IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. IV (Nov.-Dec. 2016), PP 115-121
www.iosrjournals.org

Intrusion Detection System in Network Forensic Analysis and Investigation

Hariyanto[1], Andysah Putera Utama Siahaan[2]
Faculty of Computer Science Universitas Pembangunan Panca Budi
[1,2]Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia

Abstract: *Intrusion Detection System is built to protect the network from threats of hackers, crackers and security experts from the possibility of action that does not comply with the law. Problems arise when new attacks emerge in a relatively fast so that a network administrator must create their signature and stay updated with new types of attacks that appear. IDS would oversee the packets in the network and benchmark against only those packages with a signature database that is owned by IDS systems or attributes of the attempted attacks ever known. By using IDS, network security will be more secure. Network administrators will be easier to know if network conditions change.*

Keywords: *Network Forensic, Intrusion Detection System*

I. Introduction

Computer technologies increase the computer capabilities [1][3]. The advantage is used by hacker to steal information from the network. Consequently, many third parties loss suffered as a result of abuse or crime using networks to billions of dollars annually. Attacks on network throughout the world such as viruses, worms, spam and DoS increased regarding both quantity and quality. These are categorized in cyber crime.

Many tools occupied such as antivirus protection, firewalls and Intrusion Detection Systems (IDS) has been widely used by private users and companies, but offenders are also more intelligent and sophisticated in conducting its activities [4][5][6]. On the other hand, the inability to identify and deal with offenders quickly become another weak point. Most network administrators realized their attacks against computer/network shortly after the incident took place. At that time, the evidence needed to perform loss prevention have disappeared or changed by the offender; the system administrator did not know many of the attacks.

When a safety mechanism failed to address and identify the attack quickly, it needs a complement to the security system that can monitor, capture and store digital evidence so that it can be seen how, why and when the attack occurred. Therefore we need a mechanism so that the network forensic evidence needed for further analysis is not lost or altered.

II. Theories

A. *Network Forensic*

Network Forensic is a method of capturing, storing and analyzing data network usage to find the source of a security breach or system of information security issues. The main focus of network forensics is to identify all the possible causes of security breaches and make detection and prevention mechanisms to minimize losses [1].

The network administrator can not entirely rely on IDS to maintain its network. Administrators also need a process of investigation and audit tool to investigate the incident fully and restore the network from threats or attacks [2]. The forensic network can reconstruct the scene in a system that stores all data traffic activity on the network so that investigations can be done by looking back over the events that have occurred and analyze events that occurred in the past. Based on the above requirements, then a system of network forensics at least there are some processes, such as:

1. Monitoring and data collection: Network forensics is an audit of network usage, such as traffic, bandwidth, and data content. Therefore any network forensic system required monitoring and data storage systems that can be used as digital evidence.
2. Analysis of the data content: of all the stored data, not all of them are a threat to the security of the system, so that the necessary data analysis can detect which data are disturbing the security of the system. It also deals with issues of privacy, because the data are analyzed may constitute personal data, necessitating policy regarding this issue.
3. Source traceback: for the prevention of the possibility of attacks against network security system that will come the necessary methods to determine the source of the attack, so as to minimize similar occurrences in the future.

B. Intrusion Detection System

Intrusion Detection System is a system of monitoring the network traffic and suspicious activity in a network system [7]. If found suspicious activities related to network traffic, the IDS will alert the system or network administrator. In many cases, IDS also respond to traffic that is not normal/anomaly by blocking the action of a user or IP address [9]. IDS appeared with several types and a different approach that mostly serves to detect suspicious traffic within a network. Some types of IDS are network-based (NIDS) and host-based (HIDS).

There is an IDS that works by detecting the search based on the particular characteristics of the trials are often performed. This method is similar to how the antivirus software to identify and protect the system against threats [10]. There is also the IDS that works by detecting based on a comparison of average traffic patterns that exist and then look for abnormalities of existing traffic.

III. Proposed Work

A. Data Monitoring

There are several steps to do a forensic process. It is A network forensics system always can monitor, capture and store all data traffic on the network. Systems connected to the Internet network is potential for attack. Therefore, it is necessary for applying a mechanism to monitor and detect attacks against the network using Intrusion Detection System. IDS is a tool that can collect information, analyze information on whether there is a strange activity on the network and report the results of the analysis of the detection process.

Intrusion detection techniques can be categorized into two kinds. The first is based on the signature-based detection. Signature-based detection using the example of the pattern of attacks that have saved previously to identify attacks. The second is the anomaly detection; it determines whether the deviation from normal usage patterns can be categorized as an intrusion.

Network forensics system is also equipped with a data storage unit to allow a process of analysis and investigation of the data collected previously in the event of a threat or attack against a security system. To collect data from the network to use a packet sniffer. The working principle of packet sniffer is intercepting every piece of data that passes through the network and make a copy for analysis. It requires a storage unit that is not a bit, along with the high level of use of the network and the larger the data traffic on the network, the greater the deposit required. Fortunately with the cheapening of the data storage device, then the cost is also a system of network forensics.

B. Data Analysis

Network forensics allows the process of analysis and investigation of data that have been stored previously. There are several sources of potential evidence that could be used for computer and network forensics. The file is one source of potential evidence. The output of applications such as word processors, spreadsheets, and others can store historical information, caches, backups or log activity. On the other hand, network activity may store some valuable information in revealing the occurrence of threats or network attacks. Network activity that can reveal criminal acts recorded in great detail compared to other sources.

Therefore the system log is a vital source of potential evidence. A company or organization should store information about all network activities such as login using the computer and network services such as remote Telnet or FTP. It is very useful in the investigation because the tape can store a variety of information about the activities of a particular user, such as the event date and time. It is related to internal events such as email and web access or external events that may indicate the timing of these activities (timeline). Timeline serves as a reference for the different events put in a system and connects to an allegation, makes an alibi and determine the independent crime evidence.

From the analysis of the data packets are stored can be obtained some information, such as:

- Information about the files being transferred to and from the target.
- The order was given on target
- Information about the activity time (timeline)
- The output generated by the command given
- Proof of packet scanning program that is hidden on the local computer network.

C. Traceback

The process of data analysis can reveal when and how the occurrence of an event of an attack or a threat to the network. An administrator or investigator may take anticipatory measures and improvement of network security systems to secure recovery process can take place correctly and quickly and for preventive measures from the threat or impending attack so as to minimize losses suffered.

A solution is needed that can be taken a step in the prevention of similar events. The way is to find out the cause of a misuse or disruption of network security systems. Traceback is used as the solution of the problems of disturbances of security systems such as DoS. There are two kinds of tracing approaches on the network. The first is an IP traceback and the second is the traceback across the stepping-stones (connection chain).

To understand the tracing method requires a basic knowledge of routing technology. Routing is a process of moving information between networks from source to destination. Routing involves two basic activities that determine the optimal path routingdan missed packets between networks. Protocols such as Border Gateway Protocol (BGP) and Routing information Protocol (RIP) use metrics to evaluate the best path for the package.

Here are some of the metrics used in the process of determining the path by a routing protocol:

- The length of the line: the number of hops that must be passed packets from source to destination.
- The cost of communications.
- Delay: the time required to move a packet from source to destination.
- Bandwidth: the amount of data traffic that can pass through a lane.
- Load: the level of use of network resources.
- The reliability: the level of reliability of a network such as how often the link is broken or how long link is dropping out can be improved.

Traceback expected to be determined the path of intrusion or even find the source of the attack to be used as the first step of legal action. There are several traceback methods have been developed from the earlier attacks.

ICMP Traceback

Traceback messages are carried on ICMP packets, the value of this part is determined by the IANA (Internet Assigned Numbers Authority). CODE section is set to a value of 0 and is not processed by the receiver. Figure 1 and 2 describe the ICMP Traceback messages.

TYPE
CODE
CHECKSUM

Fig. 1 ICMP Traceback Messages

Parts of the body consists of individual elements using the LENGTH TAG-VALUE (TLV).

TAG
LENGTH
VALUE

Fig. 2 ICMP Traceback body

TAG is a single octet, with values as follows: Back Link, Forward Link, Timestamp, Traced Packet Contents, Probability, RouterId, HMAC Authentication and Key Data Disclosure List. Forward and Back Link function is to facilitate the establishment of a chain of messages traceback. There her identification information and the value of this part consists of three subelemen TLV: Interface Identifier, IPv4 Address and MAC Address Pair Pair or Operator-Defined Link Identifier.

To the message can not be forged, it is necessary HMAC Authentication Data. At Key Disclosure List are key hash algorithms. This element must contain at least one sub-element Key Disclosure and the Public Key Information sub-element. The main contents of the Key Disclosure element is a key for message authentication previous traceback and start and end times when the key is used. On Disclosure Key elements there is also a digital signature. The complete illustration can be seen in Figure 3.

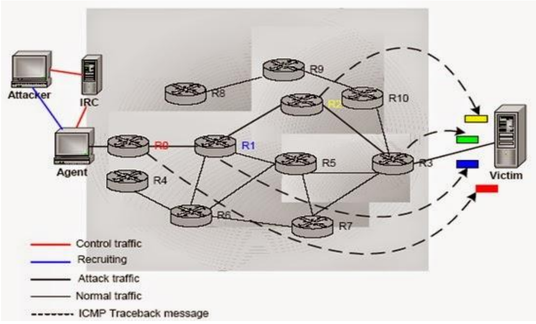

Fig. 3 ICMP Traceback scheme

Intention-Driven ICMP Traceback

Intention-Driven ICMP Traceback adds extra bits on routing and forwarding processes that can improve the performance of iTrace previously. I-D iTrace separates the functions of iTrace into two modules, decision and iTrace generation module. Decision module determines the type of message that iTrace should generate. Based on this rule, a particular bit in the packet-forwarding tables will be set to 1 and the next data packet forwarding using the input will be selected as the message iTrace. It will then be processed by iTrace generation module and a new iTrace message will be sent. The architecture is shown in Figure 4.

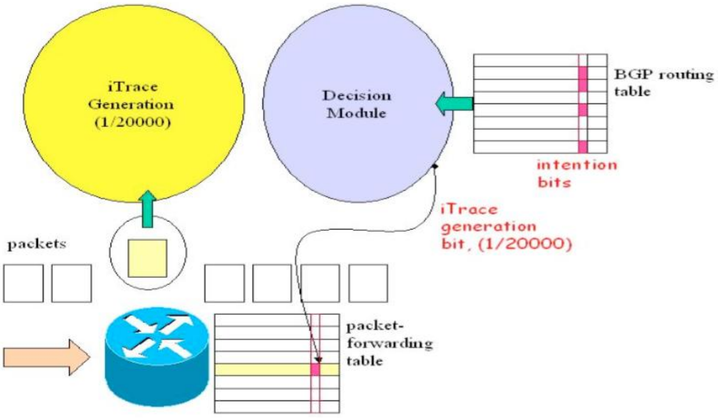

Fig. 4 Architecture of Intention-Driven iTrace

Center Track

Center Track is composed of a network overlay IP tunnel that is used selectively routing datagrams back directly from the outer edge router to the special router tracking. IP tunnel can be created on an IP network is available. Input debugging is a diagnostic feature that will show the previous hop when the attack comes from or through the hop. Created dynamic routing traffic causes only towards the victims are in the routing through the overlay network. Tracking is performed by starting on the router closest to the victim and then do the hop-by-hop. The complete illustration can be seen in Figure 5.

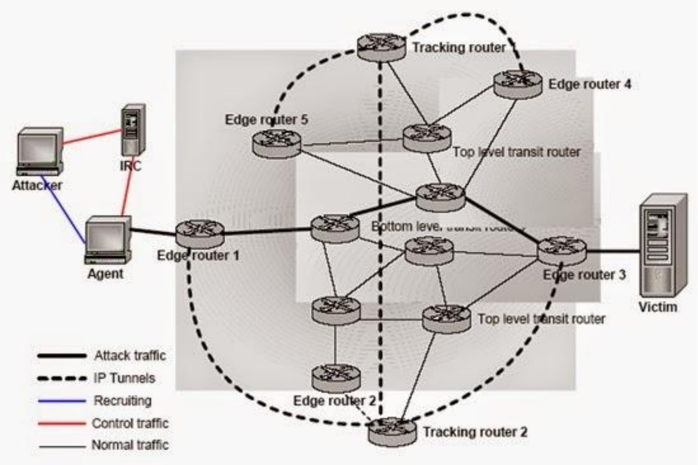

Fig. 5 Center Track scheme

Sleepy Watermark Tracing

Sleepy Watermark Tracing (SWT) was developed to conduct traceback using the principle chain relationships. This method can be used to trace the attack when the attacker using a computer controlled remote as the slave machine. SWT architecture consists of two parts; SWT guarded host and SWT guarded gateway. IDS and watermark-enabled applications on the SWT guarded host used as a supporting component. IDS serves as the initiator of SWT tracing. IDS interact with SWT subsystems through the SWT guarded host and triggers a watermark tracing when the intrusion is detected. Figure 6 illustrates the architecture of Sleepy Watermark Tracing.

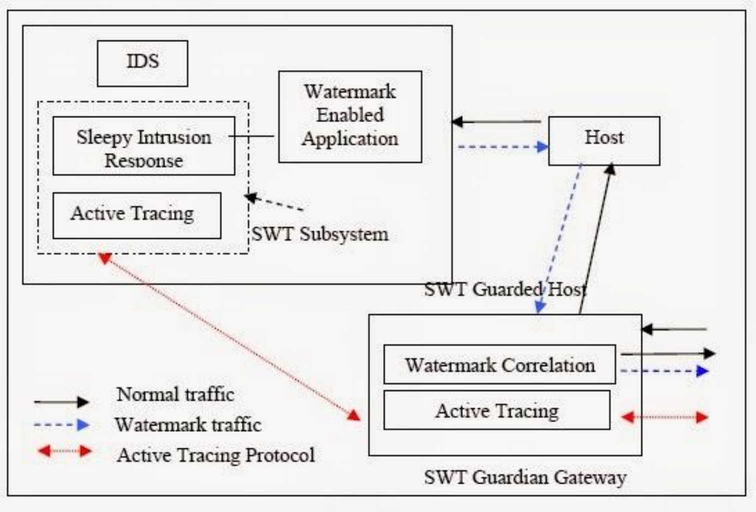

Fig. 6 Architecture of SWT

SWT system is not active in normal state. When IDS detects intrusion, IDS will notify the triggers SWT manner SIR wear connection information. On request IDS, SIR will first activate intrusion connections for a specific time period. SIR will then triggers active tracing at the guardian gateway by sending notifications trace. Finally, SIR notify applications enabled for injecting watermark WM requested. SIR also keep track of information tracing intrusion by returning to SWT guardian gateway, and IDS when requesting this information, SIR will provide the information needed.

If a certain period there was no trace information is returned to the gateway or guardian SWT no further notification from IDS, then the intrusion response component will back off. Injection watermark will only happen if there are intrusion detection and network applications only intruders would receive a response watermark.The complete illustration of Sleepy Watermark Tracing is described in Figure 7.

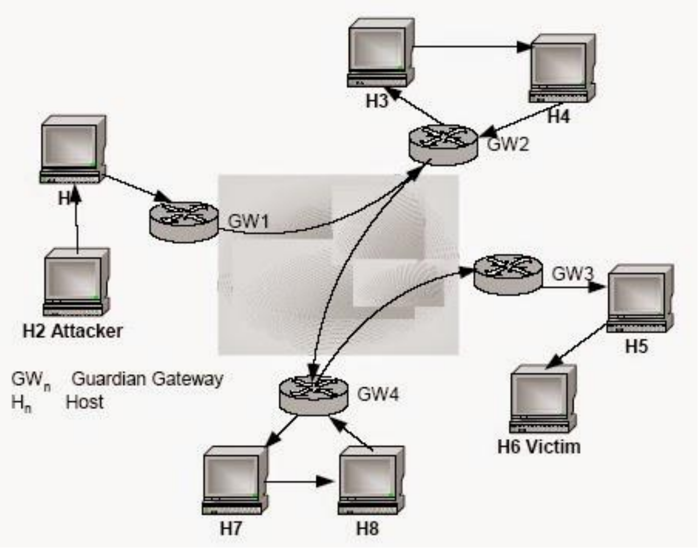

Fig. 7 Guardian Gateway and Guardian Host

IV. Implementation

The application of IDS in the real world is by implementing IDS system that is open source and free. For example, SNORT. It is available in a variety of platforms and operating systems including Linux and Windows. It has a lot of users on the network for a free; it is also equipped with a support system on the internet so that it can be done updating existing signature; it can detect the latest attack types on the Internet. IDS cannot work alone if it is used to secure a network. IDS should be utilized in conjunction with a firewall. There is a distinct line of demarcation between the firewall and IDS.

A. Bottleneck

Theorically, a network forensics system is easy to implement, in practice many obstacles in building a network forensics system. There are at least two kinds of obstacles in building a system that is network forensics technical and socio-economic.

Data Collection

It is an addition to network forensics system has a function to monitor network activity should also be able to collect all the data passing through the network. Data were collected and saved may be used to conduct an investigation if there is an attack or threat, and the results of those investigations can also be used as digital evidence if it would be conducted legal measures as a result of the implications of an attack or a threat to the network. Additionally, it will also have problems with the increasing data traffic on the network, consequently needed a data storage system that can accommodate the data if it happens.

Data Retention

Data collected possibility should be maintained or stored for a considerable period of time. It is an effect on the amount of data that can be accommodated by the system network forensics. Therefore we need a data management can reduce the amount of data stored without loss of valuable forensic information.

Data Retrieval

During the treatment, the investigation or analysis system should be able to determine the location of the data required in the wide area network. As mentioned earlier, the data stored in the system forensics can be very large in number. Therefore we need a protocol to determine the location of the necessary data quickly.

Privacy

Surveillance network with user privacy will always be the opposite. It is due to the system overall forensic examination is required of a system that can make the user uncomfortable. The solution is to investigate all the traffic data, but only store information that is necessary for forensic only. This is possible because of the processing speed of today's computers faster than the speed of storing data. By doing so, the storage of information that is very personal and less valuable to forensic system can be reduced.

Economy

The development of a judicial system also depends on the profit from the service provider. It will greatly affect the price of a legal system. Forensic system is also very useful in reducing the level of threats and attacks against the organization or company network, so as to reduce the losses suffered as a result of the threat.

B. Development

There are some network forensics systems were developed either for commercial or academic purposes. NIKSUN's NetVCR and NetIntercept are several commercial systems sold in the market and is quite widely used in enterprises today. As for research purposes, there are several free methodologies such as ForNet and Honeytraps. In other words, there is currently no standard value for a system of network forensics. Therefore, it is also required an effort to standardize the system of network forensics.

C. Network Forensics Tools

Network forensics tool is the application used for the forensic experts who used to do things related to forensic such as monitoring and audit on the network. Toolkit for forensic testing allows investigators to gather and analyze data such as E-Detective, NetFlow v5 / 9, netcat, NetDetector, tcpdump, Wireshark / Ethereal, Argus, NFR, TCPWrapper, sniffer, nstat, and tripwire.

Some examples of network forensic tools:

1. Wireshark

An analyzer and monitoring network that is popular. The features in Wireshark, such as:

- Can checks for hundreds of protocols in depth
- Able to capture direct and analyzed offline
- Multi platform can run on Windows, Linux, Mac OS X, Solaris, FreeBSD, NetBSD, and others.
- Data networks have been captured can be displayed via the GUI or via the TTY-mode.
- Can filter the view with many filter options.
- Can read and store different formats.

2. Netcat

It is a utility tool that is used for a wide range of issues related to TCP or UDP protocol. That can open TCP connections, sending UDP packets, listen on the TCP and UDP port -Port, scanning ports, and by IPV4 and IPV6. This Netcat typically used by hackers to connect back to the target system so that hackers gain root access through the port that has been set by the hacker.

3. E-Detective

It is an interception system that makes the process of the Internet in real-time, monitoring and forensics systems that capture, code reading, and restore some types of Internet traffic. These systems are typically used in corporate Internet and monitor behavior, audit, storage of records, forensic analysis, and investigations. E-Detective can read the code, reassembly, and recover various types of Internet Applications and services this example, Email, Webmail, Instant Messaging, File Transfer, Online Games, Telnet, HTTP, VOIP, and others.

V. Conclusion

Crimes involving network weaknesses often happen anywhere. Computer system security using firewalls and IDS is now no longer sufficient, so that the necessary forensic capability in network security system implementation. Firewalls can be deceived by a virus or hacker attack on the system. Network forensics will conduct further searches of the system that has been disturbed. There will be a trade-off between the forensic system with privacy therefore we need a policy of legal system that will be used by a company or organization. Forensic system that is currently used methodology and system development approach that is different so the need for standardization efforts within the system network forensics. With network forensic, system leaks will be more easily addressed.

References

[1]. B. Ruchandani, M. Kumar, A. Kumar, K. Kumari dan A. Sinha, “Experimentation In Network Forensics Analysis,” dalam Proceedings of the Term Paper Series under CDACCNIE, Bangalore, India, 2006.

[2]. A. Lubis dan A. P. U. Siahaan, “WLAN Penetration Examination of The University of Pembangunan Panca Budi,” International Journal of Engineering Trends and Technology, vol. 37, no. 3, pp. 165 - 168, 2016.

[3]. N. Meghanathan, S. R. Allam dan L. A. Moore, “Tools and Techniques for Network,” International Journal of Network Security & Its Applications, vol. 1, no. 1, pp. 14-25, 2009.

[4]. B.-H. Kang, “A Generic Framework for Network Forensics,” International Journal of Computer Applications, vol. 1, no. 11, pp. 1-6, 2010.

[5]. M. Cohen, “An Advanced Network Forensic Framework,” dalam The Digital Forensic Research Conference, USA, 2008.

[6]. M. T., B. B., B. T. M., R. Rajaram dan B. V. K., “Network Forensic Investigation of HTTPS Protocol,” International Journal of Modern Engineering Research, vol. 3, no. 5, pp. 3096-3106, 2013.

[7]. I. Riadi, J. E. Istiyanto, A. Ashari dan Subanar, “Log Analysis Techniques using Clustering in Network Forensics,” International Journal of Computer Science and Information Security, vol. 10, no. 7, 2012.

[8]. V. Das, V. Pathak, S. Sharma, Sreevathsan, S.Srikanth dan G. K. T., “Network Intrusion Detection System Based On Machine Learning Algorithms,” International Journal of Computer Science & Information Technology, vol. 2, no. 6, pp. 138-151, 2010.

[9]. D. Stiawan, A. H. Abdullah dan M. Y. Idris, “Characterizing Network Intrusion Prevention System,” International Journal of Computer Applications, vol. 14, no. 1, pp. 11-18, 2011.

[10]. N. Deb, M. Chakraborty dan N. Chaki, “The Evolution of Ids Solutions in Wireless Ad-Hoc Networks to Wireless Mesh Networks,” International Journal of Network Security & Its Applications, vol. 3, no. 6, pp. 39-58, 2011.