Overview

Network based intrusion detection systems are systems that monitor the network for packets and detect malicious behaviour and take actions or responses to prevent an attack.

Host based Desktop Security suites are typically software running on host machines that are responsible for host protection. They perform packet filtering on host machines(typically host based firewalls) and detect malicious activities on the host.

The basic similarities between these two systems lies in the fact that both the systems detect malicious code and activities and provide a response scheme

However The network based system has the network interfaces where it monitors for malicious activities while the host based security suites are monitoring the hosts.

Similarities and differences

1)Rulesets

• Signature based rules for an network based IDS

A network based IDS has basically 2 rule sets viz. signature based and anomalies based. The signature based rule set consists of a knowledge base where all the known signatures are stored. These signatures are matched with any malicious signature the Intrusion detection system detects.

There are typically 3 types of signature rules the IDS checks for

1)String based Signatures

These are typical signatures in the payload of the packet which match the signatures in the database. These are simple string compare operations with known strings that are identified as malicious

2)Port based Signatures

Port based signatures involves scanning of the packet to determine the port field. There are few ports identified as not used or temporarily down for the system. If the packet consist of such a port it signifies that an adversary is trying to ping a port that is currently not in use. Such a packet may be of a packet sent to scan ports on the network for the machine.

3)header condition signatures

Header based signatures scan for header fields which will cause the system to behave abnormally. For instance setting of both syn and fin flags in the TCP header. It may be also used along with deep packet inspection to determine if the packet is actually the packet that it claims to be. For instance an adversary may modify header fields for the packet to look like http response to get it pass firewalls and may embed malicious data in the packet .

• Signature based rules for Host based Desktop security Suites

These types of security suites also have signature based inspections. They are similar to the network based intrusion signature system . They have a knowledge base similar to that of network based IDS and signatures are compared with this knowledge base. The only difference being the methods applied to detect signatures.

The signature based methods in the host based security suites are

1) Byte signatures

These are signatures based on sequence of bytes. If a code with similar sequence of bytes is detected then the security suite detects it.

2)Binary diffing

This is the process of comparing multiple executable files in an antivirus suite

3)Hash values

This is the process of comparing the hash of the code with standard hash values stored in database identified as malicious

4)Heuristic based approach

Since viruses change dynamically and avoid detection in all possible ways heuristic rules are applied to estimate whether a given piece of code is malicious or safe.

• Anomaly based rules approaches in network IDS

Anomaly based approach is a very important network intrusion based detection methodology which detects some abnormal behaviour and reports it. This approach has specific rule sets like 'if the outbound packet rate suddenly increases report the intrusion'. This approach however may generate false positives. Contrasting to anomaly based in network IDS we have activity based approach in host based tied antivirus suites

• Activity Based rules in Host based security suites

Activity based rule sets are very important host based rule sets where a security suite detects malicious activity on a host, based on the nature of that activity. For instance if a program tries to write to the boot sector of the disk it is killed or a file tries to write to system files it is terminated.

Firewalls or packet filter rules(iptables) are used to filter packets which host may not want to receive or send out.

2)Sources of event information

• Network based IDS

1)Network log files

2)knowledge base about existing signatures

3)Passive monitoring or honeypots(logging information of what attacker does in a protective environment without the attacker knowing it)

4)Packets log

• Host based Security Suites

1)System log files like syslog on unix

2)log files depicting which and what files were accessed at a given time

3)O.S audits

4)Knowledge based signature repositories

5)tripwires(checksums of files indicating which file has changed or modified)

3) Attacks for which Network Based IDS is more suited

Network based IDS is suited for network based attacks before the intruder has not gained control of the hosts the IDS protects. A network based IDS may not be tied to a host machine and a compromise of the host does not compromise the network based IDS system. This is a very nice advantage provided

The network IDS is more suited for following attacks

1)port scanning attacks

2)Denial of service attacks(DOS)

3)malicious attacks on well known ports

4)IP spoofing attacks

5)worms flooding the network

6)Attacks of encapsulating data in false headers(identified by deep packet inspections)

All these attacks are attacks where the attacker is trying to gain access to the host from a network and the host is not yet compromised. Such attacks can be successfully thwarted by network based IDS since they sniff packets over network and then report any unusual behaviour.

For instance a network based IDS can easily detect flooding of packets(packets trying to flood network and cause denial of service). Such attacks cannot be detected by host based security suites like anti viruses. They can also get information of other attacks in the network and log them so as to protect their other hosts which they are connected to.

A network based IDS may protect many hosts and this may cause a management issue. An attack is closely tied to operating system and architecture of a host. The network based IDS has to keep track of all these systems architecture to provide protection. Thus although it guards against variety of attacks its management is a difficult problem

Attacks for which host based security suites is more suited

Host based security suites are more tied to the applications architecture and are easy to manage . They are efficient against following attacks

1)attacks through malicious encrypted packets(network based IDS does not provide defence against such attacks since they cannot deep packet inspect encrypted data. Data is decrypted at the host and hence host based systems are effective against this attack) .

2)privilege escalation attack where a user tries to increase his privilege on the system

3)Trojan horses , viruses and worms attached to applications

4)attack on Operating systems like trying to overflow the buffer or trying to write to system files

4)Response functions

Response functions for a network based IDS is as follows

• Notify administrator after the attack

• System Lockdown(prefer partial lockdown to avoid customers from not getting services)

• Place attacker in controlled environments

• slow the system for offending processes

• kill the process

• isolate affected node

• create backups and restore from backups lost data

• block the ip through which malicious content was received

• shutdown attacked ports

Response functions for a host based security suites are

• Notify host admin

• restore systems using system logs

• restore files using tripwires

• create backups and restore files using backups

• quarantine malicious process

• set system restore points and backup from those points.

Thus typically network based responses mostly try to manipulate the network by detecting affected nodes in network and taking action against them(like shutting them down) while host based security suites try to recover the host from a failure to a safe state where it can operate. the response of a host based security does not affect any other nodes except the host however the response of a network based IDS may affect multiple nodes and resulting traffic on the network.