

ABSTRACT

The development of internet technology makes it easier for users to find the information they need, such as the emergence of websites that make it easier for users to view the information that has been provided. There are websites that are static or dynamic which form a series of interrelated architectures where each can be connected through a network of pages. Because websites usually have information, it is not uncommon for attacks to occur on these websites to get information or damage the system.

Based on the problems that occur, the author creates a honeypot system to trap attackers. The honeypot is used to capture attack activity and the StatusCake monitoring system is added which provides email notifications when an attack occurs. The server is connected to StatusCake by using a public IP. In this final project, the author uses a proxy that connects to a VPN Server to get a public IP and then redirects the public IP to the server's local IP so that it can be connected to StatusCake. Attack information on dionaea logs will be analyzed using splunk.

The result of this final project is an analysis using wireshark where the throughput when attacked by DoS with dionaea defense has an overall throughput average of 6.5916 kbps and when the webserver is attacked by DoS without dionaea defense it has an overall average throughput of 1.093 kbps. There was a decrease in the throughput value of 83.38%.

keywords : Dionaea, DoS, StatusCake, SQL Injection, Webserver