Understanding Intrusion Detection Systems

PETER MELL

Intrusion detection is the process of detecting an unauthorized use of, or attack upon, a computer or a telecommunication network. Intrusion detection systems (IDSs) are designed and installed to aid in deterring or mitigating the damage that can be caused by hacking, or breaking into sensitive IT systems. IDSs are software or hardware mechanisms that detect such misuse. IDSs can detect attempts to compromise the confidentiality, integrity, and availability of a computer or network. The attacks can come from outsider attackers on the Internet, authorized insiders who misuse the privileges that have been given them, and unauthorized insiders who attempt to gain unauthorized privileges. IDSs cannot be used in isolation, but must be part of a larger framework of IT security measures.

The Basis for Acquiring IDSs

At least three reasons justify the acquisition of an IDS. The three are:

1. To provide the means for detecting attacks and other security violations that cannot be prevented
2. To prevent attackers from probing a network
3. To document the intrusion threat to an organization

Detecting Attacks That Cannot Be Prevented

Using well-known techniques, attackers can penetrate many networks. Often, this happens when known vulnerabilities in the network cannot be fixed. For example, in many legacy systems, the operating systems cannot be updated; and in those systems that can be updated, the administrators may not have, or take, the time to install all the necessary patches in a large number of hosts. In addition, it is usually impossible to map perfectly an organization’s computer use policy to its access control mechanisms. Authorized users can often perform unauthorized actions. In addition, users may demand network services and protocols that are known to be flawed and subject to attack. Although ideally it would be preferable to fix all of the vulnerabilities, seldom is this possible.
Thus, an excellent approach to protecting a network may be the use of an IDS to detect when an attacker has penetrated a system using the vulnerability that can be created by an uncorrectable flaw. At least it is better to know that a system has been penetrated so that its administrators can perform damage control and recovery than not to know that the system has been penetrated.

**Preventing Attackers from Probing a Network**

A computer or network without an IDS may allow attackers to explore its weaknesses, leisurely and without retribution. If a single, known vulnerability exists in such a network, a determined attacker will eventually find and exploit it. The same network in which an IDS has been installed is a much more formidable challenge to an attacker. Although the attacker may continue to probe the network for weaknesses, the IDS should detect these attempts. In addition, the IDS can block these attempts and it can alert IT security personnel who can then take appropriate action in response to the probes.

**Documenting the Threat**

It is important to verify that a network is under attack or is likely to be attacked in order to justify spending money for securing the network. Furthermore, it is important to understand the frequency and characteristics of attacks to understand what security measures are appropriate for the network. IDSs can itemize, characterize, and verify the threats from both outside and inside attacks. Thus, the operation of IDSs can provide a sound foundation for IT security expenditures. Using IDSs in this manner is important because many people believe — and mistakenly so — that no one would be interested in breaking into their networks. (Typically, this type of mistaken thinking makes no distinction between threats from either outsiders or insiders.)

**EDPACS NOVEMBER 2001**
TYPES OF IDSs

There are several types of IDSs available. They are characterized by different monitoring and analysis approaches. Each type has distinct uses, advantages, and disadvantages. IDSs can monitor events at three different levels: network, host, and application. They can analyze these events using two techniques: signature detection and anomaly detection. Some IDSs have the ability to respond automatically to attacks that are detected.

IDS MONITORING APPROACHES

One way to define the types of IDSs is to look at what they monitor. Some IDSs listen on network backbones and analyze network packets to find attackers. Other IDSs reside on the hosts that they are defending and monitor the operating system for signs of intrusion. Still others monitor individual applications.

Network-Based IDSs

Network-based IDSs are the most common type of commercial product offering. These mechanisms detect attacks by capturing and analyzing network packets. Listening on a network backbone, a single network-based IDS can monitor a large amount of information. Network-based IDSs usually consist of a set of single-purpose hosts that “sniff” or capture network traffic in various parts of a network and report attacks to a single management console. Because no other applications run on the hosts that are used by a network-based IDS, they can be secured against attack. Many of them have “stealth” modes, which make it extremely difficult for an attacker to detect their presence and to locate them.

Advantages. A few well-placed network-based IDSs can monitor a large network. The deployment of network-based IDSs has little impact on the performance of an existing network. Network-based IDSs are typically passive devices that listen on a network wire without interfering with normal network operation. Thus, usually, it is easy to retrofit a network to include network-based IDSs with a minimal installation effort. Network-based IDSs can be made very secure against attack and can even be made invisible to many attackers.

Disadvantages. Network-based IDSs may have difficulty processing all packets in a large or busy network. Therefore, such mechanisms may fail to recognize an attack that is launched during periods of high traffic. IDSs that are completely implemented in hardware are much faster than those that have been totally realized in software. In addition, the need to analyze packets quickly forces vendors to try and detect attacks with as few computing resources as possible. This may reduce detection effectiveness.
Many of the advantages of network-based IDSs do not always apply to the more modern switch-based networks. Switches can subdivide networks into many small segments; this will usually be implemented with one fast Ethernet wire per host. Switches can provide dedicated links between hosts that are serviced by the same switch. Most switches do not provide universal monitoring ports. This reduces the monitoring range of a network-based IDS sensor to a single host. In switches that do provide such monitoring ports, the single port is frequently unable to mirror all the traffic that is moving through the switch.

Network-based IDSs cannot analyze encrypted information. Increasingly, this limitation will become a problem as the use of encryption, both by organizations and by the attackers, increases. Most network-based IDSs do not report whether or not an attack was successful. These mechanisms only report that an attack was initiated. After an attack has been detected, administrators must manually investigate each host that has been attacked to determine which hosts were penetrated.

**Host-Based IDSs**

Host-based IDSs analyze the activity on a particular computer. Thus, they must collect information from the host they are monitoring. This allows an IDS to analyze activities on the host at a very fine granularity and to determine exactly which processes and users are performing malicious activities on the operating system. Some host-based IDSs simplify the administration of a set of hosts by having the administration functions and attack reports centralized at a single IT security console. Others generate messages that are compatible with network administration systems.

- **Advantages.** Host-based IDSs can detect attacks that are not detectable by a network-based IDS because this type has a view of events that are local to a host. Host-based IDSs can operate in a network that is using encryption when the encrypted information is decrypted on (or before) reaching the host that is being monitored. Host-based IDSs can operate in switched networks.

- **Disadvantages.** The collection mechanisms must usually be installed and maintained on every host that is to be monitored. Because portions of these systems reside on the host that is being attacked, host-based IDSs may be attacked and disabled by a clever attacker. Host-based IDSs are not well-suited for detecting network scans of all the hosts in a network because the IDS at each host sees only the network packets that the host receives. Host-based IDSs frequently have difficulty detecting and operating in the face of denial-of-service attacks. Host-based IDSs use the computing resources of the hosts they are monitoring.
Application-Based IDSs

Application-based IDSs monitor the events that are transpiring within an application. They often detect attacks by analyzing the application’s log files. By interfacing with an application directly and having significant domain or application knowledge, application-based IDSs are more likely to have a more discerning or fine-grained view of suspicious activity in the application.

- **Advantages.** Application-based IDSs can monitor activity at a very fine granularity, which allows them, often, to track unauthorized activity to individual users. Application-based IDSs can work in encrypted environments, because they interface with the application that may be performing encryption.

- **Disadvantages.** Application-based IDSs may be more vulnerable than host-based IDSs to being attacked and disabled because they run as an application on the host that they are monitoring.

The distinction between an application-based IDS and a host-based IDS is not always clear. Thus, for the remainder of this article, both types will be referred to as host-based IDSs.

**IDS EVENT ANALYSIS APPROACHES**

There are two primary approaches to analyzing computer and networks events to detect attacks: signature detection and anomaly detection. Signature detection is the primary technique used by most commercial IDS products. However, anomaly detection is the subject of much research and is used in limited form by a number of IDSs.

**Signature-Based IDSs**

Signature-based detection looks for activity that matches a pre-defined set of events that uniquely describe a known attack. Signature-based IDSs must be specifically programmed to detect each known attack. This technique is extremely effective and is the primary method used in commercial products for detecting attacks.

- **Advantages.** Signature-based IDSs are very effective in detecting attacks without generating an overwhelming number of false alarms.

- **Disadvantages.** Signature-based IDSs must be programmed to detect each attack and thus must be constantly updated with the signatures of new attacks. Many signature-based IDSs have narrowly defined signatures that prevent them from detecting variants of common attacks.

**Anomaly-Based IDSs**

Anomaly-based IDSs find attacks by identifying unusual behavior (i.e., anomalies) that occurs on a host or network. They
function on the observation that some attackers behave differently than “normal” users and thus can be detected by systems that identify these differences. Anomaly-based IDSs establish a baseline of normal behavior by profiling particular users or network connections and then statistically measure when the activity being monitored deviates from the norm. These IDSs frequently produce a large number of false alarms because normal user and network behaviors can vary widely. Despite this weakness, the researchers working on applying this technology assert that anomaly-based IDSs are able to detect never-before-seen attacks, unlike signature-based IDSs that rely on an analysis of past attacks. Although some commercial IDSs include restricted forms of anomaly detection, few, if any, rely solely on this technology. However, research on anomaly detection IDS products continues.

Advantages. Anomaly-based IDSs detect unusual behavior and thus have the ability to detect attacks without having to be specifically programmed to detect them.

Disadvantages. Anomaly detection approaches typically produce a large number of false alarms due to the unpredictable nature of computing and telecommunication users and networks. Anomaly detection approaches frequently require extensive “training sets” of system event records to characterize normal behavior patterns.

IDSs THAT AUTOMATICALLY RESPOND TO ATTACKS

Because human administrators are not always available when an attack occurs, some IDSs can be configured to automatically respond to attacks. The simplest form of automated response is active notification. Upon detecting an attack, an IDS can e-mail or page an administrator. A more active response is to stop an attack in progress and then block future access by the attacker. Typically, IDSs do not have the ability to block a particular person, but instead block the Internet Protocol (IP) addresses from which an attacker is operating. It is very difficult to automatically stop a determined and knowledgeable attacker. However, IDSs can often deter expert attackers or stop novice hackers by:

- Cutting TCP (Terminal Control Protocol) connections by injecting reset packets into the attacker’s connections that go to the target of the attack
- Reconfiguring routers and firewalls to block packets from reaching the attacker’s location (i.e., the IP address or site)
- Reconfiguring routers and firewalls to block the protocols that are being used by an attacker
- Reconfiguring routers and firewalls to sever all the connections, in extreme situations, that are using particular network interfaces

A more aggressive way in which to respond to an attacker is to launch attacks against, or attempt to gain information actively about, the attacker’s host or site. However, this type of response can prove extremely dangerous for an organization to...
undertake because doing so may be illegal or may cause damage to innocent Internet users. It is even more dangerous to allow IDSs to launch these attacks automatically, but limited, automated “strike-back” strategies are sometimes used for critical systems. (It would be wise to obtain legal advice before pursuing any of these options.)

TOOLS THAT COMPLEMENT IDSs

Several tools exist that complement IDSs and are often labeled as IDSs by vendors because they perform functions that are similar to those accomplished by IDSs. These complementary tools are honey pot systems, padded cell systems, and vulnerability assessment tools. It is important to understand how these products differ from conventional IDSs.

Honey Pot and Padded Cell Systems

Honey pots are decoy systems that attempt to lure an attacker away from critical systems. These systems are filled with information that is seemingly valuable but which has been fabricated and which would not be accessed by an honest user. Thus, when access to the honey pot is detected, there is a high likelihood that it is an attacker. Monitors and event loggers on the honey pot detect these unauthorized accesses and collect information about an attacker’s activities. The purpose of the honey pot is to divert an attacker from accessing critical systems, collect information about the attacker’s activity, and encourage the attacker to stay on the system long enough for administrators to respond to the intrusion.

Padded cells take a different approach. Instead of trying to attract attackers with tempting data, a padded cell waits for a traditional IDS to detect an attacker. The attacker is seamlessly transferred to a special padded cell host. The attacker may not realize anything has happened, but is now in a simulated environment where no harm can be caused. Similar to the honey pot, this simulated environment can be filled with interesting data to convince an attacker that the attack is going according to plan. Padded cells offer unique opportunities to monitor the actions of an attacker. IDS researchers have used padded cell and honey pot systems since the late 1980s, but until recently no commercial products have been available.

- **Advantages.** Attackers can be diverted to system targets that they cannot damage. Administrators can be given time to decide how to respond to an attacker. An attacker’s actions can be monitored more easily and the results used to improve the system’s protections. Honey pots may be effective in catching insiders who are snooping around a network.

- **Disadvantages.** Honey pots and padded cells have not been shown, as yet, to be widely useful security technologies. Once an expert attacker has been diverted into a decoy system, the invader may become angry and launch a more hostile attack against an organization’s systems. A
high level of expertise is needed for administrators and security managers to use these systems. The legal implications of using such mechanisms are not well-defined.

**Vulnerability Assessment Tools**

Vulnerability assessment tools determine when a network or host is vulnerable to known attacks. Because this activity is actually related to detecting attacks, these mechanisms are sometimes referred to as intrusion detection tools. They come in two varieties: passive and active.

- Passive vulnerability assessment tools scan the host on which they reside for the presence of insecure configurations, software versions known to contain exploitable flaws, and weak passwords.
- Active assessment tools reside on a single host and scan a network looking for vulnerable hosts. The tool sends a variety of network packets at target hosts and, from the responses, the tool can determine the server and operating system software on each host. In addition, it can identify specific versions of software and determine the presence or absence of security-related patches. The active assessment tool compares this information with a library of software version numbers known to be insecure and determines if the hosts are vulnerable to known attacks from these sources.

**LIMITATIONS OF IDSs**

Intrusion detection products have limitations that one must be aware of before endeavoring to deploy an IDS. Despite vendor claims to the contrary, most IDSs do not scale well as enterprisewide solutions. The problems include the lack of sufficient integration with other IT security tools and sophisticated network administration systems, the inability of IDSs to assess and visualize enterprise-level threats, and the inability of organizations to investigate the large number of alarms that can be generated by hundreds or thousands of IDS sensors.

- 1. Many IDSs create a large number of false positives that waste administrators’ time and may even initiate damaging automated responses.
- 2. While almost all IDSs are marketed as real-time systems, during heavy network or host activity, an IDS may take several minutes before it reports and responds to an attack automatically. Usually, IDSs cannot detect newly published attacks or variants of existing attacks. This can be a serious problem as 30 to 40 new attacks are posted on the World Wide Web every month. An attacker may wait for a new attack to be posted and then quickly penetrate a target network.
- 3. Automated responses of IDSs are often ineffective against sophisticated attackers. These responses usually stop novice hackers but if they are improperly configured,
these reactions can harm a network by interrupting its legitimate traffic.

4. IDSs must be monitored by skilled IT security personnel to achieve maximum benefits from their operation and to understand the significance of what is detected. IDS maintenance and monitoring can require a substantial amount of personnel resources.

5. Many IDSs are not failsafe. They are not well-protected from attack or subversion.

6. Many IDSs do not have interfaces that allow users to discover cooperative or coordinated attacks.

DEPLOYMENT OF IDSs

Intrusion detection technology is a necessary addition to every large organization's IT security framework. However, given the weaknesses that are found in some of these products, and the relatively limited security skill level of most system administrators, careful planning, preparation, prototyping, testing, and specialized training are critical steps for an effective IDS deployment.

It is suggested that a thorough requirements analysis be performed before IDSs are deployed. The intrusion detection strategy and solution selected should be compatible with the organization's network infrastructure, policies, and resource level.

Organizations should consider a staged deployment of IDSs to gain experience with their operation. Thus, they can ascertain how many monitoring and maintenance resources are required. There is a large variance in the resource requirements for each type of IDS. IDSs require significant preparation and ongoing human interaction. Organizations must have appropriate IT security policies, plans, and procedures in place so that the personnel involved will know how to react to the many and varied alarms that the IDSs will produce.

A combination of network-based IDSs and host-based IDSs should be considered to protect an enterprise-wide network. First deploy network-based IDSs because they are usually the simplest to install and maintain. The next step should be to defend the critical servers with host-based IDSs.

Honey pots should be used judiciously and only by organizations with a highly skilled technical staff willing to experiment with leading-edge technology. Currently, padded cells are available only as research prototypes.

Deploying Network-Based IDSs

There are many options for placing a network-based IDS and there are different advantages for each location. See Exhibit 1 for a listing of these options.

Deploying Host-Based IDSs

Once an organization has deployed network-based IDSs, the deployment of host-based IDSs can offer an additional level of protection. However, it can be time-consuming to install host-based IDSs on every host in an enterprise. Therefore, it is often
preferable to begin by installing host-based IDSs on critical servers only. This placement will decrease the overall costs associated with the deployment and will allow the limited number of personnel available to work with the IDSs to focus on the alarms that are generated from the most important hosts.

Once the operation and maintenance of host-based IDSs become routine, more IT security-conscious organizations may consider installing host-based IDSs on the majority of their hosts. In this case, it would be wise to purchase host-based systems that have an easy-to-use centralized supervision and reporting function because the administration of alert responses from a large set of hosts can be intimidating.

Note:
1. Stealth modes make it extremely difficult for an attacker to detect their presence and to locate them.

Peter Mell is on the staff of the (U.S.) National Institute of Standards and Technology’s (NIST’s) Computer Security Division. He is a member of the System and Network Security Group.

UNDERSTANDING AND AUDITING THE FUNCTION OF QUALITY IN IT: PART I

BELDEN MENKUS

This article explains why IT auditors should have a continuing concern regarding the presence of quality in every aspect of the computing activities of an enterprise and the efforts that are being made to realize it. In addition, this article presents an audit work program for reviewing the nature of the organization’s effort to enhance the quality of its IT activities.