EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 5.685 www.in-academy.uz

ATTACK DETECTION SYSTEMS

[1]Ibragimova Mohigul Komiljon Qizi
mohigul9618@gmail.com
Termiz State University
Teacher of the Department of Information Technologies,
[2]Xurramov Ruslan Erkin O‘g‘li
ruslanxurramov852@gmail.com
Termiz State University
Teacher of the Department of Information Technologies.
https://doi.org/10.5281/zenodo.7467392

ARTICLE INFO

Received: 10th December 2022
Accepted: 20th December 2022
Online: 21th December 2022

KEY WORDS

ADS-Attack detection systems, hardware systems, Access detection, Security design, security strategy.

ABSTRACT

An intrusion detection system is a software or hardware tool designed to detect unauthorized access to or control of a computer system or network, mainly via the Internet. Today, there are several types of IDS that differ in their monitoring and analysis methods. Each approach has its own advantages and disadvantages. In addition, all approaches can be described from a general point of view.

Intrusion detection systems (ADS) are software or hardware systems that automate the process of monitoring and analyzing events occurring in a computer system or network for signs of security problems. As the number of network attacks has increased and over the past few years, intrusion detection systems have become a necessary addition to the security infrastructure of many organizations. This guidance document is intended as a primer on intrusion detection, designed for those who need to understand what security objectives are served by intrusion detection mechanisms, how to select and configure intrusion detection systems for specific system and network environments, how to managing the output of intrusion detection systems and how to integrate intrusion detection with the rest of the organization's security infrastructure. References to other resources are also provided for the reader who is specialized or requires more detailed advice on specific issues of identifying aggression.

2. General description of attack detection systems:

2.1. What is access detection?

Intrusion detection is the process of monitoring events that occur on a computer, defined as attempts on a system or network, analyzing them for signs of an attack to violate privacy, integrity, availability, or bypass security computer or network mechanisms. Attacks occur as a result of attackers entering systems from the Internet, authorized users of systems who try to gain additional privileges not authorized for them, and improper use of privileges granted to them by authorized users. Intrusion Detection Systems (ADS) are software or hardware products that automate this monitoring and analysis process.

2.2. Why should I use intrusion detection systems?

Attack detection enables organizations to protect their systems from

threats that come with increased network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security experts is not whether to use intrusion detection, but which intrusion detection features and options to use. ADS is an infrastructure that is accepted as a necessary addition to the security of every organization. Despite the documented contributions, intrusion detection technologies still need to justify the purchase of ADSs in many organizations to ensure system security. There are several compelling reasons to acquire and use ADSs:

1. Deter problematic behavior by increasing the risk of detection and punishing those who attack or otherwise abuse the system.

2. Security measures to detect attacks and other security breaches that cannot be prevented by others.

3. Identifying and solving the precursors of attacks (usually experienced as such

network probes and other "doorknob knocking" activities).

4. Documenting the existing threat to the organization.

5. Act as quality control for security design and management, especially large and complex enterprises.

6. Enables fast and reliable reporting of vulnerabilities, providing useful information about ongoing attacks, improved diagnostics, recovery and root cause correction.

However, in the real world this rarely happens due to our reliance on commercial software, where flaws and vulnerabilities are discovered every day. Given this situation, Attack Detection can be a very good approach to system protection. ADS can detect when an attacker has infiltrated a system using an unpatched or unpatched flaw. In addition, it can play an important role in protecting the system by administrators who can contain and recover from any damage caused by an attack on the system. It is preferable to ignore network security threats where this allows attackers to continue to gain access to systems and the data they contain. Detection of precursors to attacks (probes and other tests for existing vulnerabilities, often as a network). When adversaries attack a system, they usually do so in predictable stages. The first stage of an attack is usually to probe or probe the system. In systems without ADS, an attacker can scan the entire system with little risk of detection. Given this unrestricted access, a determined attacker will eventually find a vulnerability in such a network and exploit it to gain access.

The same network as ADS, which controls its activity, offers many things. Although an attacker can investigate for network vulnerabilities, ADS monitors probes, identifies them as suspicious, can actively block the attacker's access to the target system, and then alerts security personnel who can take appropriate action to block the attacker's further access actions to do. Even the presence of an attacker's response to network probing increases the level of risk the attacker perceives, which deters further attempts to target the network.

Documenting an existing threat: When you're budgeting for network security, it's often helpful to substantiate claims that the network is likely to be attacked, or even that it is currently under

attack. In addition, understanding the frequency and characteristics of attacks allows us to understand what security measures are appropriate to protect the network from these attacks. ADSs investigate, classify, and characterize external and internal threats to your organization's network, helping you make the right decisions.

The way ADSs are used is important because many people are interested in letting the wrong person (stranger or insider) access their network. In addition, ADSs allow you to make informed security strategy decisions about the source and nature of attacks.

Quality control for security design and management: As ADSs operate over a period of time, system usage patterns and problems can be identified. It can highlight flaws in the design, and security management for the system in a way that supports security management to fix those flaws before an incident occurs.

References:

1. "Intrusion Detection Systems" Rebecca Bace1 and Peter Mell2
2. For an overview of ADS and their capabilities, see "Evaluating Intrusion Detection for System and Network Security Management" http://www.icsa.net/services/consortia/intrusion/intrusion.pdf.
3. "Intrusion Detection System Product Survey"
4. http://lib-www.lanl.gov/lapubs/00416750.pdf
5. NIST's ICAT Vulnerability Index allows you to search for information about specific vulnerabilities. It is located at: http://csrc.nist.gov/icat.
6. Information on computer attacks detected by ADSs can be found in the May 1999 ITL bulletin "Computer Attacks: What They Are and How to Protect Against Them".
7. http://www.nist.gov/itl/lab/bulletns/cslbull1.htm
8. Snort is a lightweight network intrusion detection system with a variety of functions for recording and analyzing traffic on IP networks. This freeware product is published under the terms of the GNU General Public License by the Free Software Foundation.
9. http://www.snort.org
10. Center for education and research in the field of information provision and security
11. At Purdue University (CERIAS) developed many widely used network security tools, including the first widely used vulnerability assessment tool, COPS, and the first widely used file integrity checker, Tripwire. CERIAS is a free tool repository for security managers with extensive ftp, including many attack detection and vulnerability assessment tools.
12. http://www.cerias.purdue.edu
13. 7. SecurityFocus.com has web pages for detecting attacks
14. includes news, information, discussions and tools. found in
15. http://www.securityfocus.com
16. ENERGIYA SAMARADORLIGINI NAZORAT VA BOSHQARISHNING AXBOROT DASTURIY TA'MINOTI VA SMART QURILMALAR. A Abdumalikov, Y Anvar, B Doniyor