Chapter 5
Network Forensics for Human-Driven Cyber Attacks

T. C. Swetha Priya
https://orcid.org/0000-0002-0644-4329
Stanley College of Engineering and Technology for Women, India

ABSTRACT

Network Forensics is a part of Digital Forensics that helps in monitoring and analysis of Computer network traffic for gathering information, evidence, or intrusion detection. This helps in capture, analysis and interpretation of network traffic to uncover evidence of malicious activities and to support incidence response efforts. Unlike the automated Cyber intrusions, human-driven attacks are often carried out by skilled adversaries such as hackers, Cyber Criminals and malicious users. Such attacks are targeted, persistent and are adaptive in nature. Such attacks exploit not only the vulnerabilities in technology but also the human behavior and strategic planning bypassing the traditional security measures. Human-driven attacks try to exploit specific vulnerabilities making their detection demanding. This chapter focuses on how Network forensics provides a methodological framework and technical tools for monitoring, capturing, analyzing and reconstructing the network activities thereby enabling incident response and helps the analysts to trace the origin, method and impact of attacks. It also helps in mitigating human-driven cyber threats. Human-driven attacks typically follow a structured format. This chapter highlights the forensic techniques such as packet inspection, traffic flow analysis, anomaly detection, etc. With the integration of Machine learning and Artificial Intelligence (AI) technology into network forensic systems, the ability to detect indicators of advanced persistent threats has enhanced. Such techniques play a crucial role in environments where the attackers actively evade detection by misleading that as legitimate traffic

DOI: 10.4018/979-8-3373-4898-8.ch005

through encryption, spoofing or data exfiltration. This chapter explores the basic forensic process that involves systematic collection, preservation, and analysis of evidence collected from network traffic. Generally, human-driven cyber attacks follow a sequence of phases such as reconnaissance, intrusion, data collection, and exfiltration. Because tampered evidence will not be valid, the forensic investigators must preserve the evidence through a proper chain of custody which is essential for acceptance before the court of law. Network forensics provides incident response and threat identification in a proactive manner by continuously monitoring network behaviour using forensic tools that flags anomalies and suspicious behaviour in real-time enabling the organizations to respond spontaneously before damage occurs. This chapter also identifies and addresses the challenges in network forensics by providing the solutions across distribute environments in real-time.

1. INTRODUCTION

Network Forensics is a branch of digital forensics that focuses on monitoring, capturing, analyzing and preserving the evidence collected from network traffic for finding the source and the type of cyber incidents. This plays a major role in the identification of malicious activities, responding timely to the data breaches, reconstructing the evidence and supporting legal investigations based on the network evidence data. Unlike other Digital Forensics that deals with collecting the evidence in static form, Network forensics works in an environment that is dynamic making it relevant for real-time data analysis and faster decision-making. = A huge amount of cyber threats are common in real world because of the automated malicious software. Apart from these, human-driven attacks have become increasingly widespread and dangerous. Human-driven cyber attacks are attacks that are done by individuals or group of people who are skilled professionals involving the human intervention and sufficient planning. Some examples of such human-driven cyber attacks are social engineering, phishing, insider threats, whaling etc. Such threats are dangerous and challenging in nature as they involve taking advantage of human behaviour, trust and vulnerabilities making it difficult for prediction using common tools. Identifying human-driven attacks is complicated when compared to the automated attacks. As it involves manipulating human behaviour, the attackers may use encrypted communications over network, may pass through various networks by exfiltrating the data slowly to avoid detection or may fragment the forensic evidence (Guan, 2014).

This chapter focuses on providing a clear understanding about the Network Forensics, the challenges that are faced while collecting dynamic evidence from networks by highlighting the threats posed by the human-driven cyber attacks. It

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186