Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Precise Survey on Intrusion Detection Systems

Sudha Singaraju[1]
Asst Professor
Department of CA
Sreenidhi Institute of Science and Technology
India

Parsi Kalpana[2]
Asst Professor
Department of CA
Sreenidhi Institute of Science and Technology
India

Abstract— A system monitoring the events that are occurring in a computer system or Network and analysing the cyber threats such as Intrusions in the network is defined as Intrusion Detection System (IDSs).In the present days as the cost of Information processing and Internet accessibility falls down, Organizations are becoming highly vulnerable to various threats. So, there is a mere need to provide secure and safe transactions. In this paper an overview of types of IDSs are briefly given and the task done by IDSs are given. Two approaches Network Based Intrusion Detection System and Signature Based Intrusion Detection system are taken from the classification of IDSs for payload Extraction and Signature Detection. . To ensure the security of data, we wish to concentrate on the Search Algorithms which can reduce unnecessary scans by the IDS which results in low response time and high through put and low memory usage.

Keywords—Cyber Threats, Intrusions, Vulnerable, IDSs, Payload, Signature.

I. INTRODUCTION

Network services are extremely important since many companies provide services over Internet. Wide variety of Internet based applications has created a strong demand for content aware services, network policies and security Management. Data in the Network is transmitted in the form of packets. Large volumes of data are transmitted through packet payloads. Payloads may contain signatures or the patterns which acts as fingerprints of malicious code.

Low level network equipment such as firewalls are inadequate for checking signatures because it only checks the packet headers. Hence high level packet inspection is needed which is also called in-depth packet inspection. Usually high level network equipments like IDSs are used for deep packet inspection. The deep packet inspection or in-depth packet inspection is done to detect signatures in the packet header as well as packet Payload.

Packet which carries data through the network consists of 2 sections header section which carries the destination address and data section which carries data. This section is also called as packet payload section. In the network when packet is transmitted IDS captures the packet and extracts the payload of the packet (Fig1). In the given packet capturing and Payload extraction Process a packet is captured from the Network and payload is been extracted which is done in three stages.

Stage 1: Capturing Network packet and extracting Ethernet packet.
Stage 2: Extracting IP packet.
Stage 3: Extracting TCP Packet.

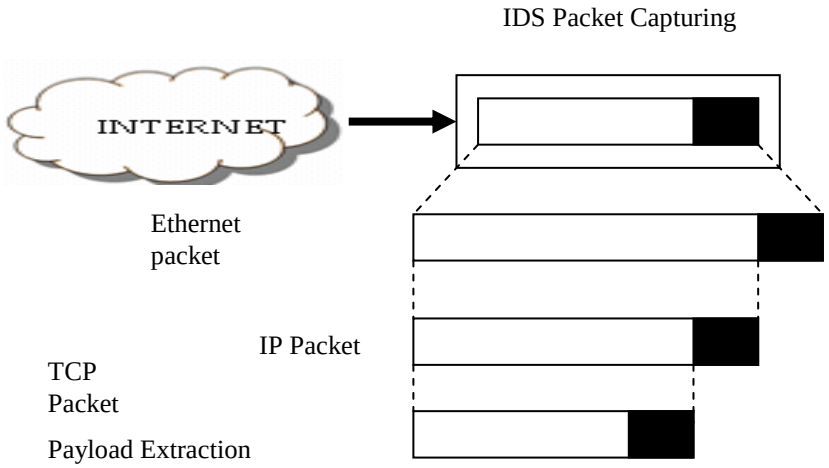

Fig1: Packet Capturing and Payload Extraction.

II. IDSs Vs FIREWALLS

IDSs are commonly mistaken for a firewall, while they both relate to network security.

Firewall:

A firewall is a computer program that monitors the system and blocks the entry of viruses and other unwanted programs. Firewalls are of 2 types:

1. Hardware Firewalls
2. Software Firewalls

Hardware Firewalls:

Hardware Firewall is a piece of Hardware that sits between your modem and system. These are used in broad band gateways and wired or wireless routers. .

Software Firewalls:

Software Firewall is a piece of software installed in the system to protect your computer from unauthorized access.

What does firewall do?

1. A firewall blocks open ports through which an intruder can gain access to your system.
2. It blocks malicious viruses entering into your system.
3. Firewalls can detect only external threats caused by outsiders.

IDSs:

An Intrusion Detection System is a Software application or Hardware Device that monitors a system, network, and database and analyse them for intrusions.

What does IDSs do?

1. An IDSs monitors the activities of the system.
2. Provides Integrity to your system.
3. Helps Administrator to set up policies.

III. TYPES OF IDSs

IDSs are commonly defined in 2 types.

Active IDSs and Passive IDSs:

An Active IDSs is also known as Intrusion Detection and Prevention System (IDPS). IDPS is configured automatically to block the suspected attacks without any intervention of the operator. An Active IDS is capable of performing any protective and corrective function on its own.

A Passive IDS is a system that is configured to only monitor and analyse network traffic and alert operator to potential vulnerabilities and attacks.

IV. CLASSIFICATION OF IDSs

Every ID System is capable of analysing. IDS are classified into one of the fallowing categories based on the type of analysis they perform.

Network-based Intrusion Detection Systems:

Network Intrusion Detection Systems usually consists of network appliance router and switches to route the traffic to a destination place (Fig 2).

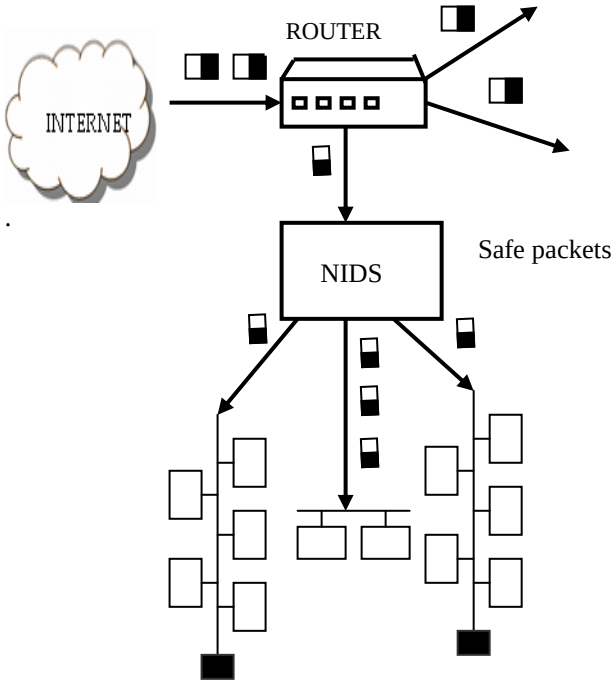

Fig2: Hardware Architecture of Network Intrusion Detection System

Host-based Intrusion Detection Systems:

A Host-based Intrusion Detection Systems are software applications which are called Software Agents installed on workstations which are to be monitored. The agents monitor the operating system an write data to the files and when vulnerabilities are traced they raise or trigger the alarms. Host-based Intrusion detection systems are used to monitor the individual work stations on which agents are installed but it cannot monitor the entire network.

Signature –based Intrusion Detection Systems:

A Signature-based Intrusion Detection Systems which are also known as Knowledge-based Intrusion Detection Systems. They refer a database of previous attacks, signatures, system Vulnerabilities. The meaning of a word signature, when we talk about Intrusion detection systems is a recorded evidence of an intrusion or an attack. Each intrusion leaves a finger print or a foot print behind, these foot prints or finger prints are called signatures or patterns and can be used to identify the same attack in future.

Anomaly-based Intrusion Detection Systems:

Anamoly-based Intrusion Detection Systems which are also known as Behavioural-based Intrusion Detection Systems. They refer a base lined or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this base lined or pattern can cause an alarm to be triggered.

V. TASKS TO BE PERFORMED BY IDSS

The main task of Intrusion Detection system is to defence the computer system by detecting an attack and possibly repel it. Detecting attacks depends on the number and type of appropriate actions (Fig 3).

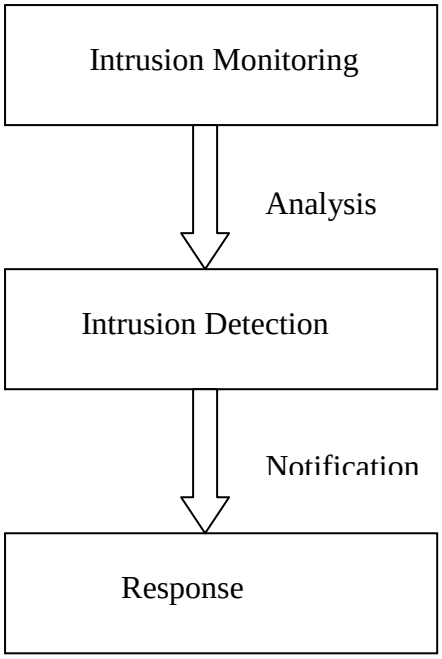

Fig3: Tasks done by intrusion Detection System

Infrastructure of IDSs

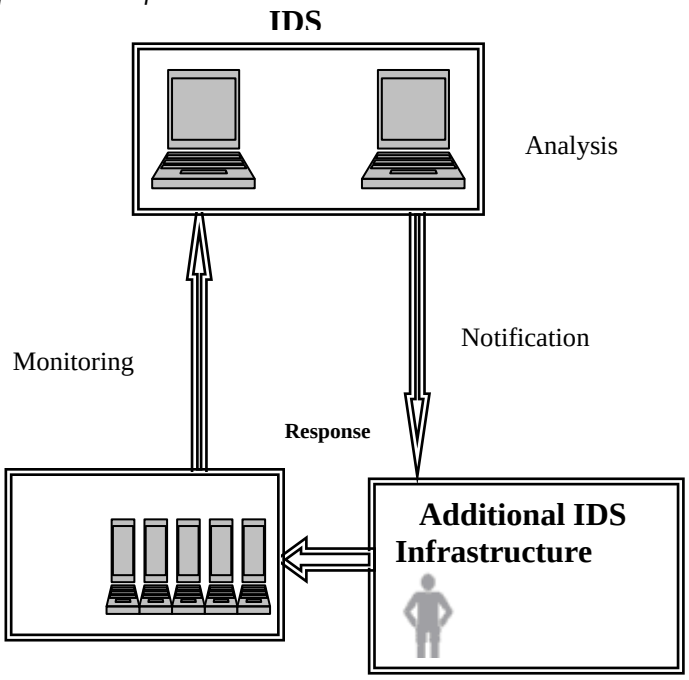

Fig4: Infrastructure of IDS.

VI. IDS COMPONENTS

IDS consists two primary Software Components they are Pattern Matching Engines (PMEs) which works with Pattern Matching Algorithms. Pattern Matching Algorithms are of 2 types:

1. Fixed-Pattern Matching Algorithms
2. Regular-expression Pattern Matchings

Fixed-Pattern Matching:

If the given pattern is constant until the search is complete. we call it as Fixed-Pattern matching . Fixed Pattern matching is further divide into single Pattern matching and Multiple Pattern Matching.

Many existing algorithms like Boyer Moore, Aho-corasick and von-Nuemon are been used as Fixed Single Pattern Matching Algorithms.

Regular-Expression Pattern Matching:

If the given Pattern for searching is not constant until the search is complete. We call it as Regular-expression Pattern. Regular expressions are used with mixed patterns and symbols and many wild character pattern strings. Regular expression can be used with various symbols like

Symbols	*Description*
\d	Matches with a single digit.
\w	Matches with a single character.
\W	Matches with a non word character.
\s	Matches with a single space character.
\S	Matches with a non space character.

VII. FUTURE WORK AND CONCLUSION

Survey of Intrusion Detection Systems is quite younger comparative to many other areas of systems research and it is understandable that this topic offers a number of opportunities for future Exploration. It is likely to expect that an Intrusion Detection System is capable of detecting the pattern or signature correctly, Perfect detection and perfect security is simply not an attainable task in the complexity and rapid evolution of modern systems. IDS can however strive to increase its efficiency in Pattern Matching schemes. In Future we would like to find out how to improve the through put and response time of IDSs and reduce the space complexity for storage of the Signatures.

REFERENCES

[1] Puketza.N.M.Chung, R.Olsson, B.Mukherjee, "A Software Platform for Testing Intrusion Detection Systems", IEEE Software, Sep/Oct, 1997.
[2] Northcutt.S, "Network Intrusion Detection: An Analyst's Handbook", New Riders, Indianapolis, 1999.
[3] Bace.R, "An Introduction to Intrusion Detection and ssessment: For System and Network Security Management", ICSA White Paper, 1998.
[4] http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf
[5] SANS Institute Staff, "Intrusion Detection and Vulnerability Testing Tools: What Works? 101 Security Solutions E-Alert Newsletters", 2001.
[6] Marinova Boncheva.V, "Applying a Data Mining Method for Intrusion Detection", International Conference on Computer Systems and Technologies CompSysTech", University of Rousse, Session IIIA, IIIA.7-1-III.A7-6, 14-15 Jun 2007.
[7] Rebecca Bace, Peter Mell, "NIST Special Publication on Intrusion Detection Systems", 16 Aug 2001.
[8] Eleazar Eskin, "Anomaly Detection over Noisy Data Using Learned Probability Distributions", Proceedings of the Seventeenth International Conference on Machine Learning (ICML-2000), Palo Alto, California, Jul 2000.
[9] Anup K. Ghosh, James Wanken, Frank Charron, "Detecting Anomalous and Unknown Intrusions Against Programs", Annual Computer Security Applications Conference (ACSAC'98), Scottsdale, Arizona, 7-11 Dec 1998.
[10] Mark Handley, Vern Paxson, Christian Kreibich, "Network Intrusion Detection: Evasion, Trace Normalization, and End-to-End Protocol Semantics," 10th USENIX Security Symposium, Washington, D.C., 13-17 Aug 2001.
[11] Koral Ilgun, Richard A. Kemmerer, Phillip A. Porras, "A State Transition Analysis Tool for Intrusion Detection", IEEE Transactions on Software Engineering, 1995.
[12] Sandeep Kumar and Eugene H. Spa_ord, " Pattern Matching Model for Misuse Intrusion Detection", Proceedings of the 17th National Computer Security Conference, pp. 11-21, Oct 1994.

