Advanced Engineering Days

aed.mersin.edu.tr

Detection and prevention of intrusions into computer systems

Fatmir Basholli*[1], Adisa Daberdini [2], Armand Basholli [3]

[1]*Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al*
[2]*Aleksander Xhuvani University, Informatics Department, Elbasan, adisa.daberdini@uniel.edu.al*
[3]*Vodafone Albania/Safety & Security Lead, Tirana, Albania, armand.basholli@vodafone.com*

Cite this study: Basholli, F., Daberdini, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days, 6, 138-141

Keywords
Intrusion detection
Denial of Service
Network-based
Interventions
Detection systems

Abstract

Historically, the concept of ownership has dictated that individuals and groups tend to protect valuable resources. No matter how much protection is given to the property, there is always a weak point, where the security provided at certain points fails.
This general notion has guided the concept of systems security and defined the disciplines in cyber security and especially that of computer networks. Computer network security consists of three principles: prevention, detection and reaction/response. Although these three are the basic components of security, the main focus is on detection and prevention resources because if we are able to detect and prevent all security threats, then there is no need for reaction and response. Intrusion prevention is the art of preventing unauthorized access to system resources. The two processes are related in a sense, where intrusion detection passively watches for intrusions into the system, and intrusion prevention actively filters network traffic to prevent intrusion attempts. In the continuation of the treatment, we will focus on these two processes.

Introduction

The notion of detecting intrusions in computer networks is a phenomenon born around 1980 and treated continuously by many researchers with works on "Computer security, computer networks, monitoring and surveillance of threats" etc. In their studies, it has been emphasized that through computer audit trails we gain vital information that can be valuable in tracking misuse and understanding user behavior. An intrusion is a deliberate unauthorized attempt, successful or not, to break the security, gain access, manipulate or misuse some valuable information and where the misuse can result in its deformation making it unreliable or unusable. This action could be performed by a person who is often called an intruder.

The process of breaking into a system involves a series of stages that begin with target identification, followed by reconnaissance that provides as much information about the target as possible. Once sufficient information is gathered about the target and vulnerabilities are mapped, the next step is to gain access to the system and finally the actual use of system resources. The software and hardware used for intrusion detection has the ability to safely analyze the collected data and derive useful results to take appropriate protection measures, which is more intelligent than other network security tools [1-4]. This paper will introduce the concept of "detection" of misuses and specific user behaviors and will recommend the development of intrusion detection systems.

Material and Methods

Detection is the process of gathering information about the target system, details of its operation, and weak points. Hackers rarely attack an organization's network before they have gathered enough information about the target network. They collect information about the type of information used on that network, where it is stored,

how it is stored, and the weak point of access to that information. They perform detection by scanning the system for vulnerabilities [5].

Vulnerability assessment is an automated process in which a scanning program sends network traffic to all computers or selected computers on the network and waits for traffic to return that will indicate whether those computers have known vulnerabilities. These vulnerabilities may include: vulnerabilities in operating systems, application software and protocols.

In addition to scanning the network for information that will eventually enable intruders to illegally access an organization's network, intruders can also access an organization's network by disguising himself as a legitimate user. They can do this in a number of ways ranging from obtaining special administrative privileges to low-privilege user on system accounts. The intruder could also gain remote access privileges [6].

Denial-of-service (DoS) attacks are where an intruder tries to crash a service (or machine), overload network connections, overload the CPU, or fill up (block) the hard drive. The risks of system intrusion are numerous, including the loss of personal data that may be stored on a computer. More problematic is the way digital information is lost which is not the same as losing physical data. In the case of physical data loss, if it is stolen, then someone has it, so you can take precautions. For example, you can report to the police and call your credit card issuer. Physical loss is not the same as digital loss because in digital loss you may never know your data is lost. Hackers can break into your system and copy your data and you'll never know. Therefore, we emphasize that the damage from the loss of personal digital data can be much bigger [7, 8].

Intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer systems and networks. Intrusion detection mechanisms can be put into three models: anomaly-based detection, signature-based detection and hybrid detection. Malfunction detection is different from anomaly detection where we label each intrusive activity as an anomaly, assumes that each intrusive activity is represented by a unique pattern or signature so that small variations of the same activity produce a new signature and hence he can be discovered. Malfunction detection systems are commonly known as signature systems. Malfunction pattern analysis is performed better by expert systems, pattern-based reasoning, or neural networks.

Two main problems arising from this concept:

• The system cannot detect unknown attacks with unmapped and unarchived signatures.

• The system cannot predict new attacks and therefore will respond after an attack has occurred. This means that the system will never detect a new attack [9-11].

Identification of intrusions into the system is supposed to identify three categories of users: legitimate users, legitimate users performing unauthorized activities and of course intruders who have illegally obtained the required identification and authentication.

Results and Discussions

Types of intrusion detection systems. Figure 1 Architecture of a network-based intrusion detection system. Intrusion detection systems are also classified based on their monitoring scope. Those that monitor a wide area are known as network-based intrusion detection and those that have a limited scope are known as host-based detections. Network-based intrusion detection systems (NIDS) have the entire network as their monitoring scope. They monitor network traffic to detect intrusions. They are responsible for detecting anomalies, inappropriate or other data that may be considered unauthorized. Only when the traffic matches an acceptable pattern is it allowed to proceed regardless of what the packet contains. A NIDS also captures and inspects every packet that is destined for the network, regardless of whether it is allowed or not. If the packet signature based on the packet content is not among the acceptable signatures, then an alert is generated [12-14].

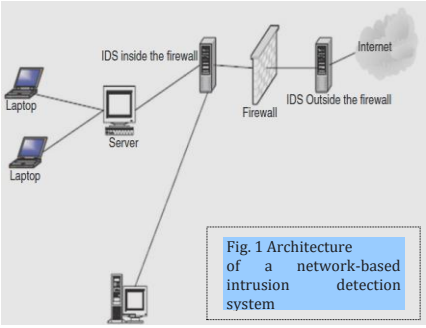

Fig. 1 Architecture of a network-based intrusion detection system

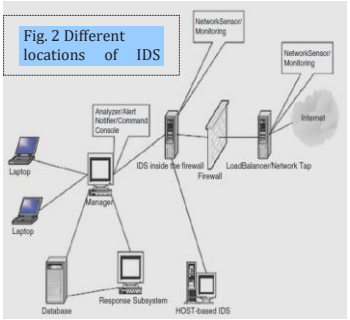

Fig. 2 Different locations of IDS

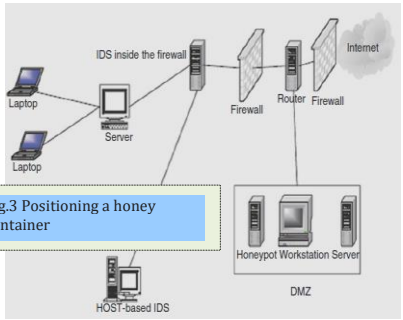

Fig.3 Positioning a honey container

The network-based intrusion detection architecture consists of several parts that must work together to produce an alarm. However, it is normal practice to deploy IDS Sensors in the following areas:

• Inside the DMZ.
• Between the firewall and the Internet.

• Behind the front-end network firewall.
• Within the network.

Host-based intrusion detection systems (HIDS) have shown that the problem of misuse of organizational information is not limited to "bad" outsiders, and to address this problem, security experts have turned to inspecting systems within an organizational network. This local inspection of systems is called Host Based Intrusion Detection Systems (HIDS).

The Hybrid Intrusion Detection System envisages the deployment of NIDS and HIDS where each patrol of its own area of the network to verify unwanted and illegal network traffic. Both bring network security to their strengths and weaknesses that best complement and add to network security. Having both components provide better flexibility in their deployment options. Although NIDS and HIDS and their hybrids are the most widely used tools in network intrusion detection, there are others that are less used but more targeted and therefore more specialized.

a. System integrity verifiers (SIVs) monitor critical files in a system, such as the file system, to find out if an intruder has changed them. Figure 2 shows the different places where ID sensors can be placed.

b. Log File Monitors (LFMs) first create a record of log files generated by network services.
A honeypot is a system designed to look like something an intruder could hack. They are built for many purposes, but the main one is to deceive attackers and learn about their tools and methods [15, 16]. Figure 3 shows the positioning of a honey pot. Response to system intrusion. A good intrusion detection system alarm should produce an appropriate response. The type of response is related to the type of attack. Some attacks require no response, others require a preliminary response. The Incident Response Team (IRT) is a primary and centralized group of dedicated people charged with the responsibility of being the first team of contact whenever an incident occurs. An IRT should have the following responsibilities:

• Keeping up to date with the latest threats and incidents. • Being the main point of contact for incident reporting. • Notifying others whenever an incident occurs. • Assessing the damage and impact of each incident. • Finding how to avoid exploiting the same vulnerability. • Eliminating the effects (Healing) from the incident.
There is a particularly difficult challenge facing organizations trying to deploy IDS on their networks. Network-based IDS sensors should be placed in areas where they can "see" network traffic packets [17,18]. Among the things to consider, in addition to the IDS, in setting up a good IDS for the company's network, the following measures should be taken:
• In updating the Operating Systems. • Improving services in web servers, e-mail and databases. • In updating Firewalls.
• In the Network Management Platform.

Conclusion

In the process of computer network security, the research and design of the intrusion detection system is very important. A good intrusion detection system can effectively compensate for the shortcomings of the firewall, can provide a reliable guarantee for the security of the computer network, and is the most effective protection technology in modern network security measures.

All network-based intrusion detection systems and tools can provide probes in addition to port and host scans. As monitoring tools, they provide information on:

• Hundreds of thousands of network connections. • Attempts at external penetration. • Internal scans. • Misuse of confidential data models. • Unencrypted remote logins or web sessions. • Observed unusual or potentially troublesome network traffic.

References

1. Chand, N., Mishra, P., Krishna, C. R., Pilli, E. S., & Govil, M. C. (2016, April). A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection. In *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring)* (pp. 1-6). IEEE.
2. Kizza, J. M., Kizza, W., & Wheeler. (2013). Guide to computer network security.
3. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409.

4. SANS Institute, "The History and Evolution of Intrusion Detection." [Online]. Available: https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344. [Accessed: 20-Feb-2016].
5. Sharma, R. K., & Pippal, R. S. (2020, September). Malicious Attack and Intrusion Prevention in IoT Network Using Blockchain Based Security Analysis. In *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 380-385). IEEE.
6. Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, *46*(4), 1-29.
7. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing*, *164*, 55-68.
8. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, *9*, 59353-59377.
9. Liu, Y. S., Lai, Y. K., Wang, Z. H., & Yan, H. B. (2019). A new learning approach to malware classification using discriminative feature extraction. *IEEE Access*, *7*, 13015-13023.
10. Masduki, B. W., Ramli, K., Saputra, F. A., & Sugiarto, D. (2015, August). Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS). In *2015 International Conference on Quality in Research (QiR)* (pp. 56-64). IEEE.
11. Basati, A., & Faghih, M. M. (2022). PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders. *Information Sciences*, *598*, 57-74.
12. McHugh, J. (2000). Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. *ACM Transactions on Information and System Security (TISSEC)*, *3*(4), 262-294.
13. Al-Taleb, N., & Saqib, N. A. (2020, September). Attacks Detection and Prevention Systems for IoT Networks: A Survey. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-5). IEEE.
14. http://www.combofix.org/what-it-is-network-intrusion-detection-system.php
15. Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy.
16. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.
17. https://cyber-defense.sans.org/resources/papers/gsec/host-vs-network-based-intrusion-detection-systems-102574.
18. Soniya, S. S., & Vigila, S. M. C. (2016, March). Intrusion detection system: Classification and techniques. In *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)* (pp. 1-7). IEEE.