

INTISARI

Pesatnya perkembangan teknologi tentu tidak lepas dari ancaman yang mengancam pengguna internet di Indonesia menurut Badan Siber dan Sandi Negara pada “lanskap kemandirian siber Indonesia tahun 2022”, BSSN mencatat total 976.429.996 trafik anomali di Indonesia. Salah satu sistem yang dapat membantu dalam pencegahan serangan pada lalu lintas jaringan adalah *firewall*. Salah satu *firewall* yang dapat digunakan secara gratis adalah *firewall pfsense*. Akan tetapi *firewall pfsense* sendiri tidak lepas dari kerentanan, terdapat suatu kerentanan yaitu CVE-2021-41282. Hal tersebut melatarbelakangi penelitian ini, diperlukan solusi yang dapat mempermudah dan mempersingkat proses *penetration testing* untuk kerentanan CVE-2021-41282. Penelitian ini bertujuan untuk membangun sebuah program otomatisasi yang mampu melakukan pemindaian, mendeteksi, mengeksploitasi dan melakukan pembuatan laporan secara otomatis kerentanan CVE-2021-41282 pada *firewall pfsense* sehingga dapat mempercepat dan mempermudah kegiatan *penetration testing*. Pengujian pada penelitian ini dibagi menjadi dua bagian, yaitu pengujian fungsionalitas program otomatisasi dan pengujian waktu eksekusi antara metode manual dengan metode menggunakan program otomatisasi. Hasil pengujian menunjukkan bahwa program mampu melakukan keseluruhan fungsionalitas untuk melakukan *penetration testing* otomatis, mulai dari proses pemindaian, cek kerentanan, eksploitasi, dan pembuatan laporan. Dengan mengimplementasikan program otomatisasi ini, proses *penetration testing* kerentanan CVE-2021-41282 pada *firewall pfsense* dapat dilakukan 30.12% lebih cepat dibanding melakukan *penetration testing* secara manual.

Kata kunci: Otomatisasi, *Penetration testing*, CVE-2021-41282, *Pfsense*, Python, *Metasploit*

ABSTRACT

The rapid development of technology cannot be separated from the threats that threaten internet users in Indonesia according to the National Cyber and Crypto Agency in the Indonesian cyber security landscape in 2022 the total anomalous traffic in Indonesia during 2022 was 976,429,996 anomalies. One system that can help in preventing attacks on network traffic is a firewall. One of the firewalls that can be used for free is the pfsense firewall. However, the pfsense firewall itself is not free from vulnerabilities, there is a vulnerability, namely CVE-2021-41282. Based on that background, a solution is needed that can simplify and shorten the penetration testing process for the CVE-2021-41282 vulnerability. This research aims to build an automation program that is able to automatically scan, detect, exploit and report the CVE-2021-41282 vulnerability in the pfsense firewall so that it can speed up and simplify penetration testing activities. Testing in this study is divided into two parts, namely testing the functionality of the automation program and testing the execution time between the manual method and the method using the automation program. The results of this research show that the program is able to perform the entire functionality to perform automated penetration testing, starting from the scanning process, vulnerability checking, exploitation, and reporting. Through this automation program, the penetration testing process for the CVE-2021-41282 vulnerability in the pfsense firewall can be done 30.12% faster than doing penetration testing manually.

Keywords: Automation, Penetration Testing, CVE-2021-41282, Pfsense, Python, Metasploit