ISSN 2229-5518

NIDS using Attack Patterns

Manoj R. Gaikwad, Sandip A. Patil, Shekhar S. Kausalye, Yogesh S. Modhe

Abstract— Now a days Intrusion Detection system becomes important topic because of its capabilities. Intrusion detection becomes a vital part of a systems as it detect various network attacks. Various intrusion detection systems are developed up till now, depending upon their capabilities. This paper proposes the intrusion detection system based on pattern matching and uses the concept of CIDF architecture. The system consists of five modules which are used for capturing, decoding, detecting and taking appropriate action on the packets over network. The main focus is on packet sniffer and its working, various network attacks, their detection using pattern based NIDS and actions taken on infected packets that may be an intrusion.

Index Terms— Intrusion detection, Detection pattern, Network attacks, Packet capturing, Packet decoding, Action on packet.

1 Introduction

Intrusion detection has been an active field of research for about two decades, starting in1980 with the publication of John Anderson's "Computer Security Threat Monitoring and Surveillance", which was one of the earliest papers in the field. Anderson defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or Render a system unreliable or unusable. Dorothy Denning's seminal paper, "An Intrusion Detection Model," published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for commercial products. Despite of limitaitons of IDS, it is useful as a defensive posture, but should not be relied upon as a sole means of protection [1].

Today, successful denial-of-service attacks can put e-commerce based organizations such as online stockbrokers and retail sites out of business. Successful IDSs (Intrusion Detection Sytems) can recognize both intrusions and denial-of-service activities and invoke countermeasures against them in real time. To realize this potential, we'll need more accurate detection and reduced false-alarm rates. In order to know when you're under attack Intrusion Detection tools are generated which solve this problem by discovering and responding to attacks. Depending on the characteristics of the attacking pattern Intrusion Detection can be classified into two categories: an Anomaly based and a Pattern based. In anomaly based detection system detects intruders by observing network behavior and identifying deviation from normal network behavior as attack. While in misuse based detection system intruders are targeted by known patterns of attack or normal packets. This paper concentrates on pattern based detection system for network intruders which is came from CIDF (Common Intrusion Detection Framework) architecture. This paper covers the present theory, CIDF architecture, various network attacks, proposed architecture and proposed system description.

- *Manoj Gaikwad is currently pursuing Masters Engineering program in Computer engineering in Pune University, and working as a Lecturer in KBP Polytechnic, Maharashtra, India.E-mail: manojgaikwad90@gmail.com*
- *Sandip Patil is currently pursuing Masters Engineering program in Computer engineering in Pune University, and working as a Lecturer in KBP Polytechnic, Maharashtra, India. E-mail: sandippatil@gmx.com*
- *Shekhar Kausalye is currently pursuing Masters Engineering program in Computer engineering in Pune University, and working as a Lecturer in KBP Polytechnic, Maharashtra, India. E-mail: shekhar_sk@hotmail.com*
- *Yogesh Modhe is currently pursuing Masters Engineering program in Computer engineering in Pune University, and working as a Lecturer in KBP Polytechnic, Maharashtra, India. E-mail: y.modhe@gmail.com*

2 Kinds of Network Attack

To make IDS effective we must know various network attacks. The various network attacks are as follows

2.1 Denial of Service Attack

The recent increase in denial-of-service attacks, their power and their use by organized criminal make necessary to consider them as one of the major issues. In DOS attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting victims computer and its network connection, an attacker prevent victim from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer. The most common & and obvious type of DoS attack occurs when an attacker "floods" a network with information.

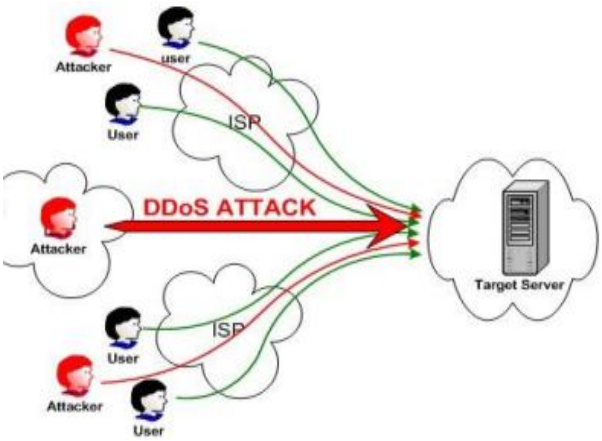

Fig. 1. Simple Denial of Service Attack

2.2 Malicious Use

In this category fall miscellaneous attacks such as file deletion, viruses, resource hogging etc. Anything that is unauthorized or which performs the unauthorized operation and can damage data or system is falls under the malicious use category.

2.3 IP Spoofing

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

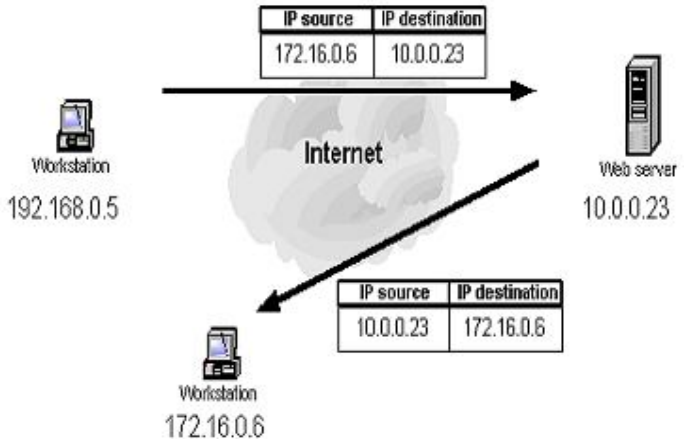

Fig. 2. IP Spoofing Attack

2.4 Source Routing Attack

This is a protocol exploit that is used by hackers to reach private IP addresses on an internal network by routing traffic through another machine that can be reached from both the Internet and the local network. TCP/IP to allow those sending network data to route the packets through a specific network point for better performance supports source routing.

3 Basic Requirment of IDS

To build powerful IDS, it is necessary to enumerate the desirable characteristics. It must run continually. It must run in the background of the system being monitored. The security analyst must always be able to monitor its status. Fault tolerance - ability to recover from system crashes and re-initializations. Crashes must not require retraining or relearning of rules/behavior. The IDS itself must not be vulnerable. The system must ideally be able to monitor itself to avoid subversion. The IDS must be able to handle the load as the network grows[2].

4 The CDIF Architechture

Researchers from universities and company's joined the force in Intrusion Detection technology. To enhance the interoperability between IDS products, components and other security products, a series of projects funded by DARPA (Defense Advanced Research Programs Agency, US) initiated a collaborative effort in February 1997 called The Common Intrusion Detection Framework (CIDF). It provides an architectural overview of the CIDF, including each individual component that composes an IDS systems, and the layered model for communication between those components.

CIDF consists of the following things

- A set of architectural conventions for how different parts of intrusion detection systems can be modeled as CIDF components.

-A way to represent gidos (generalized intrusion detection

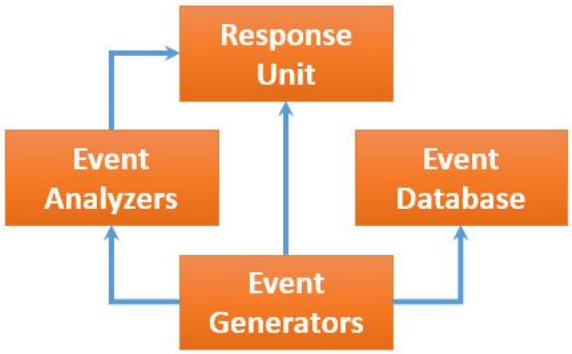

Fig. 3 The CIDF Architecture

objects). Gidos can describe events that have happened in the systems by an IDS, instruct an IDS to carry out some action query an IDS as to what has happened.

-A way to encode gidos into streams of bytes suitable for transmission over a network or storage in a file.

-Protocols for CIDF components to find each other over a network and exchange gidos.

-Application Programming Interfaces to re-use CIDF components. The CIDF architecture consists of four components: Event generators, Event analyzers, Event databases and Response units. Event generator components collect, filter and convert event data.

Analyzer components: It analyze any kind of event data transmitted to them by any CIDF component.

Database components: These are the repositories for any kind of data when the storage is necessary.

Response components: This component issue commands in response to attacks and carry out actions such as killing processes, resetting connections, altering file permissions, etc. CIDF is designed to be an open architectural standard. It is

independent of implementation languages, operating systems, and network protocols [3].

5 System Description

The NIDS system proposed is consist of five modules shows in figure 4, which are capturing module which captures raw data (packets), Decode module which decode raw packets, Detection module which detects attacks, Known Pattern module which consists of database of known attack patterns and finally Action module which perform appropriate actions. All these modules are work in sequence, one after one and passes ones output to next module. Captured packet goes through three stages in its lifetime as Network packet while captured by Network as raw data, Event packet while Decode module filter and decode the raw data to generate Event packet and finally Attack packet. This model can be placed at host side as well as on network [4], [6].

5.1 Capturing Module

This is the first module which monitor packets on network and captured packets as raw data. For this generally Packet Sniffer are used as a part of IDS. Traditionally, an application program can only capture packets sent intentionally only to local host i.e. its destination address is local host and discards all other packets. But this system monitor all packets on network including packets that are not for local host. For this the Ethernet adapter should be configured to promiscuous mode to receive packets having destination address other than local host.

5.2 Decode Module

This is the second module which processes on raw data captured by packet sniffer. This involves decoding of data to obtain predefined packet format. This predefined packet format

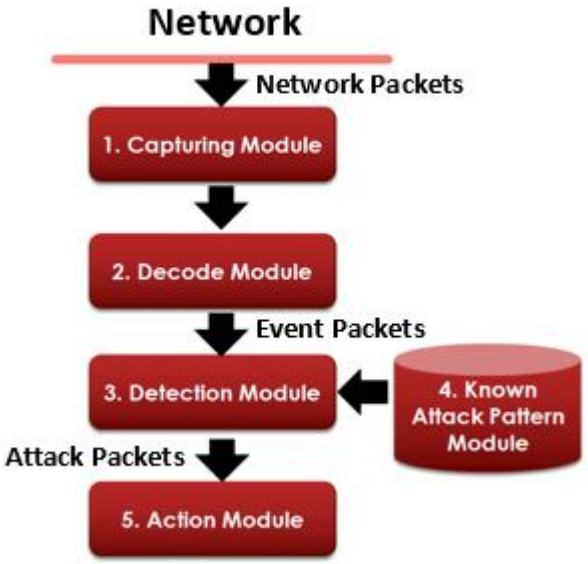

Fig. 4. CD^2A Model for IDS

simplifies the process of the later detection module and action module which uses this decoded data as input for their processing. Without decoding the captured data is not readable for users.

5.3 Detection Module

This is the third module which takes decoded packet i.e. Event packet as input and implements intrusion detection with the use of known pattern module. Here the packet formatted by Decode module is compared with database of Known patterns to make the decision of whether or not a packet has attacking behavior. The Detection module match the current packet with database, if the match is found it passes the packet as Attack packet to Action module for appropriate action to be performed else discards the packet as it is safe.

5.4 Known Attack Pattern Module

This is the fourth module which is a database of known attack patterns. Every IDS based on pattern matching needs a predefined patterns of possible intruders. For this there is need of describing intrusion behavior which is implemented with Snort rule library. After describing the intrusion behavior we need to classify the different intrusions into corresponding categories to reduce the confusion by same attack having different behaviors.

5.5 Action Module

This is the last module of the proposed system. This module perform the actions on confirmed attack behaviors, such as recording attack data, storing captured data, alerting system administrator, alerting to user by sounding or displaying attack alert message, cutting of TCP connection from hackers and so on. The action module stores the original data captured by Capturing module and Decode module.

6 Conclusion

This paper explains various kinds of IDS and different network attacks, their behavior on system. Then it also explains standard CIDF architecture which is used to propose a pattern based NIDS to overcome the limitations of intrusion detection technology. This paper proposed the CD^2A (Capture Detect Decode Action) model of NIDS having five modules viz. capturing module, decode module, detect module, known attack pattern module and action module.

Acknowledgment

It is with the greatest and pride that we present this paper. At this moment, it would unfair to neglect all those who helped us in the successful completion of this paper. We are very much thankful to our respected guide Prof. A. R. Mirikar, for his help proved to be valuable and helpful during creation of paper. We would also like to thank all the faculties who have cleared all the major concepts that were involved in the understanding of techniques behind this paper. Lastly, we are thankful to our friends who shared their knowledge in this fields

with us.

REFERENCES

[1] John McHugh, Alan Christie, and Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems", IEEE, September/October 2000.

[2] Dorothy Denning, "An intrusion-detection model", IEEE Transactions on Software Engineering, 2005.

[3] Thosmas H. Ptacek, Timothy N. Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", Secure Network, Inc. January 1998.

[4] S. Ansari, Rajeev S.G. and Chandrasekhar H.S, "Packet Sniffing: Brief Introduction", IEEE Potentials, Dec 2002- Jan 2003.

[5] A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007.

[6] Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi, "A Taxonomy of computer program security flaws", ACM Computing Surveys, sept 1994.