© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 02 | April - June 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in

A Review of Intrusion Detection System And Security Of Multimedia Data

Pooja Bansal

Email id poojasinghal273@gmail.com

ABSTRACT:- Network Security is an organization's strategy & provisions for ensuring security of its assets & of all network traffic. Network security is manifested in an implementation of security hardware, & software. Most definitions of network security are narrowed to enforcement mechanism. Multimedia consists of graphics, audio, video & textual data. Multimedia contents are generally of large size. This research gives complete study about types of IDS, life cycle, various domains, types of attacks & tools. IDS are becoming essential for day today security in corporate world & for network users. IPS defines about preventing measures for security. In lifecycle phases developed & stages are illustrated. Still, there are more challenges to overcome.

Keyword:- Network Security , Intrusion Detection System, intrusion detection

[1] INTRODUCTION

"Network Security is an organization's strategy & provisions for ensuring security of its assets & of all network traffic. Network security is manifested in an implementation of security hardware, & software. Most definitions of network security are narrowed to enforcement mechanism. Enforcement concerns analyzing all network traffic flows & should aim to preserve confidentiality, integrity & availability of all systems & information on network. These three principles compose CIA triad: Confidentiality involves protection of assets from unauthorized entities Integrity ensuring modification of assets is handled in a specified & authorized manner Availability a state of system in which authorized users have continuous access to said assets. Strong enforcement strives to provide CIA to network traffic flows. This begins within a classification of traffic flows by application, user, & content. As vehicle for content, all applications must first be identified by firewall regardless of port, protocol, evasive tactic, or SSL. Proper application identification allows for full visibility of content it carries. Policy management could be simplified by identifying applications & mapping their use to a user identity while inspecting content at all times for preservation of CIA.

Prevention from external attacks

The IPS often sits directly behind firewall & it provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor Intrusion Detection System (IDS)—which is a passive system that scans traffic & reports back on threats—the IPS is placed inline (in direct communication path between source & destination), actively analyzing & taking automated actions on all traffic flows that enter network. Specifically, these actions include:

1. Sending an alarm to administrator (as would be seen in an IDS)
2. Dropping malicious packets
3. Blocking traffic from source address
4. Resetting connection

As an inline security component, IPS very important work efficiently to avoid degrading network performance. It must also work fast because exploits could happen in near real-time.

[2] LITERATURE REVIEW

Intrusion detection concept was introduced in early 1980's after evolution of internet within surveillance end monitoring threas.

There was a sudden rise in reputation & incorporation in security infrastructure. Since Several events in IDS technology had been advanced intrusion detection to its current state. James Anderson's wrote a paper for a government organization & imported an approach that audit trails contained important information that could be valuable in tracking misuse & understanding of user behavior [16]. Then detection appeared & audit data & its importance led to terrific improvements in subsystems of every operating system [16]. IDS & Host Based Intrusion Detection System (HIDS) were first defined. In 1983, SRI International & Dorothy Denning began working on a project that launched a latest effort into intrusion detection system development [17]. Around 1990s revenues are generated & intrusion detection market has been raised. Real secure is an intrusion detection network developed by ISS. After a year, Cisco recognized priority for network intrusion detection & purchased Wheel Group for attaining security solutions [17]. Government actions such as Federal Intrusion Detection Networks were designed under Presidential Decision Directive 63 are also adding impulse to IDS [17].

Allam Appa Rao, P.Srinivas, B. Chakravarthy, K.Marx, & P. Kiran did research on A Java Based Network Intrusion Detection System (IDS)

The number of hacking & intrusion incidents is increasing alarmingly each year as latest technology rolls out. Unfortunately in today's digitally connected world & no place to hide. DNS, NSlookup, Newsgroups, web site trawling, e-mail properties etc. are just some of many ways in which you could be found. In this research project, they designed & build an Intrusion Detection System (IDS) that implements pre-defined algorithms for identifying attacks over a network. Java programming language is used to develop system, JPCap must be used to provide access to winpcap. packets in network are captured online i.e., as they come on interface of network. IDS is designed to provide basic detection techniques so as to secure systems present in networks that are directly or indirectly connected to Internet.

Dr. S.Vijayarani1 & Ms. Maria Sylviaa.S did research on INTRUSION DETECTION SYSTEM – A STUDY

Intrusion Detection System (IDS) is meant to be a software application which monitors network or system activities & finds if any malicious operations occur. Tremendous growth & usage of internet raises concerns about how to protect & communicate digital information in a safe manner. Nowadays, hackers use different types of attacks for getting valuable information. Many intrusion detection techniques, methods & algorithms help to detect these attacks. This main objective of this paper is to provide a complete study about definition of intrusion detection, history, life cycle, types of intrusion detection methods, types of attacks, different tools & techniques, research needs, challenges & applications.

[3] TYPES OF INTRUSION DETECTION SYSTEM

There are many types of IDS technologies based on the type of events that they monitor and the ways in which they are deployed. Here in this document we discuss the following four types

1. Network Based IDS
2. Wireless IDS
3. Network Behavior Anomaly Detection
4. Host Based IDS

1 NETWORK BASED IDS

Network based IDS (NIDS) monitors' network traffic for a particular network segment and analyses the network and application protocol activity to identify suspicious activity. It is most commonly deployed at a boundary between networks such as in routers, firewalls, virtual private networks etc.

2 WIRELESS IDS

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyse network traffic. However, it will also analyse wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security..

3 NETWORK BEHAVIOR ANOMALY DETECTION

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and base lining to determine the nominal amount of a segment's traffic

4 HOST BASED IDS

In Host-based IDS (HIDS) technology, software agents are installed on each of the computer hosts of the network to monitor the events occurring within that host only. HIDS analyze network traffic and system-specific settings such as

software calls, local security policy, local log audits, and more. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. HIDS are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

[4] IDS WORKING

1) Establishment of Network

Local area network. Each node is connected neighboring node. This is independently deployed in network area. & also deploy each port no is authorized in a node.

2) Packet Creation

Sender module would select multimedia file. & selected data would be converted into fixed size of packets. Then packet would be send from source to detector.

3) Find authorized & un authorized port

The intrusion detection is defined as a mechanism for a WSN to detect existence of inappropriate, incorrect, or anomalous moving attackers. Checking would be done whether path is authorized or unauthorized. If route is authorized data packet of multimedia file is send to valid destination. Otherwise packet would be deleted".

REFERENCE

[1] Corinne Lawrence- IPS – Future of Intrusion Detection- University of Auckland - 26th October 2004.

[2] Karthikeyan .K.R & A. Indra- Intrusion Detection Tools & Techniques a Survey

[3] Anita K. Jones & Robert S. Sielken – Computer System Intrusion Detection A Survey International Journal of Computer Theory & Engineering, Vol.2, No.6, December, 2010

[4] Vera Marinova-Boncheva-A Short Survey of Intrusion Detection Systems-. Bulgarian academy of sciences.

[5] Carl Endorf, Eugene Schultz, Jim Mellander Intrusion detection & prevention by Written-published by McGraw-Hill.

[6] Top 125 Network Security Tools-SecTools.Org- http://sectools.org/tag/ids/sec [7] PeymanKabiri & Ali A.Ghorbani-Research on Intrusion Detection & Response Survey-International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005

[8] Christopher Low –Understanding Wireless attacks &detection -GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005 -SANS Institute InfoSec Reading Room. [9] Bace, Rebecca-An Introduction to Intrusion Detection &Assessment- Infidel, Inc. for ICSA, Inc.

[10] Rebecca Gurley Bace-Intrusion Detection-Macmillan Technical Publishing, 2000.

[11] Denning, Dorothy E. – An Intrusion Detection Model- Proceedings of Seventh IEEE Symposium on Security & Privacy might 1986

[12] Intrusion detection system buyer's guide

[13] Global Information Assurance Certification Paper- Copyright SANS Institute Copyright SANS Institute Author Retains Full Rights

[14] SANS penetration testing copyright by SANS-Copyright SANS Institute Author Retains Full Rights.

[15] Sriram Sundar Rajan, Vijaya Krishna Cherukuri-An Overview of Intrusion Detection Systems.

[16] Asmaa Shaker Ashoor, Prof. Sharad Gore – Importance of Intrusion Detection System-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.