ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 06 June 2024

Determining and Preempting Assaults by Employing Network Intrusion Detection Systems (NIDS)

[1] Nikhil Kulkarni, [2] Shridhar Pawar, [3] Kaushik Munde, [4] Radhika Purandare

[1][2][3][4] Vishwakarma Institute of Information Technology (VIIT), Pune India
Email: [1] devendra.22110033@viit.ac.in, [2] shridhar.22111225@viit.ac.in, [3] kaushik.22111149@viit.ac.in, [4] radhika.purandare@viit.ac.in

***Abstract*— In the commercial sector, intrusion detection is widely recognized as a critical technology and remains an active area of research. Its significance lies in its role as a fundamental tool for safeguarding sensitive data. It is a vital tool for information security. Administrators can proactively mitigate risks by employing Network Intrusion Detection Systems to monitor networks for potential breaches or unauthorized access and promptly alert relevant stakeholders. In today's interconnected environment, where computer systems form distributed networks spanning vast distances and multiple locations, the network serves as both a means of communication and a potential entry point for intrusion. The primary objective of such systems is to identify and mitigate common network attacks, utilizing signature-based methods similar to traditional IDS (intrusion detection systems). These systems inspect network packets, cross-referencing them with a repository of recognized malicious signatures to identify potential threats.**

***Index Terms*— Network Intrusion Detection System(NIDS), Intrusion Detection System(IDS), Information Security, Signature**

I. INTRODUCTION

Evolution of the network technology and its applications has resulted in a notable increase in both the frequency and severity of network attacks. Intrusion Detection System (IDS), a foundational element in the realm of network security, plays a crucial role in securing networks and detecting various types of attacks. The primary objective of IDS is to detect intrusions within routine audit data, a task centered around categorization. As an effective security technology, intrusion detection systems (IDS) are capable of identifying, halting, and potentially responding to attacks. They monitor designated areas of operation, such as auditing and analyzing network traffic data within computer or network systems that require security measures, employing diverse methods to deliver protective services.

Symantec's recent findings [1] highlight a concerning trend: the proliferation of phishing attacks aimed at acquiring sensitive data like credit card details and passwords. The frequency of these attacks surged from 9 million to over 33 million within a year. One potential remedy lies in employing Network Intrusion Detection Systems (NIDS) [2], capable of identifying attacks through the observation of diverse network behaviors. As a result, it is critical for these systems to show precision in determining attacks., have rapid training capabilities, and reduce false positives to a minimum. This document outlines the extent and advancement of our investigation into misuse detection[2,3]. Section 2 provides an outline of commonly encountered network attacks, delves into existing research endeavors, and presents the findings of experiments conducted. Subsequently, in Section 3, concluding remarks are provided along with insights into the future prospects of this research. Section 4 offers a succinct overview of the references utilized.

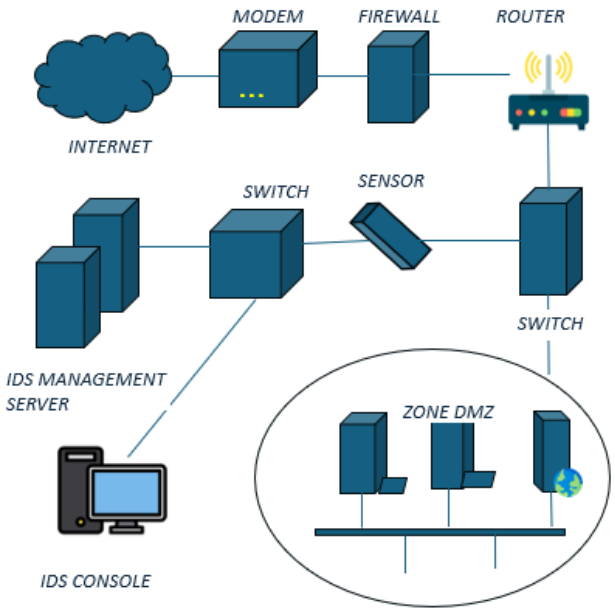

Figure 1 Computer network with Intrusion Detection Systems

II. NETWORKING ATTACKS

A. Network Intrusion Detection System (NIDS) is used to keep an eye out for [4] intrusions or attacks on networks and notify the administrator of any discovered intrusions so that preventive measures can be taken. On a backbone

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 06 June 2024

network, a sizable NIDS server can be configured to watch over all network traffic. Alternatively, more compact systems can be established to oversee the traffic directed towards a specific gateway, switch or router, as illustrated in Figure 1.

B. Tools to help manage threats and vulnerabilities in this dynamic environment are intrusion detection products. Individuals or organizations that pose a risk to your computer system are considered threats. These could be a nosy adolescent, a displeased worker, or espionage from a foreign government or competitor business.

C. Networks and corporate institutions may be severely impacted by destructive cyberattacks on computer systems. These attacks must be stopped, and an intrusion detection system can help find the incursions. Without an NIDS, it would be impossible to keep an eye on any network activity, which could do the network of an organization irreversibly harm.

D. An attacker who gains access to your network with the intent to read, corrupt, or steal data is known as an intrusion attack. Pre-intrusion activities and intrusions are the two subcategories into which these attacks fall.

2.1. PRELIMINARY INTRUSION ACTIONS

Preliminary intrusion action is taken to get a network ready for an intrusion. These encompass IP spoofing to conceal the perpetrator's identity or intruder's identity and port scanning to identify an entry point into the network.

• **Port scans:** A scanner is a tool that hackers employ to remotely probe a system to find out which TCP or UPD ports susceptible for attack. Scanner can identify a computer that is susceptible to attack over the Internet, find out which services are active on the system, and then identify any vulnerabilities in those services. Equal numbers of UDP ports and TCP ports total 65,535. In order to evade detection, stealth scanners send only the initial or final packets during an IP half scan, rather than establishing a connection.

• **IP spoofing:** This technique modifies a packet's header data to impersonate the source IP address. By using spoofing,[5] one can pretend to be a machine other than the one that supplied the data in the first place. This method can be employed either to pinpoint the machine associated with the false address or to circumvent detection. By utilizing a counterfeit address on a trusted port, an assailant can acquire packets through a firewall.

Below is a list of several network intrusions:

• **Source routing attack**: This type of exploit involves hackers utilizing a protocol vulnerability to reroute data through an alternate machine that is reachable from both the local network and the Internet. This tactic aims to gain access to private IP addresses within an internal network. Source routing is a feature supported by TCP/IP, allowing network data senders to direct their packets through specific network points for improved performance. Additionally, administrators utilize source routing to map their networks and address routing challenges.

• **Trojan attacks:** Trojans are basically the programs that pose as legitimate ones, giving hackers access to your computer so they may explore your disks, download or upload files, and more[6]. For instance, a Trojan program file named Picture.exe was created in 1999 with the intention of gathering private information from an infected computer's hard drive and sending it to a designated email address. For these programs it is called that Ports commonly associated with Trojan are frequent targets for attacks.

• **File less Malware attack:** In this kind of assault, a user gains access to the registry of computer and updates its settings. Set permissions such that no group has access in order to thwart such an assault.

• **Password hijacking attacks:** Obtaining a valid password is the simplest approach to obtain unauthorized access to a system that is protected. This can be accomplished through the use of brute force techniques or social engineering, which involves convincing authorized people to reveal their passwords through coercion, fear, or deception[7].

2.2. ILLUSTRATION OF THE SYSTEM

2.2.1. PACKET SNIFFER

The responsibility of this module is to capture all network traffic. On the end system of the network where the traffic needs to be recorded, the sniffer will be deployed. The sniffer uses the network adapter in promiscuous mode to record all network activity.

2.2.2. IDENTIFYING THE SIGNS OF AN ATTACK

The term "attack signature" describes the attack traffic pattern. Based on the packet header pattern that individual assault uses, signatures are modelled. It involves counting the packets coming from a destination or specific source or target. It can alternatively be depicted using additional packet attributes such as protocol, Time to Live and flag bits.

2.2.3. ATTACK IDENTIFICATION

To identify an attack, this process involves extracting pertinent information from captured local traffic, such as source and destination IP addresses, protocol type, header length, source and destination ports, among other details. These parameters are subsequently compared against modeled attack signatures.

2.2.4. DISCLOSURE OF ATTACK INFORMATION

This entails alerting the administrator of the attack so that he can take covert action.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 06 June 2024

Reporting involves providing details about the attack, including the IP addresses of the attacker and victim, the timestamp of the attack, and most importantly, the type of information compromised.

2.3 OBSERVATIONS

2.3.1 DETECTION OF INTRUSION BASED ON SIGNATURES

Similar to antivirus software, signature-based intrusion detection systems function by scanning a database of signatures to identify a matching signature for each particular instance of intrusion[4]. To detect intrusions, events observed in signature-based intrusion detection systems are cross-referenced with a database of attack signatures.

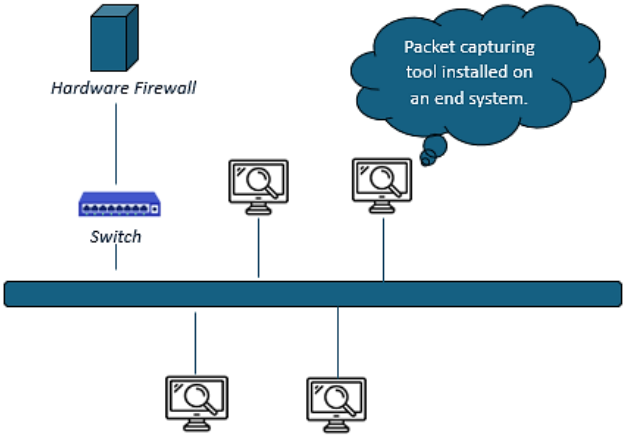

Figure 2: IDS in Diverse Mode

As the signature database necessitates manual updating to accommodate each newly identified intrusion type, signature-based intrusion detection systems are ineffective at detecting emerging threats that remain undiscovered.

Additionally, there is frequently a significant delay in the distribution of a new attack across networks once it is identified and its signature is created. SNORT, Network Flight Recorder, NetRanger, RealSecure, Computer Misuse Detection System (CMDS™), NetProwler, Haystack, and MuSig (Misuse Signatures) are some of the most well-known signature-based IDS.

This system determines assaults using the signature-based IDs methodology. Network packets are tracked by a signature-based intrusion detection system (IDS), which then compares them to a database of characteristics or signatures from known malicious threats. Most intrusion detection systems rely on signatures. This implies that they function similarly to the virus scanner, looking for signature for every individual intrusion occurrence. Furthermore, although signature-based intrusion detection systems are highly effective in identifying known attacks, they do, like antivirus programs, rely on regular signature updates to stay abreast of changes in hacker tactics.

Two more issues come up right away since signature-based IDS is as good as the size of signature database. First of all, by altering the methods of attack, signature-based solutions are easily tricked. This method merely avoids the signature database kept in the intrusion detection system, providing the hacker with a perfect chance to enter the network.

The defense in depth method can be used to get around this. Second, the CPU burden on the system responsible for processing each signature increases with the sophistication of the signature database. This inevitably implies that packets over the allotted bandwidth may be dropped. By employing capture drivers that handle networks to 1 Giga Bits Per Second, we have solved these issues with our IDS system.

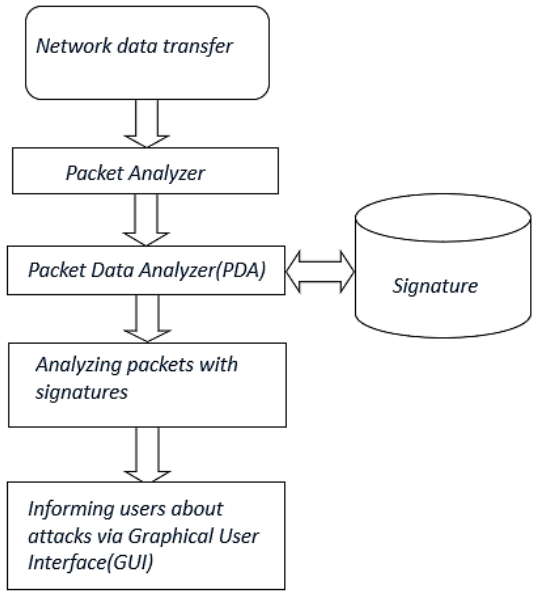

Figure 3: Implementation Architecture

2.3.2. ATTACKS THAT SOFTWARE RECORDS

1. DoS Assault:

A denial-of-service attack (DOS) [8] in computer security is an effort to prevent authorized users from accessing a computer resource. The attack aims to render the hosted online pages inaccessible on the internet, usually targeting well-known web servers. According to the Internet Architecture Board (IAB), It's a computer crime that violates the proper usage guidelines of the Internet.

DOS assaults often take two forms:

a) Make the victim computer or computers reset or use up so much of its resources that they are unable to perform the desired function.

b) Make it impossible for the victim and the targeted users to communicate effectively by obstructing their communication channels.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 06 June 2024

An intentional attempt by attackers to stop authorized users from utilizing a service is what defines a denial-of-service attack. Examples include flooding a network and blocking legal traffic, as well as interrupting service to a particular system or individual.

Any network device can be the target of an attack, including those that target web, email, DNS, and routing servers. usage of computational resources, including CPU time, storage space, and bandwidth.

2. NMAP:

The SHADOW ID Systems dispersed around the Internet began detecting unusual new scan patterns that were traced back to NMAP[9]. SYN packets transmitted to seemingly random target ports within a discrete range of values describe this scan's signature. After examining several packets sent to TCP and UDP ports with high numbers, it's common to notice a restricted amount of packets directed towards a frequently encountered destination port at the conclusion of these scans. SYN scanning and TCP connect() scanning, alternatively referred to as half-open or stealth scanning, are methods often utilized in this process this are the two fundamental scan types that are most frequently employed in NMAP.

3. DOS Bloop:

Launching fabricated ICMP packets indiscriminately constitutes a Denial of Service (DOS) attack. Considering that almost all websites recognize ICMP packets, ICMP flooding emerges as one of the most prevalent types of Denial of Service (DOS) attacks [10]. This is because it can be used to easily take down websites. The assault causes the user's computer to freeze or increases CPU consumption to the point of excessive latency.

In order to prevent a genuine user from accessing the server, Internet Control Messsage Protocol (ICMP) flooding entails the transmission of a substantial volume of ICMP packets to the designated target system. Because the remote computer must respond to each packet, the system's capacity would be exhausted. Pings, sometimes referred to as ICMP packets, are used to check if a distant computer is online.

4. DOS Conseal:

A flaw within the Conseal firewall software allows [10] for a significant surge of falsified UDP packets to penetrate the firewall, resulting in system instability leading to either rebooting or freezing. There are two ways in which this attack destroys the machine.

- When Conseal is configured in "learning" mode, a flood of packets from various IP addresses and ports will force the software to keep trying to create new rules.
- If Conseal is set up to detect attacks and report them, the excessive packet influx once again strains system resources, resulting in instability of the machine. This gradual depletion of resources culminates in system freeze and eventual reboot.

III. CONCLUSION

We have conducted research on an IDS (Intrusion Detection System) based on signature analysis for deployment on networks. By using a promiscuous mode of operation, it is able to successfully capture packets transmitted over the whole network and differentiate the traffic with specially created network attack by the signatures. Administrator can take evasive action by viewing the list of attacks in the attack log. In the case that a whole network is the target of an attack, this system functions as a warning mechanism. It can monitor the network and operate in the background.

REFERENCES

[1] Alkhalil Zainab, Hewage Chaminda, Nawaf Liqaa, Khan Imtiaz TITLE=Phishing Attacks: A Recent Comprehensive Study and a New Anatomy JOURNAL=Frontiers in Computer Science VOLUME=3, YEAR=2021 URL=https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060

[2] Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[3] Kumar, Gulshan, Amanjeet Kaur, and Sania Sethi. "Computer network attacks-a study." Int. J. Comput. Sci. Mob. Appl 2 (2014): 24-32.

[4] Innella, Paul. "The evolution of intrusion detection systems." Tetrad Digital Integrity 9 (2001).

[5] Alqurashi, R. K., Al-Harthi, O. S., & Alzahrani, S. M. (2020). Detection of IP spoofing attack. Allergy, Asthma and Immunology Research, 13(10), 2736-2741.

[6] Manju Rajan, Mayank Choksey, John Jose, Secure Routing Framework for Mitigating Time-Delay Trojan Attack in System-on-Chip,Journal of Systems Architecture,Volume 144,2023,103006,ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2023.103006. (https://www.sciencedirect.com/science/article/pii/S1383762123001856)

[7] Han, Lifeng. "Password cracking and countermeasures in computer security: A survey." arXiv preprint arXiv:1411.7803 (2014).

[8] Lubna Fayez Eliyan, Roberto Di Pietro, DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges,Future Generation Computer Systems,Volume 122,2021,Pages 149-171,ISSN 0167-739X, https://doi.org/10.1016/j.future.2021.03.011. (https://www.sciencedirect.com/science/article/pii/S0167739X21000911)

[9] Nadean H. Tanner, "Nmap—The Network Mapper," in Cybersecurity Blue Team Toolkit , Wiley, 2019, pp.31-41, doi: 10.1002/9781119552963.ch3.

[10] Wu, Zhijun, Liyuan Zhang, and Meng Yue. "Low-rate DoS attacks detection based on network multifractal." IEEE Transactions on Dependable and Secure Computing 13.5 (2015): 559-567.