COMPRATIVE ANALYSIS OF THREE TYPES OF HONEYPOT AGAINST WEB SERVER ATTACK

Student Name	: Win Nazofa Iqbal
Student ID Number	: 640421006
Supervisor 1	: Danuri, M.Cs
Supervisor 2	: Nurmi Hidayasari, ST., M.Kom

ABSTRACT

In the continuously evolving digital era, the internet becomes a cornerstone in information technology, with its usage ever-increasing and its geographical reach expanding. This growth not only brings benefits but also opens opportunities for cyber-attacks against critical infrastructure such as web servers. Serving as central hubs of information services, web servers face threats like data theft, infrastructure damage, and financial losses due to DDoS, Brute Force, and SQL Injection attacks. Given the importance of maintaining the reliability and security of web servers, the use of honeypots as attack detection tools becomes increasingly relevant. Honeypots, designed to attract and record attacker activities, are categorized into three types based on the level of interaction: low, medium, and high interaction. This study aims to analyze and compare the effectiveness of these three types of honeypots in detecting attacks against web servers. Through comparative analysis, this research endeavors to determine which honeypot is most effective in identifying cyber-attacks with high accuracy and recommends the most suitable type of honeypot for organizations to protect their web server infrastructure. The findings of this study are expected to provide valuable guidance for the development of more effective and proactive cyber security strategies in the face of current and future cyber threats, as well as serving as a reference for future researchers and organizations involved in deploying honeypots for web server security.

Keywoards: Internet, Information Technologi, Web Server, Honeypot.