UNIVERSITI TEKNOLOGI MARA

DETECTING BRUTE FORCE ATTACKS AND ANALYZING NETWORK TRAFFIC USING WIRESHARK

NUR KHAIRA BINTI AHMAD SHAH

BACHELOR OF COMPUTER SCIENCES (HONS.) DATA COMMUNICATION AND NETWORKING

JULY 2022

Universiti Teknologi MARA

Detecting Brute Force Attacks and Analyzing Network Traffic Using Wireshark

Nur Khaira Binti Ahmad Shah

**A thesis submitted in fulfilment of the requirement for Bachelor of Science (Hons.) Data Communication and Networking
Faculty of Computer and Mathematical Science**

July 2022

SUPERVISOR APPROVAL

DETECTING BRUTE FORCE ATTACKS AND ANALYZING NETWORK TRAFFIC USING WIRESHARK

By

NUR KHAIRA BINTI AHMAD SHAH
2019405558

This thesis was prepared under the supervision of the project supervisor Ts Dr Abidah Binti Haji Mat Taib. It was submitted to the Faculty of Computer and Mathematical Sciences and was accepted in partial fulfilment of the requirements for the degree of Bachelor of Computer Science (Hons.) Data Communication and Networking.

Approved by

....

Ts Dr Abidah Binti Haji Mat Taib
Project Supervisor

JULY 18, 2022

STUDENT DECLARATION

I certify that this thesis and the project to which it refers is the product of my work and that any idea or quotation from the work of other people, published or otherwise is fully acknowledged in accordance with the standard referring practices of the discipline.

....
NUR KHAIRA BINTI AHMAD SHAH
2019405558

JULY 18, 2022

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 and Scenario 3. Furthermore, filters such as http. request.method=="POST" and http.response.code==302 are used in Wireshark to identify login attempts. Moreover, 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.