Detecting Brute Force Attack and Analyzing Network Traffic Using Wireshark

Nur Khaira Ahmad Shah[1], Abidah Haji Mat Taib[2], Nor Azira Mohd Radzi[3]
[1]*nurkhaira2@gmail.com*
[2]*abidah@uitm.edu.my*
[3]*norazira202@uitm.edu.my*

ABSTRACT

Brute force attacks remain a serious cybersecurity issue, and much research is being conducted to create brute force attack prevention and detection approaches. However, employees' lack of security awareness when it comes to brute force attacks makes them ideal targets for hackers and cybercriminals. Furthermore, the current increase in cybersecurity attacks makes network traffic analysis even more vital. Monitoring network traffic for anomalous behaviour allows for the discovery and prevention of cybersecurity attacks in real-time. Nonetheless, the lack of proper analysis on cybersecurity activities such as network traffic allows the hacker to abuse the website by benefiting from advertisements, stealing personal data, and spreading malware to create disruptions. As a result, this study presents a brute force attack analysis on an experimental testbed for subsequent deployment in SMEs by utilising Wireshark. The research objectives are to create an experimental testbed for showing brute force activities and analyzing network traffic with Graphical Network Simulator-3 (GNS3), as well as to assess limit login attempts in WordPress by examining its capacity to identify and filter brute force attacks. An experimental testbed comprised of one web server, one attacker host, two Cisco 3745 Routers, two GNS3 generic Ethernet switches, and three GNS3 Virtual PC Simulators is developed. Hydra in Kali Linux was used to generate the brute force attack. This project has produced three scenarios. The first and second scenarios examine network traffic before and after the brute force attack respectively, while the third scenario examines one of the brute force attack mitigation measures. For Scenarios 1 and 2, Wireshark is used to examine network traffic. Scenario 2 has a higher total number of packets, average packet size, and average packet per second than Scenario 1. Furthermore, filters such as http. request.method=="POST" and http.response.code==302 are used in Wireshark to identify login attempts. Furthermore, WordPress's restricted login attempts successfully mitigate brute force attacks. This project can be expanded in the future to include an application that detects brute force attacks and notifies the user of the intrusion through notice or email.

Keywords: Network Security, Brute Force Attack, Analyze Network Traffic, Wireshark, GNS3, Hydra