Study of Current Network Intrusion Detection Techniques And Future Trends

Ms.S.Vijaya Rani
Assistant Professor,MCA Department
Brindavan College, DwarakaNagar
vrani_s@yahoo.co.in

Mr.R.Sekhar
MCA Student, Bharathiyar University
Coimbatore
sekhar_r14@yahoo.co.in

Abstract: **Intrusion detection system is one of the device for security of network. Radware, cisco, Axent, cybersafe, ISS and shadow are premiers in manufacturing IDS. Network security has recently received an enormous attention due to the mounting security concern in today's network. The vulnerabilities are the access of computer systems by unauthorized individuals and the misuse of system resources by authorized system users. The need for effective intrusion detection system is for prevention of attacks and vulnerabilities caused by legitimate and illegal users and hackers.**

Keywords: Signature based, anomaly based, misuse detection, unauthorized access, Artificial Intelligence, Neural Networks.

I. INTRODUCTION

According to Halme and Bauer the six components of anti intrusion techniques are prevention, preemption, deterrence, deflection, detection and counter measures. A NIDS aims at detecting possible intrusions such as malicious activity, computer attack, computer misuse, spread of virus etc and alert upon detection. It monitors and analyses the travel over a network looking for suspicious activities. The deployment of NIDS is on need basis such as monitoring traffic of a particular server, switch, gateway, router, centralized server to scan the system files, identify unauthorized activity and to maintain data integrity. The primary approaches of NIDS are signature based and anomaly based. The signature based NIDS maintains a collection of signature and compare it with a signature of the stored data. Traditionally security signature has been specified as a string signature, port signature and header condition signature.

String signature [3] is a string of ASCII symbols that characterizes a known attack. Examples of a known attacks are "cat"++">/.rhosts" – signatures in UNIX – If executed the system become vulnerable to network attack. Other examples are "cgi-bin" AND "aglimpse" AND "IFS" – web server attack.

Port signatures use connection setup attempts to well known and frequently attacked ports Examples are Telnet (TCP port 23), FTP (TCP port 20/21), SUNRPC (TCP/UDP port 111) and IMAP (TCP port 143). Header signature watches dangerous or illegitimate combinations in packet header files. Example, Winnuke.[5]

Anomaly based NIDS monitors network traffic and compares with the normal traffic profile. Normal traffic profiles are normal bandwidth usage, common protocols, correct combination of port numbers and devices. It creates high rate of false detection. Example, It can't distinguish flash crowd from DDoS attack and raise false alarm for flash crowds. [4]

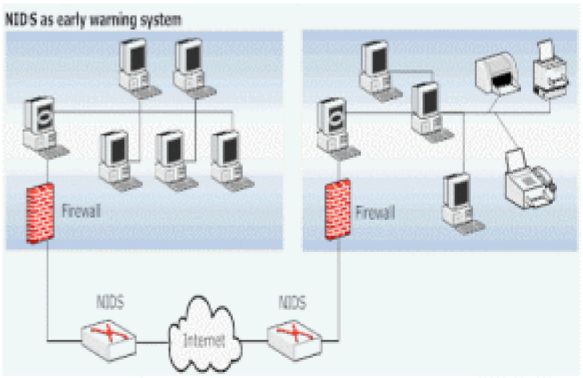

Fig 1. Early detection system

Here NIDs are employed outside the perimeter of firewall and hence all the traffic entering the host or local network is scanned by the NIDS. However attacks initiated by host within the firewall perimeter cannot be detected. If firewall blocks any traffic false alarm will be generated.

A.NIDS in internal deployment:

It enhances the security of networks, it is deployed near switching nodes in local area network, routers at network boundary. This configuration is popularly used in web, mail, database and storage servers.

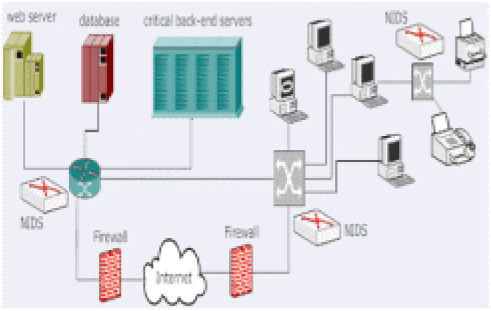

Fig2. Deployment mode of NIDS

NIDS plays a very important role in detection of common attacks which have its signatures in the database. It can easily detect worms, viruses and exploitation of a known security hole. Advanced NIDS recognize patterns that correspond to a known security threats. It can enforce access controls, block IP address, ports, security policies. Anomaly based NIDS can recognize new attacks and abnormal patterns whose signatures are not available in the database. However it will alert the network administrator and reduce the damage effect of the network due to new attacks.

B. Vulnerabilities in NIDS:

Buffer overflow, input validation error, access control vulnerability, boundary condition error are some of the vulnerabilities in NIDS.

I. ARCHITECTURE OF SIGNATURE BASED NIDS:[4]

Well known NIDS that employ signature based technology are snort, Bro, tipping. Snort is the most popular open source NIDS. Its main capabilities are stateful inspection, pattern matching and protocol anomaly detection. Bro is UNIX based NIDS the passively monitors network traffic and looks for anomaly traffic behavior. The tipping point NIDS inspect the packet at very great speed of the order of gigabits per second.

II. ANAMOLY DETECTION BASED NIDS

The common techniques to detect anomaly are statistical anomaly detection, machine learning, data mining algorithms,etc.

Design aspect of IDS[2]:

- Authorized and unauthorized access system users should be monitored.
- To identify an attack or indication of an attack
- Information received from IDS should be used to enhance the overall security level of system.
- Should be capable of analysis of an attack in real time.
- Anomaly detection
- Pattern recognition
- Misuse detection
- Network monitoring

III. CURRENT INTRUSION DETECTION TECHNIQUES:

A. NIDES: It integrates a statistical analysis based anomaly detector and a rule based misuse detection system. This combination gives the ability to detect penetration from internal and external attacks

B. DIDS: DIDS incorporates a monitor on each host, a monitor on the local area network and a DIDS director.

C. STAT/USTAT: The State Transition Analysis Tool and Unix based State Transition Analysis Tool are rule based penetration detection approaches which characterizes the process of an attack on a computer system as a series of transitions from an initial state to a compromised state.

D. TRIPWIRE: It is a good tool for monitoring the status of system files. It makes no pretense of insuring the complete security of the computer system.

Graph-based IDS: It incorporates supplementary information in the form of attributes to the tree like structure of the diagram. Information received from other intrusion detection devices and network monitors can be included in the attributes of the activity graphs.

Thumb printing: It is a method of tracking intruders through sequence of logins. The summaries would be generated by passively monitoring the network traffic at each host. Cooperating security managers: It consists of elements such as Security Manager, The command monitor, CSM intrusion handler, TCP communication handler etc.

IV. FUTURE TRENDS IN IDS:

-Artificial neural network, Artificial Intelligence,[1] Machine learning. By using concept learning, clustering, predictive learning etc

-Improved software Development Techniques. The use of structured software validation and verification methods improves design flaws. The reduction of software faults offers better security systems. Operational and administrative flaws also reduce security aspects.

V.CONCLUSION

In this paper, we have discussed about types of Intrusion detection system, its architecture and mechanisms. Due to rise in network threats, new attacks and vulnerabilities the success rate of current IDS is low. Hence introduction of artificial neural network, Artificial Intelligence, Machine learning, best software tools may be a solution of increasing network threats.

REFERENCES

[1] Next generation Intrusion Detection Expert System-Anderson,D,Frivold.T & Valdes A
[2] Network Intrusion Detection.IEEE Network.-Mukherjee.B. Heberlein,L.T & Levitt,K.N
[3] A Comparitive Analysis of current Intrusion Detection Technologies.-James Cannady and Juy Harrell
[4] Survey of current network intrusion detection techniques- Sailesh Kumar
[5] Guide to Intrusion Detection and Prevention systems-Karen Scarfone and Peter Mell