IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 7, April 2023

Intrusion Prevention System for Website Attacks

Yash Sharma, Jyoti Chaudhary, Vimmi Malhotra

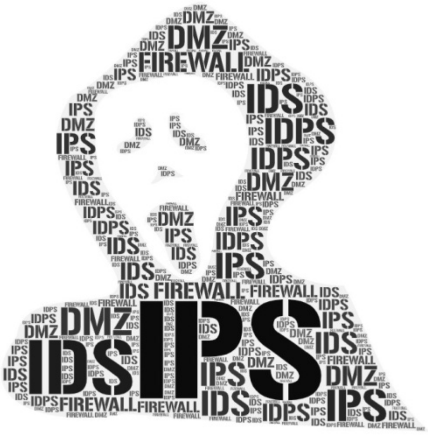
Department of Computer Science and Information Technology
Dronacharya College of Engineering, Gurugram, Haryana, India

Abstract: *Personal computers and computer networks have become increasingly vulnerable to numerous types of attacks since the introduction of the Internet. Information has evolved into a valuable asset that must be pro- tected from cyber-attacks. Privacy may be violated, and vital data may be destroyed as a result of the attack. Typically, the attacks are brought on by a failure to put security rules in place and to use easily available security tools Firewall, Intrusion Detection System, and Intrusion Prevention Systems are some of the security solutions that are accessible. Each tool comes with its own set of features. its characteristics, benefits, and drawbacks.*

Keywords: Intrusion Prevention system, Intrusion Detection System, Firewall

I. INTRODUCTION

Malicious software (malware) is evolving at a rapid pace, posing a significant challenge to the design of intrusion detection systems (IDS). Malicious assaults have evolved, and the most difficult task is identifying unknown and obfuscated malware since mal- ware developers employ various evasion tactics for information concealment to avoid detection by an IDS. Furthermore, security concerns such as zero-day attacks meant to target internet users have increased. As a result, as the use of information technology has become more prevalent in our daily lives, computer security has become increasingly important. As a result, zero-day assaults have wreaked havoc on countries like Australia and the United States. The next step in the evolution of intrusion detection systems is an intrusion prevention system (IPS) (IDS). IPS is software or hardware that can identify and block known and unknown assaults, allowing the work to be completed successfully. The process of doing intrusion detection and attempting to avoid discovered probable occurrences is known as intrusion prevention. IDPSs are primarily concerned with detecting possible security breaches, logging information about them, attempting to prevent them, and reporting them to security administrators. The primary goal of IDPSs is to detect potential events. An IDPS might, for example, identify when an attacker has successfully compromised a system by exploiting a vulnerability. The IDPs may then notify the event to security administrators, who could then swiftly launch incident response activities to limit the incident's impact.



The IDPS might also keep track of information that incident handlers could need. Many IDPSs may also be set to detect security policy breaches. Some IDPSs, for example, maybe designed to look like firewall rule sets, allowing them to identify network traffic that violates the organization's security or acceptable usage regulations. Some IDPSs may also track file transfers and flag those that appear suspicious, such as moving a huge database to a user's laptop. There are a variety of IDPS systems, which differ largely in terms of the sorts of events they can detect and the methodology they employ to identify incidents. All types of IDPS systems often conduct the following activities in addition to monitoring and analyzing events to identify harmful activity:

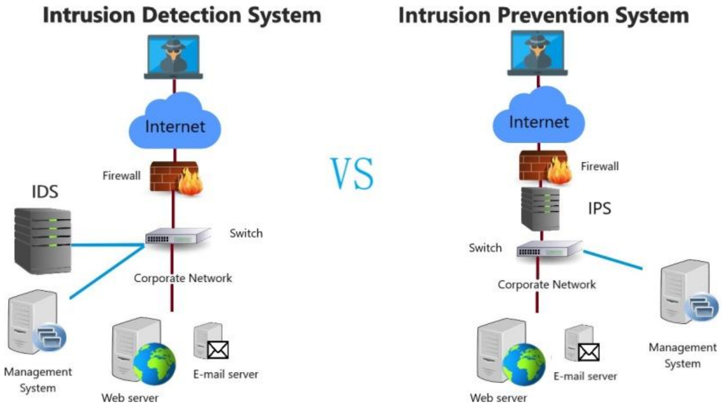
Keeping track of data relating to witnessed occurrences. Information is often stored locally, but it may also be forwarded to other systems such as centralized logging servers, SIEM solutions, and corporate management systems.

Important noticed occurrences are reported to security administrators. E-mails, pages, messages on the IDPS user interface, Simple Network Management Pro- tocol (SNMP) traps, Syslog messages, and user-defined applications and scripts are all examples of alerts. Typically, a notification message only contains the most basic information about an incident; administrators must consult the IDPS for further information.

Creating reports is a common task. Reports summarise the events that have been tracked or offer details on specific occurrences of interest. When a new threat is discovered, certain IDPs can modify their security profile. After malicious behavior is discovered inside a session, an IDPS, for example, may be able to collect additional comprehensive information for that session.

II. IPS ADVANTAGES AND DISADVANTAGES

There are pros and cons to each new development. One of the most typical issues with an IPS is the identification of false positives or false negatives . This occurs when the system blocks activity on the network because it is out of the ordinary and thus assumes it is malicious, causing a denial of service to valid users who are attempting to perform a valid procedure; or, in the case of a false negative, allowing a malicious to pass. Given that this problem is present in IDS, network managers and IPS makers should make it one of their top priorities to reduce it as much as possible. Another issue with IPS is that it becomes rather costly after a while. Furthermore, if there are many IPSs on the network, every packet of data must make multiple stops on its way to the end-user, resulting in a loss of network performance and another issue. Even with these drawbacks, the advantages of IPs that we obtain give us the protection that no other security approach can match. One of the benefits of IPS is that it may behave like antivirus software by identifying dangerous signatures, blocking them, and then displaying where they came from and where they were attempting to go. IPSs can keep hackers from destroying data on a user’s computer or triggering a network traffic overflow.



III. IDPS DETECTION METHODOLOGIES

IDPs employ a variety of approaches to identify changes in the systems they monitor. External assaults or internal staff abuse might cause these changes. Four techniques stand out among the numerous others and are extensively employed. Signature-based, anomaly-based, Stateful protocol analysis-based and hybrid-based are the four types. The hybrid technique, which combines various methodologies to provide superior de- tection and prevention capabilities, is used by the majority of modern IDPS systems. All of the approaches follow the same general concept, with the primary differences being in how they analyze the data they collect from the monitored environment to determine if a policy violation has happened. These approaches are detailed in greater depth further down.

DOI: 10.48175/IJARSCT-9492

Signature-Based Detection

A signature-based IDS (also known as a knowledge-based IDS) analyses data traffic for patterns that match known signatures—that is, attack patterns that have been preset and predefined. A signature is a pattern that is associated with a certain assault or attack type. The practice of correlating signatures to observable events to identify probable attacks is known as signature-based detection. The following are some examples of signatures:

1. A telnet attempt using the login ”root,” which is against the security policy of the business
2. An e-mail with the subject ”Free images!” and the attachment filename ”freep- ics.exe,” both of which are indicators of malware.
3. An entry in the operating system log with the status code 645, indicating that the host's auditing has been deactivated.

Because many threats have obvious and unique signatures, signature-based IDS tech- nology is commonly employed. The difficulty with a signature-based method is that when new attack tactics emerge, the IDS' signature database must be updated regu- larly.

Anomaly-Based Detection

The practice of comparing definitions of normal activity to observable occurrences to find substantial deviations is known as anomaly-based detection. In an IDPS that employs anomaly-based detection, profiles indicate the typical behaviour of objects such as users, hosts, network connections, and applications. The profiles are created over time by observing the features of usual activities. The main advantage of anomaly- based detection approaches is that they may be quite effective in detecting previously undiscovered threats. Consider the case when a computer is infected with a new sort of virus. The virus might use up a lot of the computer's processing resources, send a lot of e-mails, make a lot of network connections, and do a lot of other things that aren't in the computer's set profiles. Inadvertently putting hostile activity within a profile, creating profiles that aren't sophisticated enough to match real-world computing activity, and generating a lot of false positives are all common issues with anomaly-based detection.

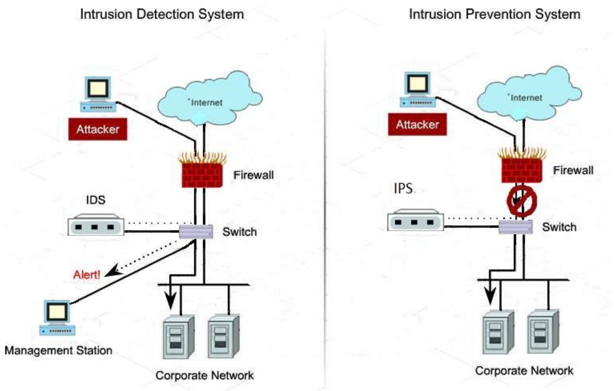
Stateful Protocol Analysis

The method of comparing preset profiles of commonly accepted definitions of benign protocol activity at each protocol state against observable events to discover deviations is known as stateful protocol analysis. Unlike anomaly-based detection, which depends on vendor-developed universal profiles that indicate how individual protocols should and should not be used, stateful protocol analysis relies on vendor-developed universal profiles that specify how specific protocols should and should not be used. The term ”stateful” in stateful protocol analysis refers to the IDPS' ability to comprehend and track the state of the network, transport, and application protocols using a state concept. Stateful protocol analysis can detect unusual command sequences, such as repeatedly issuing the same command or issuing a command without first issuing a command that it depends on. The IDPS may also maintain track of the authenticator used for each session and record the authenticator used for suspicious behavior as another state tracking function of stateful protocol analysis. Some IDPs can also employ authenticator data to determine allowed behavior for distinct groups of users or specific users.

IV. COMPARE IPS WITH IDS

Although intrusion detection systems (IDS) are useful for identifying unusual activity, they do not provide enough security against assaults. In comparison to intrusion detection systems, IPS systems offer some advantages (IDS). They are meant to sit in line with traffic flows and prevent assaults in real-time, which is a benefit. Furthermore, most IPS systems can examine (decode) layer 7 protocols such as HTTP, FTP, and SMTP, providing broader knowledge. However, while adopting network-based IPS (NIPS), it's important to evaluate if the network segment is encrypted because not all solutions can analyze encrypted data.

DOI: 10.48175/IJARSCT-9492



V. IDPS SECURITY CAPABILITIES

IDPS systems often have a wide range of detecting capabilities. Most products employ a mix of detection approaches, which allows for more accurate detection as well as greater tuning and customization options. Depending on the type of IDPS technology used, the types of events identified and the usual accuracy of detection vary substantially. To increase detection accuracy, usability, and efficacy, most IDPs require some tweaking and modification. The following are some examples of tweaking and customization possibilities.

Information Gathering Capabilities

Some IDPS systems have information-gathering features, such as the ability to collect data on hosts or networks based on observed activities. Identifying hosts, as well as the operating systems and programs they employ, and identifying network characteristics are two examples.

Logging Capabilities

Data about identified occurrences are often logged extensively by IDPs. This information may be used to verify the accuracy of warnings, analyze issues, and link events from IDPs to other logging sources. Incident date and time, event type, importance rating (e.g., priority, severity, impact, confidence), and preventative action done are all standard data variables utilized by IDPs (if any). Additional data elements are logged by certain types of IDPs, such as packet captures by network-based IDPSs and user IDs by host-based IDPSs. Administrators can often store logs locally and transfer copies of logs to centralized logging servers using IDPS technology (e.g., Syslog, security information, and event management software). To ensure the data's integrity and availability, logs should be saved both locally and centrally (e.g., If the IDPS is hacked, attackers may be able to edit or destroy its logs). IDPs should also have their clocks synchronized via the Network Time Protocol (NTP) or by making periodic manual modifications to ensure that their log entries contain accurate timestamps.

Prevention Capabilities

The particular capabilities vary by IDPS technology type. Most IDPSs offer several preventative capabilities. Administrators may generally set the preventive capability configuration for each type of alert in IDPSs. This normally entails activating or disabling prevention as well as choosing the sort of preventive capability to employ. Some IDP sensors offer a learning or simulation mode that disables all preventative measures and instead shows when one would have been taken. This allows administrators to monitor and fine-tune the setup of the prevention capabilities before allowing preventive measures, lowering the chance of blocking innocuous activities accidentally.

VI. CONCLUSION

Because of the increased trust in computers and electronic transactions, information security has become a serious issue for both enterprises and computer users. To as- sist an organization's security against threats or assaults, many strategies are employed. Attackers, on the other hand, are developing new strategies and methods to circumvent existing security regulations. The four basic types of IDPS technologies– network-based, wireless, NBA, and host-based – each have its own set of features. Each technology type has advantages over the others, such as the ability to detect assaults that the others cannot, the ability to detect attacks more precisely, and the ability to operate without severely affecting the protected hosts' performance. As a result, combining several types of IDPS technology can help to identify and block malicious activities more completely and accurately

REFERENCES

[1] Animesh Patcha, Jung-Min Park, "An overview of anomaly detection tech- niques: Existing solutions and latest technological trend, Computer Networks," The International Journal of Computer and Telecommunications Networking, Vol.51, No.12, August, 2007, pp.3448-3470.

[2] Rebecca Bace, "An introduction to intrusion detection and assessment for sys- tem and network security management." ICSA Intrusion Detection Systems Consortium Technical Report, 1999.

[3] http://en.wikipedia/wiki/Wireless Intrusion prevention system Accessed on Jan- uary 1, 2010.

[4] NIST SP 800-83, Guide to Malware Incident Prevention and Handling. Accessed on January 1, 2010. Available at http://en.wikipedia/wiki/Intrusion prevention system.

[5] Xuan D. Hoang, Jiankun Hu, Peter Bertok, "A program-based anomaly intru- sion detection scheme using multiple detection engines and fuzzy inference," Journal of Net- work and Computer Applications 32, 2009, pp. 1219–1228

[6] Shanbhag, Shashank, Tilman Wolf. "Accurate anomaly detection through par- allelism." IEEE Network 23.1, 2009, pp. 22-28

[7] Pedro Garcı´a-Teodoroa, Jesus E. Dı´az-Verdejoa, Gabriel .MaciaFerna´ndeza, Enrique Va´zquezb, "Anomaly-based network intrusion detection: Techniques, systems and challenge," Computers Security 28.1-2, 2009, pp. 18-28.

[8] Dorothy, Denning. "An intrusion-detection model," IEEE Transactions on Soft- ware Engineering, Vol. SE-13, No.2. February, 1987.

[9] Justin Lee, Stuart Moskovics, Lucas Silacci, "A Survey of Intrusion Detection Analysis Methods," CSE 221, University of California, San Diego, Spring 1999.

[10] Kenneth L. Ingham, Anil Somayaji, "A Methodology for Designing Accurate Anomaly Detection Systems," 4th international IFIPACM Latin American con- ference on Networking LANC 07, 2007, pp.139.

DOI: 10.48175/IJARSCT-9492