (IDS). This article will introduce you to IDS, specifically an overview of some types of detectable attacks, symptoms of attacks and IDS tasks, different architectures and concepts in this area.

What is IDS?

IDS (Intrusion Detection Systems) is a device or software that monitors network traffic, suspicious behaviors and alerts for system administrators. The purpose of IDS is to detect and prevent actions that damage system security, or actions in the attack process such as port detection and scanning. IDS can also distinguish between internal attacks (from employees or customers in the organization) and external attacks (from hackers). In some cases, IDS can react to unusual / malicious traffic by blocking users or network access source IP addresses.

What tools are not IDS?

There are many devices, the device is mistakenly identified as IDS, you need to make a clear distinction to avoid confusion. Specifically, the following security devices are not IDS:

1. Network logging system is used to detect vulnerabilities for denial of service (DoS) attacks on the network that are congested. These are traffic monitoring systems in the network.
2. Vulnerability assessment tools, used to check for errors and vulnerabilities in operating systems, network services (security scanners).
3. Antivirus software is designed to detect malicious software such as viruses, Trojan horses, worms, logic bombs . Although the default features can be very similar to intrusion detection systems and often provide a effective security detection tools, but overall they are not IDS.
4. Firewall: Although many modern fire ideas are built-in IDS, IDS is not a firewall.
5. Security / encryption systems, such as VPN, SSL, S / MIME, Kerberos, Radius

IDS classification

IDS has many types and access suspicious traffic in many different ways. There are network-based IDS (NIDS) and server-based (HIDS). There is IDS detection based on the search for specific signatures of known threats (similar to how anti-virus software detects and blocks malware) and IDS detected by comparing traffic patterns

with baseline and see if there is any abnormality. There are IDS only for monitoring and warning, which IDS will take action when intrusion detection. We will examine in detail below:

1. **NIDS:** Network Intrusion Detection Systems are located at a strategic point or monitoring points for incoming and outgoing traffic from all devices on the network. Ideally, you can scan all inbound and outbound traffic, but this can create bottlenecks that reduce the overall speed of the network.
2. **HIDS:** Host Intrusion Detection Systems, this intrusion detection system runs on a dedicated server or a special device on the network. HIDS only monitor inbound and outbound data packets from the device and warn users or administrators about suspicious activity detected.
3. **Signature-Based:** These are IDS-based IDs, monitor packets on the network and compare them with signature databases, properties from known threats, similar to how software kills virus works. The problem with this IDS system is that it may not detect a new threat, when the signature to identify it has not been updated by IDS yet.
4. **Anomaly-Based:** This IDS will detect threats based on anomalies. It monitors network traffic and compares with established baseline. Baseline will determine what is the normal level of the network: the type of bandwidth normally used, the common protocol, the port and the device often connect to each other, alert the network administrator or user when detecting the traffic. unusual or significant differences compared to baseline.
5. **Passive: Passive** IDS will only detect and alert. When detecting suspicious or malicious traffic, it will create a warning and send it to the administrator or user. The following action depends on the user and the administrator.
6. **Reactive:** This type of IDS besides tasks like IDS Passive, it also performs pre-set actions to immediately respond to threats, such as: blocking access, IP lock.

Some other content about IDS

Types of attacks are classified into the following two categories:

1. Passive (equipped to increase access level makes it possible to penetrate the system without the consent of IT resources)
2. Positive (results cause changes in the invalid state of IT resources)

In the form of the relationship between victim and intruder, attacks are divided into:

1. Inside, these attacks come from the employees of the company, business partners or customers
2. Outside, attacks come from outside, often via the Internet.

Attacks are also distinguished by the source category, namely the source made from internal systems (local network, Internet or remote dial-up sources). Now let's look at the types of attacks that can be detected by the IDS tool and put them into a special category. The following types of attacks can be distinguished:

1. These attacks involve unauthorized access to resources.
    1. Cracking and access violation
    2. Trojan horses
    3. Interception; Most are associated with TCP / IP theft and interception often uses additional mechanisms to compromise the system
    4. Forgery
    5. Scan ports and services, including ICMP scanning (ping), UDP, TCP

6. Remote OS Marking, such as checking responses to specific packages, standard application addresses, response applications, IP stack parameters, etc.
7. Listen to network packets (a passive attack is difficult to detect but sometimes still possible)
8. Information theft, such as disclosure of ownership information.
9. Abuse of authenticity; a type of internal attack, for example: suspecting the access of an authenticated user with strange properties (coming from an unwanted address)
10. Unauthorized network connections
11. Use IT resources for personal purposes, such as accessing sites with unhealthy activities
12. Take advantage of system weaknesses to access high-level resources or access.

2. Unauthorized change of resources (after gaining access)
    1. Distorting uniformity, for example, to obtain system administrator rights.
    2. Change and delete information
    3. Unauthorized transmission and creation of data, for example: setting up a database of stolen credit card numbers on a government computer.
    4. Unauthorized configuration changes for the system and network services (servers)
3. Denial of service (DoS)
    1. Flooding - compromises a system by sending a large amount of non-valuable information to block limited service traffic.
        1. Ping (Smurf) - a large number of ICMP packets are sent to a broadcast address.
        2. Send mail - flood with hundreds or thousands of messages in a short time.
        3. SYN - initiates a large number of TCP requests and does not proceed with the handshake completely as required for a protocol.
        4. Limited service dispersion; from many different sources
    2. Damage the system by taking advantage of its vulnerabilities
        1. Buffer overflow (eg 'Ping of Death' - sending a large number of ICMP (exceeding 64KB))
        2. Turn off the remote system
4. Web application attack; Attacks that take advantage of application errors can cause as mentioned above.

You need to remember that most attacks are not a single action, but that they usually consist of several individual events.

Do you encounter risks

In order to recognize attacks, we have to check for any unscrupulous behavior of the system. This can be a useful way of detecting real attacks. Let's take a look at the symptoms so that we can track the intruders' traces.

Use known vulnerabilities

In most cases, trying to take advantage of errors in an organization's security system may be considered an offensive behavior, which is also the most common symptom for an intrusion. However, the organizations themselves may have to take measures against the attacker by using tools to help protect the network - the tool is called a file status and security scanner. They operate internally or remotely, but they are also often studied by intruders.

These tools are usually a double-edged sword, available to both users and attackers. Checking the correctness of file usage with integrity scanners and understanding vulnerability scans is essential to detecting attacks that are in progress or following failures from successful attacks. From these problems, the following technological problems arise:

1. The detection of the scanner. The file integrity checking tool works in a systematic way to use modeling techniques and special tools for detection purposes, for example, anti-SATAN software.
2. A correlation between scanning and usage is essential - scanning for vulnerabilities may need to use a service feature more in depth, which means it can foresee possible attacks. in the future.

Other network activities are often periodic

An intruder is trying to attack a system that often exploits applications and conducts many testing methods. Intrusion activities are often different from the activities of users who are working with the system. Any penetration testing tool can distinguish suspicious activities after a threshold. If a certain threshold has been exceeded, a warning will appear and announce to you. This is a passive technique that allows an intruder to be detected without having to find a clear evidence, just through quantitative testing.

The passive method used in intrusion detection is controlled from the database of recurring attack signals and is reviewed in the following aspects:

1. Repeat thresholds are intended to help distinguish valid and suspicious activity (to trigger alerts). Network activities can be identified using multiple parameter values ??taken from (for example) user profiles or Session states.
2. The time between iterations is a parameter to determine the elapsed time between events that occur adjacent to each other, for example, an activity that is suspected if it occurs within about 2 minutes has up to 3 logins success.
3. Build a database corresponding to the attack signs. An attacker can take neutral actions (most likely during the exploration phase) and that may mislead IDS prevention devices.

Commands cannot be typed or answered in automatic sessions

Network services and protocols are demonstrated in strict ways and use identification software tools. Any incompatibility with the given patterns (including human errors such as the appearance of a print error in the network package) can be valuable information to detect the service being targeted. by intruder.

If the inspection system uses facilities, such as delaying mail, its record chain will show a normal or predictable habit. However, if the record indicates that a particular process has provided invalid commands, this may still be a symptom of a normal event or a spoofing event.

Check for attack effects:

1. Detect an attack to restore the following commands or answers by launching them.
2. Detecting some failed attacks can see the syntax of previous successful attacks.
3. The detection of attacks is under investigation to adapt to catch errors related to the same object (service, host). After a certain period, these errors will stop.

Direct conflict in traffic

Any direct inconsistencies in packages or sessions are one of the potential attacks. Consider source and location data (domestic or foreign) that can be identified directly on a packet.

Session sessions are identified directly from the first packet. However, the requirement for services in the intranet is an on-going session and a process of activating a service-based Web from an internal network is an outgoing session.

The direct contradiction below can be seen as signs of an attack:

1. Packages come from the Internet and are identified by their internal network address - service requests are coming from outside, in which case the packets have their internal source addresses. This situation may be a sign of an external IP spoofing attack. Such problems can be solved at routers, they can compare source landlords with destination locations. In fact, few routers support this security feature because this is the area for firewalls.
2. Packages are generated in the local network (sent) and sent to an external network with its destination address - the opposite. Intruders perform from outside and target an external system
3. Packages with unwanted source and destination ports - if the source port of an on-going package or outgoing request does not match the service type, this will act as an intrusion (or system scan). . For example, requesting Telnet Service on port 100 in an environment can occur, such a service cannot be supported (if any). Direct inconsistencies can almost be detected by firewalls to get rid of invalid packages. However, firewalls are not always preferred for intrusion detection systems.

Unexpected attributes

The most common cases are those where a large number of package properties or specific service requirements are handled. We can completely define the expected attribute template. If the properties encountered do not match this pattern, it may be an intrusion.

1. Time and schedule attributes - in certain environments, specific network behavior can occur on a regular basis at a certain time of day. If this normal behavior is broken, this case needs to be checked. For example, we use a company, where shipping is conducted on Friday afternoon. That way, the number of data exchanged during the working sessions at that time or on that day is treated as normal actions. However, if Friday is a holiday and data transmission is still available, this issue needs to be checked.
2. System resource properties. Certain intrusions often negatively affect some of the system properties. Cracking by repeatedly repeating passwords often involves the use of most CPU performance like DoS attacks with system services. Using a lot of system resources (processors, memory, drives, system processes, services, and network connections), especially non-critical times, can be a sign.
3. For packages with unexpected TCP response settings. If there is a set of ACK-flags via a packet and no previous SYN-packet is sent, it can also be an attack (or scan of the service). Such a situation may also be the case of a packet failure, a network problem for the software, not necessarily an attack.
4. Service mixes attributes. Usually we can define a standard set of input and output services to provide for a specific user. For example, if the user is on their business trip, he wants to use mail and file transfer options. Any attempt on his account via Telnet to access the ports may be attacks.

There is also a more general concept than service mix, namely users and service profiles that help in distinguishing typical attributes and unwanted attributes. A sign file that holds some of the common services of a specific user can also store additional attribute information. This information includes working hours related to the user's system, the location of the workstation (geographic location, IP address), resource usage intensity, typical session duration by single services.

The problem is not explained

A masked intruder can design dangerous actions, these actions will often cause weird problems in the behavior of a system. Examining such effects is often difficult because their location is difficult to detect. Here are some of its uses:

1. Unexpected problems with hardware or system software, for example slow servers, some inactive utilities, unexpected system reboots, changing system clock settings .
2. System resource issues: file system overflow; Unusual use of CPU performance.
3. Bizarre notifications from system utilities, system utilities that are inactive or destroyed. Such symptoms must always be suspicious.
4. System performance issues (routers or system services have long server response times)
5. Unexpected user behavior, for example: unwanted access to system resources.
6. Unexpected behavior test. Audit records shrink in size (unless intentionally made by the system administrator).

The tasks need to be performed

The main task of intrusion detection systems is to prevent a computer system by detecting signs of attack and can repel it. The detection of attacks depends on the number and type of appropriate action (Figure 1). In order to prevent good intrusions, a good combination of 'baits and traps' is needed for the study of threats. Commanding the focus of intruders on protected resources is another important task. Both the real system and the trap system need to be tested continuously. Data generated by intrusion detection systems is carefully checked (this is the main task for each IDS) to detect attack signals (intrusion).

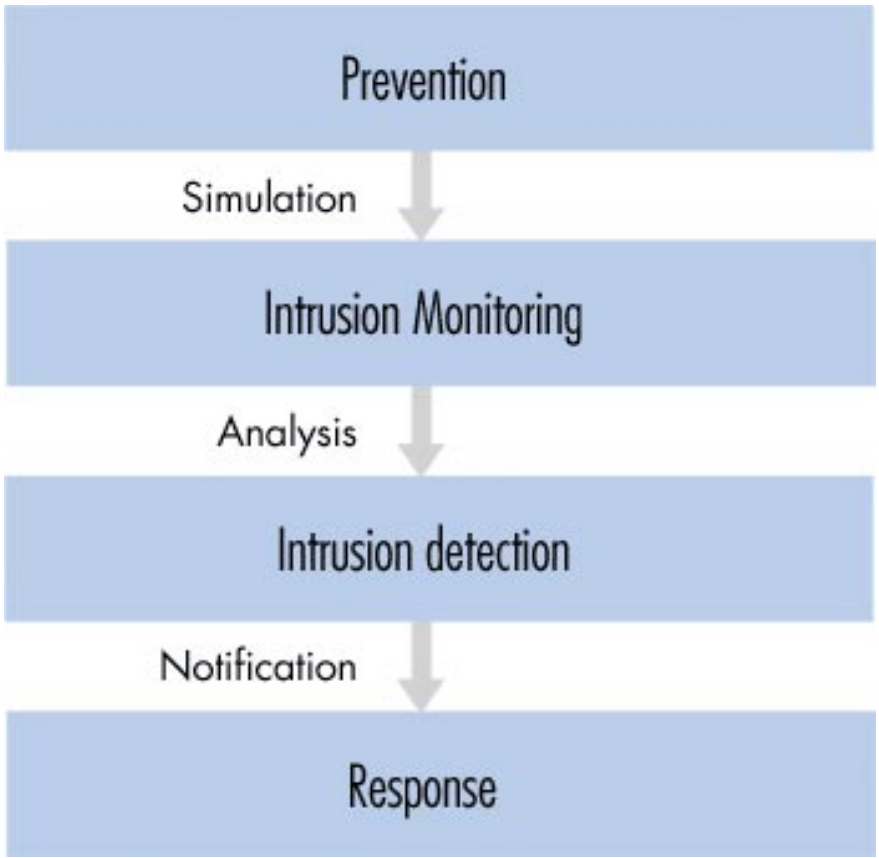

Figure 1: Process of IDS

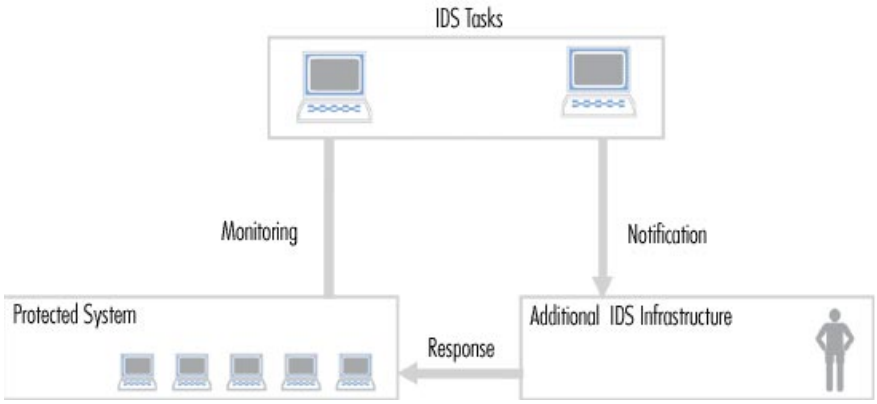

Figure 2: IDS infrastructure

When an intrusion is detected, IDS issues alerts to system administrators about this incident. The next step is done by the administrator or it may be the IDS itself by taking advantage of additional measurement parameters (locking functions to limit sessions, system backups, routing connections to traps system, valid infrastructure, .) - according to the security policies of organizations (Figure 2). An IDS is a component within the security policy.

Between different IDS tasks, identifying intruders is one of the basic tasks. It is also useful in legal research of circumstances and the installation of appropriate patches to allow future attacks to be targeted at specific individuals or system resources.

Intrusion detection can sometimes produce false alarms, such as problems that occur due to network interface problems or the sending of attack descriptions or signatures via email.

Architecture of intrusion detection system

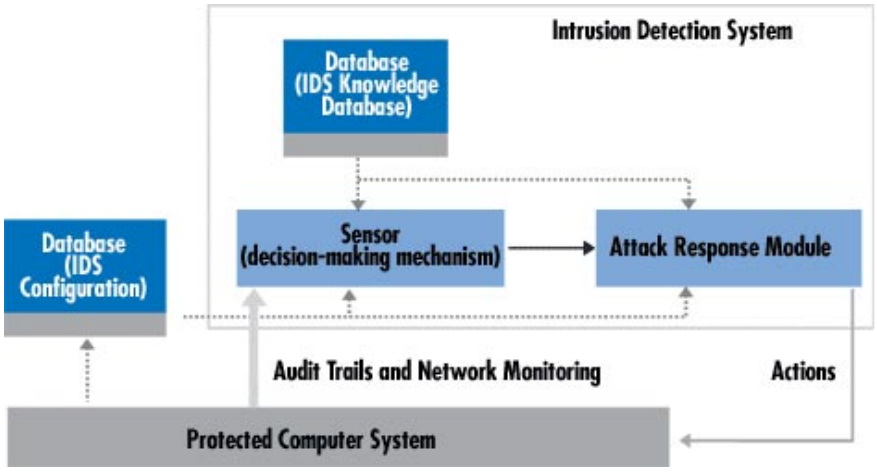

Figure 3: A sample IDS. Narrow width corresponds to the quantity
Information flow between system components

The sensor is integrated with the data collection component (Figure 4) - an event generator. This collection method is determined by the event creation policy to define the event information filtering mode. Event generators (operating systems, networks, applications) provide a number of appropriate policies for events, be it

a record of system events or network packets. This policy number, along with policy information, can be stored in a protected or external system. In some cases, for example, when the event data stream is transmitted directly to the analyzer without any data storage being performed. This also involves a bit of network packets.

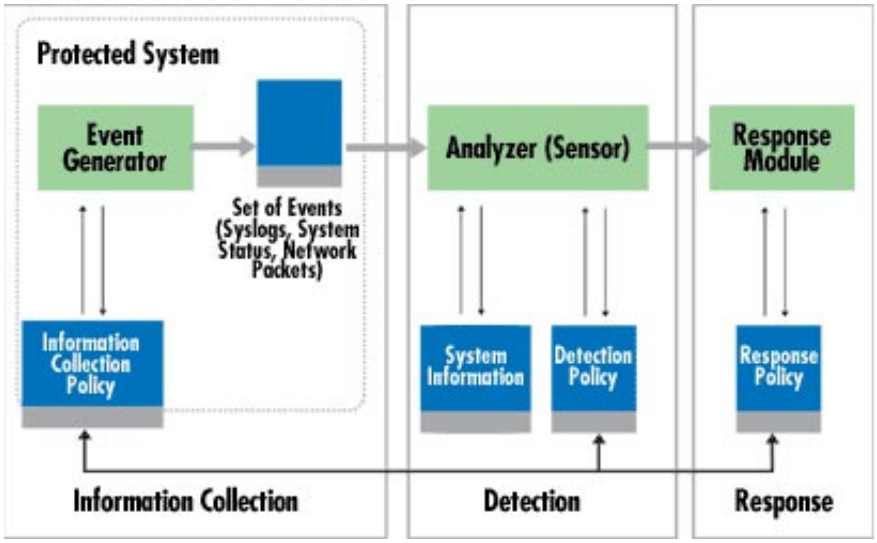

Figure 4: IDS components

The role of the sensor is to filter information and remove incompatible data obtained from events related to the protection system, so suspicious actions can be detected. The parser uses the detection policy database for this item. There are also components: attack signs, normal behavior profiles, necessary parameters (eg thresholds). In addition, the database holds configuration parameters, including communication modes with the response module. The sensor also has its own database, including data stored on potentially complex intrusions (created from various actions).

IDS can be arranged centrally (eg integrated into a firewall) or distributed. A distributed IDS includes many different IDSs on a large network, all of them communicate with each other. Many sophisticated systems follow the single-agent structure principle, where small modules are organized on a host in a protected network.

The role of the agent is to test and filter all actions within the protected area and depending on the method in question - create an initial analysis and even take action in response. The network of collaborating agents reporting to the central analytics server is one of the key components of IDS. DIDS can use more sophisticated analysis tools, especially equipped with detection of distributed attacks. Other actors' roles are related to its mobility and roaming properties in physical locations. In addition, agents can be specifically for detecting certain known attack signs. This is a decisive factor when it comes to protection means related to new types of attacks. IDS-based agent solutions also use less complex mechanisms for responding policy upgrades.

The multi-agent architecture solution introduced in 1994 is AAFID (autonomous agents for intrusion detection) - see Figure 5. It uses agents to examine certain aspects of behaviors. system at a certain time. For example, an actor might indicate an unusual number of telnet sessions within the system it checks. The agent is able to issue a warning when a suspicious event is detected. Agents can be cloned and changed inside other systems (autonomous feature). M?t ph?n trong các tác nhân, h? th?ng có th? có các b? ph?n thu phát ?? ki?m tra t?t c? các hành ??ng ???c ki?m soát b?i các tác nhân ? m?t host c? th? nào ?ó. Các b? thu nh?n luôn luôn g?i các k?t qu ? ho?t ??ng c?a chúng ??n b? ki?m tra duy nh?t. Các b? ki?m tra nh?n thông tin t? các m?ng (không ch? t? m?t

host), ?i?u ?ó có ngh?a là chúng có th? t??ng quan v?i thông tin phân tán. Thêm vào ?ó, m?t s? b? l?c có th? ???c ??a ra ?? ch?n l?c và thu th?p d? li?u.

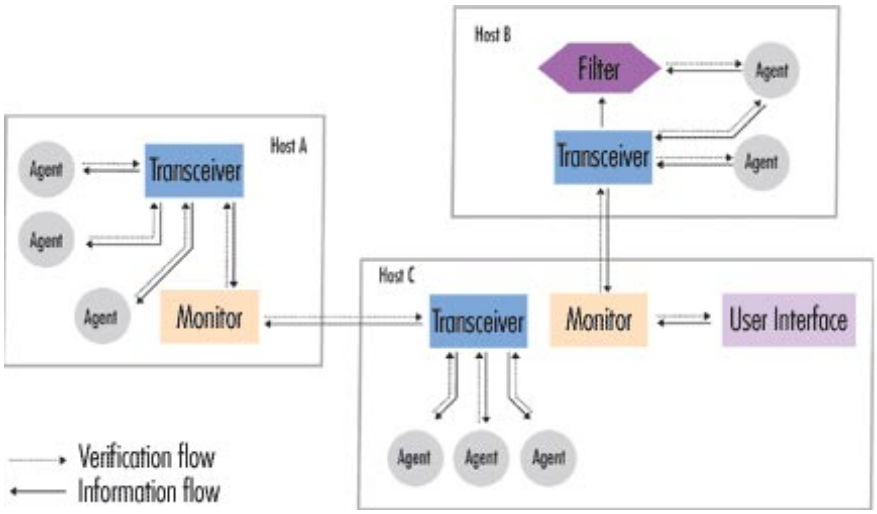

Figure 5

Xem ti?p ph?n II

You finished reading the article "**Intrusion detection system (IDS) (Part 1)**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.