International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-016 PAGE NO: 081-084

INTRUSION DETECTION SYSTEM ON COMPUTER NETWORK SECURITY (IDS-CNS)

M.Sathish Kumar [#1], R.Vasanthi [*2]

[#1]Department of Computer science and Engineering,
Alagappa University, Karaikudi.
India.
[*2] Computer Centre,
Madurai Kamaraj University, Madurai.
India.

***Abstract*— Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. An Intrusion Detection System (IDS) is software that automates the intrusion detection process. An Intrusion Prevention System (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Here we propose a distributed intrusion detection system (DIDS). It allows administrators to gather all information about anomalous traffic assists in network crime investigation and also helps in preventing port scanning attacks in a network .This system also carries out intrusion detection and monitors malicious activities by using honey pot network. Hence rules development work, carried out for such DIDS has been quite sensitive and vital task.**

Keywords: **IDS, Security, Attacks, Intrusion, Detection, DIDS, IPS.**

I. INTRODUCTION

Intrusion Detection Techniques for Mobile Wireless Networks is the rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network Security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. We need to search for new architecture and mechanisms to protect the wireless networks and mobile computing application. The implication of mobile computing on network security research can be further demonstrated by the follow case. *Intrusion detection* is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not.

II. INTRUSION DETECTION AND THE CHALLENGES OF MOBILE AD-HOC NETWORKS

1.1 BACKGROUND ON INTRUSION DETECTION

When an intrusion defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource takes place, intrusion prevention techniques, such as encryption and authentication (e.g., using passwords or biometrics), are usually the first line of defence. However, intrusion prevention alone is not sufficient because as systems become ever more complex, and as security is still often the after-thought, there are always exploitable Weaknesses in the systems due to design and programming errors, or various socially engineered penetration techniques. For example, even

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-016 PAGE NO: 081-084

though they were first reported many years ago, exploitable buffer overflow security holes, which can lead to an unauthorized root shell, still exist in some recent system software's. Furthermore, as illustrated by the Distributed Denial-Of-Services (DDoS) attacks launched against several major Internet sites where security measures were in place, the protocols and systems that are designed to provide services (to the public) are inherently subject to attacks such as DDoS. Intrusion detection can be used as a second wall to protect network systems because once an intrusion is detected, e.g., in the early stage of a DDoS attack, response can be put into place to minimize damages, gather evidence for prosecution, and even launch counter-attacks.

1.2 USES OF IDPS TECHNOLOGIES

IDPSs are primarily focused on identifying possible incidents. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting vulnerability in the system. The IDPS could then report the incident to security administrators, who could quickly initiate incident response actions to minimize the damage caused by the incident. The IDPS could also log information that could be used by the incident handlers. Many IDPSs can also be configured to recognize violations of security policies. For example, some IDPSs can be configured with firewall rule set like settings, allowing them to identify network traffic that violates the organization's security or acceptable use policies. Also, some IDPSs can monitor file transfers and identify ones that might be suspicious, such as copying a large database onto a user's laptop.

III. COMPONENTS AND ARCHITECTURE

2.1 TYPICAL COMPONENTS

- **Sensor or Agent.** Sensors and agents monitor and analyze activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term agent is typically used for host-based IDPS technologies.
- **Management Server.** A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.
- **Database Server.** A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers.
- **Console.** A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

2.2 NETWORK ARCHITECTURES

IDPS components can be connected to each other through an organization's standard networks or through a separate network strictly designed for security software management known as a management network. If a management network is used, each sensor or agent host has an additional network interface known as a management interface that connects to the management network. Also, each sensor or agent host is unable to pass any traffic between its management interface and any of its other network interfaces. The management servers, database servers, and consoles are attached to the management network only. This architecture effectively isolates

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-016 PAGE NO: 081-084

the management network from the production networks. The benefits of doing this are to conceal the existence and identity of the IDPS from attackers; to protect the IDPS from attack; and to ensure that the IDPS has adequate bandwidth to function under adverse conditions (e.g., worm attack or distributed denial of service [DDoS] on the monitored networks). Disadvantages of using a management network include the additional costs in networking equipment and other hardware (e.g., PCs for the consoles) and the inconvenience for IDPS users and administrators of using separate computers for IDPS management and monitoring.

IV. INTRUSION DETECTION SYSTEM

In the **(Fig 1)** mobile ad-hoc network participates in intrusion detection and response. Each node is responsible for detecting signs of intrusion locally and independently, but neighbouring nodes can collaboratively investigate in a broader range. In the systems aspect, individual IDS agents are placed on each and every node. Each IDS agent runs independently and monitors local activities (including user and systems activities, and communication activities within the radio range). It detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighbouring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agent collectively form the IDS system to defend the mobile ad-hoc network.

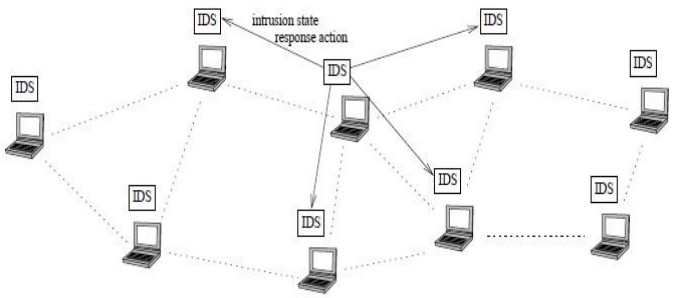

Figure 1. The IDS Architecture for Wireless Ad-Hoc Network

V. NETWORK OVERVIEW

Four Types of TCP/IP Layers

3.1 **Application Layer.** This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).

3.2 **Transport Layer.** This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally ensure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.

3.3 **Internet Protocol (IP) Layer (also known as Network Layer).** This layer routes packets across networks. IPv4 is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are IPv6, Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).

3.4 **Hardware Layer (also known as Data Link Layer).** This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

VI. LOGGING CAPABILITIES

Network-based IDPSs typically perform extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, to investigate incidents, and to correlate events between the IDPS and other logging sources. Data fields commonly logged by network-based IDPSs include the following

- Timestamp (usually date and time)
- Connection or session ID (typically a consecutive or unique number assigned to each TCP connection or to like groups of packets for connectionless protocols) Event or alert type21
- Rating (e.g., priority, severity, impact, confidence)
- Network, transport, and application layer protocols
- Source and destination IP addresses
- Source and destination TCP or UDP ports, or ICMP types and codes
- Number of bytes transmitted over the connection
- Decoded payload data, such as application requests and responses
- State-related information (e.g., authenticated username)

VII. DETECTION CAPABILITIES

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-016 PAGE NO: 081-084

Network-based IDPSs typically offer extensive and broad detection capabilities. Most products use a combination of signature-based detection, anomaly-based detection, and state full protocol analysis techniques to perform in-depth analysis of common protocols; organizations should use network-based IDPS products that use such a combination of techniques. The detection methods are usually tightly interwoven; for example, a state full protocol analysis engine might parse activity into requests and responses, each of which is examined for anomalies and compared to signatures of known bad activity. Some products also use the same techniques and provide the same functionality as network behaviour analysis (NBA) software.

This section discusses the following aspects of detection capabilities:

- Types of events detected
- Detection accuracy
- Tuning and Customization
- Technology Limitations.

VIII. CONCLUSIONS

We have totally discussed that any secure network will have vulnerability that an adversary could exploit. This is especially true for mobile wireless networks. Intrusion detection can compliment intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to secure the mobile computing intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to secure the mobile computing environment. However, new techniques must be developed to make intrusion detection work better for wireless networks. We focused our research on ad-hoc routing protocols because they are the foundation of a mobile ad-hoc network, technologies, architectures ,layers and capabilities and distributed intrusion detection system(DIDS).

ACKNOWLEDGMENT

I am greatly indebted to my parents and department faculties for their great encouragement and co-operation in all aspects to develop this paper.

I wish to thank everyone who helped us directly or indirectly for the successful completion of this paper.

REFERENCES

I. Distributed Intrusion Detection System(DIDS) Using Snort Technology, S.Dharani, M.Saranya,Page no 69,ISBN 938054310-7 National Conference proceedings.

II. Intrusion Detection Techniques for Mobile Wireless Networks *,Yongguang Zhang HRL Laboratories LLC, Malibu, California. Mobile Networks and Applications (2003) 1 16,Wenke Lee, Yi-An Huang,College of Computing, Georgia Institute of Technology

III. GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS),Karen Scarfone Peter Mell.Computer Security Division,Information Technology Laboratory ,National Institute of Standards and Technology ,Gaithersburg, MD 20899-8930.February 2007 U.S.

IV. Battlefield Intrusion Detection System, Robert K.Cunningham,David A.Kassay,Cynthia D.McLain,MIT Lincoln Laboratory,Lexing,MA.

V. Intrusion Detection System as Evidence,Peter Sommer,Computer Security Research Centre,London School of Economics & Political Science. P.M Sommer@lse.ac.uk

VI. Intrusion Detection System as Evidence,Peter Sommer,Computer Security Research Centre,London School of Economics & Political Science. P.M Sommer@lse.ac.uk.