ISSN No. 2395-0900
International Journal of Engineering Studies and Technical Approach
IJESTA

Design and Development of "Spy Based" Approach for Intrusion Detection

Sudan Jha
PhD Scholar, PG Department of Computer Science and Applications,Utkal University, Vani Vihar
&
Associate Professor, Principal, Eastern College of Engineering, Biratnagar, Nepal

ABSTRACT:

Till date the IDS system has been used to offer security to a single hot or a group of interconnected systems in the network. For single host, the IDS are called as host based Intrusion Detection Systems. and that for an entire network is called as network-based intrusion detection system. The drawback of the host-based intrusion detection system is that it is not able to detect new types of attacks in the system. The network-based intrusion detection system is difficult to maintain, it cannot detect encrypted packets, and transmitting the log information over the entire network is time-consuming and may result in enormous traffic which would in turn affect the performance of the entire system. Hence a spy-based intrusion detection system is used which combines the efficacies of the two networks and reduces the disadvantages of these two networks defined before.

Keywords—*Anomaly Intrusion, Misused Intrusion; Honey Pots; Log Files; Tracer; Sensors;*

I. INTRODUCTION

No doubt, Internet has become a key resource of information. On the other hand, it is also accepted that Internet has been an ease of medium by terrorists, criminals and others to communicate information about unlawful activities. Various Companies' intellectual property is not safe and they are indulged with their competitors. It has become necessary to rethink about network monitoring tools very sensitively to capture suspected communications over the network and to analyze them. There is a compulsion of need for development of sophisticated tools that can monitor and detect undesirable communications over the network.

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.[1]

ISSN No. 2395-0900
International Journal of
Engineering Studies and Technical Approach
IJESTA

A. Anomaly Intrusion Detection

An anomaly intrusion detection system records users' activities on the system and builds statistical profiles from these records. It considers any activity remarkably different as intrusions.

B. Misuse Intrusion Detection

The misuse intrusion detection refers to any intrusion that follows well defined intrusion patterns as intrusions. It may not act or identify any new type of intrusion detection.

C. Basic Components

The spy-based intrusion detection system consists of

1. Controller
2. Honeypots
3. Sensors to connect to the network
4. Spy
5. Log files
6. Tracer
7. Database

II. FUNCTIONALITY OF THE SYSTEM

1. Controllers*:* - The controller is the central unit of the proposed IDS system. It is centralized and runs in the system which may be present next to a personal firewall. The controller is responsible for maintaining information about the intruders in the network. It is connected to the transmission line through the sensor. The controller maintains information about the list of signatures which may lead to the threat in the network. It also holds information about the intruder who was banned or disconnected from the system due to his previous intrusion attempt.

2. Honeypots*:* - Honeypots are programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack. In some cases, a honeypot is simply a "box". From the outside it appears vulnerable, while it logs traffic and also analyzes it. Thus, because Honeypots appear vulnerable and no connections should be created every connection to the honeypot is seen as suspicious.

3 Sensors*:* - The sensors are the physical interface through which the IDS system is connected to the network. The sensors are designed so that in runs in the promiscuous mode. In the promiscuous mode the sensor is transparent to any in the network and it captures all the packets that are traveling through the network either it is addressed to it or not. The sensor is controlled by the Central Controller which analyses the packets. Thus it acts as a gateway to the network.

ISSN No. 2395-0900
International Journal of
Engineering Studies and Technical Approach
IJESTA

4. Spy*:* - The spy is a program which runs in the distributed environment over the network. This may be implemented as a thread which travels through the network and periodically contacting the server program. The client runs a part of the security software which just analyses the traffic, looks for any suspicious packets, and maintains an entry in the log file about the packet. The client program also monitors any change to the system files (e.g. /etc/passwd, /etc/shadow, /etc/hosts/.equiv, .rhosts) and records the previous value and the value updated in the system file. The spy travels through the network and monitors the log file and detects any anomaly in the local system. It can then inform the server in case of any possibility of severe attack tried to impose on the system.

5. Log Files: - The log file is the file which is maintained and updated by the client program which contains information about any suspicious packet and the time when the system file was tried to be modified by the intruder.

6. Tracer*:* - The tracer is the utility which is used to trace back the intruder of the system. The intruder may conceal information about himself by changing the Source IP Address field in the packets that he may transmit. In case of Ping-Sweep attacks the intruder may replace the IP address of the Source machine as the IP address of the Destination machine itself in the ping-request packet so that the ping-reply is sent by the destined machine to itself thereby increasing the traffic in the system. In more severe cases, this ping-sweep is amplified by more than one destination machine which increases the traffic in the end system causing system failure. The tracer tracks the intruder by means of backtracking through the path traveled by the packet which can thus allow undertaking legal action against the intruder.

7. Database: - The database is the repository of information collected from previous attack attempts or contains signatures that must not be allowed into the system to execute. The database thus allows in detecting in the same attempt in the future and can be dynamically updated by the Spy to include information about any fraudulent attempts made by the intruder.

III. PROPOSED DESIGN OF THE SYSTEM

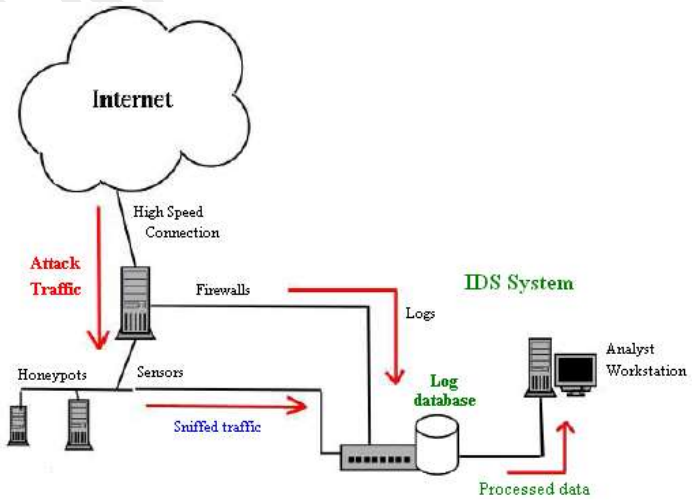

Figure 3.1: Architecture of Proposed Detection

ISSN No. 2395-0900
International Journal of Engineering Studies and Technical Approach
IJESTA

IV. STRUCTURE OF THE IDS SYSTEM

4.1Tracing the intruder in the system: When the sensor detects the intruder in the system, the information is sent to the target machine, and the target machine is instructed to collect relevant information about the sender of the particular packet. Then a spy is called to propagate through the network looking for similar packets or the source machine from which these packets arrive. It maintains a list of all the routers it encounters in the path and it uses this information to backtrack in case if the machine it reached is the dead-end. It may be used along with a collection of similar spies and detect the machine through which it can search for the intruder. The spy may periodically inform about its status to the Controller which can guide the spies and provide sufficient information.

4.2 Identifying any threat to the system: Buffer Overflow attempt

i. Executing root shell
ii. Attempt to change any system files(e.g. /etc/passwd, /etc/shadow,etc/hosts/.equiv, .rhosts)
iii. Any attempt to get the privileges of the super-user (e.g. su command in UNIX environment)
iv. Any DoS or DDoS attacks made to the system
v. Any malicious CGI script(e.g. | mail < /etc/passwd)
vi. Port scanning to find any open port
vii. Attempt to change the file mode

4.3 Implementing the Honeypot: The honeypot can be implemented by means of having open promiscuous ports on the network on intent of trapping the intruder. These ports can be allowed to support a duplicate shell running on the system. It may pretend to have fake system files like /etc/passwd. The honeypot can be used as a trap to find the intruder. The intruder can be monitored by means of logging into a file his continuous activity on the server. It thus allows detecting the different modes of security features he likes to tweak in and thus allow the system manager to detect the flaws that may be present in the system.

4.4. Implementation of Traffic Sniffer: The traffic sniffer connects to the node in the network and receives the packets traveling through the network. It is connected to the network in the promiscuous mode, and therefore is transparent to the network. It simply receives the packets and creates a log file about the type of the packet received, the time of arrival, the source and the destination address and denotes whether any threat is being noticed in the packet.

It consists of the following modules:

i. Sniffing module
ii. Analysis module
iii. Decision module
iv. Sniffing module:

ISSN No. 2395-0900
International Journal of
Engineering Studies and Technical Approach
IJESTA

The Sniffing module is responsible for gathering all the packets traveling in the network. It operates in the promiscuous mode which may be present along with a fire wall. It checks whether the incoming packet follows any of the valid protocols like TCP/UDP/ICMP. If the packet belongs to any of these protocol structures then it is allowed to travel through the network. Thus it ensures that the valid packets alone are transmitted in the network. Then it forwards the packets to the analysis module.

V. DESIGN OF THE PROPOSED IDS SYSTEM

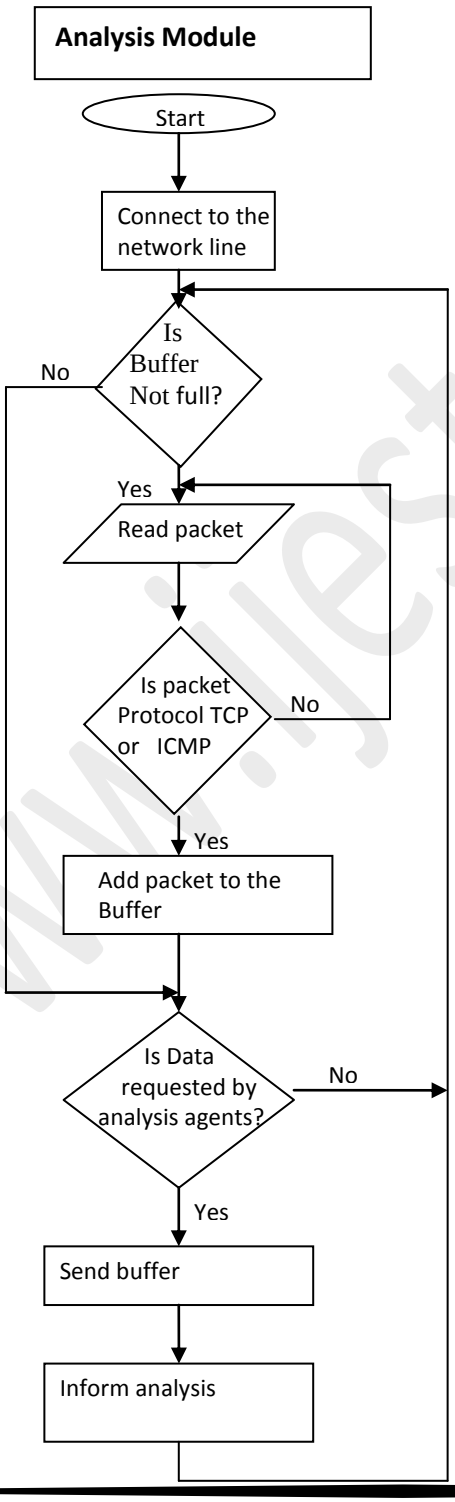

Figure 5.1: Design of the Proposed IDS System

ISSN No. 2395-0900
International Journal of
Engineering Studies and Technical Approach
IJESTA

5.1 Analysis module:

The analysis module builds a list of suspicious packets. It then searches the packet through a list of predefined signatures (the signatures are those which may be used for a previous attack like 'ping sweep attack'). It then maintains a log file where it continuously monitors the suspicious packets. It also maintains the sender and the receiver (who is likely to be attacked).

5.2 Decision module:

The decision module continuously reads the log file created by the analysis module and calculates the severity of attack from likely parameters such as the number of attempts tried by the sender with suspect packets.A decision agent may then stop receiving/forwarding such packets and disconnect the attacker. It may also generate an alert message to the system administrator through the alert generator.

VI. OUPUT SCREEN OF TRAFFIC SNIFFING

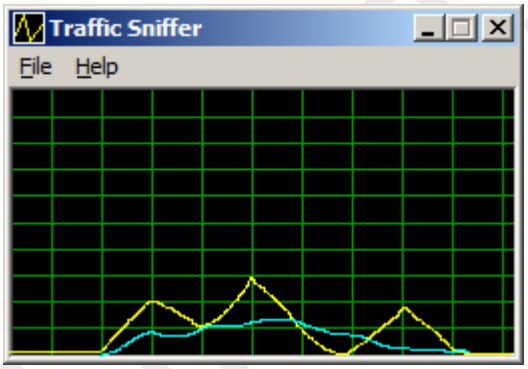

Figure 6.1: Snapshot of the Output

VII. CONCLUSION

Since the spy based network intrusion detection is used, it can satisfy both the host and the network. It can detect attack on any particular machine depending on the statistical information present in the client rather than in the central controller. Hence it can detect most attempts targeted on a single machine. The spies can operate independent of each other and they can thus collect and detect any threat immediately. It can support both signature based intrusion detection and any new security threat imposed on the system. Since it operates at both host level and network level it can effectively detect any encrypted packet. It avoids transferring large amount of control information between the controller and the spy thus reducing the traffic that would be otherwise needed for effectively detecting the attack attempt. It facilitates packet sniffing, packet monitoring and trace back of the intruder without his knowledge. It facilitates monitoring the networking without human intervention.

REFERENCES

i STEPHEN NORTHCUTT, JUDY NOVAK, Network Intrusion Detection

ii KAREN KENT FREDERICK, Intrusion Signatures and Analysis

iii CURRY, D., AND DEBAR, H. Intrusion Detection Message Exchange Format data model and Extensible Markup Language (XML) Document Type Definition

iv W. R. CHESWICK, S. M. BELLOVIN , "Firewalls and Internet Security : Repelling the wily hacker "

v "SunSHIELD Basic Security Module Guide" Sun MicroSystems Inc.

vi Loris Degioanni, Fulvio Eisso, and Piero Viano, "Windump". http://netgroup-serv.polito.it/windump,

vii erald Combs et al. "Ethereal". Available at http://www.ethereal.eom.

viii "Etherpeek nx". http://www.wildpaekets.eom.

ix "Gaim:A multi-protocol instant messaging (im) client", "http: //gaim.sourceforge.net/".

x "Ipv6: The Next Generation Internet!", "http://www.ipv6.org".

xi Van Jacobson, Craig Leres, and Steven MeCanne, "tepdump : A Network Monitoring and Packet Capturing Tool". Available via anonymous FTP from ftp://ftp.ee.lbl.gov and www.tcpdump.org.

xii Neeraj Kapoor. "Design and Implementation of a Network Monitoring Tool". Technical report, Department of Computer Science & Engineering, IIT Kanpur, Apr 2001.

xiii http://www.cse.iitk.ac.in/research/mtech2000/Y011111.html.

xiv Steve MeCanne and Van Jacobson. "The BSD Packet Filter: A New Architecture for User-level Packet Capture". In *Proceedings of USENIX Winter Conference*, pages 259-269, San Diego, California, Jan 1993.

xv "Network Associates Incorporated", http://www.sniffer.com.