TELKOMNIKA, Vol. 11, No. 10, October 2013, pp. 6258 ~ 6266
ISSN: 2302-4046

A Distributed Network Intrusion Detection System with Active Surveillance Agent

Bin Zeng*, Lu Yao, Rui Wang
Department of Management, Naval University of Engineering
JieFang Road 717, wuhan, Hubei, China, Ph./Fax: +86-02783443158/83443544
*Corresponding author, e-mail: zbtrueice@163.com

Abstract

A distributed network intrusion detection system (IDS) called SA-NIDS is proposed based on the network-based intrusion detection architecture. It includes three basic components, Local Intrusion Detection Monitor (LIDM), Global Intrusion Detection Controller (GIDC), and Surveillance Agent (SA). Basically, the LIDM is used to do packets capturing, packets de-multiplexing, local intrusion detection and intrusion inferring. The GIDC is installed in administration center for communicating and managing LIDMs, it can also do the intrusion detection and intrusion inferring. The SA contains several optional functions for information gathering. After an attack behavior is discovered, the SA may be used to launch some kinds of information gathering to the attacker, so that the proposed SA-NIDS has the active surveillance ability. For the intrusion inferring, the pattern matching and the statistical approach are applied in SA-NIDS. The experimental results can satisfy the needs of network information safety.

***Keywords**: Information Security, Intrusion Detection System, Multi-Agent System, Pattern Matching*

1. Introduction

Information security depends on the five functions: data integrity, authentication, non-repudiation, confidentiality, and access control [1]. Unfortunately, it is difficult to achieve altogether these five goals of the information security for the sake of rapid growth of Internet. Current Internet is based on TCP/IP network infrastructures, it includes hardware, software and protocols. All the components have their own security problems. Even the entire system is safe, the careless network managers may neglect something so that the malicious users can do something bad to the system. The inherent characteristics of the TCP/IP network are that it is not originally designed for secure communication and has a lot of vulnerabilities [2-5].

Intrusion detection is defined as the processes to identify the internal or external users who intend to do something unauthorized against the computer system [6]. Identifying the IDS by the monitoring approach used, we can categorize the IDS into two types, that is Host-based IDS (HIDS) and Network-based IDS (NIDS) [7]. HIDSs have agents that take the operating system's various audit trails as the main data source. After a central collector assembles all kinds of logs from each agent, the analyzing agent does the actual intrusion detection. NIDSs are different from HIDSs which are designed to support only a single host, monitor packets on the network wire, take these network packets as the data sources and discover if an intruder is attempting to break a system. For the broadcast property of some LAN technology (e.g., Ethernet), the NIDS sets its network adapter to the promiscuous mode and generally can see all packets on the same segment of network.

Identifying the IDSs by the intrusion inference modes or detecting algorithm, we can categorize the IDS into two types, Statistical IDS (SIDS) and Rule-based IDS (RIDS) [8]. SIDSs use statistical anomaly detection as their detection approach. SIDSs build up profiles of all users, subjects and objects in the host/network as the hypothesis of normal behaviors. SIDSs define a set of parameters such as the login frequency, failure of login attempt, resource availability, memory used, unauthorized file system access attempt, and so on. Statistical approaches are used to look for deviations from statistical measures or existing system profiles to detect unusual behaviors. To infer whether a suspicious activity is an attack, a threshold is set up for each parameter according to the system profile. If the parameter value is higher or lower than the threshold (according to the parameter type), we regard the suspicious activity as

Received May 27, 2013; Revised July 17, 2013; Accepted July 26, 2013

an attack. In RIDSs, we build up an intrusion signature database about historically known intrusion techniques and malicious behaviors as the rules. These rules may be a single activity, sequences of activities, thresholds of events, general commands or syntax in which operator is allowed. RIDSs compare the parameters in the rule database of the user sessions and the user commands, and data to each intrusion signature in the database. If the information somewhere or user commands match the intrusion signature, the suspicious activities will be regarded as attacks.

2. The Proposed Method

The proposed SA-NIDS is based on the network-based intrusion detection techniques. It is extended from the architecture of NSM [9] and DIDS [10] developed in U.C. Davis as reference. The SA-NIDS architecture (see Figure 1) proposed in this paper is basically composed of three components: Local Intrusion Detection Monitor (LIDM), Global Intrusion Detection Controller (GIDC) and Surveillance Agent (SA).

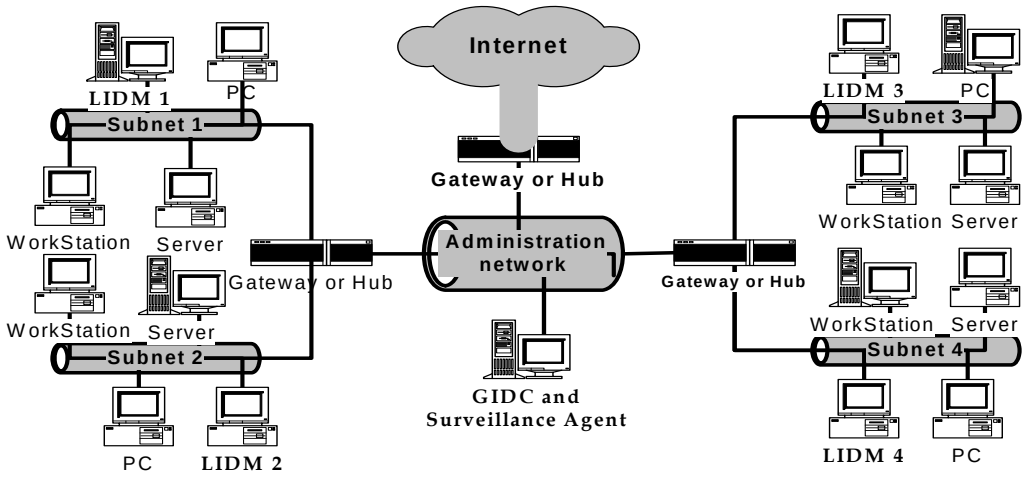

Figure 1. The architecture of the proposed SA-NIDS

2.1. Architecture of the Proposed SA-NIDS

Generally, there is usually one GIDC in the central administration network of a large network and an LIDM in each segment. The GIDC and LIDMs securely communicate in the client-server mode. The Surveillance Agent and GIDC physically reside in the same host with different logical functions. The functions of each component are described in detail below.

- Local Intrusion Detection Monitor

An LIDM stands alone in each segment of LAN. It is responsible for the local packet capturing and local intrusion detection. LIDM is the basic and the most important part of the proposed SA-NIDS. It has four main components:

- Packet Catcher
- Packet Parser
- Intrusion Signature Database (ISD) configurator, and
- Primary Inference Engine

In an appropriately constructed topology of network, the Packet Catcher captures most network packets flowing across the segment of the network. After capturing the packets, the Packet Catcher passes the packets to the Packet Parser. The Packet Parser does the TCP/IP demultiplexing to the packets for further packet analyzing and pattern matching intrusion detection by the Primary Inference Engine. The Primary Inference Engine infers whether local suspicious activities discovered by LIDM is a malicious behavior. The ISD configurator manages the ISD that is the collection of sequence descriptions of the network intrusions. The Network

Security Officer (NSO) updates new intrusion signatures when new attack techniques are discovered.

- Global Intrusion Detection Controller

A GIDC is installed into the network center to communicate with LIDMs and administrate the entire network. For the distributed architecture, the NSO in network center can detect attacks from the outside or inside of network after receiving the information from each LIDM. A GIDC contains five components:

- Information Receiver
- Network Fact Database (NFD) configurator
- Intrusion Signature Database (ISD) configurator
- Advanced Inference Engine, and
- Alert Manager

The Information Receiver takes each LIDM's intrusion detection information as the input and passes it to the Advanced Inference Engine. The Advanced Inference Engine decides whether the suspicious activity is a malicious behavior by observing current network facts and comparing the information to the GIDC intrusion signature. The NFD has the knowledge of the topology and construction of the entire network that the NSO administrates. The ISD has the knowledge of historically known intrusion scenarios. When the topology of the network changes or new intrusion techniques are discovered, the NFD and ISD configurator dynamic updates the configuration database. The Alert Manager manages the alert generated by Advanced Inference Engine.

- Surveillance Agent

Surveillance is an optional function in the proposed SA-NIDS. It is installed physically on the same host with GIDC. It is composed of two components: Surveillance Launching Agent and Surveillance functions. Surveillance Launching Agent is responsible for the network information gathering and launching the information gathering process with the Surveillance techniques specified in various Surveillance functions.

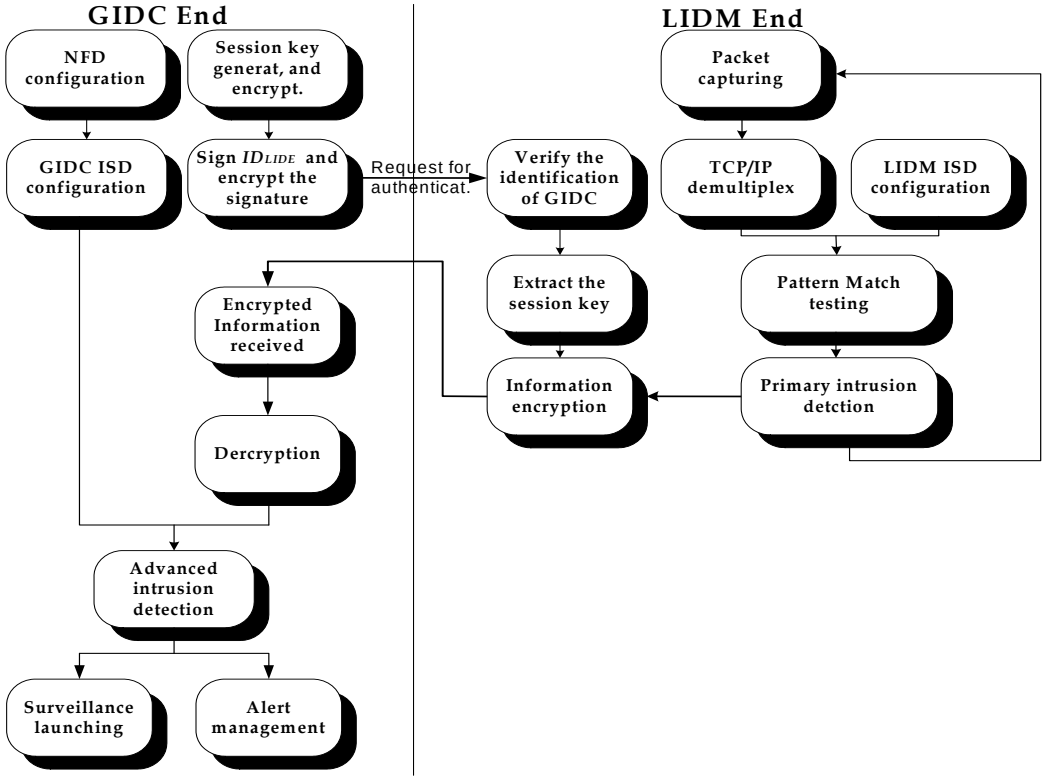

Figure 2. Procedures of the system operation

2.2. Procedures of the SA-NIDS Operation

A block diagram is drawn in Figure 2 to show the procedures of the SA-NIDS operation and each operation is described below:

- Packet Capturing

Some local area network techniques have the broadcast property that the network adapters can be configured and set to run in the promiscuous mode, which allows the adapter to grab all of the packets that it sees on the network segment. The packet capturing capability is the lowest layer function provided by the Packet Catcher in an LIDM. Packet Catcher uses a framework of the low-level network monitoring to provide an interface for user-level network raw data capturing.

- TCP/IP Demultiplexing

After the Packet Catcher capturing the monitoring raw data, it passes the raw data to the Packet Parser. The Packet Parser demultiplexes the raw data from the low-level network protocol to the high layer network protocol and maps the raw data to its corresponding network protocol header and payload information step by step.

- Intrusion Signature Database (ISD) and Network Fact Database (NFD) Configuration

Historically known network intrusions and their scenarios techniques can be regulated to sequences of events. Intrusion signatures are attacking profiles that are descriptions of these sequences of events. The ISD contains lists and collections of these known intrusion signatures. The NSO uses the ISD configurator to update the ISD frequently to reflect the new discovered vulnerabilities or network intrusion techniques. Every LIDM has its own ISD suitable for its own network environment. According to each ISD, the NSO can inference the primary information of the network intrusion of each LAN.

NFD, resides in the GIDC, is the topology and the security information of current network. It contains the network component information and how they are connected each other. Such as the host IP address and netmask, the subnet IP address and netmask, the Internet server location, the server operating system type and so on.

The GIDC also has its ISD suitable for the entire network topology. Different from each LIDM intrusion signature, the GIDC intrusion signature emphasizes the attacking profiles of entire network (composed of several segments of networks). For example, the distributed network attack should be formulated in GIDC intrusion signature for the characteristics that the distributed attack could not be discovered simply by each LIDM.

The NSO uses the NFD configurator to figure and modify the NFD when the topology of the network changed. The same procedures as in each LIDM's ISD configurator, the NSO also uses the ISD configurator to update the ISD to reflect the new discovered vulnerabilities or network intrusion techniques frequently.

- Pattern Matching Intrusion Detection

Each LIDM compares the protocol layer information with the LIDM intrusion signatures to see if some of the lists of the intrusion signature match somewhere in the protocol layer information. If it does, the protocol layer information is forwarded to the GIDC for further pattern matching intrusion detection. If it does not, the protocol layer information is discarded or logged into the LIDM's file system for further analyzing. Some intrusion behaviors can be investigated only by the LIDM. If such intrusion behaviors are discovered in the segment, the information will also be forwarded to the GIDC to generate the alert or do launch the Surveillance process.

The GIDC takes the protocol information received from each LIDM as the input and passes it to the lists of the GIDC intrusion signature to see if some of the lists of the intrusion signatures match somewhere in the protocol layer information. If it does, the protocol layer information is forwarded to the Inference Engine. If it does not, the protocol layer information is discarded or logged into the GIDC's file system for further analyzing.

- Secure Communications

In the proposed SA-NIDS, We would like to establish a secure channel between each LIDM and GIDC, so that the sensitive information will be encrypted. To form a secure channel, the cryptography-based mechanisms such as authentication and identification are applied. Thus no one can eavesdrop the sensitive information during transmission. Also each LIDM needs to verify the identification of the GIDC to prevent others from spoofing the GIDC.

- Inference and Alert Management

After pattern matching is done by LIDM and GIDC, the analyzed protocol layer information will be passed to the Inference Engine. According to the NFD in GIDC, the historical

events and the security knowledge known by NSO, the Inference Engine decides whether the suspicious activity is an intrusion behavior. If it does, GIDC generates some alert and passes the alert to the Alert Manager for the alert information management. The Alert Manager manages the alerts in the file system, and then mails them to the NSO. The alerts also can be sent to the NFD configurator and ISD configurator in GIDC for updating configuration.

- Surveillance Launching

After the Inference Engine discovers some attacks from the outside or inside. Surveillance Launching Agent takes the protocol address of the intruder and the Surveillance functions as input. The Surveillance Agent launching slight network Surveillance such as WHOIS lookup, TCP/UDP service information probing, and the operating system type investigating.

3. Research Method

The reliability and network features are the most important factors for IDS, in the proposed SA-NIDS, the UNIX operating systems are chosen. The SA-NIDS will be developed on Linux (Redhat-6.0), FreeBSD-3.4, and SunOS-5.x/Solaris2.x. However, the SA-NIDS can be easily modified to port to other UNIX systems.

3.1. LIDM Pattern Matching Mechanisms

The LIDM ISD has three main components: the intrusion type, the intrusion header, and the intrusion options. {Intrusion type, Intrusion header, Intrusion option} forms the LIDM intrusion signature. Intrusion type is the categorization of current network intrusion techniques that have been discovered. Now there are six categories of intrusion type. They are information gathering, trivial attempts, buffer overflow, backdoor driving, web probing, and DoS attacking. All network intrusion techniques will be categorized into these six types.

Each intrusion type maintains a two-dimension linked list of logical structure. One dimension is the intrusion header. Each intrusion header handles the other dimension linked lists, the intrusion option. Intrusion header is a list of general packet header information you want to monitor for possible malicious behaviors. There are usually five general intrusion header elements:

- Protocol: The protocol of the packet that will be monitored, such as TCP, UDP or ICMP.
- Source IP address/CIDR block: Source IP address/CIDR block specifies where the possible intrusion from.
- Destination IP address/CIDR block: The destination IP address/CIDR block specifies the possible local targets of network intrusions from the external or internal.
- Source port range: The source port range specifies which port will be the possible intrusions from.
- Destination port range: Destination port range specifies the possible local target port or port range the intruder will attack against.

Each intrusion header handles a linked list of intrusion option. Intrusion option is the more detailed description and information of network intrusion techniques. It contains detailed information of some specific characteristics of malicious behaviors. Intrusion option is the last step to formalize an intrusion technique. The general intrusion option elements are:

- Name and Descriptions of Intrusion: This is the name and descriptions of possible malicious behaviors after specifying the intrusion type and going down the two-dimension linked lists from a specific intrusion header to a specific intrusion option.
- IP header options: Some of the IP header options related to network security for examples are IP_TTL, FSAG_ID, IP_OPT.
- ICMP header options: Some of the ICMP header options related to network security for examples are ICMP_TYPE, ICMP_CODE, ICMP_SEQ.
- TCP header options: Some of the TCP header options related to network security are FLAG, SEQ_NUMBER, ACK_NUMBER.
- Payload options: The specific data may be some ASCII strings for CGI attack or some binary data to overflow the local destination victims.

In the LIDM side, to do the pattern matching intrusion detection, the Packet Parser parsed the network packets, and send to the Primary Inference Engine. The packets are recursively passed to LIDM from the intrusion type, intrusion header to the intrusion option step

by step. If somewhere in the packets match all information indicated in a specific intrusion signature, the packets will be considered as the suspicious or malicious, and transfer the packets to GIDC for further analyzing or alert generating.

3.2. GIDC Pattern Matching Mechanisms

The GIDC ISD also contains three components: the conventional intrusion type, the header/option information, and the header/option thresholds. {Conventional intrusion type, Header/Option information, Header/Option threshold} forms the GIDC intrusion signature. The conventional intrusion types indicated some intrusion types (in LIDM intrusion signature), which can be extended to the distributed intrusion techniques. Each conventional intrusion type has a two-dimensional linked list. One dimension is the header/option information and each of these handles the other linked list, the header/option threshold.

Each conventional intrusion type handles another linked list, header/option information. The header information is similar to the intrusion header specified in the LIDM ISD. The option information is similar to the intrusion option specified in the LIDM ISD. The main difference between the LIDM ISD's intrusion header/information and the GIDC ISD's header/option information is that the header/option information in GIDC ISD is almost designed for the entire network. The detailed information about header/option information can be found in the section 3.

Each header/option information handles the other linked list, header/option threshold. The header/option threshold specifies some statistical characteristic about a specific distributed network intrusion. These characteristics are represented in some kind of the threshold value of specific network packet (header or option) information. If the collections or sets of packets have some network packet information that reach the threshold value, the Inference Engine will regard them as the malicious packets. Some network packet information about distributed network attacks and its threshold are used in the SA-NIDS, they are Distribution of source IP addresses, Distribution of destination IP addresses, Source port ranges, Destination port ranges, Time statistics, and Other statistics.

In the GIDC side, to do the pattern matching intrusion detection, the packets received from the Information Receiver are passed to the GIDC intrusion signature. If somewhere in the information matches the last two sets of intrusion signature (the header/option information and the header/option statistics), the Inference Engine will regard the packet as a malicious packet and view the suspicious activity as the malicious behavior. Then the packet is sent to the Alert Manager to do some responsive activity.

3.3. Surveillance Techniques

To achieve the Surveillance techniques, the NMAP program [11] is employed into the Surveillance Agent of the SA-NIDS as optional functions. The Surveillance techniques currently have two sets of functions, the Surveillance launching functions and the Surveillance functions. The Surveillance launching functions will take malicious packets' source IP/CIDR block and source port ranges as the input and specifies the Surveillance type that wishes to scan the source host or network. After specifying the type, the Surveillance Launching Agent chooses corresponding Surveillance functions to do the actual information gathering. The more detailed information about the Surveillance techniques can be found in most TCP/IP Network textbooks [12].

4. Results and Analysis

In this section, we will apply the SA-NIDS to our campus network to simulate the real attack scenarios and intrusion detection processes. For the security considerations, we restrict the whole experiment network structure to the campus network in Naval Engineering University (NEU). The offensive/defensive experiment network can be seen in Figure 3.

In the defensive side, we construct the defensive network includes one GIDC, GIDC-EE in NEU E.E. network and three LIDMs, LIDM-EE, LIDM-DOR, and LIDM-CC distributed in NEU E.E. Network, NEU dormitory network, and NEU Computer Center network. In the other side, we construct the offensive network in NEU and one attacker host in TianJin School (NETS). Attacker-1 is in the NEU dormitory network, Attacker-2 and Attacker-3 are in the NEU E.E. network, and Attacker-4 is in the NETS network. The simulated attack utilities we used are

Nessus vulnerability assessment tool [13], SATAN vulnerability assessment tool [14], Nmap port scanner [11], and SIP DDoS tools [15]. All of their operating system is the UNIX clone. The experiment network is shown in Figure 3.

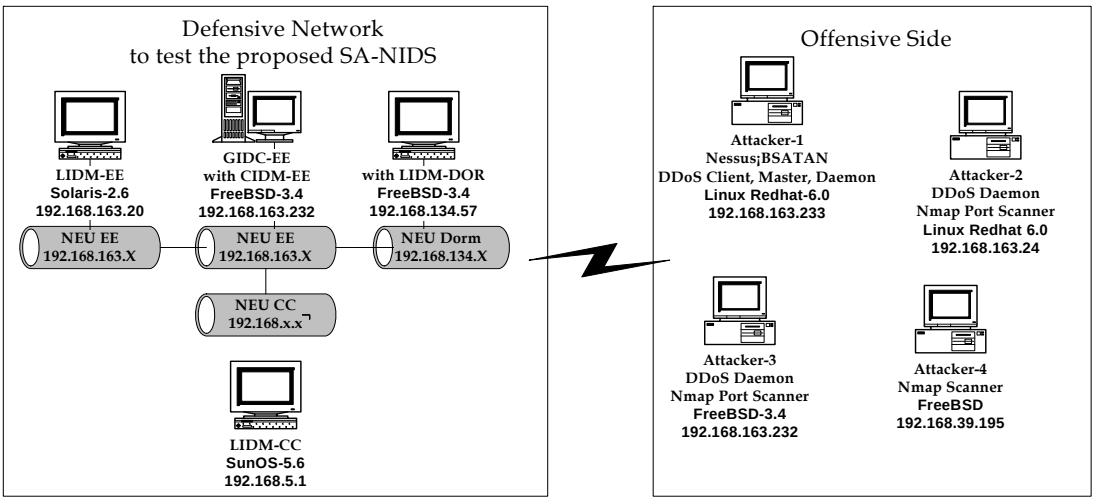

Figure 3. Experiment offensive/defensive network to test the proposed SA-NIDS

We have categorized the network intrusions into six types that are the trivial attempts, buffer overflow attack, information gathering, backdoor driving, web probing and the DoS attack [16]. To be suitable for our SA-NIDS distributed intrusion detection architecture, we can further define some subsets in these six categories. We define the trivial attempt, buffer overflow, backdoor driving and the web probing attacks as the deterministic network intrusions and then define the information gathering and the DoS attacks as the ambiguous network intrusions. The deterministic network intrusions can be detected simply via the primary pattern matching mechanisms in the LIDM side. For the deterministic network intrusions, the GIDC only need to receive the intrusion detection results from the LIDMs and then generates the alert. For the ambiguous attacks, it is not enough to do the primary pattern matching intrusion detection in the LIDM side. The LIDMs have to further pass the suspicious packets to the GIDC side for advanced pattern matching detection or statistical techniques applied. Then the GIDC generates and manages the alert after the advanced intrusion detection for the ambiguous network intrusion detection done.

4.1. Examples of the Deterministic Intrusions

To launch the deterministic attacks in the offensive side, the Attacker-1 is chosen to launch the deterministic attacks to one of the hosts in the defensive network and install a set of widely spread vulnerability tools, e.g., Nessus and SATAN. To detect these deterministic attacks, we first construct the LIDM intrusion detection signature in the ISD. All the packets received by the LIDM will be recursive parsed to the signatures to do the primary pattern matching intrusion detection. Thus, based on the assumption of all the malicious packets can be captured by the LIDMs' Packet Catcher, if the deterministic network intrusions launched by Nessus and SATAN can be formulated into the signatures, we can detect these intrusions and obtain the IP address of attacker. We further optionally specify the Surveillance options to determine the properties of Attacker-1. The TCP/UDP ports opened by him are all be detected and we can correctly guess its operating system type.

4.2. Examples of the Ambiguous Intrusions

We take the information gathering attack as the example. In this section, we do the ambiguous network intrusions detection in the same architecture shown in Figure 3. In the offensive side, we choose Attacker-2, Attacker-3 and Attacker-4 to do the port scanning against

a host, a group of hosts, or an entire subnet of the defensive network. We use the excellent public-domain information gathering tools NMAP to do the real attack.

According to the various kinds of scan techniques, we construct the LIDM intrusion signatures with the same step as we did in the detection example of the deterministic intrusions for logging large suspicious packets in the LIDM end.

In the GIDC side, we receive all the suspicious packets captured by LIDMs. The most important GIDC intrusion signatures about the information gathering attacks are the threshold of the number of the intended connection to the same destination, threshold of the number of packet to the same destination, threshold of time interval and the threshold of the time duration. To detect the various port scanning techniques, we simply define the GIDC intrusion signature as a rule. This rule specifies the statistical thresholds to infer whether the suspicious packets are malicious. When attackers launch the NMAP process, they will be detected.

4.3. Detection Rate of SA-NIDS

A basic way to evaluate the performance of IDS is the detection rate. To test the detection rate of the SA-NIDS, the Nessus software is employed as an attacker to perform attack activities. According to the functions in the Nessus, we divided attack types that already included in the SA-NIDS into eight categories and collected the detection rate from the offensive/defensive experiment network. The detection rate is shown in Table 1.

Table 1. The Detection Rate of SA-NIDS

Categories	No. of Attack	No. of Detection	Detection Rate
Backdoors	26	16	61.54%
CGI abuses	128	75	58.59%
Firewalls	8	5	62.50%
FTP	25	19	76.00%
General	23	13	56.52%
Misc.	17	9	52.94%
NIS	2	1	50.00%
Remote file access	23	8	34.78%
Overall	252	146	57.94%

We can see from the Table 1, the top detection rate (76%) is on FTP attacks and the overall detection rate is 57.94%. The detection rate is dependent on the intrusion patterns in the ISD. To improve the performance of the SA-NIDS, we may add more intrusion patterns into the ISD to increase the detection rate.

5. Conclusion

In this paper, we integrate the rule-based detection algorithm and the statistical anomaly detection approach into the proposed SA-NIDS that is based on the network-based intrusion detection architecture. It includes three basic components, Local Intrusion Detection Monitor (LIDM), Global Intrusion Detection Controller (GIDC), and Surveillance Agent (SA). These three components cooperate with each other to achieve intrusion detection, intrusion inferring and attacking Surveillance.

For effectiveness, more precise intrusion detection mechanisms should be developed to reduce the system false alarm. For efficiency, the IDSs should work in ways that do not affect the computer system performance too much. The proposed SA-NIDS still has many features that can be improved such as applying more precise intrusion detection mechanism to reduce the false alarm. Many implementation details still needed to be completed, such as cryptography features. More user friendly configuration of the intrusion signature database and the network fact database is needed. The user interface should be improved so that the SA-NIDS is practically applied in current network architectures by the NSO.

A successful intrusion detection system depends on several parameters, such as efficiency, effectiveness, flexibility, security, transparency and so on. The future works include improving the performance of RD-NIIDS, developing anomaly detection models, intrusion types collection, and heterogeneous IDS integration.

References

[1] Meera G, Srivatsa SK. Detecting and preventing attacks using network intrusion detection systems. *International Journal of Computer Science and Security*. 2011; 2(1): 49-60.

[2] Tartakovsky AG, Polunchenko AS, Sokolov G. Efficient Computer Network Anomaly Detection by Changepoint Detection Methods. *IEEE Journal of Selected Topics in Signal Processing*. 2013; 7(1): 4-11.

[3] Horasani Zadeh HK, Idris NB. *Distributed Intrusion Detection trust management through integrity and expertise evaluation*. Proceeding(s) of 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). Kuala Lumpur. 2012; 1: 133-138.

[4] Saeid AT, Behzad ZD, Ahmad H, Behzad B. Synthetic Feature Transformation with RBF neural network to improve the Intrusion Detection System Accuracy and Decrease Computational Costs. *International Journal of Information and Network Security*. 2012; 1(1): 28-36.

[5] Thuzar. Feature Selection and Fuzzy Decision Tree for Network Intrusion Detection. *International Journal of Informatics and Communication Technology*. 2012; 1(2): 109-118.

[6] Liang Z, Xiao-Hui Z. *Research on Reconfigurable Intrusion Detection System*. Proceeding(s) of 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES). Nanjing. 2012; 1: 913-917.

[7] Francois J, Aib I, Boutaba R. FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. *IEEE/ACM Transactions on Networking*. 2012; 20(6): 1828-1841.

[8] Haque MJ, Magld KW, Hundewale N. *An intelligent approach for Intrusion Detection based on data mining techniques*. Proceeding(s) of 2012 International Conference on Multimedia Computing and Systems (ICMCS). Morocco. 2012; 1: 12-16.

[9] Kunlun G, Jianming L, Jian G, Rui A. *Study on data acquisition solution of network security monitoring system*. Proceeding(s) of 2010 IEEE International Conference on Information Theory and Information Security (ICITIS). Beijing. 2010; 1: 674-677.

[10] Zaman S, Karray FT. *Collaborative architecture for distributed intrusion detection system*. Proceeding(s) of IEEE Symposium on Computational Intelligence for Security and Defense Applications. Ottawa. 2009; 1: 1-6.

[11] Kocher JE, Gilliam DP. *Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning*. Proceeding(s) of 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise. Linkoping. 2005; 1: 139-143.

[12] Barry BIA, Chan HA. *A Cross-protocol approach to detect TCP Hijacking attacks*. Proceeding(s) of IEEE International Conference on Signal Processing and Communications. Dubai. 2007; 1: 57-60.

[13] Chao D, Danfeng Y, Yun Y, Fangchun Y. *A domain-oriented distributed vulnerability scanning mechanism*. Proceeding(s) of 2nd IEEE International Conference on Broadband Network & Multimedia Technology(IC-BNMT '09). Beijing. 2009; 1: 831-836.

[14] IváN Arce. Vulnerabilities: Vulnerability management at the crossroads. *Journal of Network Security*. 2008; 20(5): 11-13.

[15] Stanek J, Kencl L. *SIPp-DD: SIP DDoS Flood-Attack Simulation Tool*. Proceedings of the 20th International Conference on Computer Communications and Networks (ICCCN), Hawaii. 2011; 1: 1-7.

[16] Meixing L, Stavrou A, Kang BB, DoubleGuard: Detecting Intrusions in Multitier Web Applications. *IEEE Transactions on Dependable and Secure Computing*. 2012; 9(4): 512-525.