CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 5, No. 2, November 2022, hlm. 83-88

IMPLEMENTASI *SECURITY AUDITOR* UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS MENGGUNAKAN CIS *BENCHMARK*

Muhammad Najib[1], Bambang Purnomosidi[2], Muhammad Agung Nugroho[3]

[1]Informatika, Universitas Teknologi Digital Indonesia
Email: [1]175410171@students.akakom.ac.id, [2]bpdp@utdi.ac.id, [3]m.agung.n@utdi.ac.id

Abstrak

Pertumbuhan layanan sistem pada era ini semakin banyak dan variatif, termasuk juga adalah layasan SaaS. Pada layanan SaaS kebutuhan sebuah kemanan informasi itu cukup penting dan vital. Salah satu cara meningkatkan keamanan adalah dengan melakukan *hardening* pada server yang digunakan. Hardening dapat dilakukan jika memiliki data konfigurasi pada sistem dan kontrol terdahap isu-isu kemanan informasi. Penelitian ini bertujuan untuk mengimplementasikan CIS *Security* untuk mengetahui hasil audit dari CIS *Benchmark* berupa penilaian sehingga dapat meningkatkan keamanan sistem operasi Centos 6.10 dengan rekomendasi dari CIS Security ini. Sistem ini dibuat bertujuan untuk melakukan audit pada server dengan sistem operasi Centos 6. 10, kemudian hasil dari audit akan ditampilkan dalam data agar lebih mudah dibaca dan dapat dijadikan bahan untuk menjadi evaluasi bagi instalasi layanan SaaS agar lebih baik. Dalam sistem security auditor ini terdapat 2 buah server, masing-masing adalah *server testing* dan *server pool*. *Server testing* adalah server yang akan di audit menggunakan program audit yang disesuaikan dengan CIS *Benchmark*. Program audit ini ditulis dalam bahasa *bash script*. Hasil audit dapat dikirimkan ke server pool dan ditampilkan oleh *server pool* dengan halaman web. Pada server pool ini menggunakan PHP sebagai *backend* dengan manajemen datanya adalah mysql. Sedangkan menggunakan *framework Bootsrap* untuk memudahkan dari sisi frontend. Enviroment *server pool* ini dijalankan dengan virtulasisasi *docker*. Berdasarkan analisa yang dilakukan sehingga diperoleh hasil yaitu sistem security auditor untuk standardisasi instalasi server pada layanan SaaS menggunakan CIS *Benchmark*. Untuk membangun sebuah security auditor membutuhkan standardisasi yang sudah diakui dunia. CIS *Control* memiliki kaitan penting dalam implementasi ISO 27001. Dalam sistem security auditor ini dapat memberikan nilai pada setiap hasil audit yang dijalankan pada server testing dengan CIS *Benchmark* berdasarkan CIS *Control*. Selain itu sistem ini memberikan ceklist data hasil audit yang dapat digunakan *System Administrator* untuk mengevaluasi instalasi server pada layanan SaaS.

Kata kunci: audit keamanan sistem, CIS *benchmark*, CIS *Control*, CIS *Security*, ISO 27001

THE IMPLEMENTATION OF A SECURITY AUDITOR FOR STANDARDIZATION OF SERVER INSTALLATION ON SAAS SERVICES USING CIS BENCHMARK

Abstract

The development of system services this year is increasing, especially SaaS services. In SaaS services, the need for information security is quite important. One of the solutions to improve security in the system is to harden the server used. Hardening can be done if you have configuration data on the design and controls for information security issues. This study aims to implement CIS Security to find out the results of an audit from CIS Benchmark in the form of an assessment so that it can improve the security of the Centos 6.10 operating system with recommendations from CIS Security. This research is building a system to conduct an audit on a server with the Centos 6.10 operating system; then, the audit results will be displayed in the data so that it is easier to read and can be used as material for evaluation for better SaaS service installations. In this security auditor system, there are two servers: a testing server and a pool server. Server testing is a server that will be audited using an audit program that is adjusted to the CIS Benchmark. This audit program is written in a bash script language. Audit results can be sent to the pool server and displayed by the pool server with a web page. This server pool uses PHP as the backend, with MySQL as data management.

At the same time, use the Bootstrap framework to beautify the front end. The server pool environment is run with docker virtualization. Based on the analysis, the results are a security auditor system for standardizing server installations in SaaS services using CIS Benchmarks. Building a security auditor requires standardization that has been recognized worldwide. CIS Control has an important link in the implementation of ISO 27001. The system can give a value to each audit result run on the testing server with CIS Benchmark based on CIS Control. In addition, this system provides a checklist of audit results data that System Administrators can use to evaluate server installations on SaaS services.

Keywords*: network security auditing, CIS benchmark, CIS control, CIS security, ISO 27001*

1. PENDAHULUAN

Di era industri 4.0 ketergantungan dunia terhadap layanan daring semakin tinggi. Dengan demikian kebutuhan akan layanan-layanan berbasis internet semakin meningkat. Seiring dengan kebutuhan, *traffic*, dan layanan yang semakin tinggi, semakin meningkat juga ancaman siber yang terjadi. Ancaman-ancaman (Yudha and Panji, 2018) ini terdiri dari Ancaman terhadap penyedia layanan, yang secara umum memiliki ancaman pada sisi server seperti *SQL Injection*, *command injection*, *command execution*, *file inclusion*, dan *server take over*. Sementara dari sisi internet provider, ancaman dapat berupa DDOS, *smurfing*, *ARP poisoning*, dan BGP *Attacking*. Selain ancaman terhadap penyedia layanan, pengguna juga mendapatkan ancaman serangan keamanan seperti *client-side hacking*, XSS, CSRF *Injection*, *virus*, *trojan*, dsb (Afif, 2017). Dalam pendekatan lain, serangan dapat berupa social engineering dimana metode yang digunakan untuk mendapatkan informasi penting dengan cara menipu pemilik informasi, mekanismenya dapat dilakukan dengan telpon, aplikasi internet, dan pendekatan lain seperti menggunakan teknik XSS.

CIS *Security* merupakan metode yang dikembangkan oleh CIS, yang memiliki misi untuk identifikasi, pengembangan, validasi, promosi, dan mempertahankan solusi terbaik untuk pertahanan cyber, membangun mindset masyarakat untuk meningkatkan lingkungan terpercaya di dunia maya. Metode yang dikembangkan adalah model *crowdsourcing* (keterlibatan pihak lain dalam pengembangan konten dan sumber daya/source). CIS menerapkan crowdsourcing secara tertutup (closed contribution). CIS *Security* (Sedano and Salman, 2021) memiliki program pada lingkungan-lingkungan seperti CIS *Control*, CIS *Benchmark*, CIS *Communities*, dan CIS *Cybermarket*.

Dalam penelitian ini, penulis menggunakan objek pada layanan SaaS yang dikembangkan oleh salah satu perusahaan teknologi dan informasi di Jogja. SaaS ini merupakan layanan sistem akademik untuk perguruan tinggi dengan integrasi kesesuaian dengan regulasi DIKTI. Sistem ini dikenal dengan E-campuz yang mengelola proses admisi, registrasi, pembayaran, akademik, pelaporan PDDikti dan portal mahasiswa (Rozady, 2022). Penggunaan sistem E-campuz ini yang berbasis Cloud Computing dengan model SaaS. Layanan e-campuz berjalan secara *cloud*, dan penulis akan menganalisis keamanan pada layanan ini berdasarkan standar implementasi CIS *benchmark* (Najib, 2021). Tujuan dari penelitian ini adalah untuk mendapatkan data ceklist kemanan pada layanan SaaS dengan CIS *Control* menggunakan CIS *Benchmark*, meningkatkan kemanan pada layanan SaaS dengan mengimplementasikan standardisasi CIS *Control* dari CIS *Security*, implementasi ISO 27001 berdasarkan CIS, dan *control* pada layanan SaaS, dan membantu *System Administrator* dalam melakukan evaluasi dari instalasi layanan Saas yang bersifat rutin.

1.A. Sistem Manajemen Keamanan Informasi

Keamanan Informasi di dunia maya atau kemanan siber adalah teknologi, proses dan praktik yang dirancang untuk melindungi jaringan, komputer, program dan data dari serangan, kerusakan atau akses yang tidak sah (Sari et al., 2020). Cyber security juga disebut sebagai upaya untuk melindungi informasi dari adanya *cyber attack*. Sistem Manajemen Keamanan Informasi adalah suatu sistem manajemen yang berhubungan dengan penerapan keamanan informasi di suatu organisasi yang meliputi kegiatan perancangan, penerapan, dan pemeliharaan suatu rangkaian terpadu proses dan sistem untuk secara efektif mengelola keamanan informasi khususnya kerahasian, integritas, dan ketersediaan aset informasi sekaligus meminimalisasi risiko yang menyertainya.

1.B. ISO 27001

ISO 27001 adalah standar sistem manajemen yang di terbitkan oleh ISO (*International Organization for Standardization*) yang bekerja sama dengan IEC (*International Electrotechnical Commission*) yang berfokus kepada sistem keamanan informasi. Standar ini menggunakan pendekatan manajemen yang berbasis kontrol berdasarkan analisis risiko. Standar ini banyak diterapkan terutama bagi perusahaan/organisasi yang menganggap bahwa informasi merupakan aset perusahaan yang harus dilindungi (Februari and Fitria, 2019). Selanjutnya ISO/IEC 27001 dijelaskan sebagai salah satu metode dengan standard keamanan informasi yang diterbitkan International *Organization for Standarization dan International Electrotecnical Comission*. ISO 27001 juga didefinisikan sebagai dokumen standar sistem manajemen keamanan informasi (Arini, 2019) atau *Information Security Management System*, biasa disebut ISMS, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah institusi dalam usaha mereka untuk mengevaluasi, mengimplementasikan, dan memelihara keamanan informasi berdasarkan *best practice* dalam pengamanan informasi

1.C. CIS *Benchmark*

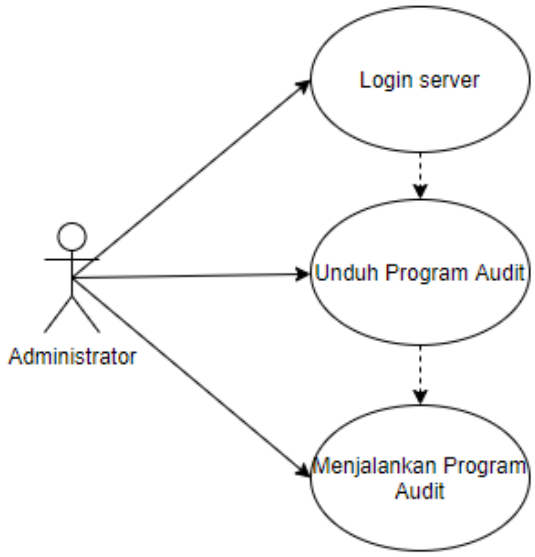
CIS *Benchmark* merupakan garis dasar konfigurasi dan praktik terbaik untuk mengonfigurasi sistem dengan aman. Setiap rekomendasi panduan merujuk pada satu atau lebih CIS *Control* yang dikembangkan untuk membantu organisasi meningkatkan kemampuan pertahanan dunia maya mereka. CIS *Control* (cisecurity, 2022) memetakan ke banyak standar yang ditetapkan dan kerangka kerja

peraturan, termasuk Kerangka Kerja Keamanan Siber (CSF) NIST dan NIST SP 800-53, seri standar ISO 27000, PCI DSS, HIPAA, dan lainnya. Dapat diarktikan juga CIS *Benchmark* (Prastika et al., 2018) adalah sebuah best-pratice yang diterbitkan oleh *Center for Internet Security* (CIS) dan didokumentasikan untuk mengonfigurasi sistem, perangkat lunak, dan jaringan TI dengan aman. CIS Benchmark dikembangkan melalui proses berbasis konsensus unik yang melibatkan komunitas profesional keamanan siber dan pakar materi pelajaran di seluruh dunia, yang masing-masing terus mengidentifikasi, menyempurnakan, dan memvalidasi praktik terbaik keamanan dalam area fokus mereka.

2. METODOLOGI

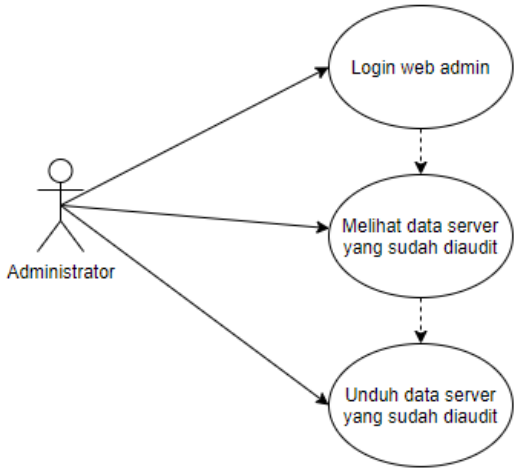
2.A. Rancangan Sistem

Rancangan proses pada penelitian ini di jelaskan pada gambar 1. untuk menjalankan program audit, mulai dari administrator melakukan login pada server kemudian dapat melakukan unduh program terlebih dahulu, kemudian menjalankan program pada server yang akan di audit.



Gambar 1. Use case diagram menjalankan program audit

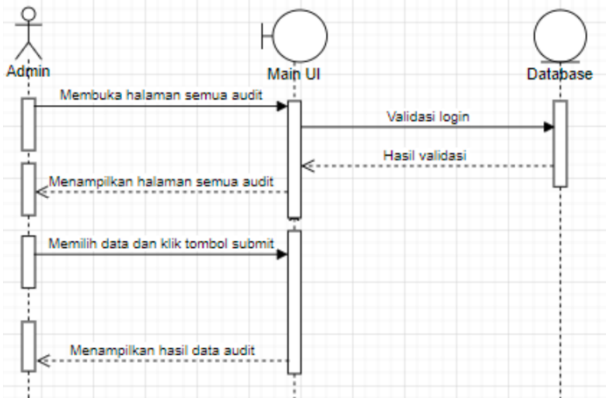
Use Case Diagram melihat dan mengunduh data hasil audit digambarkan pada gambar 2, yaitu ketika administrator melakukan login pada web admin kemudian administrator dapat melihat server mana saja yang sudah diaudit serta adminstrator dapat mengunduh data hasil audit dari server pool.



Gambar 2. Use case diagram melihat dan mengunduh data

Activity Diagram Proses Audit digambarkan terdapat 3 bagian yaitu administrator, sistem dan *server pool*. Adminstrator adalah sebagai aktor. Ketiga bagian tersebut saling berhubungan mulai dari administrator melakukan login sebagai *root* ke sistem/server yang akan di audit kemudian mengunduh program audit, kemudian selanjutnya adalah menjalankan program audit sehingga sistem akan memproses setiap audit bersamaan dengan sistem menampilkan data yang sudah diaudit pada monitor, kemudian jika server tersebut memiliki koneksi akan langsung mengirim data pada *server pool* apabila jika tidak makan akan muncul pesan *error* pada layar. Setelah *server pool* mendapatkan data dari sistem yang diaudit, maka *server pool* akan mengolah data tersebut menjadi data visual dan dokumen yang kemudian dapat diunduh oleh administrator.

Squence diagram pada aplikasi yang dibuat oleh penulis dideskripsikan pada gambar 3, menjelaskan tentang alur Admin pada saat membuka halaman semua audit. Hal ini terjadi saat Admin membuka halaman semua audit system akan langsung melakukan validasi apakah Admin sudah login atau belum, jika belum akan diarahkan ke halaman login, jika sudah akan menampilkan halaman semua audit.



Gambar 3. *Squence* Diagram melihat semua data audit

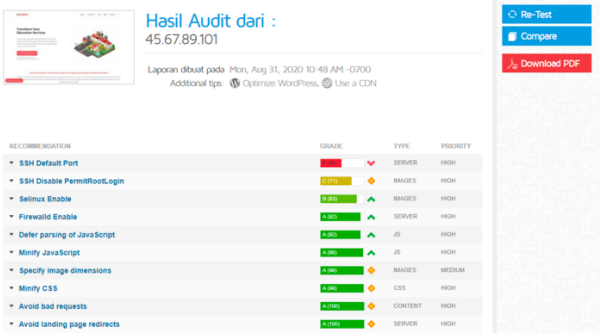
2.B. Rancangan Antarmuka

Pada sistem ini rancangan antarmuka dibagi menjadi dua macam, yaitu rancangan antarmuka untuk *console base* dan juga untuk *web base*. Gambar 4 mendeskripsikan Rancangan Console Base yang merupakan rancangan antarmuka pada saat menjalankan program audit berdasarkan CIS *Benchmark*. Program audit ini akan ditulis dalam bahasa *python*. Pada layar monitor akan menampilkan semua data yang telah diaudit dan akan terlihat pada layar monitor.

```
root@najib # ./cis_centos_7_scoring.py
starting......
Checking SSH Default port ..... pass
Checking SSH Disable PermitRootLogin ..... pass
Checking Selinux Enable .... pass
Checking Firewalld Enable .... pass
Checking disable FTP.... Pass
Checking rkhunter installed?..... pass
Checking gcc disable ..... pass
.
.
.
Sending result to server..... success
```

Gambar 4. Rancangan antarmuka *console base*

Untuk rancangan antarmuka dalam bentuk web digambarkan pada gambar 5. Halaman ini untuk tampilan *dashboard* pada web browser, jadi pada halaman ini langsung terlihat hasil audit dan juga tombol untuk mengunduh hasil audit berupa PDF.



Gambar 5. Rancangan antarmuka web base

3. PEMBAHASAN

Pada penelitian ini script CIS *Benchmark* ditulis menggunakan bahasa pemrograman bash, dalam CIS_CentOS_Linux_7_Benchmark_v2.1.1 ini terdapat 223 poin yang dijalankan untuk mendokumentasikan konfigurasi pada suatu sistem yang diaudit seperti digambarkan pada hasil gambar 6.

Gambar 6. Tampilan hasil audit

Setelah poin-poin tersebut diaudit akan dilakukan sebuah penilaian berdasarkan *Profile Definitions* dari CIS *Benchmark*.

3.A. Informasi Penilaian

Status penilaian menunjukkan apakah kepatuhan terhadap rekomendasi yang diberikan berdampak pada menilai skor *benchmark* pada server yang diaudit. Berikut adalah patokan dari status yang digunakan:

1) *SCORED*, Kegagalan untuk mematuhi rekomendasi "SCORED" akan menurunkan skor benchmark akhir. Kepatuhan dengan rekomendasi "SCORED" akan meningkatkan skor *benchmark* akhir.

2) *NOT SCORED*, Kegagalan untuk mematuhi rekomendasi "Not Scored" tidak akan menurunkan final skor *benchmark*. Kepatuhan dengan rekomendasi "Not Scored" tidak akan meningkatkan skor patokan akhir.

3.B. *Profile Definitions*

Profile Definitions atau definisi profil bersarkan CIS dibagai menjadi 4, yaitu : Level 1 – *Server*, Level 2 – *Server*, Level 1 – *Workstations* dan Level 2 – *Workstations*. Masing-masing profil memiliki karakteristik dan maksud yang bermacam-macam berikut adalah definisi lengkapnya :

1) Level 1 – *Server*, Item di profil ini bermaksud untuk Bersikap praktis dan bijaksana; Memberikan manfaat keamanan yang jelas; dan Tidak menghambat penggunaan teknologi di luar kemampuan yang dapat diterima.

2) Level 2 – *Server*, Profil ini memperluas profil "Level 1 - Server". Item di profil ini menunjukkan satu atau lebih dari karakteristik berikut: Dimaksudkan untuk lingkungan atau kasus penggunaan di mana keamanan adalah yang terpenting; Bertindak sebagai pertahanan

secara mendalam; Dapat secara negatif menghambat utilitas atau kinerja teknologi.

3) Level 1 – *Workstation*, terdiri dari Bersikap praktis dan bijaksana; Memberikan manfaat keamanan yang jelas; dan Tidak menghambat penggunaan teknologi di luar kemampuan yang dapat diterima.

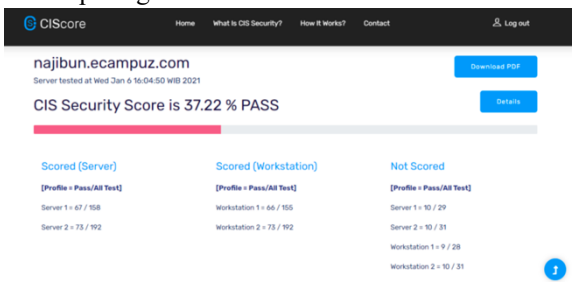
4) Level 2 – *Workstation*, Profil ini memperluas profil "Level 1 - Workstation". Item di profil ini menunjukkan satu atau lebih dari karakteristik berikut : Dimaksudkan untuk lingkungan atau kasus penggunaan di mana keamanan adalah yang terpenting; Bertindak sebagai pertahanan secara mendalam; Dapat secara negatif menghambat utilitas atau kinerja teknologi.

Sistem yang dikembangkan dapat melakukan proses penyimpanan hasil audit berdasarkan CIS *benchmark* seperti yang pada gambar 7.

```
Results

Scored (Server)
=================================
Server 1 = 67 / 158
Server 2 = 73 / 192

Scored (Workstation)
=================================
Workstation 1 = 66 / 155
Workstation 2 = 73 / 192

Not Scored (Server)
=================================
Server 1 = 10 / 29
Server 2 = 10 / 31

Not Scored (Workstation)
=================================
Workstation 1 = 9 / 28
Workstation 2 = 10 / 31
Do you want to save and send the result? [y,n]y
Please wait
..................................... Done
202102101222.azzahra.ecampuz.com
najib@185.53.129.97's password:
202102101222.azzahra.ecampuz.com
```

Gambar 7. Proses menyimpan dan mengirimkan hasil audit

Hasil ujicoba sistem, script pada server dapat berjalan dan memberikan hasil pengujian dalam bentuk CIS security score untuk ditampilkan dari sisi front end. CIS security score menggunakan profile penilaian dan profile definitions, hasil dari sistem ini dapat dilihat pada gambar 8.



Gambar 8. Hasil audit

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan pada saat Implementasi *Security Auditor* untuk Standardisasi Instalasi Server Pada Layanan SaaS Menggunakan CIS *Benchmark* dapat disimpulkan perancangan sistem diperlukan standarisasi yang diakui terkait manajemen keamanan informasi, salah satunya adalah standar ISO 27001. Sistem yang dibuat mengadopsi ISO 27001 dengan menggunakan CIS *Security* Untuk menjalankan CIS *Control* pada sebuah sistem memerlukan proses membaca dan mendokumentasikan konfigurasi pada sebuah server. Proses membaca dan mendokumentasikan konfigurasi berdasarkan CIS *Control* berdasarkan CIS *Benchmark*. Perancangan sistem security auditor dapat berjalan dengan baik dan mampu diimplementasikan dengan script yang dijalankan untuk mengaudit sebuah sistem operasi linux, pengembangan frontend dan backend menggunakan PHP.

Saran yang diperlukan untuk pengembangan sistem ini seperti menambahkan beberapa script audit pada sistem operasi selain Centos. Karena saat ini script CIS *Benchmark* hanya berjalan pada sistem operasi Centos. Menambahkan satu modul atau fitur yang digunakan untuk menambah user pada aplikasi. Karena saat ini untuk penambahan user masih melalui database. Menambahkan fitur untuk memfilter data hasil audit agar mempermudah dalam pencarian data.

DAFTAR PUSTAKA

AFIF, M.F., 2017. IMPLEMENTASI KEAMANAN OWASP TERHADAP APLIKASI BERBASIS GTFW (skripsi). STMIK AKAKOM Yogyakarta.

ARINI, A., 2019. PENDETEKSIAN DINI TINGKAT KEMANAN INFORMASI BERBASIS ISO 27001: 2013 MENGGUNAKAN METODE AHP (ANALYTICAL HIERARCHY PROCESS). Cyber Secur. Dan Forensik Digit. 2, 57–64.

CISECURITY, 2022. CIS Controls Version 8 [WWW Document]. Cent. Internet Secur. URL https://www.cisecurity.org/controls/v8/ (accessed 1.4.23).

FEBRUARI, P., FITRIA, F., 2019. Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung. POSITIF J. Sist. Dan Teknol. Inf. 5, 97–102. https://doi.org/10.31961/positif.v5i2.833

NAJIB, M., 2021. IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS ECAMPUZ MENGGUNAKAN CIS BENCHMARK (skripsi). STMIK AKAKOM YOGYAKARTA.

PRASTIKA, D.P., TRIYONO, J., LESTARI, U., 2018. AUDIT DAN IMPLEMENTASI CIS BENCHMARK PADA SISTEM OPERASI LINUX DEBIAN SERVER (STUDI KASUS: SERVER LABORATORIUM JARINGAN DAN KOMPUTER 6, INSTITUT SAINS & TEKNOLOGI AKPRIND YOGYAKARTA). J. Jarkom 6, 1–12.

ROZADY, M.P.N., 2022. TATA KELOLA TI DALAM PEMANFAATAN SISTEM E-CAMPUZ BERBASIS CLOUD COMPUTING PADA UNIVERSITAS NUSA NIPA MAUMERE. Increate - Inov. Dan Kreasi Dalam Teknol. Inf. 5.

SARI, I.Y., MUTTAQIN, M., JAMALUDIN, J., SIMARMATA, J., RAHMAN, M.A., ISKANDAR, A., PAKPAHAN, A.F., SUGIANTO, A.K., GIAP, Y.C., HAZRIANI, H., YENDRIANOF, D., MANULLANG, S.O., WATRIANTHOS, R., 2020. Keamanan Data dan Informasi. Yayasan Kita Menulis.

SEDANO, W.K., SALMAN, M., 2021. Auditing Linux Operating System with Center for Internet Security (CIS) Standard, in: 2021 International Conference on Information Technology (ICIT). Presented at the 2021 International Conference on Information Technology (ICIT), pp. 466–471. https://doi.org/10.1109/ICIT52682.2021.9491663

YUDHA, F., PANJI, A.M., 2018. PERANCANGAN APLIKASI PENGUJIAN CELAH KEAMANAN PADA APLIKASI BERBASIS WEB. Cyber Secur. Dan Forensik Digit. 1, 1–6. https://doi.org/10.14421/csecurity.2018.1.1.1216