Computer Science and Information Technologies
Vol. 5, No. 1, March 2024, pp. 1~6
ISSN: 2722-3221, DOI: 10.11591/csit.v5i1.p1-6

Collecting and analyzing network-based evidence

Ashwini K. Singh[1], Dhwaniket Kamble[2], Abhishek Bains[1], Naman Tiwari[1], Tejas R. Deshmukh[1], Sanidhya Pandey[1], Hemant Kumar[1], Diksha M. Bhalerao[2]
[1]Department of Information Technology, Bharti Vidyapeeth Deemed University, Maharashtra, Navi Mumbai-410210, India
[2]Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University, Maharashtra, Navi Mumbai-410210, India

Article Info

Article history:

Received Dec 28, 2022
Revised May 29, 2023
Accepted Dec 23, 2023

Keywords:

Analysis
Evidence
Network forensics
Network traffic
Sniffing

ABSTRACT

Since nearly the beginning of the Internet, malware has been a significant deterrent to productivity for end users, both personal and business related. Due to the pervasiveness of digital technologies in all aspects of human lives, it is increasingly unlikely that a digital device is involved as goal, medium or simply 'witness' of a criminal event. Forensic investigations include collection, recovery, analysis, and presentation of information stored on network devices and related to network crimes. These activities often involve wide range of analysis tools and application of different methods. This work presents methods that helps digital investigators to correlate and present information acquired from forensic data, with the aim to get a more valuable reconstructions of events or action to reach case conclusions. Main aim of network forensic is to gather evidence. Additionally, the evidence obtained during the investigation must be produced through a rigorous investigation procedure in a legal context.

Corresponding Author:

Dhwaniket Kamble
Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University
Navi Mumbai – 410210, India
Email: drkamble@bvucoep.edu.in

1. INTRODUCTION

Integrating network sniffing, capturing, and analysis is part of network forensics. Utilizing traffic and event logs, a network security incident can be analyzed. Network forensics are essential to determine the kind of network assault and find the offenders. Additionally, the evidence obtained during the investigation must be produced through a rigorous investigation procedure in a legal context [1]. Nevertheless, there are several reasons why network forensics is a difficult task. First, while capturing network traffic through a network is straightforward in theory, it is somewhat challenging in practice because of several underlying issues, such as the volume of data flowing over the network and the complexity of Internet protocols. As a result, extensive resources are needed for network traffic recording [2]. Due to the huge quantities, it is frequently impossible to record all the data that is transmitted across the network. Again, for later examination, this recorded data needs to be backed up to free recording medium [3], [4]. Furthermore, the most important and time-consuming duty is the examination of recorded data [5]. There are several automated analysis tools available for forensic use, but they are insufficient because there is no way to distinguish malicious traffic produced by an attacker from a pool of legitimate traffic with absolute certainty. Because there is always a danger of receiving false positive results when using automated traffic analysis tools, human judgement is equally essential. However, precautions should be taken to assure network forensics preparedness in advance, such as by setting up proper event recording and data collection systems that can provide important artifacts for examination during forensics inquiry.

2. METHOD

2.1. Collecting evidence

Locating and gathering information that is often present among network devices and along the traffic paths inside a network. This data gathering is essential in the event of an incident where an outside threat source is trying to control internal systems or steal information from the network [6], [7]. When evaluating host evidence, network-based evidence is particularly helpful since it offers a second source of event corroboration, which is crucial for identifying an incident's primary cause [8], [9].

2.1.1. Via sniffers

A network's information traffic can be a useful source of information about intrusions or strange connections. Network sniffers, also known as packet sniffers, are tools that can intercept and record network traffic. They were created in response to the necessity to collect this data. Sniffers place network interface cards (NICs) in promiscuous mode, allowing them to listen to and record every bit of data sent over the network. Hardware taps and spanned ports make switched networks easier to sniff [10]. In addition to the physical and data-link layer, sniffers also capture traffic from the network and transport levels. Because of its monitoring and analysis capabilities, a packet sniffer is used in network forensics to manage traffic, monitor network components, and detect breaches. Sniffers are used by forensic investigators to examine any suspicious application or apparatus. A few examples of sniffers are as follows:

a. Sniffing tool: tcpdump

When a Boolean input expression matches a packet on a network interface, Tcpdump prints out a description of the contents of the packet. The -w parameter instructs the programme to store the packet data to a file for subsequent analysis, and the -r flag instructs the programme to read packets from a saved packet file as opposed to a network interface. Tcpdump only ever examines packets that exactly match the supplied phrase. Tcpdump captures packets until it is interrupted by a signals intelligence (SIGINT) or SIGTERM signal, or if the specified number of packets have been processed, if it is run without the -c flag. If run with the -c flag, it captures packets until it is interrupted by a SIGINT or SIGTERM signal, or if the specified number of packets have been processed.

b. Sniffing tool: wireshark

A GUI network protocol analyzer is titled Wireshark. It allows the investigator to interactively view packet data from either a captured file or a live network. The native capture file format for Wireshark is libpcap, which is also the format supported by tcpdump and a number of other utilities. Investigators have the option to do live capture and offline analysis while also being able to perform thorough inspection of hundreds of protocols using Wireshark. It works with several operating systems, including Windows OS, Linux, macOS, Solaris, FreeBSD, and NetBSD. Any file type that has been compressed using gzip may be read by Wireshark. The .gz extension is not necessary for Wireshark to recognize this; it does so directly from the file [11]. Three views of a packet are displayed in Wireshark's main window, similar to other protocol analyzers. It displays a line that summarizes the contents of the packet. It displays a protocol tree that enables the researcher to dig down to the specific protocol or topic of interest. A hex dump demonstrates exactly how the packet appears as it travels across the wire.

2.1.2. Via security information and event management system (SIEM)

The nature of signing on to network devices is a major issue that a lot of companies face. Log files are frequently rolled over, whereby new log files are written over previous log files, due to a lack of space. As a result, an organization can occasionally only have a few days or even a few hours' worth of crucial logs. The incident response team will lack crucial pieces of evidence if a possible event occurred several weeks earlier [12].

An enterprise-wide technology that has gained popularity is the SIEM system. These appliances have the capacity to gather log and event information from several network sources and consolidate it in one place. This eliminates the need to look at individual systems and enables the computer security incident response team (CSIRT) and other security experts to monitor activities across the whole network [13], [14].

Logs are set to be sent to the SIEM from a number of sources, including structured query language (SQL) databases and security controls. The user account was used in this instance to copy a database to the remote server at 10.88.6.12, according to the SQL database at 10.100.20.18. This kind of behavior may be quickly examined thanks to the SIEM. If it is discovered that the account was hacked, for instance, CSIRT analysts can instantly search the SIEM for any activity involving that account. The log record indicating a database copy to the remote computer would then be visible to them. Without the SIEM, CSIRT analysts would have to search every single system that may have been accessed, which might be a time-consuming procedure [15], [16].

2.2. Analyzing evidence

In this procedure, we analyze the information obtained during the previous step in this phase using instruments and methods that may transform readily available information into strong proof that aids in resolving the "W questions: what, when, what, where, and how?". This stage allows us to fully comprehend the case and reasons that could be at play [17], [18]. It may be feasible to clearly identify the Case type: unintentional, dissatisfied employee, industrial espionage.

2.2.1. Analyzing traffic for sniffing attempts and SMB password cracking attempts

In eavesdropping techniques like sniffing and man-in-the-middle assaults, an attacker places oneself in between a client and a server to intercept messages. Attackers snoop through network traffic looking for private data [11]. When trying to crack a server message block (SMB) password, Wireshark's network traffic analysis would show many attempts to log in using various identities [19], [20]. A brute-force attack attempt on the SMB protocol is clearly suggested by the data intercepted by Wireshark, which also shows many usernames and the message "Error: STATUS LOGON FAILURE."

2.2.2. Analyze traffic for MAC flooding attempt

A port on the switch is connected to by the attacker while using the active sniffing technique known as media access control attack or MAC flooding. They fire out an onslaught of Ethernet transmissions with phoney MAC addresses. The attacker is attempting to access a content addressable memory (CAM) table that the switch keeps. As a result, another name for this attack is CAM flooding attack [21].

MAC flooded packets are regarded as faulty packets by Wireshark. Wireshark's source and destination addresses, as well as the packet's time to live, can help an investigator identify a MAC flooding effort (TTL). To accomplish this, go to the Analyze Expert Information tab and look at the corrupted packets [22].

2.2.3. Analyze traffic for TCP SYN flood DoS attack

SYN flooding is a sort of DoS attack in which the attacker uses several fake IP addresses to deliver a huge volume of SYN packets to the target server continuously. The server transmits SYN-ACK packets in response to the SYN packets, but no ACK packet is received from the client to complete the three-way TCP handshake. Thus, the attacker may swiftly deplete the target server's CPU and RAM resources and make it unresponsive, which finally leads to DoS.

2.2.4. Analyze traffic for file transfer protocol (FTP) password cracking attempts

Password cracking is the process of acquiring or recovering passwords either by performing a password guessing effort using a file containing frequently used passwords, or by utilising trial and error. Dictionary assaults and brute force attacks are the names of these strategies, respectively. By counting the number of login attempts made from the same IP address or username, a detective can spot this kind of assault.

The FTP is a widely used protocol for transferring files between computers utilizing the TCP/IP suite over the Internet. FTP is a client-server protocol that uses two channels of communication to connect a client and server. The management of the discussions is done by one, and the transmission of the actual material is done by the other. The server replies to a client's request for a download by providing the specific file requested. The user must enter their username and password to log into the FTP server before starting an FTP session. An FTP password assault involves the attacker attempting to discover any authorized user's password.

2.2.5. Analyze traffic for ARP poisoning attempt

A port on the switch is connected to by the attacker while using the active sniffing technique known as MAC flooding. They fire out an onslaught of Ethernet transmissions with phoney MAC addresses. The attacker is attempting to access a content addressable memory (CAM) table that the switch keeps. As a result, another name for this attack is CAM flooding attack. The warning message "multiple usage of IP address> detected" is displayed by Wireshark when duplicate IP addresses are found on the ARP protocol. After collecting the packets, you may use the filter arp.duplicate-addressdetected to look for signs of an ARP poisoning attack.

2.2.6. Analyze traffic to detect malware activity

The traces of a malware infection can be found in the ongoing network traffic patterns. Once installed on the target machine, malware often try to connect to their Command-and-Control (C2) server for data exfiltration or further instructions. It accomplishes this task by connecting to certain IP addresses or opening certain ports on the target system, which can be tracked by tools like Wireshark [23].

Run Wireshark on the computer that is thought to be infected with malware, then look through the current traffic patterns for any oddities. Once any suspicious or odd ports or IP addresses have been identified, you should search internet databases to see whether any malware is using those ports or if they are susceptible. As seen in the picture below, internet research into the suspicious port using speedguide.net's port database discovered that the njRAT malware frequently uses it as a default port.

2.2.7. Analyze traffic for SYN-FIN flood DoS attack

A connection is established by the SYN flag, and it is broken by the FIN flag. The attacker floods the network by setting both the SYN and FIN flags in a SYN/FIN DoS attempt. SYN and FIN are not often set at the same time in a TCP conversation. A SYN/FIN DDoS attack is evident if an administrator notices traffic that has both the SYN and FIN flags set. The server's firewall might get overloaded during a SYN/FIN DDoS attack by delivering the packets continuously.

3. CONCLUSION

The main objective of the following research was to collect and analyze network-based evidence. The aim has been achieved successfully. Collection of evidence is accomplished via various sniffer tools such as tcpdump, wireshark, and Security information and Event management system (SIEM), an automated system used by large enterprises to sort through system logs to generate possible attack report. Whereas for analysis of evidence is performed by analyzing the traffic for Sniffing Attempts, MAC Flooding Attempt, FTP Password Cracking Attempts, ARP Poisoning Attempt, Malware Activity and others. Evidence are not just collected in hard disks and secondary storages. There is a wealth of information available from network devices spread throughout the environment. With proper preparation, a CSIRT may be able to leverage the evidence provided by these devices through solutions such as a SIEM. Greatest challenges in network forensics is quantity of data generated by the network which counts around gigabytes of memory per day. This paper will help to create legal boundaries and present evidence in more analyzed way by preparing for the legal and tackle all the technical challenges of network evidence collection and Analyses.

REFERENCES

[1] J. He, C. Chang, P. He, and M. S. Pathan, "Network Forensics Method Based on Evidence Graph and Vulnerability Reasoning," *Future Internet*, vol. 8, no. 4, 2016, doi: 10.3390/fi8040054.

[2] S. Qureshi, S. Tunio, F. Akhtar, A. Wajahat, A. Nazir, and F. Ullah, "Network Forensics: A Comprehensive Review of Tools and Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 12, p. 2021, May 2021, doi: 10.14569/IJACSA.2021.01205103.

[3] Y. Ping, "Study on the main form of network crime from the view of criminology," *Proceedings 2011 International Conference on Human Health and Biomedical Engineering, HHBE 2011*, pp. 1108–1111, 2011, doi: 10.1109/HHBE.2011.6029018.

[4] P. Wright and W. Fone, "Designing and managing networks to aid the capture and preservation of evidence to support the fight against e-crime," *2007 IEEE International Conference on Networking, Sensing and Control, ICNSC'07*, pp. 251–254, 2007, doi: 10.1109/ICNSC.2007.372786.

[5] Z. Tian, W. Jiang, Y. Li, and L. Dong, "A digital evidence fusion method in network forensics systems with Dempster-shafer theory," *China Communications*, vol. 11, no. 5, pp. 91–97, 2014, doi: 10.1109/CC.2014.6880464.

[6] B. C. Cheng and H. Chen, "Quality assurance for evidence collection in network forensics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4298 LNCS, pp. 121–132, 2007, doi: 10.1007/978-3-540-71093-6_10/COVER.

[7] A. Castiglione, G. Cattaneo, G. De Maio, and A. De Santis, "Forensically-Sound Methods to Collect Live Network Evidence," *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 405–412, 2013, doi: 10.1109/AINA.2013.133.

[8] H. S. Kim and H. K. Kim, "Network Forensic Evidence Acquisition (NFEA) with packet marking," *Proceedings - 9th IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, ISPAW 2011 - ICASE 2011, SGH 2011, GSDP 2011*, pp. 388–393, 2011, doi: 10.1109/ISPAW.2011.27.

[9] M. Kumar, M. Hanumanthappa, and T. V. S. Kumar, "Crime investigation and criminal network analysis using archive call detail records," *2016 8th International Conference on Advanced Computing, ICoAC 2016*, pp. 46–50, Jun. 2017, doi: 10.1109/ICOAC.2017.7951743.

[10] B. Turnbull and J. Slay, "Wi-Fi network signals as a source of digital evidence: Wireless network forensics," *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*, pp. 1355–1360, 2008, doi: 10.1109/ARES.2008.135.

[11] N. Paxton, G. J. Ahn, and B. Chu, "Towards practical framework for collecting and analyzing network-centric attacks," *2007 IEEE International Conference on Information Reuse and Integration, IEEE IRI-2007*, pp. 73–78, 2007, doi: 10.1109/IRI.2007.4296600.

[12] J. O. Nehinbe and P. Damuut, "Security issues in sensor networks and gathering admissible evidence in network forensics," *Proceedings - UKSim 5th European Modelling Symposium on Computer Modelling and Simulation, EMS 2011*, pp. 394–399, 2011, doi: 10.1109/EMS.2011.95.

[13] A. J. Masys, Ed., "Networks and Network Analysis for Defence and Security," 2014, doi: 10.1007/978-3-319-04147-6.

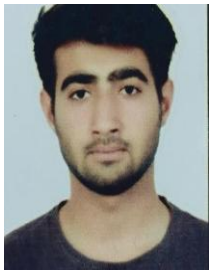
[14] Digital Forensics Essentials Professional Series and EC-COUNCIL OFFICIAL CURRICULA., *Digital Forensics Essentials Version 1.* , Version 1., vol. 1. EC-COUNCIL, 2021.

[15] C. Liu, A. Singhal, and D. Wijesekera, "A logic-based network forensic model for evidence analysis," *IFIP Adv Inf Commun Technol*, vol. 462, pp. 129–145, 2015, doi: 10.1007/978-3-319-24123-4_8/COVER.
[16] "Network Forensics: An Analysis of Techniques, Tools and Trends | Request PDF." https://www.researchgate.net/publication/311739657_Network_Forensics_An_Analysis_of_Techniques_Tools_and_Trends (accessed May 30, 2023).
[17] B. B. Jayasingh and M. R. Patra, "Rule Based Evidence Mining for Network Attack," pp. 23–28, Apr. 2008, doi: 10.1109/ICIT.2007.47.
[18] I. Volarevic, M. Tomic, and L. Milohanic, "Network forensics," *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology, MIPRO 2022 - Proceedings*, pp. 1025–1030, 2022, doi: 10.23919/MIPRO55190.2022.9803427.
[19] Y. H. Liu, G. L. Chen, and L. Xie, "An email forensics analysis method based on social network analysis," *Proceedings - 2013 International Conference on Cloud Computing and Big Data, CLOUDCOM-ASIA 2013*, pp. 563–569, 2013, doi: 10.1109/CLOUDCOM-ASIA.2013.38.
[20] "Network Evidence Collection | Packt Hub." https://hub.packtpub.com/network-evidence-collection/ (accessed May 30, 2023).
[21] D. H. Kim and H. P. In, "Cyber criminal activity analysis models using Markov Chain for digital forensics," *Proceedings of the 2nd International Conference on Information Security and Assurance, ISA 2008*, pp. 193–198, 2008, doi: 10.1109/ISA.2008.90.
[22] N. Mohd Zainudin, M. Merabti, and D. Llewellyn-Jones, "Online social networks as supporting evidence: A digital forensic investigation model and its application design," *2011 International Conference on Research and Innovation in Information Systems, ICRIIS'11*, 2011, doi: 10.1109/ICRIIS.2011.6125728.
[23] R. Zhang, M. Xie, and J. Bian, "ReLF: Scalable Remote Live Forensics for Android," *Proceedings - 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021*, pp. 822–831, 2021, doi: 10.1109/TRUSTCOM53373.2021.00117.

BIOGRAPHIES OF AUTHORS

Ashwini Kumar Singh is a student studying at Bharti Vidyapeeth Deemed University. Department of Engineering and Technology, in the Department of Information Technology. He can be contacted at email: ashwinikmrsngh@gmail.com.

Dhwaniket Kamble is working as an Assistant Professor at Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, in the Computer Science and Engineering Department. His academic qualification is Ph.D. (Pursuing), M.E (IT), B.E (IT), and Diploma (IT). His research area includes Digital Forensics, Ethical Hacking, Cyber Security and Cyber Laws, Design Thinking and Software Engineering. He has published various International Journal papers. He can be contacted at email: drkamble@bvucoep.edu.in



Abhishek Bains is a student studying at Bharti Vidyapeeth Deemed University. Department of Engineering and Technology, in the Department of Information Technology. He can be contacted at email: abhishekbains1212@gmail.com.

Naman Tiwari is a student studying at Bharti Vidyapeeth Deemed University. Department of Engineering and Technology, in the Department of Information Technology. He can be contacted at email: naman.tiwari2022@gmail.com.

Tejas Ravindra Deshmukh is a student studying at Bharti Vidyapeeth Deemed University. Department of Engineering and Technology, in the Department of Information Technology.

Sanidhya Pandey is a student studying at Bharti Vidyapeeth Deemed University. Department of Engineering and Technology, in the Department of Information Technology.

Hemant Kumar is a student studying at Bharti Vidyapeeth Deemed University. Department of Engineering and Technology, in the Department of Information Technology.

Diksha M. Bhalerao is working as an Assistant Professor in Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, in Computer Science Engineering. Her academic qualification is M.E (Computer Engineering), B.E (Computer Engineering). Her research area includes Machine Learning and Web Service. She can be contacted at email: dmbhalerao@bvucoep.edu.in.