BOOK CHAPTER | *"Let the Dead Bury Their Dead"*

Effective ways of Carrying Out Network Autopsy

Louis Opoku Gyamfi
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: louis.gyamfi@st.gimpa.edu.gh
Phone: +233246529891

ABSTRACT

By focusing on intrinsic network weaknesses and communication processes, network forensics techniques aid in the tracking of internal and external network attacks. However, when cyber criminals remove traces in order to evade detection, the investigation of cybercrime becomes more difficult. As a result, network forensics approaches use mechanisms to make inquiry easier by recording every packet and event that passes over the network. As a result, it is possible to determine the source of the assault by reconstructing the captured data. The purpose of this paper is to outline effectives way of carrying out network autopsy.

Keywords: Network Autopsy, Network Forensics, Network Security, Packets, Data Capture.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Louis Opoku Gyamfi (2022): Effective ways of Carrying Out Network Autopsy
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 329-334
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P52

1. INTRODUCTION

Networks and computers have become the bloodline for most businesses today. This has made networks targets for both old fashioned and new criminals. For any cyber-attack to occur within an organization, the attackers first go through the network. Therefore, it has become necessary to know what happens on a network to take measures to protect against these attacks. This requires an analysis of the activities on the network to be able to know what has happened and what is happening on the network. The term autopsy is an analysis of something after it has been done or made.(Autopsy Definition & Meaning | Dictionary.Com, n.d.). Network autopsy in this context is interchanged with network forensics which is a branch of digital forensics that deals with collecting and analyzing network traffic in order to better understand and prevent cybercrime. E-mails, instant messaging, online surfing operations, and file transfers can all be recovered and recreated using network forensics to disclose the original transaction. The paper is organized in the following sections: Section 2 discusses the background of the study. Section 3 is a review of related literation. Section 4 looks at the findings of the study. Section 5 is a conclusion of the study. Section 6 is recommendation for policy and practice.

1.1 Background of The Study

Network Security

In the past, networks were isolated. They were limited to a single geographic location and were assessable by only those within that location. With the introduction of the Transmission Control Protocol / Internetwork Protocol (TCP/IP) and the internet, devices on different networks can communicate with each other irrespective of their location.(A Brief History of the Internet, n.d.). The interoperability nature of today's networks has made it the preferred means of communication for both private and public organizations. Business processes and Infrastructure are being digitized and they all rely on networks to perform their functions. (Hodapp & Hanelt, 2022). This has therefore made networks targets of attacks. Network security used to be an afterthought but in today's world, network security is a global concern and the core of all business technology infrastructure.

Network security is a comprehensive term that covers hardware and software solutions, as well as policies, regulations, and configurations related to network use, network access, and the general protection against threats. Network security includes access control, malware protection, application security, network analytics, many types of network-related security (endpoint, internet, wireless), VPN encryption, firewalls, and more. All of these safeguards are in place to protect networks and data from breaches, invasions, and other dangers.

Network Forensics

Most of the cyber-attacks pass through a network before reaching the target. According to the Lockard's Exchange Principle, when two objects come into contact with each other something is exchanged and taken away by both objects. This is the basis of the transfer and recovery of all scientific evidence.(Gooch & Williams, 2007) Therefore whenever an attacker initiates an attack on a network, there is going to be evidence that can be collected, analyzed and used to trace the source of the cyber attack and bring the cyber criminals to justice. This overarching process is what is referred to as network forensics. By definition, "network forensics is the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities."(Palmer, 1982).

Network forensic investigations is based on data that is volatile. Network forensics differs from computer forensics in that, computer forensics deals with static data that does not change. Network forensic on the other hand deals with data is in motion. This means the data is being sent over a network and then it will be erased after the transfer is complete. To effectively carry out network forensics, plans must be put in place before a cyber security incident occurs to capture the network data and store it. Failure to do so will make is extremely difficult to investigate after the event has occurred over the network.

2. RELATED LITERATURE

The given table presents the review of studies conducted in the context of network forensics.

Table 1 Review of studies conducted in context of network forensics

Authors	Work on network Forensics
(Almulhem, 2009)	In this paper, various aspects of network forensics are reviewed as well as related technologies and their limitations. Also, challenges in deploying a network forensics infrastructure are highlighted.
(Sehrawat et al., 2018)	The paper proposes a model for network traffic analysis which is useful for detecting malicious packets received from intruders.
(Sikos, 2020)	This paper is a comprehensive survey of the utilization of packet analysis, including deep packet inspection, in network forensics, and provides a review of AIpowered packet analysis methods with advanced network traffic classification and pattern identification capabilities.
(Amran & Saad, 2014)	This paper proposes a model for network forensics analysis that captures appropriately defined adversarial capability and structured by a layered approach to investigation.
(Qureshi et al., 2021)	This paper provides a comprehensive analysis of the concept of network forensic investigation and describing the methodologies and tools employed in network forensic investigations by emphasizing on the study and analysis of the OSCAR methodology.
(Khan et al., 2016)	This paper reviews the fundamental mechanism of network forensics techniques to determine how network attacks are identified in the network. Through an extensive review of related literature, a thematic taxonomy is proposed for the classification of current network forensics techniques based on its implementation as well as target data sets involved in the conducting of forensic investigations
(Meghanathan et al., 2010)	This paper discusses the different tools and techniques available to conduct network forensics.

3. EFFECTIVE WAY TO CARRY OUT NETWORK FORENSICS

The purpose of network forensics is straightforward. It's commonly used to monitor a network for unusual traffic or an impending attack. On the other hand, it is used to gather evidence by analyzing network traffic data to pinpoint the source of an assault. Irrespective of the purpose for which the forensics analysis is being carried out, a typical network forensics analysis follows the following steps:

Identification of Security Threat and Attacks

As this stage leads to the case's conclusion, the identification procedure has a significant impact on the subsequent processes. This stage entails detecting and identifying an incident using network indicators. Investigators must grasp application and network protocols to identify attack trends. Web protocols such as http and https, file transfer protocols such as Server Message Block/SMB and Network File System/NFS, and email protocols such as Simple Mail Transfer Protocol/SMTP are all prevalent protocols used on networks.

Understanding these protocols will go a long way toward assisting investigators in detecting traffic abnormalities during a cyber-attack, as the attack will differ from typical data flow.

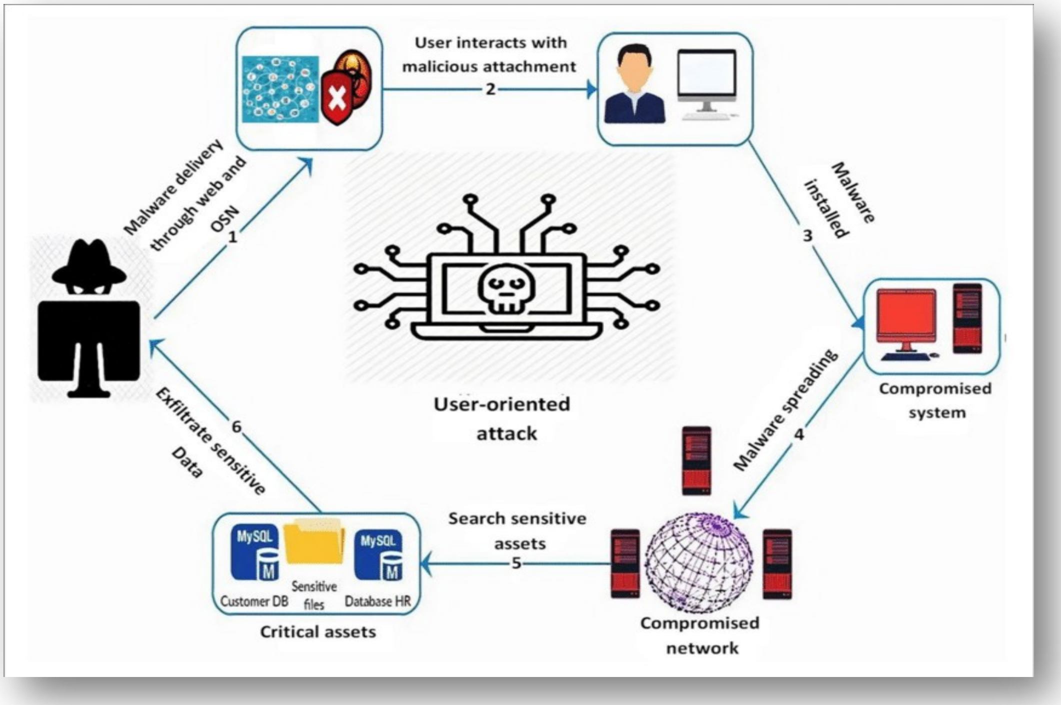

Fig 1: Autopsy of a User-Oriented Attack
Source:https://www.researchgate.net/figure/The-autopsy-of-a-user-oriented-attack_fig1_344424221

Collecting and Preserving the Evidence

All network devices generate logs. From routers, firewalls, switches, intrusion prevention systems, mail relay systems to network authentication systems, they all generate logs. Most networks usually have many of these devices scattered across, therefore it is essential that all the traffics that traverse these systems are monitored from a single location. This will ensure that nothing gets past the investigator. One tool that is key in that regards is the Security information and event management (SIEM). SIEM collects data from a variety of sources within an organization's network. Logs and flow data from users, applications, assets, cloud environments, and networks are collected, saved, and analyzed in real-time, allowing IT and security teams to centrally manage their network's event log and network flow data. The SIEM also serve as the best place for the investigator to monitor traffic and extract the data they need for analysis.

Examining The Data That Has Been Gathered

This procedure entails keeping track of all observable data. Many elements of metadata from data could be discovered by the examiner and brought to court.

Analyzing The Collected Data And Drawing Conclusions

The SIEM assists in event correlation following the identification and preservation of evidence (data). Event correlation uses advanced analytics to find and analyze complex data patterns, allowing for quick detection and mitigation of security issues. The SIEM program keeps track of network activity. With security information management (SIM), which collects, analyses, and reports on log data, SIEM technologies analyze log and event data in real time to provide threat listening, event correlation, and incident response. The investigator concludes based on evidence after analyzing the data.

Presenting The Conclusions Made

The aim of any forensics process is to gather evidence in a manner that will be admissible in court. Therefore, after collecting logs and analyzing the logs, the conclusions are to be documented. This should be written in a layperson's term using abstracted terminologies and all the abstract terminologies should reference the specific details.

By so doing, it will make it easier for the court to understand the information and make decisions based on the presentation.

4. RESEARCH FINDINGS

One of the most difficult aspects of network forensics is ensuring that the network is forensically ready. An effective network investigation necessitates the network's own infrastructure to adequately assist the inquiry.(Almulhem, 2009). Secondly, gaining access to an intruder's originating IP address is a critical step in network forensics. The origin of the attack is indicated by the source IP address, which aids in identifying the intruder and preventing the attacks (Khan et al., 2016). However this is a very difficult task as most intruders employ mechanisms to hide their identity. In some cases, they even spoof their IP address, and this makes network forensics difficult. The network transmits a massive volume of data, which is gathered and examined for investigation. However, such data makes retrieving information from the network more difficult for network forensics. For example, acquired data must be saved on devices with substantial storage capacities, whereas network interconnection devices have limited storage capacities.

5. CONCLUSION

The author of this paper offered digital forensic methodologies that can be used to effectively carry out digital forensics in a network setting. The methodologies given are based on the draft international standards for digital forensic processes. Forensics analysis is conducted to know what has happened on a network.

6. RECOMMENDATION FOR POLICY AND PRACTICES

A uniform legal framework is now required to aid network forensics investigators in acquiring access to network equipment. Forensic preparation should be built into the entire network design. Provisions should be made from the beginning to allow for the recording and analysis of network traffic as needed. Tools and storage space for the large volumes of logs created by various network devices should be included. Finally, network security should be a top priority for all enterprises, particularly the public sector.

REFERENCES

1. A Brief History of the Internet. (n.d.). Retrieved May 7, 2022, from https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml
2. Almulhem, A. (2009). Network forensics: Notions and challenges. IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2009, January, 463–466. https://doi.org/10.1109/ISSPIT.2009.5407485
3. Amran, A. R., & Saad, A. (2014). An evidential network forensics analysis model with adversarial capability and layering. 2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014. https://doi.org/10.1109/WCCAIS.2014.6916615
4. Autopsy Definition & Meaning | Dictionary.com. (n.d.). Retrieved May 4, 2022, from https://www.dictionary.com/browse/autopsy
5. Gooch, G., & Williams, M. (2007). A Dictionary of Law Enforcement. A Dictionary of Law Enforcement. https://doi.org/10.1093/ACREF/9780192807021.001.0001
6. Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda: Https://Doi.Org/10.1177/02683962211064304. https://doi.org/10.1177/02683962211064304
7. Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications, 66, 214–235. https://doi.org/10.1016/j.jnca.2016.03.005
8. Meghanathan, N., Allam, S. R., & Moore, L. A. (2010). Tools and techniques for Network Forensics. 1, 14–25. http://arxiv.org/abs/1004.0570
9. Palmer, G. (1982). A Road Map for Digital Forensic Research - dfrws. In Digital Forensics Research Workshop, 24(3), 709–719. https://doi.org/10.1016/0032-3950(82)90064-8
10. Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. International Journal of Advanced Computer Science and Applications, 12(5), 879–887. https://doi.org/10.14569/IJACSA.2021.01205103
11. Sehrawat, A., Das, N. S., & Mishra, P. (2018). Application of Network Forensics in Identification of Network Traffic. 7(07), 285–288.
12. Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. Forensic Science International: Digital Investigation, 32, 200892. https://doi.org/10.1016/j.fsidi.2019.200892