World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:1, 2019

Searching for Forensic Evidence in a Compromised Virtual Web Server against SQL Injection Attacks and PHP Web Shell

Authors : Gigih Supriyatno

Abstract : SQL injection is one of the most common types of attacks and has a very critical impact on web servers. In the worst case, an attacker can perform post-exploitation after a successful SQL injection attack. In the case of forensics web servers, web server analysis is closely related to log file analysis. But sometimes large file sizes and different log types make it difficult for investigators to look for traces of attackers on the server. The purpose of this paper is to help investigator take appropriate steps to investigate when the web server gets attacked. We use attack scenarios using SQL injection attacks including PHP backdoor injection as post-exploitation. We perform post-mortem analysis of web server logs based on Hypertext Transfer Protocol (HTTP) POST and HTTP GET method approaches that are characteristic of SQL injection attacks. In addition, we also propose structured analysis method between the web server application log file, database application, and other additional logs that exist on the webserver. This method makes the investigator more structured to analyze the log file so as to produce evidence of attack with acceptable time. There is also the possibility that other attack techniques can be detected with this method. On the other side, it can help web administrators to prepare their systems for the forensic readiness.

Keywords : web forensic, SQL injection, investigation, web shell
Conference Title : ICDFCI 2019 : International Conference on Digital Forensics and Cybercrime Investigation
Conference Location : Bali, Indonesia
Conference Dates : January 14-15, 2019