INTISARI

Perkembangan teknologi mampu menciptakan berbagai macam inovasi untuk memenuhi serta mempermudah berbagai aspek maupun bidang dalam kehidupan. PaperCut merupakan bentuk nyata penggunaan teknologi dalam menciptakan kemudahan di bagian percetakan yang mampu untuk mengelola manajemen pencetakan suatu organisasi dalam melakukan pelacakan, mengelola pencetakan, penyalinan, pemindaian dan faks melalui integrasi perangkat keras. Namun dibalik kemudahan serta manfaat tersebut terdapat kerentanan CVE-2023-27350 pada PaperCut yang memungkinkan pelaku penyerangan melewati otentikasi pada sistem, sehingga berpotensi membahayakan keamanan pada seluruh jaringan. Perlu adanya bentuk implementasi di bidang keamanan informasi untuk melakukan evaluasi terhadap keamanan sistem atau perangkat PaperCut. Penelitian ini bertujuan untuk menganalisis efektivitas kinerja sistem otomatisasi uji penetrasi dalam mengidentifikasi dan mengatasi kerentanan CVE-2023-27350 pada perangkat lunak PaperCut. Metode yang digunakan adalah pengujian dan pembandingan dua sistem uji penetrasi yang berbeda, yaitu otomatisasi dan manual. Penelitian ini mempertimbangkan beberapa faktor dalam evaluasi efektivitas, seperti penggunaan waktu dan penggunaan CPU selama proses uji penetrasi berlangsung. Hasil penelitian menunjukkan bahwa fungsionalitas program uji penetrasi otomatis dapat bekerja dengan baik dan mampu mengidentifikasi kerentanan CVE-2023-27350 secara lebih efektif, akan tetapi membutuhkan beban CPU yang sedikit lebih besar dibandingkan dengan sistem uji penetrasi manual. Dalam melakukan uji penetrasi menggunakan batasan pemindaian target, program otomatisasi mampu menghemat waktu sekitar 54.95% dengan penggunaan CPU 6,08% lebih besar dari metode manual, sedangkan untuk pengujian penetrasi tanpa batasan pemindaian target, program otomatisasi mampu menghemat waktu sekitar 59.78% dengan penggunaan CPU 8,21% lebih besar dari metode manual.

Kata kunci: Otomatisasi, Uji Penetrasi, CVE-2023-27350, PaperCut, Efektivitas

ABSTRACT

The development of technology creates various kinds of innovations to fulfill and facilitate various aspects and fields in life. PaperCut is a real form of using technology creating eases in the printing department that allows organization manage printing management in tracking, managing printing, copying, scanning and faxing through hardware integration. But behind these ease and benefits is the CVE-2023-27350 vulnerability in PaperCut which allows attackers to bypass authentication system, this potentially endangering security on the entire network. Implementation in the field of information security is needed to evaluate the security of the PaperCut system or device. This study aims to analyze the effectiveness of the performance a penetration test automation system in identify and overcome the CVE-2023-27350 vulnerability in PaperCut software. The method used is testing and comparing two different penetration test systems, which are automation and manual. This study considers several factors in evaluating effectiveness, such as time usage and CPU usage during the penetration test process. The results show that the functionality of the automated penetration test program can work well and is able to identify CVE-2023-27350 vulnerabilities more effectively but requires a slightly larger CPU load compared to the manual penetration test system. in performing penetration tests using target scanning restrictions, the automation program able to save about 54.95% of time with 6.08% more CPU usage than the manual method, while for penetration testing without target scanning restrictions, the automation program able to save about 59.78% of time with 8.21% more CPU usage than the manual method.

Keywords: *Automation, Penetration Testing, CVE-2023-27350, PaperCut, Effectiveness*