БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ • BULGARIAN ACADEMY OF SCIENCES

ПРОБЛЕМИ НА ТЕХНИЧЕСКАТА КИБЕРНЕТИКА И РОБОТИКАТА, **58**
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS, **58**

София • 2007 • Sofia

A Short Survey of Intrusion Detection Systems*

Vera Marinova-Boncheva

Institute of Information Technologies, 1113 Sofia
E-mail: vboncheva@iit.bas.bg

1. Introduction

As the cost of information processing and Internet accessibility falls, organizations are becoming increasingly vulnerable to potential cyber threats such as network intrusions. So, there exists a need to provide secure and safe transactions through the use of firewalls, Intrusion Detection Systems (IDSs), encryption, authentication, and other hardware and software solutions. Many IDS variants exist which allow security managers and engineers to identify attack network packets primarily through the use of signature detection; i.e., the IDS "recognizes" attack packets due to their well-known "fingerprints" or signatures as those packets cross the network's gateway threshold. On the other hand, anomaly based ID systems determine what is normal traffic within a network and reports abnormal traffic behaviour. IDS are made so they can reliably detect Probe, DoS, U2R, R2L and data attacks against Solaris, Sun OS, Linux and Windows NT operating systems with low false alarm rates. However, for most systems, complete attack prevention is not realistically attainable due to system complexity, configuration and administration errors, and abuse by authorized users. For this reason, attack detection has been an important aspect of recent computer security efforts [2, 5] .

2. Intrusions

Intrusions are actions that attempt to bypass security mechanisms of computer systems. So they are any set of actions that threatens the integrity, availability, or

* This work was supported by the Ministry of Education and Science under Project No MU-MI-1601/2006.

confidentiality of a network resource. These properties have the following explanations:

- Confidentiality – means that information is not made available or disclosed to unauthorized individuals, entities or processes;
- Integrity – means that data has not been altered or destroyed in an unauthorized manner;
- Availability – means that a system or a system resource that ensures that it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system.

– Occasionally intrusions are caused by:

– Attackers accessing the system from Internet;

– Insider attackers – authorized users attempting to gain and misuse non-authorized privileges.

Examples of intrusions

– Denial of service (DoS): DoS is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users access to a machine. Having network connectivity available through more than one service provider can be part of the answer to this problem. At least that way, when the main entrance is blocked, you can use the emergency exit to maintain at least minimal communications such as email. There are many varieties of DoS attacks. Some DoS attacks (like a mailbomb, neptune, or smurf attack) abuse a perfectly legitimate feature. Others (teardrop, Ping of Death) create malformed packets that confuse the TCP/IP stack of the machine that is trying to reconstruct the packet. Still others (apache2, back, syslogd) take advantage of bugs in a particular network daemon.

– User to Root Attacks (U2R): this is a class of exploit in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system. There are several different types of U2R attacks where the most common is the buffer overflow attack. Buffer overflows occur when a program copies too much data into a static buffer without checking to make sure that the data will fit.

– Scan: it is the reconnaissance on the network or a particular host. The purpose of port scanning is to determine what ports are open, and hence what services that may be running on a system are available to the attacker. This result is utilized for good by network and system administrators as a part of network security audits, and for evil by attackers who wish to compromise a box by using an exploit for one of the discovered running services on its open port. Port scanning also provides a number of additional applications and the added bonus of possibly being able to determine what OS a system is using (due to inconsistent or peculiar responses each OS's implementation of the TCP/IP stack returns). Port scanning's additional applications can also tell us what hosts are up on a network and various other network topological details, such as IP addressing, MAC addressing, router and gateway filtering, firewall rules, IP-based trust relationships, etc.

- Worms and viruses: they are replicating on other hosts.
- Compromises: they obtain privileged access to a host by known vulnerabilities [6].

3. Intrusion Detection

Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, like unauthorized entrance, activity, or file modification [2, 4].

There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic;
- Identifying abnormal activities;
- Assessing severity and raising alarm.

4. Firewalls

Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Some DoS attacks are too complex for today’s firewalls, e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DoS attack traffic. Additionally, firewalls are too deep in the network hierarchy. Your router may be affected even before the firewall gets the traffic. Nonetheless, firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. We have to consider redundancy issues when building the local network. Critical components are not only the firewall and related hosts, but also servers (shadow file servers, shadow disks, surplus workstations, and hot spares). To protect against interrupted power supplies, backup power arrangements should be made. Firewalls are not the ultimate solution and must be supplemented by appropriate authentication and authorization throughout the network. To recognize attacks and possible breaches of security, adequate administration and control must be ensured. Firewalls are useless if, for example, log files are not regularly checked for suspicious activities (at least daily) (Fig. 1).

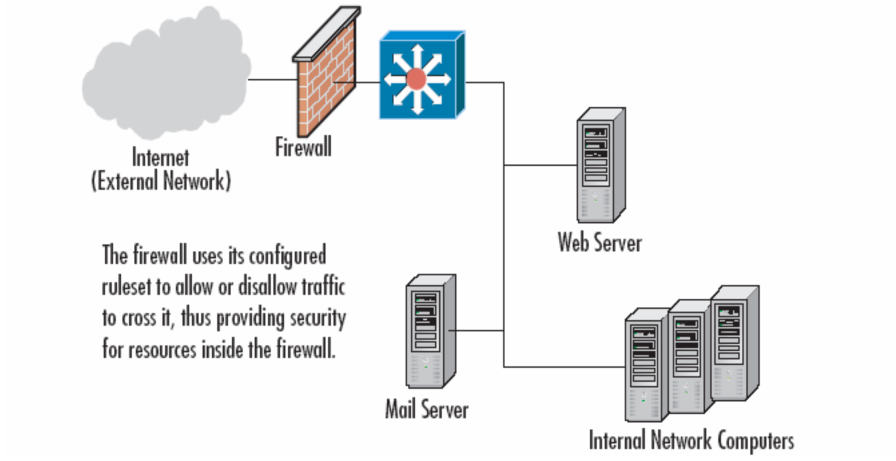
Internet
(External Network)
Firewall
Web Server
The firewall uses its configured ruleset to allow or disallow traffic to cross it, thus providing security for resources inside the firewall.
Mail Server
Internal Network Computers

Fig. 1. A basic firewall installation

5. Intrusion detection systems

Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. Intrusion Detection Systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

- **Sensors** which generate security events;
- **Console** to monitor events and alerts and control the sensors;
- Central **Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received [1].

In many simple IDS implementations these three components are combined in a single device or appliance. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. IDSs use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain IDSs have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap. Many IDSs not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts. IDSs are an integral and necessary element of a complete information security infrastructure performing as “the logical complement to network firewalls” [3]. Simply put, IDS tools allow for complete supervision of networks, regardless of the action being taken, such that information will always exist to determine the nature of the security incident and its source. Ideally the team’s network is separated from the outside world by a well-designed firewall. The outside world includes the team’s host organization.

Firewalls protect a network and attempt to prevent intrusions, while IDS tools detect whether or not the network is under attack or has, in fact, been breached. IDS tools thus form an integral part of a thorough and complete security system. They don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack such as a DoS attack. IDSs remain the only proactive means of detecting and responding to threats that stem from both inside and outside a corporate network.

Intrusion detection tools use several techniques to help them determine what qualifies as an intrusion versus normal traffic. Whether a system uses anomaly detection, misuse detection, target monitoring, or stealth probes, they generally fall into one of two categories:

- Host-based IDSs (HIDS) – examine data held on individual computers that serve as hosts. The network architecture of host-based is agent-based, which means that a software agent resides on each of the hosts that will be governed by the system.

- Network-based IDSs (NIDS) – examine data exchanged between computers. More efficient host-based intrusion detection systems are capable of monitoring and collecting system audit trails in real time as well as on a scheduled basis, thus distributing both CPU utilization and network overhead and providing for a flexible means of security administration.

Each technique has a distinct approach to monitoring and securing data and each category has strengths and weaknesses that should be measured against the requirements for each separate target environment. The two types of intrusion detection systems differ significantly from each other, but complement one another well. But in a proper IDS implementation, it would be advantageous to fully integrate the network intrusion detection system, such that it would filter alerts and notifications in an identical manner to the host-based portion of the system, controlled from the same central location. In doing so, this provides a convenient mean of managing and reacting to misuse using both types of intrusion detection.

Ideally, the best IDS tools combine both approaches under one management console. That way, the user gets comprehensive coverage, making sure to guard against as many threats as possible. As an organization introduces an IDS into its network to augment its current information security strategy, the primary focus of the intrusion detection system should be host-based. Consequently, intrusion detection systems should rely predominantly on host-based components, but should always make use of network-based IDSs to complete the defense. In short, a truly secure environment requires both a network and host-based intrusion detection implementation to provide for a robust system that is the basis for all of the monitoring, response, and detection of computer misuse [4].

6. IDS techniques

Now that we have examined the two basic types of IDS (HIDS and NIDS) and why they should be used together, we can investigate how they go about doing their job. For each of the two types, there are four basic techniques used to detect intruders: anomaly detection, misuse detection (signature detection), target monitoring and stealth probes.

- Anomaly detection: Designed to uncover abnormal patterns of behavior, the IDS establishes a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion. What is considered to be an anomaly can vary, but normally, we think as an anomaly any incident that occurs on frequency greater than or less than two standard deviations from the statistical norm. It identifies anomalies as deviations from “normal” behaviour and automatically detects any deviation from it, flagging the latter as suspect. Thus these techniques identify new types of intrusion as deviations from normal usage. It is an extremely powerful and novel tool but a potential drawback is the high false alarm rate, i.e. previously unseen (yet legitimate) system behaviours may also be recognized as anomalies, and hence flagged as potential intrusions. If a user in the graphics department suddenly starts accessing accounting programs or compiling code, the system can properly alert its administrators.

- Misuse detection (Signature detection): here each instance in a data set is labelled as “normal” or “intrusive” and a learning algorithm is trained over the labelled data. These techniques are able to automatically retrain intrusion detection models on different input data that include new types of attacks; as long as they have been labelled appropriately. Unlike signature-based IDS, models of misuse are created automatically and can be more sophisticated and precise than manually created signatures. They have high degree of accuracy in detecting known attacks and their variants. Their disadvantage is that they cannot detect unknown intrusions and they rely on signatures extracted by human experts. This method uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures. For host-based intrusion detection, one example of a signature is "three failed logins." For network intrusion detection, a signature can be as simple as a specific pattern that matches a portion of a network packet. For instance, packet content signatures and/or header content signatures can indicate unauthorized actions, such as improper FTP initiation. The occurrence of a signature might not signify an actual attempted unauthorized access. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response, or notification should be sent to the proper authorities.

- Target Monitoring – these systems do not actively search for anomalies or misuse, but instead look for the modification of specified files. This is more of a corrective control, designed to uncover an unauthorized action after it occurs in order to reverse it. One way to check for the covert editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the mission/system critical files.

- Stealth Probes – this technique attempts to detect any attackers that choose to carry out their mission over prolonged periods of time. Attackers, for example, will check for system vulnerabilities and open ports over a two-month period, and wait another two months to actually launch the attacks. Stealth probes collect a wide-variety of data throughout the system, checking for any methodical attacks over a long period of time. They take a wide-area sampling and attempt to discover any correlating attacks. In effect, this method combines anomaly detection and misuse detection in an attempt to uncover suspicious activity [4].

7. Conclusions

As security incidents become more numerous, IDS tools are becoming increasingly necessary. They round out the security arsenal, working in conjunction with other information security tools, such as firewalls, and allow for the complete supervision of all network activity. It is very likely that IDS capabilities will become core capabilities of network infrastructure (such as routers, bridges and switches) and operating systems. In future we would like to find out how data mining can help improve intrusion detection and most of all anomaly detection. For that purpose we have to understand how an IDS work to identify an intrusion. By identifying bounds for valid network activity, data mining will aid an analyst to distinguish attack activity from common everyday traffic on the network [6].

References

1. Puketza, N., M. Chung, R. Olsson, B. Mukherjee. A Software Platform for Testing Intrusion Detection Systems. – IEEE Software, September/October, 1997.
2. Northcutt, S. Network Intrusion Detection: An Analyst’s Handbook. New Riders, Indianapolis, 1999.
3. Bace, R. An Introduction to Intrusion Detection and Assessment: For System and Network Security Management, ICSA White Paper, 1998.
4. **http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf**
5. SANS Institute Staff, Intrusion Detection and Vulnerability Testing Tools: What Works? 101 Security Solutions E-Alert Newsletters. 2001.
6. Marinova-Boncheva, V. Applying a Data Mining Method for Intrusion Detection. – In: International Conference on Computer Systems and Technologies CompSysTech’07, University of Rousse, Session IIIA, IIIA.7-1-III.A7-6, 14-15 June 2007.

Краткий обзор систем обнаружения нарушений

Вера Маринова-Бончева

Институт информационных технологий, 1113 София
E-mail: vboncheva@iit.bas.bg

(Резюме)

В работе рассматриваются компьютерные атаки, которые могут привести сеть к нарушению, а также системы обнаружения и отстранения этих нарушений.

Описанные в литературе подходы, используемые при обеспечении компьютерной безопасности, направлены на предотвращение возникновения таких атак через использование защитных стен и политик безопасности.

Учитывая непрерывно растящую частоту возникновения инцидентов, связанных с безопасностью. Любой клиент Интернета должен иметь систему обнаружения нарушений, действующая как защитная перегородка. В основе большинства таких систем заложен процесс наблюдения и анализа событий, возникающих в компьютре или сети, цель которого определить проблемы безопасности.