ABSTRACT

THE IMPLEMENTATION OF OPNSENSE AS WEB SERVER SECURITY SYSTEM USING HOST INTRUSION PREVENTION SYSTEM METHOD

By :
Adi Wijaya(1)
Toibah Umi Kalsum(2)
Riska(2)

This research was conducted to detect and prevent disturbances or intrusions that occur on web servers, because by default the security system on web servers in a network still depends on the administrator, so the security of server really depends on the alertness of an administrator in responding to disturbances that occur on the web server. This research is using experimental method. This research was carried out by implementing OPNsense as a web server security system using Host Intrusion Prevention System method. The experimental results are then documented to carry out analysis so that appropriate recommendations are produced for designing a web server security system using HIPS method. The results of this research show that OPNsense can be used as a Host Intrusion Prevention System for LAN networks to secure web servers. OPNsense can prevent Port Scanning carried out on LAN networks. SQL injection process failed because no ID parameter was found. Apart from that, information is also visible that the web server is protected by WAF/IPS. Metasploit application via eth0 does not have permission to carry out a DOS attack on network devices with the address 192.168.80.200, which is the address of the web server.

Keywords: Web Server, OPNsense, HIPS, Port Scan, SQL Injection, DOS Attack

1) Student
2) Supervisors