International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

Intrusion Detection and Prevention Techniques for Dos Attack with Security Patterns

Bhavik S. Sarang*, Hinal H. Patel* and Kinjal M. Patel*,
*Babu Madhav Institute of Information Technology,
Uka Tarsadia University,
Bardoli-Mahuva Road, Tarsadi, Bardoli, Gujarat.

***Abstract* — An intrusion detection and prevention techniques are the systems used to monitor network traffic and network packets that are coming and going through the network interface. This technique is used to analyze the network for any suspicious activity and used to generate alert to the administrator to detect the unauthorized attempts. Many methods and technologies are used to monitor network traffic. This paper is focused on Dos attack which can be occurring on networks and there can be many types of Dos attacks. It is the system which can play an important role in today's network security to detect sets of existing attack or a new attack. We describe the patterns or signatures for the existing or new attack. All the methods are included with different types of technologies. It can be any host-based, network-based or wireless-based technology. To detect different types of intruders in different types of the system these different technologies can be used to detect intruders or unauthorized attempts. We also summarized the comparison of each method with its pros and cons to a clear understanding of each method with its technology used.**

Keywords* — *NIDS (network intrusion detection system), DoS (Denial of service), Abstract IDS, Signature-based IDS, Behavior-based IDS, Stateful Protocol.

1. INTRODUCTION

An intrusion detection system (IDS) is the type of security software designed to detect intruders into your network and generate alerts to notify the administrator. It is done when someone trying to compromise information systems through malicious activities. There can be multiple ways to detect intruders into your network. There are several types of methods to detect intrusion in your system or network. It can be classified as Abstract IDS, Signature-based IDS, Behavior-based IDS, and Stateful protocol analysis. These are the methods that can be used to detect intruders. Based on that there are several types of IDS technologies that can be used to recognize any type of suspicious activity. We categorized technologies into for types: Host-based IDS, Network-based IDS, Wireless based IDS, Network behavior-based IDS, Hybrid IDS, and Router-based IDS.

2. METHODS DESCRIPTION

2.1 Abstract IDS

This detection method is used to monitor and analyze the network traffic for detecting the possible attack from network traffic which passes through the network interface. It can be used to control traffic from the internet. It used as a firewall for any network interface where outsider packets are coming. Attacks can be an existing attack or it may be a new attack. These firewalls can be detected both types of attack and we need to improve our firewall to detect such type of attack.

2.2 Signature-based IDS

This method is also known as knowledge-based IDS. It is used to detect different type signatures of the existing attack. It can be only used for the known attack. It cannot detect the new attack. Because in this we already need to define database with a set of existing attack, known attack or expected attack with its signature. so, when any new request or new packet has arrived into the network then we need to check that request with our existing database which has all the possible attack information. If any signature will match then it can be attacked and it will notify the administrator to alert that one of the attacks is performed on our network.

2.3 Behavior-based IDS

This method is also known as anomaly-based IDs. It is used to detect any type of attack. It can detect both type of attack, new attack or existing attack. This method is based on network behavior. If any network's behavior will change then it can be attacked. For that, we need to define patterns of network traffic to detect network behavior. It can be normal behavior or changed behavior which may be declared an attack. This method is more reliable compared to other methods. But in this one problem is faced when we check the network behavior that sometimes network behavior will change but it may not be attacked. So, there are many chances of false detection that we need to improve.

2.4 Stateful protocol analysis

This method is based on the different types of protocol states. It is used to identify the deviation of protocol state and it is similar to the behavior-based IDS. It will identify every request with its corresponding response. Every request should have an expected response. It will trace the protocol state and differentiate if any unexpected sequence of request-response is there or not. It needs to consume resources for tracing the protocol state.

3. DOS ATTACK

3.1 SYN flood

SYN flood is one type of denial of service (DoS) attacks. TCP is a reliable protocol in which we need to do a three-way handshake before communicating with the server for that it needs to send syn (synchronization) request to start the communication and then the server will send back (acknowledgment) to a client and then the connection is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

established. But in syn flood attacker send several syn requests to the server until the server makes unresponsive and unable to handle the traffic then this attack is performed. The attacker only sends the syn request but not get the ack so at the one-point server will make unresponsive or it may be slow down.

3.2 HTTP flood

HTTP flood is a type of DDoS attack in which attackers try to legitimate the HTTP GET/POST request to attack the web application or web server. A GET request is used to get static data and POST request is used to access dynamically generated content. This attack aims to overload the server or application with several requests. This attack is very difficult to detect because it is coming from globally and it has a standard URL.

3.3 DDoS

DDoS is similar to Dos attack but the difference is that instead of being attacked from one location, the target is attacked from many locations at once. In DDoS, there can be multiple resources from where an attack is performed. Multiple systems target to a server or network resource to flooding the targeted system with traffic.

4. TECHNOLOGY DESCRIPTION

4.1 Host-based IDS

Host-based intrusion detection system or HIDS is a technology based on any host or computer system. It is used to check any intruders into your system or application. It checks the application log or system log for any suspicious activity. It detects an intruder using a firewall and if the firewall detects any unauthorized attempt into the system then it will notify an administrator.

4.2 Network-based IDS

Network-based IDS or NIDS is used to detect intruders from network or network media. It captures the data packets from network traffic and checks if there is an attack is performed or not. It also checks the signatures and patterns to detect an existing attack or new attack. If any pattern is matched with the database then alert is generated and send it to an administrator.

4.3 Wireless based IDS

Wireless based IDS is similar to Network-based IDS but NIDS capture packets from network cables while wireless-based IDS capture the packets from wireless network traffic where no cables or any media is there to capture packets.

4.4 Network behavior-based IDS

Network behavior-based IDS is used to recognize unexpected network traffic to detect an attack. It checks the network behavior for any suspicious activity and if network behavior is changed then it may be an attack. It used in behavior-based IDS to check the behavior of the network. If it changed then alert is generated and send it to an administrator.

4.5 Hybrid IDS

There are different technologies for different methods, this is the technology that combines all of the technology to increase the detection rate. Signature-based IDS can detect an only known attack and behavior-based IDS can detect a new attack but maybe with some false detection so this is the Mixed IDS(MIDS) which can be overcome this problem.

4.6 Router-based IDS

Router-based IDS is used to protect the network infrastructure. In host-based IDS it is only based on host or computer system and in network-based IDS it only based on network traffic while Router-based IDS manage the whole network infrastructure where multiple host and multiple networks can be there. It provides a reliable connection between multiple hosts and networks. While any intruder is coming from outside this router can immediately stop intruders from entering into networks and protect the infrastructure.

5. METHODS COMPARISON

	Abstract IDS	**Signature-based IDS (Knowledge-based IDS)**	**Behavior-based IDS (Anomaly-based IDS)**	**Stateful protocol analysis**
Intent	Monitor and analyze the network traffic for detecting the possible attack which passes through the network interface.	Check every request with a database that has existing attacks.	Check every request with a pattern of network traffic.	Identify the deviation of protocol states.
Problem	An attacker may try to modify or access our system.	Whenever a packet arrives with an attack it may be a chance of harmful to that network.	Whenever a packet arrives with an attack it may be a chance of harmful to that network.	It can be harmful to the network, transport and application layer protocol.
Solution	Check each request before accessing the network whether it is an attack or not.	Match the current attack signature with previously performing attack signatures.	Check the behavior of the network every time to detect the possible deviation.	Tracking the state of network, transport and application layer protocol.
Advantages	Real-time detection, detect suspicious user, flexibility	Known attack, flexibility	New attack, real-time response	Differentiate unexpected sequence of request-response command.
Disadvantages	Some of the attacks may be hard to recognize because it can be so fast.	It only works for the known attack. The new attack will not be detected. Some attacks don't have well-defined signatures.	Lots of false detection. It can't be implemented in networks that don't have traffic patterns.	We need to consume the resources for tracing the protocol. It cannot detect attacks that do not accept protocol behavior.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

6. METHODS WITH TECHNOLOGY USED

	Abstract IDS	Signature-based IDS (Knowledge-based IDS)	Behavior-based IDS (Anomaly-based IDS)	Stateful protocol analysis
Host based IDS	✓	✓		
Network based IDS	✓	✓	✓	✓
Wireless based IDS				✓
Network behavior-based IDS		✓	✓	✓
Hybrid IDS			✓	
Router based IDS	✓	✓	✓	✓

7. CONCLUSION

We have described the different methods for intrusion detection system with its technologies. More than one technology can be used in a single method. We have described the four methods Abstract, Signature-based, Behavior-based and Stateful protocol analysis. All methods have pros and cons. The behavior-based method or anomaly-based method is more effective because it checks the request against patterns and it can also detect a new attack where Signature-based or Abstract IDS cannot detect a new attack. But there is one problem faced when we check the network behavior that sometimes network behavior will change, but it may not be attacked. So, there are many chances of false detection that we need to improve.

8. REFERENCES

[1] Suchita Patil, Dr. B.B.Meshram ,"Network Intrusion Detection and Prevention techniques for DoS attacks".
[2] Ajoy Kumar, Eduardo B. Fernandez,"Security Patterns for Intrusion Detection Systems".
[3] Intrusion detection system: A comprehensive review.
[4] Martin Roesch, "SNORT – Lightweight intrusion detection for networks".
[5] Theuns Verwoerd and Ray Hunt, "Intrusion Detection Techniques and Approaches".
[6] Teresa F. Lunt, "A survey of intrusion detection techniques".
[7] ROBERT DURST, TERRENCE CHAMPION, BRIAN WITTEN, ERIC MILLER, AND LUIGI SPAGNUOLO, "Testing and evaluating Computer intrusion detection systems".
[8] Richard P. Lippmann, David J. Fried, Isaac Graf, Joshua W. Haines, Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman, "Evaluating Intrusion Detection Systems".
[9] Chirag Modi, Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, "A survey of intrusion detection techniques in Cloud".
[10] Sahilpreet Singh, Meenakshi Bansal, "Improvement of Intrusion Detection System in Data Mining using Neural Network".
[11] Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam, "A Deep Learning Approach for Network Intrusion Detection System".
[12] Alexander G. Tartakovsky, Senior Member, IEEE, Boris L. Rozovskii, Rudolf B. Blazek, and Hongjoong Kim, "A Novel Approach to Detection of Intrusions in Computer Networks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods".