Network Forensics

Sumedha R Kulkarni

Cyber Security Student

Aim: To capture and record each and every packet of computer network traffic and store them in a single place so it can be monitored and analyzed for the purpose of information gathering, evidence collection and intrusion detection.

I. INTRODUCTION

Sharing ideas, knowledge or any information among different people or organization made the society realize that, it helps them become united and also results in faster development of the society in all terms. For this sole purpose, the Internet was created, that is to serve the communication needs of the society. In the last few years, the Internet has enhanced and developed itself in order to fulfill and provide a wider range of services to the world with commercial as well as personal interests. Unfortunately, it has transformed into a medium where the people and the users are attacked by online attackers called as Hackers. These hackers steal and withhold user's identity and their data to commit financial fraud or destruction to the data, system or any kind of IT assets. In order to identify and prevent these hackers to cause damage or threat to the users or an organization, various methods and procedures have been created and developed by the IT industry and professionals. This paper explains how an attack is identified and prevented by a method called Network Forensics.

This paper is organized as follows: section 2 defines and introduces Computer Network and Network Forensics, section 3 details the reasons for why network forensics is performed and Section 4 lists the types of network forensic systems. Section 5 briefly explains the steps and the procedure involved in network forensics, section 6 introduces to different Network Forensics Analysis tools (NFAT) used in different situation and section 7 gives an idea of what actions are performed on obtained and collected network data or information and types of network data results. Lastly, section 8 concludes the paper on network forensics.

II. REQUIREMENTS

Basic knowledge of computer networks and their protocols, Knowledge of NFAT (Network Forensic Analysis Tools)

III. METHODOLOGY

1. NETWORK AND NETWORK FORENSICS

Network is a collection of computers, servers or any network devices which are connected so that they can communicate and share data with each other. A known and common example of a network is the Internet. It connects millions of people, server etc. all over the world so that they can communicate with each other. Another example of a network is the Home Network, which connects all the computers and other devices through a home network so that they can share data and communicate with each other.

Network Forensics is a branch of Digital Forensics whose aim is to collect information or evidence found in computer networks and communications. The Network Forensics involves monitoring, capturing, recording and further storing the network traffic data in order to analyze them in detail for the purpose to collect the relevant evidence or just as a part of security measure. The information being collected in network forensics is highly volatile and dynamic because the network traffic involves transmitting of data packets across a channel within a short time period and lost once the channel is successful, which also happens in a very short period of time. Hence Network Forensics is always conducted on-spot and the investigations are continuous.

2. WHY CONDUCT NETWORK FORENSICS?

There are far many reasons on why network forensics should be conducted and what the benefits of conducting it are. Below are some of the reasons on why network forensics is preferred conducting.

- It allows to reconstructs a network activity during a particular period of time. This helps in investigating the suspects by reconstructing the sequence of events that took place during a network based information security incident as a proof.
- Although network forensic is invaluable to address technical, operational and organizational issues, it helps in solving them by revealing who communicated with whom, when, how, how often and when and where the communication was lost or failed.
- Network forensics helps in troubleshooting network related and intermittent problems. For example, if there is an error occurring at certain conditions or at certain times, IT professionals perform network forensics, that is, they collect and record hours and days' worth of network traffic data and then search in and dig out the faulty errors and issues in order to fix them.
- It helps in troubleshooting transaction problems and helps company or organization to monitor and trail their business transaction. For example, an online payment service provider can use network forensics to resolve misunderstandings and miscommunications between what reported by the client and what's reported by the server.
- Network Forensics in performed for monitoring user activities with various department's policy. Since network forensics captures and records all the Network

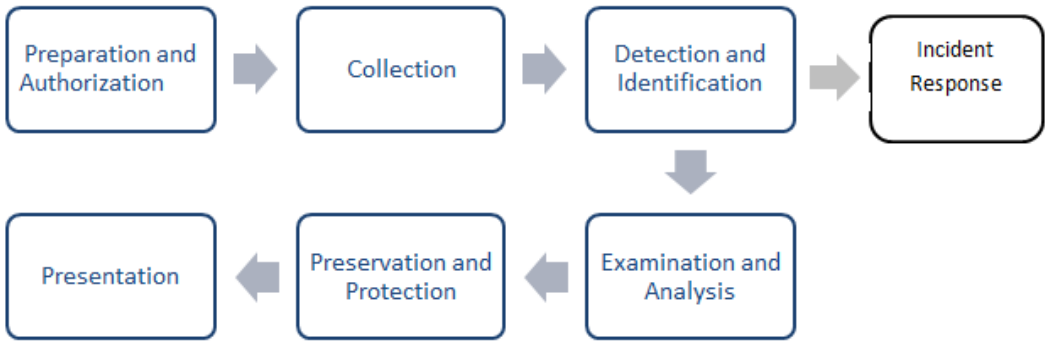
traffic, including emails along with attachments, video calls and other media communications, it can help the IT, HR and Legal department confirm that a specific user is following or not following policies in regards to network usage, data privacy and so on. It can provide hard evidence of who has transmitted what to whom. For example, if an employee of a company is using that company's network data for his personal amusement like Facebook, etc. on performing Network forensics, the company can accuse that employee along with the proof.

3. TYPES OF NETWORK FORENSIC SYSTEMS

The Network forensics systems are classified into two types:-

1. Catch it as you can: - It is a type of brute force method. In other words, a random method in which all network traffic data, as in the data packet passing through a point or a channel is captured and recorded continuously to storage. Analysis of this traffic is done after math and once all data are stored. This system requires large amount of storage capacity, since the data being stored is in bulk.
2. Stop look and listen: - In this system, each and every data packet passing through a point or a channel is firstly analyzed and monitored. The data or the information which are vital and required is stored for reporting, future analyzing and studying. This method or the system helps the organization to understand and detect the threat on-spot as network traffic is analyzed first. Hence this system is considered as valuable and intelligent.

4. Network Forensics steps and procedure



There are different steps set by various frameworks and organization. Above are the7 steps and phases of conducting network forensics from a generic framework point of view.

1. Preparation and Authorization: - It is the first phase in performing network forensics, where professionals and organization prepare to conduct to set a suitable working environment, where required NFAT tolls like Intrusion detecting systems (IDS), firewalls, packet sniffers etc. are deployed at various points and paths on the network. After that the required authorization to perform Network Forensics or to even monitor the network traffic are obtained as per the chain of custody and a well-defined policies and procedures set by the company. It is done so as to prevent violation of privacy of the individual or the organization.
2. Collection: - In this phase the well-defined procedure using suitable and reliable tools, software, applications and even the hardware set at certain points or paths on the network are used to gather maximum evidence and information data with as minimum impact as possible. These evidences and the network traffic data are collected from sensors. These sensors must be secure with limited or allowed access, tolerant and reliable. This phase also includes recording physical scene and duplicating digital evidence via certain standard policies and procedures set by the organization. This phase is considered to be difficult to perform as the network traffic data changes and travels at a very rapid speed and also the amount of data to be collected is enormous, requiring a system with huge memory space.
3. Detection: - This phase starts when alerts are generated or discovered by the deployed security tools, indicating a data or security breach or policy violation or any kind of cyber attack. Once detecting the attack and before confirming, a quick validation and assessment is done. This phase involves the working of the security tools and individual monitoring through these tools.
4. Protection and Preservation: - In this phase, the state of the evidence both physical and inside are secured and isolated from being altered due to various factors, such as system damage, unauthorized access, memory damage, power cut during storage etc. Hence, in order to do so, the collected original data is firstly stored again on a back-up device (which is also protected), and hash of all the data is taken and protected. Another copy of the data will be used for analysis and the original collected network traffic is preserved. This is done so that whenever investigation or the analysis done may want to be repeated and reexamined in case to meet the legal evidence, the original data has to be available, so that they can work or examine again on the copy of the data taken again, still preserving the original one. The main goal of this phase is to ensure Confidentiality, Integrity and Availability (CIA triad) and Accuracy is met and followed.
5. Examination and Analysis: - In this phase, an in-depth and systematic search and study of evidence is done on the collected Network data. The evidence or the data collected is dug out completely from inside out (But methodically and procedure wise) to extract specific and particular indication of the crime. The collected evidence and the attack patterns are grouped together and the incident or attack is reconstructed and replayed in order to study and understand it completely. It also involves identifying and discovering potential evidence and building detailed documentation for analysis. In order to reconstruct the incident or study it, various tricks and methods are performed such as, mapping the time line of the attack,

tracing the path to the source and the intended destination, recovery of any hidden or camouflaged data like malicious attachments, encrypted files etc.

6. Incident Response: - During the process of Network Forensics, the professionals may directly jump to this phase, whenever the impact of the attack discovered is very high, damage is very high and the recovery time is less. In this phase, a response to the attack or the intrusion detected is initiated based on the evidence or network traffic data collected to validate and assess it. The response or the action to be taken depends on the type of attack, its impact, recovery time and loss on the assets. An action, plan or method is initiated and performed, including how to prevent such attacks in the future, and save the assets from their existing impact. It also includes decision making on whether to continue with the investigation and mitigation or to just avoid or accept the attack based on its nature, type and impact.
7. Presentation: - At this last phase, summarizing and explaining the conclusion or the result of conducting Network Forensics process is done. The observations, results, conclusions and the summary of the process is presented in an understandable language to the client, while providing explanation of the standard procedures and policies used to arrive at the conclusion. This phase also includes preparing a detailed documentation, which enlists briefly type of attack or breach happened, its reasons and causes, how it was detected and identified, what methods and measures were used to stop the attack, impact of the attack, recovery rate and likelihood of the attack, the counter measures recommended to prevent such attacks to take place again and lastly the conclusion is drawn.

5. Network Forensics Analysis Tools (NFAT)

The network forensic analysis tools allow professionals and users to monitor the network traffic, collect information about malicious network traffic, hidden or camouflaged data in the network, which plays a vital role in solving a network crime investigation and helps in initiating suitable Incident Response. They also help in analyzing operating errors in the network system, insider thefts and misuse, faulty and failed network channels, predicting attacks, performing risk assessment and also evaluating network performance.

Although there are a wide range of NFAT tools, they are categorized into following categories:-

1. Packet capturing tools: - They are a set of tools which capture and record data traffic required and set by the user. Since getting access to network traffic and data packets is a pre-requisite to perform Network forensics, be it online or offline. It allows professionals to record and play back all the traffic on the network. It also allows validation of IPS/IDS alerts. Some examples of these types of tools are, TCPDUMP, KISMET, and DUMPCAP etc.
2. Pattern matching tools: - They are the security tools, which search for a pattern in a system. During detection phase, a common task is searching for a pattern in network traffic, passing through a certain point in the network. It helps in early

identification of the attack. NGREP, NetFlow Traffic Analyzer is some examples of these types of tool.

3. Network Intrusion Detection tools: - These tools are used to monitor the network traffic for the signs of malicious activities. It can be in the form of unsuccessful logs, matching signatures etc. Whenever such malicious activities are detected, a security message and an alert are initiated to the console, its owner, the host or SIEM systems. Example SNORT, FALCON, OSSEC etc.
4. Full scale analysis tools: - These tools are used to perform a full scale analysis, that is, from troubleshooting, communication paths to SIEM operations, decrypting network traffic data, dissecting protocols etc. One of the known full analysis tool is Wireshark.
5. Prevention tools: - These are the tools and applications that are deployed at the level 1 layer of the network which acts like a guard wall to the network entity. They are used to filter out unwanted network traffic, malicious data files etc. which prevents or stops the attack or data breach to occur. Firewalls, Anti-Virus are some of the preventative tools.

6. Types of Evidence data

There are various types of network based data which are collected during Network Forensics, considered as evidence. They are categorized into different groups in order to get a better understanding about the incident and attack. All these network-based evidence types have their own pros and cons with respect to forensic analysis. This section will briefly explain different types of network based evidence.

1. Full content data: - This type of data contains every single detail regarding each and every data packet on the Network traffic. They are referred to as streaming high level data. They can be extracted from NFAT tools like Wireshark without any filters and exceptions.
2. Session data: - It is a network based data, which consists of aggregated traffic data, usually a conversation between 2 network entities communicating via a channel. This type of data helps in giving details regarding the source and receiver of the communication, time of communication etc. but excluding the contents of that communication.
3. Alert data: - Whenever a malicious activity or traffic is triggered, an alert is initiated. The alert data consists of information regarding this alert such as, time of trigger, classification of the attack, which point etc. They are extracted from tools like SNORT, Firewalls or Suricata.
4. Statistical data: - They are type of evidence data which consists of network related aspects, such as number of bytes contained in a packet transfer, ports used, protocols used, active nodes or ports, number of bytes transferred, average packet rate etc. These data type are taken from tools like Wireshark.

IV. CONCLUSION

A first attempt was made in this paper to give brief idea on how Network Forensics is performed. It defines what network forensics is and why is it performed. Although various methods and procedure are performed to tackle an attack, it is always a best solution to prevent it beforehand. Network forensics can also be done in order to prevent any network-based attacks. There are shortfalls and challenges in this process that are not addressed in this paper, but they are being addressed so that it can function without any errors and the network crime rate can be brought down drastically.

V. REFERENCES

1. https://lifars.com/2020/06/the-basics-of-network-forensics/#:~:text=Network%20Forensics%20examinations%20have%20seven,and%20Presentation%20and%20Incident%20Response.com
2. https://www.researchgate.net/figure/Steps-of-network-forensics-techniques_fig1_320944549
3. https://www.e-spincorp.com/steps-to-generic-network-forensic-examination/
4. https://en.wikipedia.org/wiki/Network_forensics#:~:text=Network%20forensics%20is%20a%20sub,legal%20evidence%2C%20or%20intrusion%20detection.&text=Network%20traffic%20is%20transmitted%20and,often%20a%20pro%2Dactive%20investigation.