Forensic Analysis of Network Packets from Penetration Test Toolkits

Da-Yu KAO[a] , Yu-Siang WANG[a] , Fu-Ching TSAI[a] , Chien-Hung CHEN[b]

[a] *Department of Information Management, Central Police University, Taiwan*

[b] *Information Management Office, New Taipei City Department, Taiwan*

*Corresponding Author: dayukao@gmail.com, Tel: +886 3 328 2321*5100*

***Abstract*—Cyber-attacks are likely to continue to increase in size and frequency. As attackers get smarter than before, so do efforts made to protect against unwanted data theft. The purpose of this paper is to look for unusual patterns by repeatable experiments among the constant buzz of network packets that make up PT activities. The utilization of different PT toolkits, like Winfingerprint, Superscan, Nmap, SoftPerfect Network Scanner, NeoTrace, Nessus Vulnerability Scanner, and Path Analyzer Pro, facilitates cyber-attackers to bring down online system. It is capable of discerning network traffic on the vast streams of network information available through the connected machines from the following three phases: data collection, data reduction, and data analysis. Network forensics can aid in detecting attack behavior. This paper accommodates real-time evidence collection as a network feature against attackers. The identification of unusual patterns in network packets has been put to use in the ongoing battle to stay one step ahead of malicious hackers, who could be anyone from disgruntled customers to nation states. This approach can be easily deployed and should be applicable to any type of network-based assessment.**

***Keyword*—Forensic Analysis, Cybercrime Investigation, Network Traffic, Penetration Test, Cyber-attack**

Da-Yu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.

Yu-Siang Wang is a student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan.

Fu-Ching Tsai is a technical specialist in the Computer Center at Central Police University, Taiwan. He received his PhD degree in information management from National Cheng Kung University, Taiwan in 2013. His research interests include big data analysis, data mining, text mining, and artificial intelligence.

Chien-Hung Chen is an Officer at Information Management Office, New Taipei City Police Department. He has devoted to cybercrime investigation and CCTV System management for the past 20 years.