

White paper on Intrusion Detection and Intrusion Prevention

Introduction

The Internet is a medium for fast, efficient communication and interchange of ideas, and an unbounded marketplace for corporations, customers and suppliers to conduct business. However, the limitless opportunities of the Internet come hand-in-hand with the risks of people who take malicious advantage of the openness of the Internet. Enterprise networked systems are inevitably exposed to the increasing threats posed by hackers as well as malicious users internal to a network. The consequences are compromised confidentiality and integrity of business systems, and diminished availability of the network.

To counter these threats, organizations use tools and technology to secure their systems, through deployment of firewall and authentication systems, and by defining security policies and access control mechanisms. But with security breaches on the rise, and their associated high costs to businesses, enterprises are increasingly looking at tools that detect network security breaches and alert network administrators of intrusion attempts. Intrusion Detection systems (IDS) fall in this category of security tools.

Who are “Intruders”?

The common term for an intruder is a “hacker” or programmer who tries to break in and enter a computer system with malicious intent. Another category of intruders includes persons within a system misusing privileges to gain access to information and systems they are unauthorized to use.

Steps in Intrusion Attacks

Intrusion attacks usually follow a logical sequence of events. The intruder will at first try to discover as much public information (such as domain name, DNS tables, machine names, and FTP sites) about a network as possible without risking detection.

Next, the intruder will attempt to scan for more information, run utilities, look for CGI scripts, ping to get machine status, etc. By the end of this stage, the intruder will know the operating system and applications running on the victim’s network.

Once an intruder gets access to a user account or a machine, he/she tries to exploit possible vulnerabilities of the system by sending commands to CGI scripts, or malicious data to buffer-overflow holes. At this stage, the hacker may be able to gain control of the machine, and even crash the system. On gaining a foothold on a network, the intruder will cover tracks of the attack to delay discovery and install tools that displace the normal functioning of the system or vandalize the site, before moving to other connected networks.

Detection is possible through IDS right from the time the intruder probes and tries to scan for information. IDS successfully detect and trap attacks at a premature stage and help enterprises avoid disruption in their systems and costs associated with the likely damage of successful attempts.

How is Intrusion Detected?

An Intrusion is a deliberate unauthorized attempt to access information, manipulate information, and/or commit acts to render a system unreliable or unusable.

There are several types of intrusions - common intrusion types are reconnaissance, exploits and DoS. Reconnaissance includes ping sweeps, DNS zone transfers, email reconnaissance, TCP/UDP scans, and indexing of public web servers for CGI holes. Exploits include taking advantage of software features and bugs to gain unauthorized access to the system, send large amounts of data to known buffer-overflow holes, checking login accounts by guessing passwords, spoofing packets to cause multiple replies to a host from a single packet, and so on. Denial-of-service (DoS) attacks are vandal attacks with intentions to disrupt the services in a system. These are usually by crashing services, or overloading the CPU or network links, or filling a disk to capacity.

Intrusion detection is performed through two main checks – Anomaly Detection, and Signature Recognition.

Checking Signature Rules

This is an exercise where the IDS looks for a “signature” or pattern. IDS contain databases with strings based on patterns for known hacker techniques. IDS examine the network traffic, looking for well-known patterns of attack.

Detecting Anomalies

This is by identifying statistical anomalies with reference to a baseline of statistics on activities like CPU utilization, user logins, file activity, disk activity, and so on. When there is an abnormal or unusually high or low value from the baseline, the IDS is able to detect it.

Types of Intrusion Detection Systems

Intrusion Detection Systems can be categorized based on several criteria –deployment, scope and data processing.

By Deployment

Inline IDS

Inline IDS are placed in the line of packet transfer. IDS checks all packets passing through it for intrusions and if detected, alerts the network administrator. In addition, it can block the intrusion from going any further. Typically, IIDS are placed at the perimeter of the network, behind the firewall or along with the firewall.

Sniffer IDS

These are IDS that snoop and examine packets within a network. Sniffer IDS do not come in the way of packet transfer. Instead, they passively receive all the packets from the network and

perform intrusion analysis on these packets. Typically, sniffers are placed in a location on the network where they can read all the packets flowing through the network.

By Scope

Network Intrusion Detection Systems (NIDS)

Network Intrusion Detection Systems are deployed on a network segment to compare captured network data with a file of known malicious signatures. A network IDS uses network cards that sniff at all packets in a network segment. A typical network IDS has one or more sensors, and a console to aggregate and analyze data from the sensors.

Host-Based IDS (HIDS)

Host-based IDS are deployed on a host computer, and watch processes inside the host. The HIDS operates by monitoring changes to a number of variables on the host system. This includes system processes, Registry entries, CPU usage, file access and integrity checks. Suspicious threshold values or file changes result in the IDS sending an alert. A system integrity verifier looks for evidence of changes to key files. If there is a match, the HIDS logs and send an alert to the network or security administrator.

Hybrid IDS

A hybrid IDS is a combination of a host IDS with a network IDS. The implementation varies from instance to instance and could range from IDS placed at critical network aggregation and entry points and on hosts used for conducting business-critical functions

By Data Processing

Raw Analysis Systems

These perform signature analysis where the IDS capture frames of data from the network and compares them to strings from a database of attack signatures, looking for a match. The IDS only scans the raw data for patterns, and does not perform any processing on the data. Their limited scope makes them ideal candidates for deployment in network segments with low bandwidth utilization. Intelligent Systems

These systems not only capture the raw frames of data, but also are able to understand the protocols and rules governing their operation, and thus emulate the host and applications, based on the protocol traffic. Used for detecting complex attacks, Intelligent Systems perform considerable data processing and scale to meet the demands of network segments with high bandwidth utilization.

IPS

General Description

The IPS solution from Embedded SecuraNET enables networking equipment manufactures to add enterprise-class IPS capability to their security products. It represents the next generation in intrusion prevention systems and is based on its unique patent-pending application-aware Inline IPS technology. It provides greater intrusion detection accuracy for reduced false alarms and higher performance than traditional IDS and IPS approaches IPS sensors are located at the perimeter of a network, securing the network against intruder activities originating from within and outside the network. Inline IPS is a network IDS operating to detect, and sometimes protect, the vulnerabilities in traffic coming from external networks. Similarly, vulnerabilities internal to the

network are detected and trapped when the data passes through the network to external networks. For implementations where there are several sub-networks comprising an enterprise network, the firewall and IDS can be located at the perimeter of the enterprise network, making it effective for detecting intrusion for all networks, without compromising performance.

Detecting Reconnaissance Probes

Inline IPS can detect and mislead intruders conducting reconnaissance probes such as port scans, OS fingerprinting probes, and ICMP probes right at the network. When a reconnaissance probe is detected, Inline IPS drops the packets in the session, thereby stopping the attacker from finding out the TCP/IP and OS vendors and versions. Next, Inline IPS informs the firewall to stop the traffic from/to a specified source IP/destination IP and service for a certain period of time. This misleads the intruder into believing the service is not available, and the network is successfully protected from getting any further packets sent by the intruder. Logging & Alerts Currently, Inline IPS uses syslog or email to inform administrators of detected attacks.

Advantages over other IDS products

Stateful Inspection

Most IDS perform signature comparisons on all packets from all applications. This is because there is no classification at the application level for signature comparison. SecuraNET Inline IPS reduces processing time by keeping track of the state of the application instance, and performing signature comparison only on relevant packets. It eliminates the need to check all application signature rules against all packets, thereby accelerating performance.

Inline Intrusion Prevention

The most significant advantage that SecuraNET Inline IPS has over its competitors is in being inline with its firewall. Today, NIDS systems are integrated with general-purpose firewalls. When they detect an attack, NIDS systems inform the firewall to block the traffic. And since NIDS and the firewall are in two different systems, the current packet, which caused the detection, can't be stopped. Inline IPS is inline with the firewall. Hence, as soon as an attack is detected, it drops the malicious packet before it reaches the target machine/network.

Since Inline IPS is inline with the packet flow, attacks originating from within a network to a destination outside the network can also be effectively intercepted and trapped.

Conclusion

Intrusions are attempted break-ins in violation of defined security policies in a system. They can also be masquerade attacks or impersonations of valid users, but with detectable atypical behavior profiles. Intrusions are usually engineered by penetration of the security control system after deliberate probes and scans to study specific patterns of activity. This is followed by acts that disrupt the regular functioning of the system and its resources. Intrusion Detection is mainly through two methods – anomaly detection and signature recognition. Increased connectivity and business opportunities over the Internet also expose greater risks of subversion and endanger the information assets of enterprises. In this context, the use of Intrusion Detecting Systems on networks assumes enormous importance. IDS detect and prevent attacks from malicious intruders

on a network, and alert administrators of the attack. However, IDS detect rather than react to attacks.

