

Pengembangan One Stop CIS Benchmark Auditing Tool (OSCAT) sebagai Aplikasi Audit Konfigurasi Host Berdasarkan CIS Benchmark = One Stop CIS Benchmark Auditing Tool (OSCAT) Development as a Host Configuration Auditing Tool Based on CIS Benchmark

Ahmad Sholihin, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920564919&lokasi=lokal>

Abstrak

Audit konfigurasi host merupakan hal yang krusial dalam memastikan keamanan sistem dan kepatuhan terhadap berbagai regulasi maupun praktik terbaik keamanan siber. Kesalahan konfigurasi dapat menyebabkan kerentanan yang bisa dieksploitasi oleh pelaku kejahatan. Namun di sisi lain, melakukan audit secara manual bisa sangat memakan waktu dan juga rawan terjadi kesalahan. Untuk mengatasi hal ini, penelitian ini mengajukan untuk membangun One Stop CIS-Benchmark Auditing Tool (OSCAT), sebuah sistem yang dapat digunakan untuk mengotomasi proses audit konfigurasi host. OSCAT menggunakan standar Center of Internet Security (CIS) Benchmark yang umum digunakan di berbagai belahan dunia sebagai standar industri untuk menerapkan dan mengaudit konfigurasi sistem berdasarkan praktik keamanan terbaik. Dengan mengotomasi proses audit, OSCAT dapat mengurangi human error, meningkatkan efisiensi, dan meningkatkan postur keamanan secara keseluruhan. Penelitian ini dilakukan untuk memaparkan perancangan, arsitektur, implementasi, dan juga evaluasi dari aplikasi OSCAT. Uji coba audit dilakukan terhadap sistem operasi RedHat Enterprise Linux 7 dengan konfigurasi bawaan. Hasilnya untuk kontrol yang bersifat Automatic, hasil audit dengan OSCAT lebih akurat 20,16% dibanding tool serupa.Host configuration audits are crucial for ensuring system security and compliance to regulations and/or security best practice. Misconfigurations can lead to vulnerabilities that can be exploited by malicious actors. On the other hand, manual audits are time-consuming and error-prone. To address this challenge, this research proposed to build the One Stop CIS-Benchmark Auditing Tool (OSCAT) to automate auditing process. OSCAT leverages the Center for Internet Security (CIS) benchmarks that is widely used as industry-standard to assess system configurations against security best practices. By automating the audit process, OSCAT significantly reduces human error, improves efficiency, and enhances overall security posture. This research aims to develop, implement, and evaluate the OSCAT application. An audit trial performed on a RedHat Enterprise Linux 7 operating system with default configuration. The results for Automatic controls, the audit results using OSCAT were 20.16% more accurate than similar tools.