INTISARI

Internet di Indonesia menggunakan perangkat dari vendor yang bernama MikroTik. MikroTik adalah salah satu vendor perangkat yang umum digunakan untuk kebutuhan infrastruktur internet di Indonesia. Indonesia sendiri memiliki 230.000 perangkat MikroTik yang terpapar ke internet. Karena hal itu, Indonesia menduduki peringkat ketiga di dunia dalam hal penggunaan MikroTik pada infrastrukturnya ('*Observations on cyber threat activity and vulnerabilities in Indonesia, Malaysia, Philippines and Thailand*: The Shadowserver Foundation', 2023). MikroTik juga memiliki kerentanan atau *vulnerability* pada perangkatnya. Salah satunya CVE-2023-30799 yang bisa mengakses router dengan meningkatkan akses admin menjadi *super-admin* melalui antarmuka *winbox* atau layanan web HTTP. Kerentanan ini memungkinkan penyerang mengesekusi kode atau perintah melalui *backdoor*. Disebabkan oleh banyaknya perangkat MikroTik di Indonesia, diperlukan sebuah uji pengamanan efisien untuk CVE-2023-30799. Penelitian ini bertujuan untuk mengembangkan program eksploitasi dan *reporting* secara otomatis dengan menggunakan Python. Harapan penelitian ini agar dapat memperoleh solusi menghemat waktu dalam melakukan *security assessment* untuk CVE-2023-30799. Pengujian penelitian dibagi menjadi diua yaitu uji fungsionalitas dan uji perbandingan waktu antara metode manual dengan otomatis. Hasil penelitian menunjukkan bahwa program mampu dieksekusi tanpa kesalahan dan mampu menjalankan fungsi eksploitasi dan *reporting* dengan benar. Dengan dterapkannya program otomatisasi yang dibuat pada peneilitian ini, proses *penetration testing* pada CVE-2023-30799 pada perangkat *router* MikroTik dapat dilakukan 79,1% lebih cepat daripada metode manual

Kata kunci: mikrotik, otomatisasi, *penetration testing*, keamanan siber

ABSTRACT

The Internet infrastructure in Indonesia relies extensively on devices provided by a vendor known as MikroTik. MikroTik stands as one of the prevalent equipment vendors catering to the internet infrastructure requirements within the Indonesian context. The nation boasts a staggering count of 230,000 MikroTik devices exposed to the internet. Consequently, Indonesia occupies the third position globally in terms of MikroTik device adoption for its infrastructure ('Observations on cyber threat activity and vulnerabilities in Indonesia, Malaysia, Philippines and Thailand: The Shadowserver Foundation', 2023). However, MikroTik devices are not immune to vulnerabilities. Notably, one such vulnerability identified is CVE-2023-30799, enabling unauthorized access to routers by elevating admin privileges to super-admin via the Winbox interface or HTTP web service. This vulnerability potentially allows attackers to execute arbitrary code or commands through a backdoor. Given the pervasive presence of MikroTik devices in Indonesia, there arises a necessity for an efficient security assessment concerning CVE-2023-30799. This study aims to develop an automated exploitation and reporting program utilizing Python. The research endeavors to streamline the time-consuming security assessment process associated with CVE-2023-30799, thus envisaging time-saving solutions. The research methodology involves two primary phases: functional testing and a comparative analysis of time efficiency between manual and automated methods. The findings indicate error-free execution of the program, proficiently carrying out exploitation functions and reporting accurately. By implementing the automation program devised in this study, the penetration testing process for CVE-2023-30799 on MikroTik router devices can be expedited by 79,1% compared to manual methods.

Keywords: *mikrotik, automation, penetration testing, cyber security*