

## **INTISARI**

### **USULAN PROYEK AKHIR**

#### **PENGEMBANGAN PROGRAM OTOMATISASI UJI PENETRASI CVE-2018-14847 PADA PERANGKAT JARINGAN MIKROTIK BERBASIS PYTHON DAN SHODAN**

Indonesia merupakan salah satu negara yang menggunakan perangkat jaringan MikroTik paling tinggi, peringkat ketiga tertinggi di dunia (The Shadowserver Foundation, 2023). Dibalik penggunaan yang luas dan banyaknya manfaat yang diperoleh, terdapat kerentanan CVE-2018-14847 pada perangkat jaringan MikroTik. Kerentanan ini memungkinkan penyerang melakukan serangan jarak jauh tanpa autentikasi untuk melakukan pembacaan file dan serangan jarak jauh yang sudah terautentikasi untuk melakukan penulisan file karena adanya kerentanan *directory traversal* pada protokol Winbox. Dilatarbelakangi oleh masifnya penggunaan perangkat jaringan MikroTik di Indonesia, diperlukan solusi yang dapat mempermudah dan mempersingkat proses uji penetrasi untuk kerentanan CVE-2018-14847 pada perangkat jaringan MikroTik. Penelitian ini bertujuan untuk mengembangkan sebuah program otomatisasi yang mampu melakukan pemindaian, eksploitasi, dan pelaporan secara otomatis untuk proses uji penetrasi kerentanan CVE-2018-14847 pada perangkat jaringan MikroTik berbasis Python dan Shodan dengan harapan dapat mempermudah dan mempersingkat proses uji penetrasi. Pengujian pada penelitian ini dibagi menjadi dua bagian, yaitu uji fungsionalitas program otomatisasi dan uji perbandingan waktu antara metode manual dengan metode menggunakan program otomatisasi. Hasil dari penelitian ini menunjukkan bahwa program mampu melakukan keseluruhan fungsionalitas untuk melakukan uji penetrasi otomatis, mulai dari proses pemindaian, eksploitasi, dan pelaporan otomatis. Dengan diterapkannya program otomatisasi ini, proses uji penetrasi CVE-2018-14847 pada perangkat jaringan MikroTik dapat dilakukan 93.46% lebih cepat pada modul pencarian berdasarkan rentang alamat IP dan 94.37% lebih cepat pada modul pencarian berdasarkan nama organisasi.

**Kata kunci:** Otomatisasi, Uji Penetrasi, CVE-2018-14847, MikroTik, Python, Shodan

## ABSTRACT

*Indonesia is one of the world's highest users of MikroTik network devices, ranking third in the world (The Shadowserver Foundation, 2023). Behind the massive use and benefits obtained, there is a CVE-2018-14847 vulnerability on MikroTik network devices. This vulnerability opens the possibility for an unauthenticated remote attack that allows the attackers to read files and an authenticated remote attack to write files due to a directory traversal vulnerability in the Winbox protocol. The reasoning behind this is the extensive use of MikroTik network devices in Indonesia, a solution is needed that simplifies and shortens the penetration test process for the CVE-2018-14847 vulnerability on MikroTik network devices. This study aims to develop an automation program that is capable of scanning, exploiting, and reporting automatically for the CVE-2018-14847 vulnerability penetration testing process on Python and Shodan-based MikroTik network devices with the hope to simplify and shorten the penetration testing process. The test of this study was divided into 2 separate parts, namely testing the functionality of the automation programs, and testing the time comparison between the manual method and the method using the automation program. Results from this study indicate that the programs can carry out all the functionality to perform automatic penetration testing, starting from the process of scanning, exploiting, and reporting automatically. By implementing this automation program, the CVE-2018-14847 penetration test process on MikroTik network devices will perform 93.46% faster in the search module based on the IP address range and 94.37% faster in the search module based on the name of the organization.*

**Keywords:** *Automation, Penetration Test, CVE-2018-14847, MikroTik, Python*