International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-6 December-2012

A Review of Network Forensics Techniques for the Analysis of Web Based Attack

Sudhakar Parate[1], S. M. Nirkhi[2]
M.Tech Scholar[1], Asst. Professor[2]
Department of Computer Science and Engineering, G.H. Raisoni College of Engineering, Nagpur, India

Abstract

Network forensics has been the most prevalent technology to investigate different attack. It used for troubleshooting connection issues and helping to solve various network security problems, such as system log, router log, and access control. Network Forensic help to identify the evidences of data source as intermediate side and the end sides. This paper gives comprehensive review on various techniques that helps to improve the system, analysis of different attack, detection of attack. It focuses on the critical stages of preservation and acquisition of digital evidence from the different source to be used as evidence for aiding investigation.

Keywords

Evidence, Network Forensics, Log Files, Forensic Process, Analysis.

1. Introduction

The Network Forensics is scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence. In year 1987, “Dorothy Denning” was proposed an intrusion detection model which became a sign in the research area. In 1990, the network forensics issue was discuss by security expert “Marcus Ranum” and he defined capture, recording and analysis [4][5]. The first digital forensics research workshop was held in 2001 regarding the uncovering facts related to the planned intent, or measured success of unauthorized activities and recovering activities. DFRW came up with a framework which is involves the identification, preservation, collection, examination, analysis, presentation and decision. This framework is the basis for all the proposed models that is followed till date.

In year 2002, “Reith, Carr” and “Gunsch” was proposed a model called an abstract digital forensic model which is based on the DFRW model, where the key components of the model are involved in nine stages. There is no easy or obvious method for testing the model and that each of subcategory added to the model will make it even more effective [16][24]. “McGrath” and “Nelson” (2006) interpret network forensics and enable collection of the evidentiary data using non-intrusive network traffic record system [7]. In the early days network forensics used for the troubleshooting connection issue and it also help to solve various network security problem. For example fail router, a leaky firewall or insecure database [5]. The four types of evidences are extracted in computer hacking forensics investigator, which are authentication logs, application logs, operation system logs and network device logs. Hackers may falsify or delete the log for making attacking trajectory. If the vulnerability is detected then website will be hacked by attackers and they capture all the valuable information [3][8].

The model proposed by “Freiling” and “Schwittay” in 2007, both are for the incident response and computer forensic processes which allowed a management oriented approach in the digital investigations, while retaining the possibility of a rigorous and forensic investigation [14]. In year 2008 [28] was identifies the five categories of computer forensics research are framework, trustworthiness, computer forensics in networked environment, data detection acquisition and the last category as recovery. The goal of the recovery and detection is stated as to recognize the digital objects which may contain information about the incident and document them.

There are many ways to prevent these attacks and some systems available to detect these attacks [2]. To find the root cause of the attack and investigate in depth, once an attack occurs. Therefore concept of Network Forensics occurs. Network forensic helps tries to analyse traffic data logged through firewalls or intrusion detection system or at network devices like routers and switches. A forensics investigation requires the use of disciplined investigative techniques to discover and analyse traces of evidence left behind after a committed crime [3][6] . The other forensic sciences, Internet forensics begin by collecting a large number of intensely diverse variables or attributes, and culminate in pattern matching among these variables in order to individualize evidence [8].

As we have seen that the network threats are increasing gradually with the passing of time. Therefore securing the network resources is a big issue. The intrusion detection systems can be classified into following three categories as host based, network based and vulnerability assessment based[12][13]. A host based intrusion detection system evaluates information which is found on a single or multiple host systems, which including contents of operating systems, and application files. While network based IDS used to evaluate information which is captured from network communications and analysing the stream of packets travelling across the network. The vulnerability assessment based IDS is also used to detects vulnerabilities on internal networks and firewall [22]. Network forensics result in linking heterogeneous data sets pertaining to activities, oftentimes occurring across multiple social and the business environment, and correlating digital traces contained among different data sources, such as Web pages, computer logs, Internet newsgroups, online chat rooms [26].

Web based attacks

The web based attack is a kind of attack on a website or web-based service. The hackers can exploit the vulnerabilities of website to take advantage or gain access to private information or system resources. Web applications need defence-in-depth approach to avoid and mitigate security vulnerabilities [2]. These approaches consider that every security precaution can fail, therefore security depends on having several layers of mechanisms that cover the failures of each other. To reduce the probability of successful attacks it is necessary to introduce adequate security precautions. To achieving this goal is only possible by using various techniques and tools to ensure security in all phases [1].

2. Related Works

The network forensic investigation of digital evidence is predominantly employed as a post incident response to an activity that cannot be defined definitely as to an incident or legal that is not comply to the organizational norms and policies [18]. There are some existing techniques which is used to perform the network forensics techniques. These techniques help to detect attack which is explained below.

2.1 Intrusion Detection Systems

Intrusion detection systems are used to detect intrusions i.e. malicious attacks or abnormal behaviour in a system. It gives the responds by giving an alert. Data is collected from two main sources which are traffic passing through the network and the hosts connected to the network. And therefore, according to that they are deployed, IDSs are divided into two categories that is analyze network traffic and those that analyze information available on hosts such as operating system audit trails. The current trend in intrusion detection is to combine both host based and network based information to develop hybrid systems [6].

It is broadly classified as:

Knowledge or signature-based IDS

In Knowledge or signature-based IDS, the incoming packets are compared with known patterns of attacks which is used to detect malicious threats and if matches found then the alert is generated. The basic motivation is to measure how close a behavior to some previously established standard of misuse or normal behavior. Depending on the level of a priori or domain knowledge, it is possible to design detectors for specific categories of attack. (E.g. denial of service, user to root, remote to local) [6].

Behaviour or anomaly-based IDS

In this method, the incoming traffic which does not match the ‘normal’ or ‘expected’ or behaviour is alerted to be an intrusion. Intrusion detection systems can be implemented at network-level, host-level or application-level IDs work effectively in this type of level. Intrusion detection systems assist by generating alerts, which can enable investigation process in Network forensic systems. The basic functionality is just detection not investigation [7].

Sometimes intrusion detection system can give wrong alerts, i.e. “false alarms” we call it as either “false-positives” or “false-negatives”. “False-positive” refers to flagging of an alert even though an attack has not occurred. And false-negative that is refers to inability to flag an alert, even when an attack has occurred. The anomaly detection first requires the IDS to define and characterize to the correct and acceptable static form and dynamic behaviour of the system, which is then be used to detect abnormal changes or anomalous behaviours [26].

2.2 Firewalls

Firewall is used to provide “perimeter defense”, to prevent an attacker from entering a particular protection boundary. But, it is still susceptible to intrusions or attacks once the boundary is crossed. Therefore, a better way is to implement as “Defense in depth”, which involves a chain of firewalls [4].

Since it used to prevent malicious attacks from penetrating through the network, this reduces the work load involved in investigation process for network forensic systems. The basic functionality of the firewalls is just “prevention”. If the attacker is successful in seeping through the firewalls, the system has been compromised, and the only way is the investigate for the source of attack [2].

2.3 Honeypot

A honeypot that refers to a computer system on a network, set up to attract and trap attackers who try to intrude other people's computer systems [6]. Honeypot that assist network forensic systems by studying the moves of attackers and capture their tools and keystrokes [6]. Since this system is made to trap attackers, it is compromised, hence ‘cannot legally claim for any damages [11].

2.4 Vulnerabilities Detection Techniques

Black-box testing

Black-box testing is used to refer the analysis of program execution from an external point of view. In short, it consists of comparing the software execution outcome with the expected result. In black testing we match the current result with the expected result on the basis of software requirement specification.

White-box testing

White-box analysis consists of examining the code without executing it. Developers can do this in one of two ways: manually, during code inspections and reviews and automatically, using automated analysis tools. There are various tool which the tester used in the testing like WinRunnner, Quick test professional [2].

2.5 Double Guard Detecting Techniques

Double Guard detection is used to detect the network behaviour of user sessions across both the front-end web server and the back-end database. It help to produce Alert, and help to identify wide range of attack [3].

2.6 Hidden Markov Models (HMM)

A wide range of attacks exploits web application vulnerabilities typically it derived from input validation flaws. A new formulation of query analysis through Hidden Markov Models (HMM) and show that HMM are effective in detecting a wide range of either known or unknown attacks of web applications.HMM applied to computer security mostly in host-based IDS to model system call sequences. Previous works explicitly address the problem related to the presence of attacks inside the training set. Hidden Markov Models (HMM) used to improve the performance can be increased when a sequence of symbols is modelled by an ensemble of HMM. It explicitly address the problem related to the presence of attacks inside the training set [6].

2.7 Honeynet

The honeypot attract the attackers therefore their process methodology can be observed and analysed to improve defense. Attackers first will go through honeywall and then honeypot system will activate and it will the machine through which we will interact to the attacker via honeypot system and all the activities will be observed through Honeywell in the database. It used to observed the attack patterns and capture all activity when attack takes place. Honeypots based Model can be very useful to collect the attacker traces [4]. A single HHM and double HHM are used to model a generic sequence. An ID has been always able to detect all attacks inside dataset. It will be focusing our analysis on the evaluation of on dataset [23] [25].

3. Role of Network Forensics

In 2006 Ren and Jin was propose the first general process model of network forensics, which is comprises with the five steps: capture, copy, transfer, analysis, investigation and presentation. Related techniques are as follows.

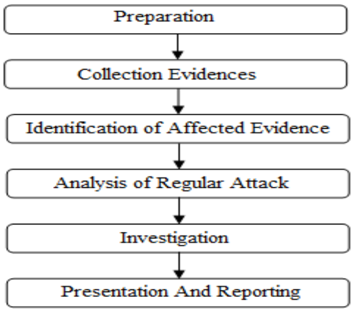
Preparation
Collection Evidences
Identification of Affected Evidence
Analysis of Regular Attack
Investigation
Presentation And Reporting

Figure 1: Network forensics investigation process

- ***Capture*****:** In this acquire the data from the different data source. Privacy is the major concern in this step. Data sources include network traffic packets, firewall logs, intrusion detection system log, and application audit logs. Some techniques like host audit system initiation (such as NTLast), traffic monitoring and management (such as MRTG), packet sniffer (such as Tcpdump, Wireshark), intrusion detection system (such as Snort), and firewall are required [22]. Moreover, all the logs should be stored in a backup device at a real-time base in case of being falsified or deleted files [21].

- ***Copy*****:** In this copy the data from the original data to read only media, transfer network or analysis machine. In order to assure the integrity of data and legal requirements, the bit-to-bit copy has to be made. Major techniques are disk image copy such as Forensic acquisition utilities and MD5/SHA [17] [19].

- ***Transfer*****:** Transfer phase is to transport the copy data to the forensics analysis machine. Primary issue is ensuring the data security during transportation. Therefore, all the transferring information including date, time, name will be detailed recorded. Major techniques involve Secure Socket Layer (such as OpenSSL), Virtual Private Network and subversion [22].

- ***Analysis*****:** This step is the most comprehensive and simple one in the whole process. It involves sub-processes like data filtering, meta-analysis, and data analysis. Major techniques include packet analysis (such as Wireshark, Tcpdump, Windump), data mining (such as TANAGRA), data fusion, data recovery (Pandora Recovery), protocol analysis (such as Wireshark, IP Sniffer), data hiding discovery, reverse engineering decryption [29].

- ***Investigation*****:** This is the primary purpose for investigation is to acquire the information of the source or attackers. The major techniques include IP trace back, mapping to geographic location, OS fingerprint (such as Network miner) remote forensics [12].

- ***Presentation*****:** In this step involves presenting the conclusion and the procedure of the conclusion. The Major techniques which include Visualization, Documentation, Computer graphics, Remote access and Remote management. Network packet analysis is very useful for finding network errors [22].

4. Different Challenges with Network Forensics

There are the several challenges generally associated with network forensics

- **Data Capture:** When data is collected from the entire network, packets, authentication log, audit log, and different other sources. The challenge is to decide which are the appropriate sources of network data depending on our usage to check whether it is for short-term basis or long-term basis [28].
- **Data granularity:** Once the data is captured, the challenge is to decide what is to be retained and what needs to be eliminated.
- **Data Integrity:** The major challenge is to ensure that the data is not tampered or forgery with, and integrity is maintained as this would gravely affect the investigation process. Different techniques will be used for ensure the data integrity.
- **Privacy:** Dealing with the sensitive information across the entire network, care has to be taken that private information of users is not compromised because private information is very useful for aiding an investigation.
- **Data Analysis:** Once all the required data has been captured from the different source with the help of network based tool, it needs to be properly analyzed and organized as this affects the decisions to be made.
- **Data as Legal Evidence:** As per legal procedures, the challenge is to preserve and archive the real time data so it can be used as evidence in courts of law [28].

5. Conclusion

Network forensics is a very important part of the entire security model, as it provides the investigative capabilities, the existing technologies used in network forensics for prevention and detection of various web based attack and for the identification. There are various tools and existing technologies are available but it use just to detect and prevention from different attack but not for the investigation. To overcome this problem and make things easier the concept of 'neurofuzzy' is used for the further implementation.

References

[1] Nuno Antunes And Marco Vieira, "Defending Against Web Application Vulnerabilities" IEEE transaction on computer, pp 66-72, 2012.

[2] Slim Rekhis And Noureddine Boudriga, "A System For Formal Digital Forensic Investigation Aware Of Anti-Forensic Attacks" IEEE transactions on information forensics and security, vol. 7, no. 2, pp 635 - 650 april 2012.

[3] Meixing Le, Angelos Stavrou, Brent Byunghoon Kang, "Doubleguard: Detecting Intrusions In Multitier Web Applications", IEEE transactions on dependable AND secure computing, vol. 9, no. 4, pp 512-525, july/august 2012.

[4] Jatinder Kaur, Gurpal Singh, Manpreet Singh," Design & Implementation Of Linux Based Network Forensic System Using Honeynet" , International Journal Of Advanced Research In Computer Engineering & Technology Volume 1, Issue 4, pp 231-238, June 2012.

[5] Yang Xiang,Ke Li, Wanlei Zhou, "Low-Rate Ddos Attacks Detection And Traceback By Using New Information Metrics", IEEE transactions on information forensics and security, vol. 6, no. 2, pp 426-437, june 2011.

[6] Igino Corona, Davide Ariu And Giorgio Giacinto,"HMM-Web: A Framework For The Detection Of Attacks Against Web Applications" IEEE International conference on communication, pp1-6, 2009.

[7] Nguyen H Vo, Josef Pieprzyk, "Protecting Web 2.0 Services From Botnet Exploitations" Cybercrime And Trustworthy Computing Workshop IEEE, pp 18-28, 2010.

[8] Stephen D. Wolthusen, "Overcast: Forensic Discovery In Cloud Environments", Fifth International Conference On IT Security Incident Management And IT Forensics, pp 3-9, 2009.

[9] Ryuya Uda, "Proposal Of Method For Digital Forensics In Physical Distribution", Second International Conference On Computer Engineering And Applications, pp 211-216, 2010.

[10] Amelia Phillips, "Computer Forensics Investigators Or Private Investigators: Who Is Investigating The Drive?", Fifth International Workshop On Systematic Approaches To Digital Forensic Engineering , pp 550-557, 2010.

[11] Sohaib Ikram, Hafiz Malik, "digital audio forensics using background noise" International conference on multimedia and expo ,pp 106-110 , 2010.

[12] CP Grobler, CP Louwrens,"Digital Evidence Management Plan", ISSA, pp 1-6, 2010.

[13] Chung-Huang Yang, Pei-Hua Yen," Fast Deployment Of Computer Forensics With Usbs", International Conference On Broadband, Wireless Computing, Communication And Applications, pp 413-416, 2010.

[14] D. Reilly, C Wren, T. Berry, "Cloud Computing: Forensic Challenges for Law Enforcement", International conference on internet technology and secured transaction pp 1-7, 2010.

[15] Ying Xuan, Incheol Shin, My T. Thai, "Detecting Application Denial-Of-Service Attacks: A Group-Testing-Based Approach", IEEE transactions on parallel and distributed systems, vol. 21, no. 8, pp 2103-1216, august 2010.

[16] Sindhu. K. K , Dr. B. B. Meshram, "A Digital Forensic Tool For Cyber Crime Data Mining", IRACST – Engineering Science And Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, 2012.

[17] Varish Mulwad, Wenjia Li, Anupam Joshi, Tim Finin And Krishnamurthy Viswanathan," Extracting Information About Security Vulnerabilities From Web Text", IEEE 2011.

[18] Abraham Yaar, Adrian Perrig, Dawn Song," Pi: A Path Identification Mechanism To Defend Against Ddos Attacks", IEEE 2003.

[19] Liang Xie, Sencun Zhu," Message Dropping Attacks In Overlay Networks:Attack Detection And Attacker Identification", IEEE 2006.

[20] Ayda Saidane, Vincent Nicomette, And Yves Deswarte, " The Design Of A Generic Intrusion-Tolerant Architecture For Web Servers", IEEE transactions on dependable and secure computing, vol. 6, no. 1, january-march 2009.

[21] Yi Xie, Shun-Zheng Yu," Monitoring The Application-Layer Ddos Attacks For Popular Websites", IEEE/ACM transactions on networking, vol. 17, no. 1, february 2009.

[22] Debasish Das, Utpal Sharma, D K Bhattacharyya," A Web Intrusion Detection Mechanism Based On Feature Based Data Clustering", 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[23] Guang Jin, Fei Zhang, Yuan Li, Honghao Zhang, Jiangbo Qian," A Hash-Based Path Identification Scheme For Ddos Attacks Defense", IEEE 2009.

[24] Veena H Bhat, Member, IAENG, Prasanth G Rao, Abhilash R V, P Deepa Shenoy, Venugopal K R And L M Patnaik ," A Data Mining Approach For Data Generation And Analysis For Digital Forensic Application", IACSIT International Journal Of Engineering And Technology, Vol.2, No.3, June 2010.

[25] Andreas Makridakis, Elias Athanasopoulos, Spiros Antonatos, Demetres Antoniades, Sotiris

Ioannidis, And Evangelos P. Markatos," Understanding The Behavior Of Malicious Applications In Social Networks", IEEE 2010.

[26] Nidal Qwasmi, Fayyaz Ahmed, Ramiro Liscano, " simulation of ddos attacks on p2p networks" , IEEE International conference on HPCC, pp 610-614, 2011.

[27] Ram Prasad Viswanathan, Youssif Al-Nashif, Salim Hariri," Application Attack Detection System (AADS):An Anomaly Based Behavior Analysis Approach", IEEE 2011.

[28] Mohd Taufik Abdullah, Ramlan Mahmod, Abdul A. A. Ghani, Mohd A Zain And Abu Bakar Md S, "Advances In Computer Forensics," International Journal Of Computer Science And Network Security, Vol. 8, No. 2, February 2008.

[29] Smita.Nirkhi,"Potential Use Of Artificial Neural Network In Data Mining " International Conference On Computer And Automation Engineering (ICCAE), pp 339-343, 2010.

Mr. Sudhakar Parate recived the B.E. in Computer Engineering from Bapurao Deshmukh College of Engineering, Seagram, Wardha in 2007 and Pursuing M.Tech in computer science and Engineering from G.H.Raisoni college of Engineering, Nagpur. His main research interests include Digital Forensics, Artificial Neural Network.