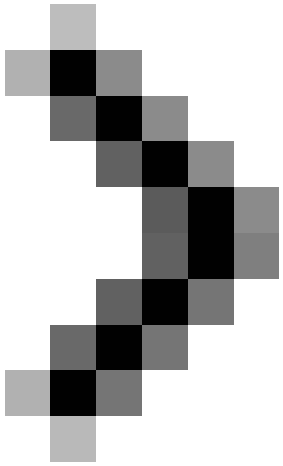
Host-Based IDS and Network-Based IDS (Part 2)

In the second part of this article we will focus on HIDS and the benefits of HIDS within a collaborative environment. Besides we also offer an analysis that helps the ash leaders



Host-Based IDS and Network-Based IDS (Part 1)

In the second part of this article we will focus on HIDS and the benefits of HIDS within a collaborative environment. We also offer an analysis that helps leaders in the IT industry calculate and decide whether HIDS or NIDS solutions are appropriate for their network organization.

What is a HIDS?

HIDS are intrusion detection systems installed on computers (hosts). What makes HIDS different from NIDS is that HIDS can be installed on different types of machines such as servers, workstations or notebooks. This method enables organizations to be flexible while the NIDS is not suitable or beyond its capabilities.

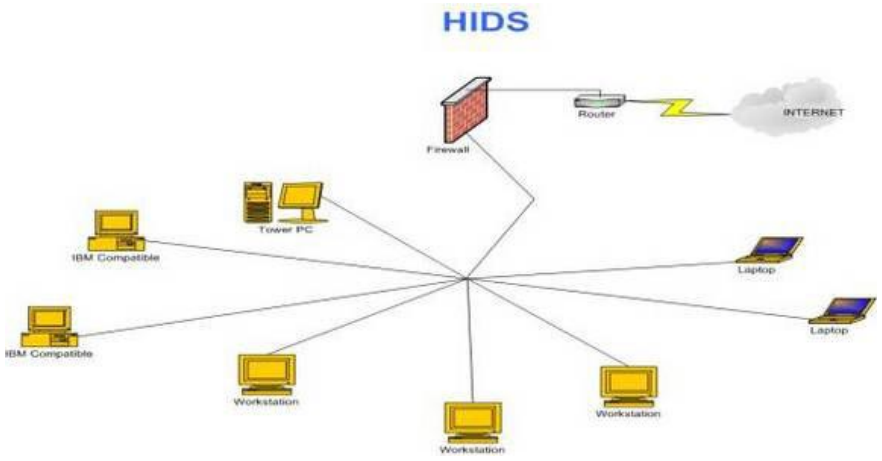
HIDS operations

When the traffic is transmitted to the host they are analyzed and passed through the host if the system does not detect packets carrying malicious code inside. HIDS are often used for local computers, while the NIDS is used for an entire network. HIDS is commonly used for Windows platforms in the computer world, but there are many products that can also work in UNIX environments and other operating systems.

Choose NIDS or HIDS?

Many security experts care about NIDS and HIDS, but how to choose the most suitable for each person's network? The answer here is HIDS for complete solutions and NIDS for LAN solutions. Just like when installing anti-virus software, not only does it install software on the main servers, but it must also be installed on all clients. There is no reason why both NIDS and HIDS are not used together in a strong IDS strategy. NIDS are easily disabled for intruders and we are inclined to this idea. Obviously, installing more detection nodes on your network with secure HIDS is more than just having a NIDS with a few detection nodes for just one network segment. If you are worried about specific computers that can be hacked, use HIDS, which will protect your computer more safely and will be equivalent to installing an alert for you.

IDS supports detailed records, many events are recorded daily, ensuring that only relevant data is selected and you are not flooded with unnecessary data. HIDS records events more closely than NIDS. If you are comparing HIDS or NIDS, make sure you find a company that has good backup techniques and that is the sample file given when there are many new vulnerabilities discovered like antivirus applications. If you have a limited LAN band, you should also consider HIDS.



The diagram shows the HIDS scenario

The following table compares the standard specifications and requirements when selecting an IDS package.

Product

INTRUST Event admin Aelita

ELM 3.0TNTsoftware

GFI LANguard SELM

SnortISS

Cisco Secure IDS

Dragon Enterasys

NIDS / HIDS HIDS HIDS HIDS NIDS NIDS NIDS **Management Interface** *** *** *** *** ** **** **Attack detection** ** *** *** *** *** * *** **Easy to use** *** *** *** ** ** *** **Price for 100 workstations and 5 servers** $ 9400 $ 10,290.00 Price taken from website $ 1620 Price taken from website FREE Package $ 7,929.79 $ 6115.89 **Easy to install and deploy** *** ** *** * ** *** **Security knowledge required (more stars mean less knowledge required)** *** **** **** * * ** **Ability to detect attackers** *** *** *** *** *** *** *** **Secure channel communication** *** * ** - - --- --- **Easy to manage activities** ** *** *** ** *** **** **Product upgrade cycle** ** ** * *** ** **** **SNMP compatibility** *** **** ** ** *** *** **Support report capabilities** **** **** **** *** *** **** **Performance** *** **** **** **** *** *** **Facility suitability h sir floor available** *** *** *** *** *** **** **Suitable ability on Windows background** *** *** *** *** *** *** **Ability to like** *** **on Unix background** *** * * **** *** *** **Backup and support capabilities** *** *** **** *** *** **** **Check log** * ** **** **** *** ** ** **Detect infringement** *** **** **** *** *** *** **Report incident****** **********

Factors

This is the administrator responsibility. Fewer actors mean less stars

**********Result**595762536162

Selection stages IDS

When choosing an IDS, consider some issues in planning for IDS. Here are some considerations that you should care about:

1. Concept phase: This stage you need to distinguish IDS requirements and define what is needed for the business and how IDS can match the needs of the business, the stage This needs to take into account all important resources and provide a security policy.

2. Solution evaluation phase: This stage must be used when selecting products that are appropriate to the needs of the business. IT staff should also use the testing forum to compare IDS software and incorporate the concept phase used as the final test when selecting the most appropriate solution.

3. Implementation and operational phase: This phase is used to implement the selected IDS solution and it must run smoothly if the plan is implemented as appropriate. This is when all problems have to be resolved. The solution must be effective when this phase is completed.

Website and information from firms

IT industry leaders have tested and produced highly competitive results for IDS products. Below are brief product information and links to the Website. More detailed information can be found on their own website.

1. Intrust

This product has many features that help it survive in a business environment. With Unix compatibility, it has a great flexibility. Offer with a reporting interface with more than 1,000 different reports, helping to control complex issues. In addition, it also supports a comprehensive warning solution that allows alerts on mobile devices and many other technologies.

1. Comprehensive alert feature
2. Comprehensive reporting feature
3. Consolidate and verify data performance from across platforms
4. Returning support for network features from client-side recording meticulously
5. Filter the data for easy review
6. Real-time inspection
7. Analyze captured data
8. Compliance with industry standards
9. Mandatory follow a principle

More information

2. ELM

TNT software is a software that supports HIDS functions, which is a comparative analysis based on ELM Enterprise Manager. It supports real-time testing, comprehensive operability and meticulous reporting methods. The database is added to make sure the software database is secure. This means that if the main ELM database is offline, ELM Server will automatically create a temporary database to store the data until the main database is online again. Here are some brief descriptions of ELM Enterprise Manager 3.0

1. ELM supports flexible MMC software module interface
2. Support checking all Microsoft servers. NET by checking event logs and performance counters.
3. Support report wizard with new version can schedule, in addition to support HTML and ASCII reports
4. Observe centralized event logs on multiple servers
5. The client can only activate the Web on a browser that supports JavaScript and XML
6. Support base knowledge interface

7. Support notifications can execute wscripts, cscripts and CMD / BAT files.

8. Support SQL Server and Oracle databases.

9. WMI-compatible queries for comparison purposes

10. Provide corrective action for intrusion detection

More information

3. GFI LANguard SELM

This product has many features and requires only simple knowledge for installation. Here are brief information about GFI LANguard SELM

1. Automated and extensive security analysis throughout the network for event logs

2. Manage network event logs

3. Detecting enhanced attacks inside

4. Reduce TOC

5. No client software or agents needed

6. Does not affect network traffic

7. Easy to improve, suitable for business networks or small networks

8. Secret file checker

9. Check the comprehensive record

10. Detect an attack if the local user account is used (online or offline)

More information

4. Snort

Snort is a great product and it won when put into operation in the UNIX environment. The latest product launched recently supported Windows platform but there are still some subtle selections. The best thing that comes with this product is open source and costs nothing except the time and bandwidth needed to download it. This solution has been developed by many people and it works very well on inexpensive hardware, which makes it possible to exist in any organization.

Here are brief information about this product:

1. Support high-performance configuration in software

2. Good support for UNIX

3. Support flexible open source

4. Good SNMP support

5. Support centralized management module

6. Support warning and intrusion detection

7. There are record packs

8. Comprehensive attack detection

9. Sophisticated output modules provide comprehensive recording capability

10. Support users on mailing lists and via email interaction

More information

5. Cisco IDS

This solution is Cisco's, with this solution you see the quality, feel as well as its traditional reputation.

Here are brief information about this device:

1. Accurate detection features significantly reduce false alarms.

2. The ability to upgrade business operations like Cisco products

3. The system detects real-time intrusion, reports and blocks unauthorized actions

4. The analysis of samples used for detection is done at many different levels

5. For high network performance

6. Manage dynamic routing access lists that are timely adapted to intruder behavior

7. Centralized GUI management

8. Remote management

9. Email event notification

More information

6. Dragon

A comprehensive solution for business operations. This product is very versatile and has the necessary security requirements in a business environment. It also supports NIDS, server management, event management, attack testing. This is a complete IDS release, perfectly designed with integrated testing. However, the weakness of this product is that its price.

Here are brief information about Dragon (Business activity version).

1. Dragon supports both NIDS and HIDS
2. Support on a variety of Windows, Linux, Solaris and AIX platforms
3. Modified and expandable
4. Check centralized management
5. Comprehensive analysis and reporting
6. High compatibility with technical details in business operations
7. Effective security check, integrated switches, firewalls and routers.
8. Compile management reports
9. There is a perfect technical update cycle

More information

Conclude

When making conclusions about these products, there are clearly two main competitors in the IT sector: Enterasys Dragon NIDS and LANguard SELM of GFI Software. Both products are highly valued in the market with its online capabilities and support. When reviewing and evaluating software we need to come up with tests, both products here have no problems and have a harmonious integration with the Windows network infrastructure. That clearly shows why these products are highly rated in the IT sector. However, other products are not too weak compared to the two products and they can catch up with those two products in the near future.