Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Implementasi CIS *Hardening* Ubuntu *Server* 22.04 LTS dan SCA Wazuh pada Aplikasi MySkanema di SMKN 5 Batam

Fitri Trisnawati[1]*, Nur Cahyono Kushardianto[2]**

*Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Batam

**Teknik Komputer, Jurusan Teknik Informatika, Politeknik Negeri Batam

[1]fitritrisnawati0912@email.com, [2]anung@polibatam.ac.id

Received : Jun 9, 2025; Revised : Nov 20, 2025; Accepted : Nov 22, 2025; Published : Dec 11, 2025
Phone Number : +62163616902

Abstract

This study implements and evaluates CIS Benchmark Level 1 *hardening* on an active production Ubuntu *Server* 22.04 LTS supporting the MySkanema academic information system at SMKN 5 Batam, using Wazuh Security Configuration Assessment (SCA) for automated compliance validation. A *pre-test*/*post-test* design was applied on the same production *server* over a 26-day period, given the constraint of maintaining uninterrupted service availability throughout implementation. Results show *compliance score* increased from 48.3% to 57.0%, improving 18 of 207 CIS controls across SSH configuration, password policy, file permissions, firewall rules, and service *hardening*. This improvement did not reach conventional statistical significance (*two-proportion z-test*, p = 0.076), consistent with the relatively short observation period. The predefined functional target of 80% compliance was not achieved, primarily due to controls requiring structural changes — such as system partition separation — that could not be performed without a scheduled maintenance window on the active production *server*. CPU usage remained at 1.5% and network latency at 0.048ms, both within acceptable thresholds, indicating *hardening* did not degrade system performance. Exploratory security *alert* observations showed day-to-day variability attributable to fluctuating external attack intensity rather than configuration changes. These findings demonstrate that CIS Benchmark *hardening* can be implemented on active production infrastructure without service disruption, while highlighting those structural and time constraints affecting compliance target achievement in similar vocational school environments.
Keywords : *CIS Benchmark, server hardening, Ubuntu Server, Wazuh SCA, compliance score.*

1. INTRODUCTION

Keamanan *server* menjadi hal yang sangat penting bagi institusi pendidikan yang sudah menjalankan layanan digital sehari-hari. SMKN 5 Batam menggunakan Ubuntu *Server* 22.04 LTS untuk menjalankan aplikasi Myskanema — sistem informasi akademik yang menyimpan data siswa, guru, dan kegiatan belajar mengajar. Berdasarkan observasi awal, *server* masih menggunakan konfigurasi bawaan tanpa pengaturan keamanan yang terstruktur, sehingga menimbulkan risiko seperti serangan *brute-force* pada layanan SSH, layanan tidak diperlukan yang masih aktif, dan potensi kebocoran data yang wajib dilindungi berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 [1].

Ancaman siber di Indonesia terus meningkat — Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 3,64 miliar anomali trafik siber selama Januari–Juli 2025, dengan sektor pendidikan sebagai salah satu target utama [2]. Kondisi ini mempertegas perlunya penguatan keamanan *server* sekolah secara sistematis.

Pendekatan yang digunakan adalah *hardening* berbasis CIS Benchmark Level 1 untuk Ubuntu *Server* 22.04 LTS, dipilih karena menyediakan panduan teknis yang spesifik dan dapat diterapkan tanpa infrastruktur tambahan yang mahal — lebih sesuai untuk konteks ini dibanding kerangka tata kelola seperti ISO/IEC 27001 atau NIST CSF yang memerlukan proses sertifikasi formal dan berfokus pada kebijakan organisasi secara menyeluruh — CIS Benchmark menyediakan panduan teknis operasional yang dapat langsung diterapkan pada konfigurasi *server* tanpa infrastruktur tambahan yang mahal. Validasi dilakukan menggunakan modul *Security Configuration Assessment* (SCA) pada *platform* Wazuh, yang menghasilkan nilai kepatuhan (*compliance score*) secara otomatis dan terukur [3]

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Penelitian sebelumnya menunjukkan efektivitas pendekatan ini: Sholihin dan Salman [4] menunjukkan bahwa otomasi audit CIS Benchmark dapat mengklasifikasikan ratusan kontrol keamanan dengan akurasi tinggi dan konsistensi yang lebih baik dibanding audit manual, sementara Dixit dan Tripathi [5] menunjukkan Wazuh SCA mampu mengaudit konfigurasi sistem dengan akurasi tinggi. Namun keduanya belum diterapkan di lingkungan sekolah vokasi — celah inilah yang diisi penelitian ini.

Penelitian ini bertujuan: (1) menerapkan *hardening* CIS Benchmark Level 1 pada *server* SMKN 5 Batam, (2) memvalidasi hasilnya menggunakan Wazuh SCA, dan (3) menganalisis efektivitasnya melalui perbandingan *compliance score, security alerts,* dan performa sistem sebelum dan sesudah implementasi. Penelitian dibatasi pada konfigurasi Ubuntu *Server* 22.04 LTS yang mendukung layanan Myskanema dan tidak mencakup implementasi SIEM menyeluruh maupun aspek keamanan di luar CIS Benchmark Level 1.

2. LITERATUR REVIEW

2.1. Penelitian Terkait

Tabel 1 menyajikan perbandingan penelitian terdahulu yang relevan

Tabel 1. Penelitian Terdahulu

Peneliti / Tahun	Metode	Hasil	Keterbatasan
Sholihin & Salman (2025)	Otomasi audit CIS Benchmark	Audit otomatis berhasil mengklasifikasikan 248 kontrol dengan tingkat akurasi tinggi (150 *pass*, 86 *fail*)	Belum diterapkan di lingkungan Pendidikan vokasi.
Dixit & Tripathi (2025)	Wazuh SCA + CIS Benchmark	Audit konfigurasi otomatis dengan akurasi tinggi.	Tidak spesifik pada Ubuntu 22.04 LTS di sekolah.
Irawan et al. (2025)	CIS *Hardening* dengan pengujian serangan simulasi.	Peningkatan ketahanan nyata terhadap serangan siber	Belum spesifik di lingkungan pendidikan vokasi.
Penelitian ini	CIS *Hardening* + Wazuh SCA	Implementasi dan validasi terukur di sekolah vokasi.	Fokus pada CIS Level 1, Ubuntu 22.04 LTS, SMKN 5 Batam.

Berdasarkan Tabel 1, belum ada penelitian yang mengkaji implementasi *hardening* Ubuntu *Server* 22.04 LTS secara spesifik di lingkungan pendidikan vokasi dengan evaluasi kuantitatif berbasis Wazuh SCA. Penelitian ini mengisi celah tersebut

2.2. Landasan Teori

2.2.1 *Hardening* Sistem Operasi

Hardening adalah proses memperkuat konfigurasi *server* dengan menonaktifkan layanan yang tidak dibutuhkan, mengatur hak akses pengguna, dan memperketat autentikasi sesuai standar keamanan global, dengan tujuan memperkecil *attack surface* yang bisa dimanfaatkan penyerang. Tujuan ini selaras dengan prinsip dasar keamanan informasi *confidentiality, integrity,* dan *availability* (CIA *Triad*), di mana *hardening* berkontribusi langsung pada aspek *integrity* dan *availability* sistem dengan mencegah perubahan konfigurasi yang tidak sah dan menjaga layanan tetap dapat diakses oleh pengguna yang sah. [6].

2.2.2 Perbandingan CIS Benchmark, ISO/IEC 27001, dan NIST CSF

Dalam ranah manajemen keamanan siber, terdapat beberapa kerangka kerja yang dapat digunakan untuk meningkatkan postur keamanan sistem, di antaranya CIS Benchmark, ISO/IEC 27001,

dan NIST Cybersecurity Framework (CSF). Ketiganya memiliki fokus dan level implementasi yang berbeda. Penelitian [7] yang membandingkan NIST CSF dan ISO/IEC 27001 menemukan bahwa NIST CSF bersifat berbasis manajemen risiko (*risk-based*), fleksibel, dan tidak memerlukan sertifikasi formal, sedangkan ISO/IEC 27001 berbasis *Information Security Management System (ISMS)* dengan kontrol yang lebih formal dan dapat memperoleh sertifikasi internasional — menjadikannya lebih relevan untuk kebutuhan audit dan kepatuhan regulasi organisasi. Penelitian tersebut menyimpulkan bahwa tidak ada satu kerangka kerja yang secara mutlak lebih unggul, karena pemilihannya bergantung pada tingkat kematangan manajemen risiko, biaya implementasi, dan kebutuhan sertifikasi organisasi.

Studi kasus pemetaan kepatuhan pada infrastruktur cloud AWS [8] memperluas perbandingan ini dengan turut menyertakan CIS Controls v8.1 dan GDPR, menunjukkan bahwa ketiga kerangka kerja tersebut dapat saling melengkapi dalam praktiknya, meskipun studi tersebut berfokus pada lingkungan *cloud* dan tidak membahas *hardening* pada *server on-premise* berbasis Linux. Sementara itu, [9] mengkaji pembaruan ISO/IEC 27001:2022 khususnya kontrol A.8.9 (*Configuration Management*), yang secara eksplisit menekankan pentingnya *hardening* dan konfigurasi aman pada *server*, perangkat jaringan, dan aplikasi — menunjukkan bahwa domain konfigurasi teknis yang menjadi fokus CIS Benchmark sebenarnya juga tercakup, meski secara tidak langsung, dalam kontrol ISO/IEC 27001:2022.
Tinjauan komprehensif oleh [10], yang dipublikasikan pada ACM Computing Surveys, membandingkan berbagai standar keamanan siber dalam konteks *operating system hardening*, termasuk NIST, ISO, CIS, FIPS, Common Criteria, dan OWASP. Penelitian tersebut menegaskan bahwa seluruh standar ini memiliki tujuan yang sama — meningkatkan keamanan sistem operasi — namun berbeda dalam granularitas dan pendekatan implementasi, sehingga organisasi perlu memilih standar yang sesuai dengan kebutuhan spesifiknya dan menerjemahkannya menjadi kontrol teknis yang dapat diterapkan secara langsung.

Berdasarkan tinjauan tersebut, penelitian ini memilih CIS Benchmark sebagai kerangka kerja utama dengan tiga pertimbangan. Pertama, CIS Benchmark bersifat prescriptive dan memberikan langkah konfigurasi teknis yang konkret pada level parameter sistem operasi, berbeda dengan ISO/IEC 27001 yang bersifat manajerial berbasis proses organisasi, maupun NIST CSF yang bersifat strategis pada level fungsi keamanan (*Identify–Protect–Detect–Respond–Recover*). Kedua, sifat teknis dan terstrukturnya memungkinkan verifikasi otomatis melalui *tools* seperti Wazuh SCA dalam bentuk pemeriksaan *pass/fail* per kontrol [3], sehingga sesuai dengan pendekatan audit otomatis yang digunakan dalam penelitian ini. Ketiga, ruang lingkup penelitian ini terbatas pada *hardening* teknis satu *server* produksi tunggal, bukan audit kepatuhan organisasi secara menyeluruh yang membutuhkan dokumentasi ISMS lengkap sebagaimana disyaratkan ISO/IEC 27001.

2.2.3 CIS Benchmark untuk Ubuntu *Server* 22.04 LTS

CIS Benchmark adalah panduan konfigurasi keamanan yang disusun oleh *Center for Internet Security* (CIS) berdasarkan praktik terbaik yang diakui secara global. Menurut Irawan et al. (2025), penerapan CIS Benchmark pada Ubuntu *Server* 22.04 LTS secara nyata meningkatkan ketahanan *server* terhadap berbagai serangan siber seperti *DDoS, brute force,* dan *scanning* [11]. Pada penelitian ini versi yang digunakan adalah CIS Ubuntu *Server* 22.04 LTS Benchmark v2.0.0. Panduan ini dibagi menjadi dua level: Level 1 untuk konfigurasi dasar yang aman tanpa mengganggu layanan produksi, dan Level 2 untuk lingkungan berisiko tinggi. Penelitian ini menggunakan Level 1 karena sesuai dengan kondisi *server* sekolah. [12]

2.2.4 Wazuh dan Modul Security Configuration Assessment (SCA)

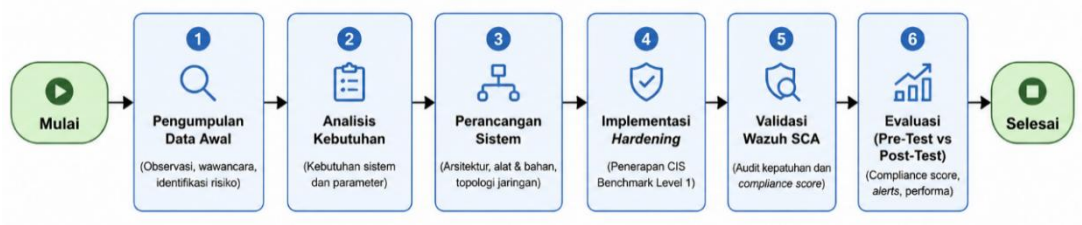
Wazuh adalah *platform* keamanan *open-source* yang pada penelitian ini digunakan modulnya yaitu *Security Configuration Assessment* (SCA). Modul ini memeriksa konfigurasi *server* secara otomatis berdasarkan *policy file* CIS Benchmark dan menghasilkan *compliance score* (0–100%) beserta daftar kontrol yang belum terpenuhi [3]. Karena tidak memerlukan lisensi berbayar, Wazuh menjadi

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

pilihan yang tepat untuk lingkungan sekolah dengan anggaran terbatas [5]. Pendekatan *project-based* menggunakan Wazuh telah terbukti efektif dalam mengajarkan *endpoint protection* dan *security configuration* di lingkungan pendidikan. [13]

3. RESEARCH METHODOLOGY

Penelitian ini menggunakan metode eksperimen kuantitatif dengan desain *pre-test* dan *post-test* — membandingkan kondisi *server* sebelum dan sesudah *hardening* diterapkan pada *server* yang sama. Gambar 1 menampilkan alur tahapan penelitian.



Gambar 1. Diagram Alur Tahapan Penelitian

3.1. Pengumpulan Data Awal

Data awal dikumpulkan melalui observasi langsung dan wawancara dengan admin jaringan SMKN 5 Batam. *Server* yang diamati menjalankan Ubuntu *Server* 22.04 LTS untuk mendukung aplikasi Myskanema, layanan basis data, dan penyimpanan internal. Hasil observasi menunjukkan *server* masih menggunakan konfigurasi bawaan tanpa kebijakan keamanan terstruktur, dengan potensi risiko antara lain: akses SSH yang tidak dibatasi, layanan tidak diperlukan yang masih aktif, dan belum adanya sistem audit keamanan otomatis. Kondisi ini menjadi titik awal (*baseline*) sebelum *hardening* diterapkan.

3.2. Analisis Kebutuhan Penelitian

Tahap ini dilakukan untuk menganalisis kebutuhan sistem dan menentukan parameter penelitian. Tujuan teknisnya adalah menerapkan *hardening* berbasis CIS Benchmark, memvalidasi menggunakan Wazuh SCA, dan menganalisis efektivitas melalui perbandingan data sebelum dan sesudah implementasi. Tabel 3 menyajikan kebutuhan fungsional dan non-fungsional sistem beserta indikator keberhasilannya.

Tabel 3. Kebutuhan Fungsional dan Non-Fungsional Sistem

No.	Jenis	Deskripsi	Indikator Sukses
1	Fungsional	*Server* dikonfigurasi sesuai CIS Ubuntu 22.04 Benchmark Level 1	*Compliance score* >80% pada Wazuh SCA
		Wazuh SCA mengaudit konfigurasi secara otomatis	Laporan audit dengan status *pass/fail* tiap kontrol
		Wazuh mendeteksi aktivitas mencurigakan secara *real-time*	*Security alert* muncul di *dashboard* Wazuh
		Analisis efektivitas dengan metode *pre-test* dan *post-test*	Perbandingan *compliance score* dan penurunan *alert* tersedia
2	Non-Fungsional	Proses validasi tidak mengganggu layanan Myskanema	CPU <20%, latensi <100ms
		Seluruh komponen menggunakan perangkat lunak *open-source*	Ubuntu, Wazuh, Proxmox tanpa lisensi berbayar

Setiap kebutuhan pada Tabel 3 memiliki indikator keberhasilan yang dapat diukur secara kuantitatif, menjadi dasar pelaksanaan eksperimen pada tahap implementasi dan evaluasi. Indikator keberhasilan pada Tabel 3 ditetapkan sebelum implementasi dimulai. Ketercapaian masing-masing indikator dibahas pada sub-bab 4.5

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

3.3. Perancangan Sistem

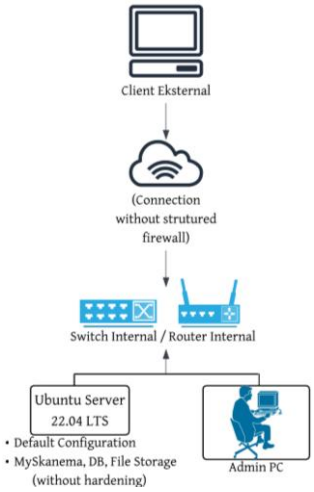
Sebelum implementasi dimulai, dirancang arsitektur sistem dan ditentukan spesifikasi komponen yang digunakan. Tabel 4 merinci alat dan bahan penelitian beserta fungsinya.

Tabel 4. Spesifikasi Alat dan Bahan Penelitian

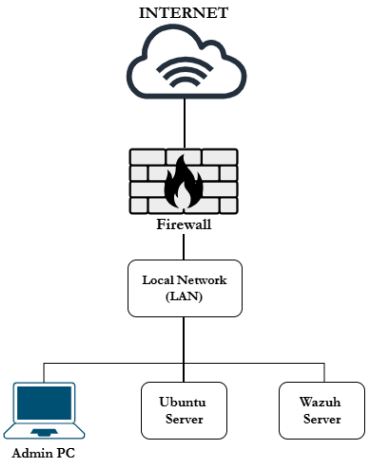
Komponen	Spesifikasi	Fungsi
Ubuntu *Server* 22.04 LTS	RAM 32GB, CPU 12 Core, Storage 50GB	Objek *hardening* dan *host* layanan Myskanema
Wazuh *Server*	Versi 4.14, RAM 8GB, CPU 4 Core, Storage 70GB	Pusat audit SCA dan pemantauan keamanan
Wazuh *Agent*	Versi 4.14	Pengirim data *log* dan konfigurasi dari Ubuntu *Server*
Proxmox VE	Versi 9.1	*Platform* virtualisasi untuk menjalankan Wazuh *Server*
Admin PC	Windows/Linux, RAM 8GB	Akses *dashboard* Wazuh dan manajemen *server* via SSH

Berdasarkan tabel 4, komponen utama yang digunakan terdiri dari Ubuntu *Server* sebagai objek penelitian, Wazuh *Server* sebagai pusat audit keamanan, Wazuh *Agent* yang dipasang di Ubuntu *Server* untuk mengirimkan data ke Wazuh *Server*, serta Proxmox VE sebagai *platform* virtualisasi yang digunakan untuk menjalankan Wazuh *Server* tempat hasil audit SCA dikumpulkan dan dipantau.

Sebelum *hardening* diterapkan, *server* terhubung ke jaringan tanpa *firewall* yang terstruktur seperti yang ditunjukkan pada Gambar 2. Kondisi ini memungkinkan akses langsung dari jaringan luar dan menjadi titik awal yang akan diperbaiki melalui proses *hardening*.



Gambar 2.
Topologi Jaringan Sebelum Implementasi *Hardening*



Gambar 3.
Topologi Jaringan Sesudah Implementasi *Hardening*

Setelah *hardening* selesai diterapkan, topologi jaringan berubah seperti yang ditunjukkan pada Gambar 3. *Server* kini dilengkapi *firewall* UFW dan terhubung aman ke Wazuh *Server* melalui Wazuh *Agent* untuk keperluan audit dan pemantauan keamanan.

3.4. Implementasi *Hardening*

Konfigurasi keamanan diterapkan secara bertahap pada Ubuntu *Server* 22.04 LTS berdasarkan kontrol CIS Benchmark Level 1. Setiap perubahan diperiksa untuk memastikan layanan Myskanema

tetap berjalan normal. Kontrol yang diterapkan meliputi pengamanan SSH, kebijakan *password*, pengaturan hak akses file, aktivasi *firewall* UFW, penonaktifan layanan yang tidak diperlukan, dan pemasangan *Fail2Ban.*

3.5. Validasi Menggunakan Wazuh

Setelah *hardening* selesai, *server* diintegrasikan ke lingkungan Wazuh. Modul SCA secara otomatis memeriksa konfigurasi *server* menggunakan *policy file* CIS Benchmark Ubuntu 22.04 LTS Level 1 yang tersedia di Wazuh [3], menghasilkan *compliance score* dan daftar kontrol yang belum terpenuhi sebagai data *post-test*.

3.6. Evaluasi

Evaluasi dilakukan dengan membandingkan tiga parameter pada kondisi sebelum dan sesudah *hardening*, sebagaimana ditampilkan pada Tabel 5.

Tabel 5. Parameter Pengukuran Efektivitas *Hardening*

No	Parameter	Penjelasan	Sumber Data
1	*Compliance score*	Nilai kepatuhan konfigurasi *server* terhadap CIS Benchmark Level 1 (0–100%).	Wazuh SCA *Dashboard*
2	*Security Alerts*	Jumlah peringatan keamanan yang terdeteksi Wazuh selama periode pengujian.	Wazuh *Dash-board*
3	Performa Sistem	Penggunaan CPU, memori, dan latensi jaringan	`top / ping`

Pengujian dibagi dua skenario: Skenario A (*pre-test) — server* dengan konfigurasi bawaan, diaudit untuk mendapatkan nilai *baseline*; dan Skenario B (*post-test*) — *server* setelah dikonfigurasi sesuai CIS Benchmark, diaudit ulang untuk mengukur perubahan.

4. RESULT

4.1. Lingkungan Pengujian

Spesifikasi sistem dan topologi jaringan yang digunakan dalam penelitian ini telah dijelaskan secara rinci pada Bab 3. *Server* Ubuntu 22.04 LTS yang mendukung layanan Myskanema di SMKN 5 Batam berjalan normal sebelum proses *hardening* dimulai. *Server* yang digunakan adalah *server* produksi aktif milik SMKN 5 Batam — bukan *server* uji coba — karena *server* cadangan milik sekolah sudah lama tidak digunakan dan membutuhkan waktu yang cukup lama untuk dapat diaktifkan kembali. Atas pertimbangan tersebut, pihak pembimbing di sekolah menyetujui penggunaan *server* produksi langsung sebagai objek penelitian. Kondisi awal *server* belum memiliki konfigurasi keamanan yang terstruktur sesuai standar CIS Benchmark.

4.2. Kondisi *Server* Sebelum *Hardening* (*Pre-test*)

Sebelum *hardening* diterapkan, dilakukan audit awal untuk mendokumentasikan kondisi ba*se-line server*. Tabel 6 merangkum temuan utama yang ditemukan pada kondisi awal.

Tabel 6. Kondisi *Server* Sebelum *Hardening*

Parameter	Kondisi Awal
SSH PermitRoot*Login*	Enabled (*login* root langsung diizinkan)
SSH MaxAuthTries	6 (belum sesuai standar CIS, seharusnya 4)
SSH LogLevel	INFO (seharusnya VERBOSE)
SSH *Login*GraceTime	120 detik (seharusnya 60 detik)
SSH ClientAliveInterval	0 (belum dikonfigurasi)
SSH Banner	Tidak ada
Firewall UFW	Tidak aktif
Apport Service	Aktif (perlu dinonaktifkan)

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Password Expiration	Tidak dikonfigurasi (PASS_MAX_DAYS:99999)
Inactive Lock	Tidak dikonfigurasi (INACTIVE: -1)
pam_faillock	Belum aktif
File permission kritis	Belum sepenuhnya sesuai standar CIS
Fail2Ban	Belum terinstall

Nilai *compliance score* yang diperoleh pada tahap ini adalah 48,3% dengan 100 kontrol yang *pass*, 97 kontrol yang *fail*, dan 10 kontrol *not applicable* dari total 207 pemeriksaan. Data ini diambil pada 19 Mei 2026 sebagai titik audit awal yang paling awal terverifikasi tersedia di *dashboard* Wazuh SCA untuk *server* produksi yang sama dengan yang digunakan pada tahap *post-test*.

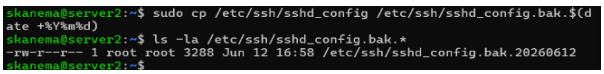
4.3. Implementasi *Hardening*

Konfigurasi keamanan diterapkan secara bertahap pada Ubuntu *Server* 22.04 LTS mengacu pada CIS Benchmark Level 1. Setiap sub-bab di bawah ini mengikuti pola: audit kondisi awal → penerapan konfigurasi → verifikasi hasil. Seluruh perubahan dikerjakan dengan tetap memastikan layanan Myskanema dan aplikasi pendukung lainnya tetap berjalan normal selama proses berlangsung.

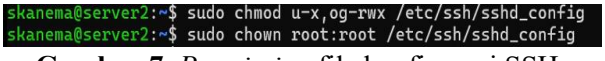
4.3.1 SSH Security

SSH merupakan satu-satunya jalur akses jarak jauh ke *server* sehingga penguatannya menjadi prioritas pertama. Audit awal menunjukkan beberapa parameter belum sesuai standar CIS seperti `PermitRootLogin yes`, `MaxAuthTries 6`, dan `LogLevel INFO`. File konfigurasi SSH dicadangkan sebelum perubahan diterapkan, kemudian seluruh kontrol CIS dikonfigurasi melalui file terpisah di direktori `sshd_config.d`. Validitas konfigurasi diuji menggunakan `sshd -t` sebelum di *reload*, dan akses SSH diverifikasi dari terminal baru untuk memastikan koneksi tetap berfungsi. Hasil implementasi disajikan pada Tabel 7.

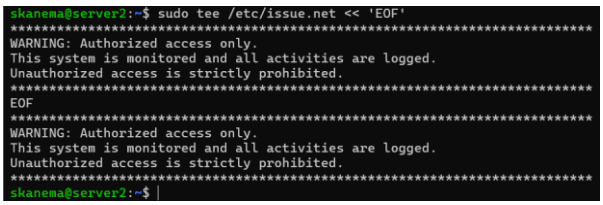
Gambar 5. Cek semua parameter SSH



Gambar 6. Backup file konfigurasi SSH

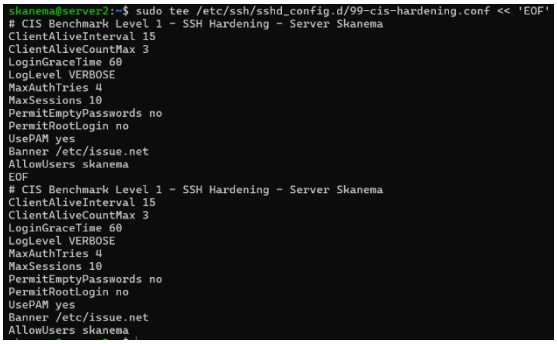


Gambar 7. *Permission* file konfigurasi SSH

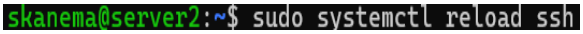


Gambar 8. Membuat file *banner* peringatan

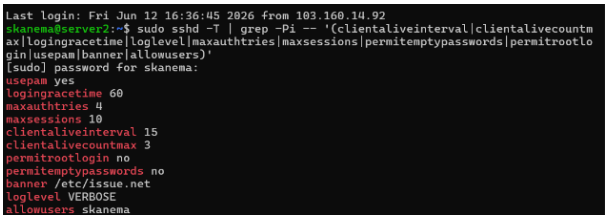
Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540



Gambar 9. Membuat file konfigurasi di folder `sshd_config.d`



Gambar 10. *Reload* SSH



Gambar 11. *Output* verifikasi `sshd -T` setelah konfigurasi SSH diterapkan

Tabel 7. Hasil Implementasi SSH *Security*

ID Kontrol	Deskripsi	Sebelum	Sesudah	Status
5.1.1	Permissions on /etc/ssh/sshd_config	0644	0600	Pass
5.1.4	sshd access is configured (AllowUsers)	Tidak ada	skanema	Pass
5.1.5	sshd Banner is configured	none	/etc/issue.net	Pass
5.1.7	sshd ClientAliveInterval is configured	0	15	Pass
5.1.13	sshd *Login*GraceTime is configured	120	60	Pass
5.1.14	sshd LogLevel is configured	INFO	VERBOSE	Pass
5.1.16	sshd MaxAuthTries is configured	6	4	Pass
5.1.17	sshd ClientAliveCountMax is configured	3	3	Pass
5.1.19	sshd PermitEmptyPasswords is disabled	no	no	Pass
5.1.20	sshd PermitRoot*Login* is disabled	yes	no	Pass
5.1.22	sshd UsePAM is enabled	yes	yes	Pass

4.3.2 *User & Password Policy*

Tahap ini mengatur kebijakan keamanan kata sandi dan penguncian akun. Audit awal menunjukkan `pam_faillock` belum aktif, `PASS_MAX_DAYS` bernilai `99999`, dan `INACTIVE` masih `-1`. Modul `pam_faillock` diaktifkan untuk mengunci akun setelah 5 kali percobaan *login* gagal selama 15 menit, `pam_pwquality` dikonfigurasi dengan panjang kata sandi min. 14 karakter, dan `pam_pwhistory` diaktifkan untuk mencegah penggunaan ulang 24 kata sandi terakhir. Masa berlaku kata sandi ditetapkan 365 hari dengan peringatan 7 hari sebelumnya dan penguncian akun 45 hari setelah kadaluarsa. Selama implementasi ditemukan kendala — `sudo su` gagal karena *password root* telah kadaluwarsa sejak Februari 2022, diselesaikan dengan memperbarui tanggal perubahan *password root* menggunakan `chage`. Hasil implementasi disajikan pada Tabel 8.

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

```
skanema@server2:~$ grep -P -- '\bpam_faillock\.so\b' /etc/pam.d/common-auth
/etc/pam.d/common-account 2>/dev/null || echo 'pam_faillock belum aktif'
pam_faillock belum aktif
```

Gambar 12. Cek status `pam_faillock`

```
skanema@server2:~$ grep -Pi -- '^(PASS_MAX_DAYS|PASS_WARN_AGE)' /etc/login.d
efs
PASS_MAX_DAYS   99999
PASS_WARN_AGE   7
skanema@server2:~$ useradd -D | grep INACTIVE
INACTIVE=-1
```

Gambar 13. Cek *password policy* & cek *default inactive lock*

```
skanema@server2:~$ sudo tee /usr/share/pam-configs/faillock << 'EOF'
Name: Enable pam_faillock to deny access
Default: yes
Priority: 0
Auth-Type: Primary
Auth:
        [default=die] pam_faillock.so authfail
EOF
[sudo] password for skanema:
Name: Enable pam_faillock to deny access
Default: yes
Priority: 0
Auth-Type: Primary
Auth:
        [default=die] pam_faillock.so authfail
skanema@server2:~$ sudo tee /usr/share/pam-configs/faillock_notify << 'EOF'
Name: Notify of failed login attempts and reset count upon success
Default: yes
Priority: 1024
Auth-Type: Primary
Auth:
        requisite pam_faillock.so preauth
Account-Type: Primary
Account:
        required pam_faillock.so
EOF
Name: Notify of failed login attempts and reset count upon success
Default: yes
Priority: 1024
Auth-Type: Primary
Auth:
        requisite pam_faillock.so preauth
Account-Type: Primary
Account:
        required pam_faillock.so
```

Gambar 14. Konfigurasi *faillock* pertama & kedua

```
skanema@server2:~$ sudo pam-auth-update --enable faillock
skanema@server2:~$ sudo pam-auth-update --enable faillock_notify
```

Gambar 15. Mengaktifkan kedua *profile faillock*

```
skanema@server2:~$ sudo tee /usr/share/pam-configs/pwquality << 'EOF'
Name: Enforce password quality standards
Default: yes
Priority: 1025
Password-Type: Primary
Password:
        requisite pam_pwquality.so retry=3
EOF
Name: Enforce password quality standards
Default: yes
Priority: 1025
Password-Type: Primary
Password:
        requisite pam_pwquality.so retry=3
```

Gambar 16. Konfigurasi `pam_pwquality`

```
skanema@server2:~$ sudo pam-auth-update --enable pwquality
```

Gambar 17. Mengaktifkan `pwquality`

```
skanema@server2:~$ sudo tee /etc/security/faillock.conf << 'EOF'
# CIS Benchmark Level 1 - faillock configuration
deny = 5
unlock_time = 900
EOF
# CIS Benchmark Level 1 - faillock configuration
deny = 5
unlock_time = 900
```

Gambar 18. Membuat `/edit faillock.conf`

```
skanema@server2:~$ sudo mkdir -p /etc/security/pwquality.conf.d/
echo 'minlen = 14' | sudo tee /etc/security/pwquality.conf.d/50-pwlength.con
f
minlen = 14
```

Gambar 19. Konfigurasi Panjang *Password*

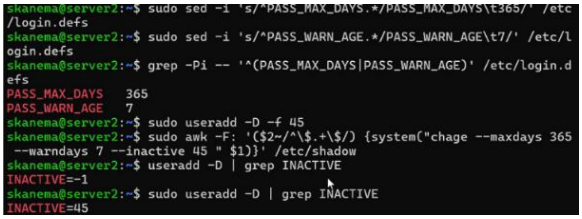
```
skanema@server2:~$ sudo tee /usr/share/pam-configs/pwhistory << 'EOF'
Name: Enforce password history
Default: yes
Priority: 1024
Password-Type: Primary
Password:
        required pam_pwhistory.so remember=24 use_authtok
EOF
Name: Enforce password history
Default: yes
Priority: 1024
Password-Type: Primary
Password:
        required pam_pwhistory.so remember=24 use_authtok
```

Gambar 20. Set *Password History*

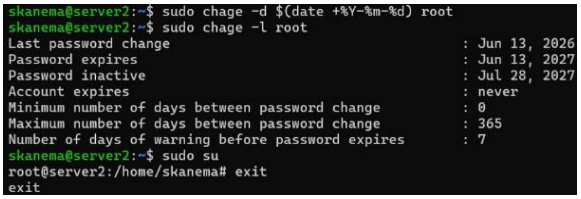
```
skanema@server2:~$ sudo pam-auth-update --enable pwhistory
```

Gambar 21. Mengaktfikan `pwhistory`

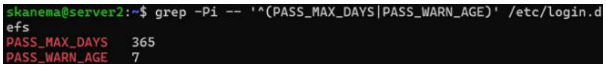
Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540



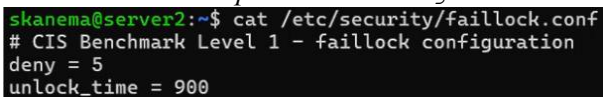
Gambar 22. Set *Password Aging*



Gambar 23. Memperbarui tanggal perubahan *Password root*



Gambar 24. *Output* verifikasi `login.defs`



Gambar 25. *Output* verifikasi `faillock.conf`

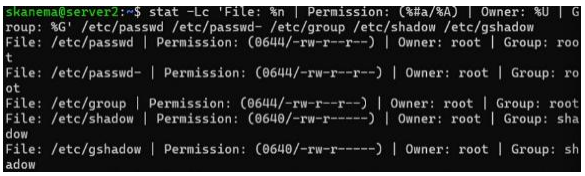
Tabel 8. Hasil Implementasi *User & Password Policy*

ID Kontrol	Deskripsi	Sebelum	Sesudah	Status
5.3.2.2	pam_faillock is enabled	Belum aktif	Aktif	Pass
5.3.2.3	pam_pwquality is enabled	Belum aktif	Aktif	Pass
5.3.3.1.1	Lockout deny count	Default (3)	5	Pass
5.3.3.1.2	Lockout unlock_time	600 detik	900 detik	Pass
5.3.3.2.2	Minimum password length	Tidak ada	14 karakter	Pass
5.3.3.3.1	Password history	Tidak ada	24 kata sandi	Pass
5.3.3.4.3	Password hashing algorithm	SHA512	SHA512	Pass
5.4.1.1	PASS_MAX_DAYS	99999	365	Pass
5.4.1.3	PASS_WARN_AGE	7	7	Pass
5.4.1.5	Inactive password lock	-1	45 hari	Pass
5.4.2.1	Root UID 0 account	root	root	Pass
5.4.2.4	Root password is set	kadaluwarsa	diperbarui	Pass

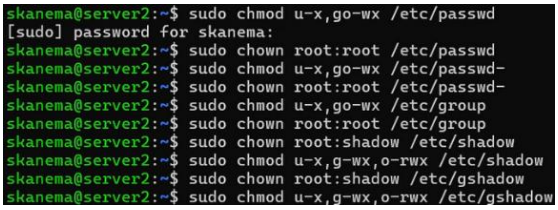
4.3.3 File *Permission*

Tahap ini memastikan file-file sistem yang penting memiliki hak akses yang benar sehingga tidak bisa diubah oleh pengguna yang tidak berwenang. Audit awal dan perbaikan permission dilakukan terhadap empat file sistem utama. Pemindaian `world writable files` menemukan dua *path*: `/var/crash` diperbaiki permissionnya, sedangkan `/var/lib/php/sessions` dibiarkan karena *sticky bit*-nya disengaja untuk kebutuhan PHP *session* aplikasi Myskanema. Verifikasi akun pengguna menunjukkan seluruh akun sudah menggunakan `shadow password`, tidak ada kata sandi kosong, dan tidak ada `UID` maupun nama pengguna yang duplikat. Hasil implementasi disajikan pada Tabel 9.

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

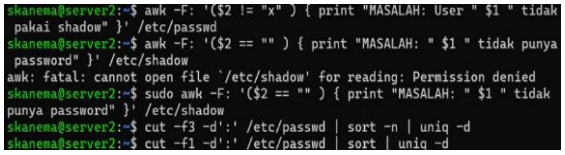


Gambar 26. Cek *permission* semua *file* sekaligus



Gambar 27. Perbaiki *permission* semua *file*

Gambar 28. Mengecek `World Writable Files`



Gambar 29. Verifikasi akun *User*

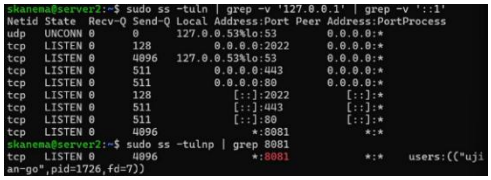
Tabel 9. Hasil Implementasi File Permission

ID Kontrol	File/Deskripsi	Permission Target	Status
7.1.1	/etc/passwd	0644, root:root	Pass
7.1.2	/etc/passwd-	0644, root:root	Pass
7.1.3	/etc/group	0644, root:root	Pass
7.1.4	/etc/group-	0644, root: root	Pass
7.1.5	/etc/shadow	0640, root:shadow	Fail
7.1.7	/etc/gshadow	0640, root:shadow	Fail
6.3.4.6	files owner	Owner: root	Pass
6.3.4.7	files group owner	Group: root	Pass
6.3.4.8	tools mode	Mode: hapus write utk group/other	Pass
6.3.4.9	tools owner	Owner: root	Pass

4.3.4 *Network Security (Firewall UFW)*

Firewall UFW (*Uncomplicated Firewall*) dikonfigurasi sebagai lapisan pertahanan jaringan untuk memblokir semua koneksi yang tidak diizinkan. Bagian ini adalah tahap yang paling berisiko karena jika port SSH tidak dibuka terlebih dahulu sebelum *firewall* diaktifkan, akses ke *server* akan langsung terputus dan tidak bisa dipulihkan dari jarak jauh. Sebelum UFW diaktifkan, audit port aktif dilakukan dan ditemukan empat port yang perlu diberi aturan: `2022 (SSH)`, `80 (HTTP)`, `443 (HTTPS)`, dan `8081 (ujian-go)`. Seluruh aturan *firewall* ditambahkan terlebih dahulu sebelum UFW diaktifkan dengan port SSH 2022 sebagai prioritas pertama — urutan ini krusial karena kesalahan konfigurasi dapat memutus akses SSH secara permanen. Setelah UFW aktif, koneksi SSH diuji dari terminal baru untuk memastikan akses tidak terputus. Hasil implementasi disajikan pada Tabel 11.

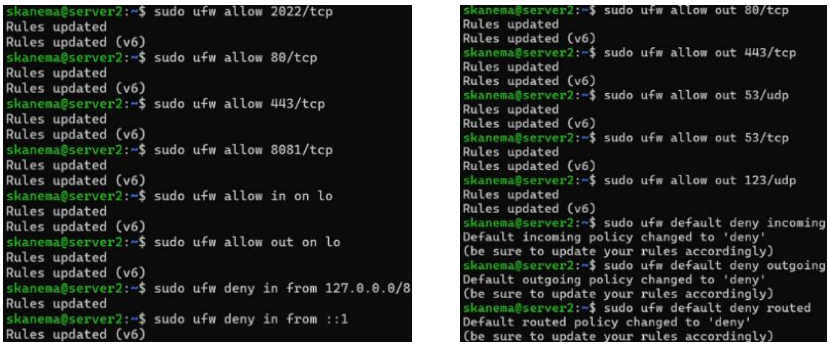
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540



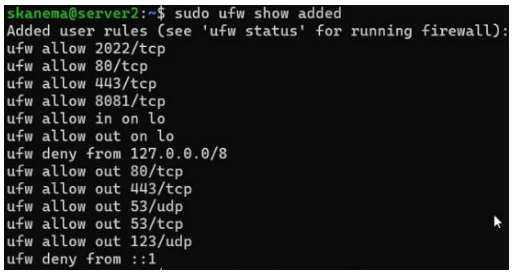
Gambar 30. Audit *port* yang aktif

Tabel 10. Hasil Audit port-port yang aktif di *server*

Port	Protokol	Layanan
2022	TCP	SSH
80	TCP	HTTP (MySkanema)
443	TCP	HTTPS (MySkanema)
8081	TCP	Aplikasi ujian-go

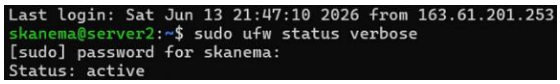


Gambar 31. Menambah *rules* sebelum *enable*



Gambar 32. Verifikasi semua *rules* sudah masuk

Gambar 33. Aktifkan UFW



Gambar 34. *Output* `sudo ufw status verbose` setelah UFW diaktfikan

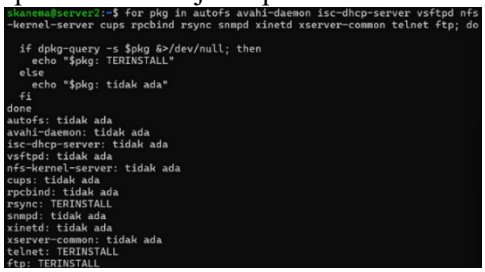
Tabel 11. Hasil Implementasi *Firewall* UFW

ID Kontrol	Deskripsi	Status
4.1.1	ufw is installed	Pass
4.1.2	iptables-persistent is not installed	Pass
4.1.3	ufw service is enabled	Pass
4.1.4	Loopback traffic is configured	Pass
4.1.7	Default deny firewall policy	Pass
4.2.5	nftables base chains exist	Pass
4.2.8	nftables default deny firewall policy	Pass

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

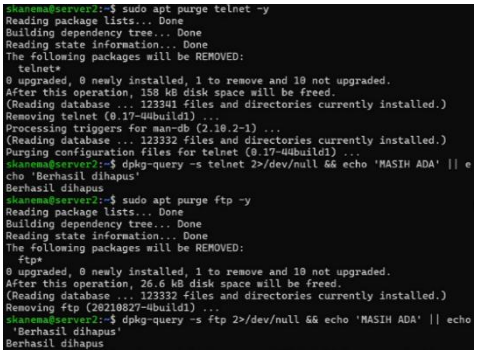
4.3.5 *System Hardening*

Tahap ini memastikan layanan-layanan yang tidak dibutuhkan tidak terinstall atau tidak aktif di *server*. Layanan yang tidak diperlukan tapi tetap berjalan dapat menjadi celah keamanan karena memperluas *attack surface server*. Audit terhadap 13 paket layanan menunjukkan `telnet` dan `ftp` terinstall dan dihapus karena merupakan protokol lama yang tidak terenkripsi. `rsync` ditemukan terinstall namun dibiarkan karena dependensi dari `ubuntu-standard` dan `mariadb-server` yang dibutuhkan aplikasi Myskanema. Layanan `apport` dinonaktifkan dan di-`mask` karena berpotensi mengumpulkan data sensitif dari memori sistem. Hasil implementasi disajikan pada Tabel 12



Gambar 35. Mengecek semua layanan yang tidak dibutuhkan

Gambar 36. Nonaktifkan `apport`



Gambar 37. Hapus `telnet` dan `ftp` *Client*

Tabel 12. Hasil Implementasi *System Hardening*

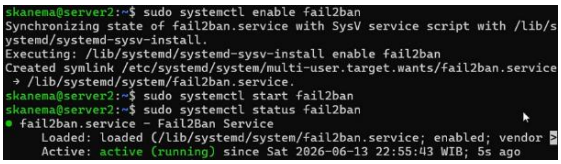
ID Kontrol	Layanan/Paket	Kondisi Awal	Tindakan	Status
1.5.5	apport	Aktif	Dinonaktifkan dan di-mask	Pass
2.1.x	autofs, avahi-daemon, isc-dhcp-*server*, vsftpd, nfs-kernel-*server*, cups, rpcbind, snmpd, xinetd, x*server*-common	Tidak terinstall	-	Pass
2.1.13	rsync	Terinstall	Dibiarkan (dependensi sistem)	Exception
2.2.4	telnet	Terinstall	Dihapus (apt purge)	Pass
2.2.6	ftp	Terinstall	Dihapus (apt purge)	Pass

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

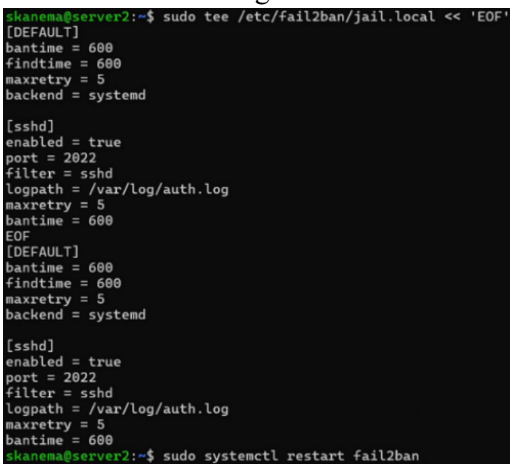
4.3.6 *Fail2Ban*

Fail2Ban adalah perangkat lunak yang secara otomatis memblokir alamat IP yang terlalu banyak melakukan percobaan *login* yang gagal. *Fail2Ban* diinstall dan dikonfigurasi untuk memantau port SSH 2022 dengan batas maksimal 5 kali percobaan *login* gagal dalam 10 menit, setelah itu IP pemohon diblokir selama 10 menit. Segera setelah aktif, *Fail2Ban* langsung mendeteksi dan memblokir 4 alamat IP yang terbukti melakukan serangan *brute-force*, membuktikan *server* memang aktif diserang dari luar. Hasil konfigurasi disajikan pada Tabel 13.

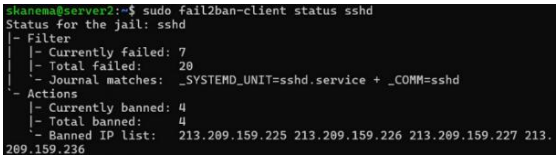
Gambar 38. *Install Fail2Ban*



Gambar 39. Mengaktifkan *Fail2Ban*



Gambar 40. Konfigurasi `jail.local` & `restart`



Gambar 41. Mengecek Alamat IP yang diblokir

Tabel 13. Hasil Implementasi *Fail2Ban*

Parameter	Konfigurasi	Status
Service	*Active, enabled*	Pass
Jail aktif	sshd	Pass
Port dipantau	2022/TCP	Pass
Maksimal percobaan gagal	5 kali	Pass
Durasi pemblokiran	600 detik	Pass
IP yang langsung terblokir	4 IP	Pass

4.4 Validasi Wazuh SCA

Wazuh SCA secara otomatis melakukan pemindaian berkala terhadap konfigurasi *server*. Data *pre-test* diambil dari pemindaian tanggal 19 Mei 2026 (sebelum implementasi *hardening* terstruktur dimulai), sedangkan data *post-test* diambil dari pemindaian tanggal 14 Juni 2026, setelah *hardening*

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

diterapkan secara bertahap. Rentang waktu 26 hari antara kedua titik pengukuran dipilih untuk meminimalkan pengaruh faktor eksternal terhadap validitas perbandingan, sekaligus memastikan kedua data berasal dari *agent* Wazuh dan *server* fisik yang sama (IP 103.156.57.230). *Compliance score* dihitung menggunakan rumus:

Compliance Score = (Jumlah kontrol Passed / Total kontrol yang diperiksa) × 100%

Data mentah SCA diekstraksi melalui modul *Configuration Assessment* → *Events* pada Wazuh, bukan dari tampilan ringkasan *dashboard* langsung, karena *agent* "skanema" mengalami *deregistration* pasca insiden *disconnect* dan tidak lagi muncul pada daftar *agent* aktif meski data historisnya tetap tersimpan pada indeks Wazuh. Data hasil ekstraksi (Lampiran C) menunjukkan 207 baris data unik untuk setiap titik waktu (*pre-test* dan *post-test*), terverifikasi berasal dari *agent* yang sama (ID 001, IP 103.156.57.230) melalui kolom metadata *agent*.id dan *agent*.ip. Visualisasi Gambar 42 dan Gambar 43 dibuat berdasarkan data ekstraksi ini untuk menjaga konsistensi format penyajian, mengingat tampilan *dashboard compliance score* bawaan Wazuh untuk *agent* tersebut tidak lagi dapat diakses secara langsung pasca *deregistration*. Tabel 14 menyajikan perbandingan hasil sebelum dan sesudah *hardening*.

Tabel 14. Perbandingan *Compliance score* Wazuh SCA

Parameter	***Pre-test* (19 Mei, 2026)**	***Post-test* (Jun 14, 2026)**	**Perubahan**
Compliance score	48,3%	57,0%	+8,7 poin
Passed	100	118	+18
Failed	97	83	-14
Not Applicable	10	6	-4
Total Pemeriksaan	207	207	-

Tabel 14a. Kontigensi 2x2

	Passed	**Failed/NA**	**Total**
Pre-test	100	107	207
Post-test	118	89	207

Peningkatan *compliance score* sebesar 8,7 poin menunjukkan bahwa 18 kontrol yang sebelumnya tidak terpenuhi berhasil diperbaiki melalui proses *hardening* dalam rentang waktu 26 hari. *Score* tidak mencapai 100% karena beberapa kontrol CIS memerlukan perubahan arsitektur sistem yang lebih mendasar, seperti pemisahan `partisi /tmp` menjadi partisi tersendiri, yang berisiko mengganggu stabilitas layanan pada *server* produksi aktif dan tidak dapat diselesaikan dalam rentang waktu penelitian yang tersedia.

Untuk menguji signifikansi statistik peningkatan *compliance score*, digunakan uji beda dua proporsi (*two-proportion z-test*) [14] dengan rumus:

$z = (p_2 - p_1) / \sqrt{[\hat{p}(1-\hat{p})(1/n_1 + 1/n_2)]}$, dengan $\hat{p} = (x_1 + x_2) / (n_1 + n_2)$

di mana $x_1 = 100$ (kontrol *passed pre-test*), $n_1 = 207$; $x_2 = 118$ (kontrol *passed post-test*), $n_2 = 207$; $p_1 = x_1/n_1 = 0{,}483$; $p_2 = x_2/n_2 = 0{,}570$; dan $\hat{p} = (100+118)/(207+207) = 0{,}500$.

Substitusi ke rumus menghasilkan:

$z = (0{,}570 - 0{,}483) / \sqrt{[0{,}500 \times 0{,}500 \times (1/207 + 1/207)]} = 0{,}087 / 0{,}0491 = 1{,}77$

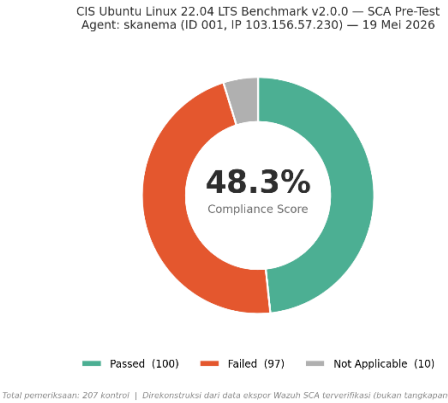
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Nilai z dikonversi menjadi *p*-value dua sisi menggunakan tabel distribusi normal standar [14], menghasilkan $p = 0{,}076$. Sebagai uji pembanding, dilakukan pula *Chi-square test of independence* [15] pada tabel kontingensi 2×2 (Tabel 14a) dengan rumus:

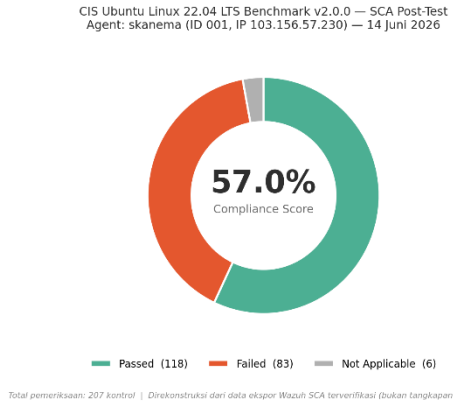
$$\chi^2 = \Sigma\ (O - E)^2 / E$$

menghasilkan $\chi^2 = 3{,}14$ dengan derajat kebebasan (df) = 1, setara dengan *p*-value = 0,076. Hasil ini konsisten dengan *two-proportion z-test* ($p = 0{,}076$).

Pada ambang signifikansi konvensional $\alpha = 0{,}05$ [14] — batas maksimum peluang kesalahan (*Type I error*) yang lazim digunakan dalam penelitian ilmiah [14] — kedua hasil uji menunjukkan bahwa peningkatan *compliance score* belum signifikan secara statistik, meskipun *p*-value mendekati ambang $\alpha = 0{,}10$.



Gambar 42. Visualisasi *Compliance score* SCA *Pre-test*, direkonstruksi dari data ekspor Wazuh terverifikasi (*Agent* skanema, 19 Mei 2026)



Gambar 43. Visualisasi *Compliance score* SCA *Post-test*, direkonstruksi dari data ekspor Wazuh terverifikasi (*Agent* skanema, 14 Juni 2026)

4.5 Evaluasi Perbandingan

4.5.1 *Compliance score*

Hardening yang diterapkan meningkatkan *compliance score* dari 48,3% menjadi 57,0% dalam rentang waktu 26 hari, mencerminkan perbaikan pada 18 kontrol yang sebelumnya gagal, mencakup area SSH *security*, kebijakan kata sandi, permission file sistem, *firewall*, penghapusan layanan yang tidak diperlukan, dan pemasangan *Fail2Ban*. Meskipun peningkatan ini belum signifikan secara statistik pada rentang waktu penelitian (lihat 4.4), tren peningkatan yang konsisten pada seluruh area *hardening* mengindikasikan efek yang nyata, bukan variasi acak. Kontrol yang belum terpenuhi umumnya memerlukan perubahan infrastruktur pada level sistem yang tidak dapat dilakukan tanpa risiko *downtime* pada *server* produksi aktif dalam jangka waktu penelitian yang tersedia.

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

4.5.2 Security *Alert*s

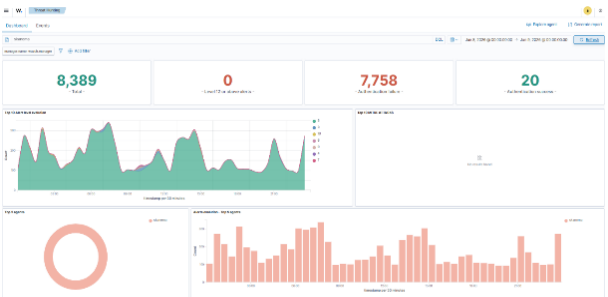
Berikut Tabel perbandingan aktivitas *Security Alerts* yang diambil dari *Dashboard Threat Hunting* di Wazuh.

Tabel 15. Perbandingan Aktivitas *Security Alerts* (Data Eksploratif)

Parameter	*Pre-test* (8 Juni 2026)	*Post-test* (14 Juni 2026)
Total *Alert s*	8.389	9.672
Authentication Failure	7.758	7.169
Authentication Success	20	3
Level 12 ke atas	0	0

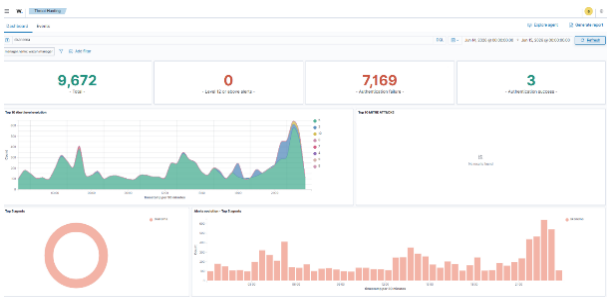
Selain *compliance score*, dilakukan pula pengamatan terhadap volume *security alerts* sebagai data pendukung. Hasil pengamatan pada dua titik waktu 24 jam (8 Juni dan 14 Juni 2026) menunjukkan total *alert* yang relatif fluktuatif (8.389 menjadi 9.672), dengan *authentication failure* yang sedikit menurun (7.758 menjadi 7.169). Fluktuasi ini kemungkinan dipengaruhi oleh variasi intensitas percobaan serangan dari luar yang bersifat harian dan tidak sepenuhnya berkorelasi langsung dengan konfigurasi *hardening* pada *server*. Oleh karena itu, perbandingan *snapshot* 24 jam ini tidak dijadikan bukti utama efektivitas *hardening* dalam penelitian ini — bukti utama tetap mengacu pada peningkatan *compliance score* SCA (Tabel 14) dan jumlah IP penyerang yang berhasil diblokir *Fail2Ban* (Tabel 13), yang tidak terpengaruh oleh fluktuasi intensitas serangan harian. Tidak adanya *alert* level 12 ke atas pada kedua titik pengamatan tetap mengonfirmasi tidak adanya insiden keamanan serius.

Untuk memperkuat interpretasi fluktuasi ini, dilakukan pula pengamatan tambahan terhadap tren *security alert* selama seluruh periode penelitian (19 Mei–14 Juni 2026, 26 hari). Data menunjukkan total 339.750 *alert* selama periode tersebut, dengan pola yang didominasi dua lonjakan signifikan yang tervisualisasikan pada Gambar 45a — satu di sekitar akhir Mei dan satu lagi menjelang pertengahan Juni 2026 — sementara periode di antaranya menunjukkan aktivitas yang relatif stabil pada kisaran yang jauh lebih rendah. Pola ini mengindikasikan bahwa lonjakan *alert* bersifat episodik dan tidak berkorelasi langsung dengan jadwal penerapan kontrol *hardening* yang dilakukan secara bertahap sepanjang periode yang sama, mendukung interpretasi bahwa fluktuasi *alert* lebih dipengaruhi oleh variasi intensitas percobaan serangan eksternal. Perlu dicatat bahwa penelitian ini tidak melakukan uji korelasi statistik formal antara jadwal implementasi *hardening* dan volume *alert* harian; hal ini menjadi rekomendasi metodologis untuk penelitian lanjutan (lihat sub-bab keterbatasan penelitian).

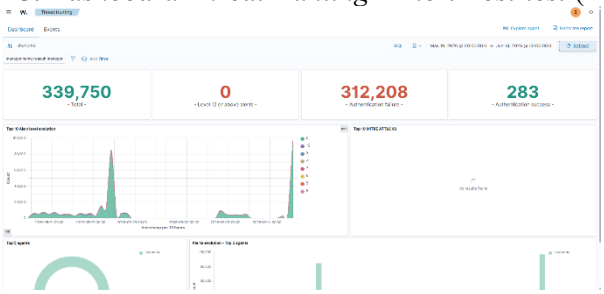


Gambar 44. *Dashboard Threat Hunting – Alert Pre-test* (8 Juni,2026)

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540



Gambar 45. *Dashboard Threat Hunting – Alert Post-test* (14 Juni,2026)



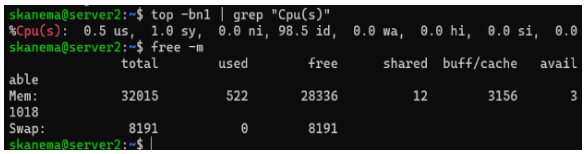
Gambar 45a. Tren *Security Alert* Periode Penelitian (19 Mei – 14 Juni 2026)

4.5.3 Performa Sistem

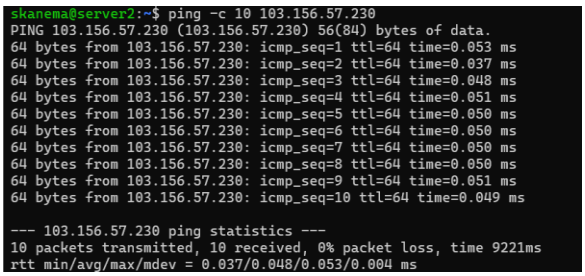
Pengukuran performa sistem dilakukan setelah seluruh *hardening* selesai untuk memastikan konfigurasi keamanan tidak membebani *server*. Tabel 16 menampilkan hasil pengukuran performa sistem setelah dilakukannya *Hardening*, dan tidak melewati batas indikator sukses.

Tabel 16. Performa Sistem Setelah *Hardening*

Parameter	Hasil Pengukuran	Indikator Sukses
CPU Usage	1.5%	<20%
RAM Terpakai	522 MB / 32 GB (~1,6%)	-
RAM Tersedia	±31 GB	-
Swap Terpakai	0 MB	-
Latensi Jaringan	0.048 ms (rata-rata)	<100ms



Gambar 46. Cek penggunaan CPU pada *server* skanema



Gambar 47. Cek Latensi pada *server* skanema

Hasil pengukuran menunjukkan bahwa proses *hardening* tidak memberikan beban tambahan yang berat pada *server*. Penggunaan CPU hanya 1.5% dan RAM yang terpakai kurang dari 2% dari total kapasitas, jauh di bawah ambang batas yang ditetapkan sebagai indikator keberhasilan (CPU < 20%). Layanan Myskanema tetap berjalan normal selama dan setelah proses *hardening* berlangsung.

5. DISCUSSION

Peningkatan *compliance score* dari 48,3% menjadi 57,0% dalam rentang 26 hari menunjukkan bahwa penerapan CIS Benchmark Level 1 secara bertahap memberikan perbaikan pada konfigurasi keamanan *server*, meskipun belum mencapai target 80% yang ditetapkan di awal dan belum menunjukkan signifikansi statistik formal pada rentang waktu observasi ini (p = 0,076; lihat 4.4). Dibandingkan dengan penelitian Sholihin dan Salman [4] yang mengaudit 248 kontrol CIS pada lingkungan RHEL 7 terkontrol dengan hasil 150 kontrol (60,5%) lolos, hasil penelitian ini tetap menunjukkan tren peningkatan yang sebanding meski dilakukan langsung pada *server* produksi aktif tanpa jendela pemeliharaan khusus. Hasil ini juga sejalan dengan temuan Wazuh Blog [16] bahwa otomatisasi *hardening* menggunakan Wazuh SCA dapat meningkatkan *compliance score* pada sistem Ubuntu.

Ketidaktercapaian target 80% disebabkan oleh dua faktor. Secara teknis, sebagian kontrol CIS yang belum terpenuhi memerlukan perubahan arsitektur mendasar — seperti pemisahan `partisi /tmp` dan konfigurasi kernel parameter — yang berisiko mengganggu layanan Myskanema bila diterapkan tanpa jendela pemeliharaan terjadwal. Implementasi *hardening* dilakukan secara bertahap sejak pertengahan Mei 2026, dengan sejumlah kontrol individual diterapkan secara eksploratif pada awal Juni 2026. Gangguan akses SSH pada *server* selama 1–7 Juni 2026 sempat memperlambat proses pengerjaan, sehingga penerapan menyeluruh terhadap keenam area *hardening* secara terstruktur baru dapat diselesaikan pada 12–14 Juni 2026, tepat sebelum pengambilan data *post-test* pada 14 Juni 2026.

Selama periode *post-test*, ditemukan pula insiden *disconnect* Wazuh *agent* selama 67 jam (15 Juni pukul 18:00 – 18 Juni pukul 13:00 WIB), yang setelah ditelusuri disebabkan oleh kebijakan `default deny outgoing` pada firewall (kontrol 4.1.7) yang belum disertai *`allowlist`* eksplisit untuk port komunikasi *agent* (TCP 1514/1515). Insiden ini berhasil diatasi dengan menambahkan rule `ACCEPT` untuk port tersebut, dan menjadi catatan penting bahwa kebijakan `default deny` yang ketat perlu disertai *`allowlist`* yang menyeluruh agar tidak melumpuhkan sistem pemantauan keamanan itu sendiri.

Pengamatan terhadap volume *security alerts* pada periode 24 jam yang setara menunjukkan hasil yang fluktuatif — total *alert* pada 8 Juni (8.389) dan 14 Juni (9.672) — yang lebih mencerminkan variasi intensitas serangan eksternal harian dibanding efek langsung *hardening*. Indikator yang lebih dapat diandalkan adalah keberhasilan *Fail2Ban* memblokir 4 IP penyerang secara otomatis, serta tidak adanya satu pun *alert* level 12 ke atas pada seluruh periode pengujian, yang mengindikasikan tidak ada insiden keamanan serius yang terjadi.

Dari sisi performa, CPU *usage* hanya 1,5% dan latensi jaringan rata-rata 0,048 ms — keduanya jauh di bawah ambang batas indikator keberhasilan — menunjukkan bahwa keamanan *server* dapat ditingkatkan tanpa mengorbankan ketersediaan layanan Myskanema.

Beberapa keterbatasan penelitian perlu diakui: (1) penelitian ini merupakan studi kasus tunggal pada satu *server* produksi tanpa kelompok kontrol maupun replikasi pada *server* lain, sehingga generalisasi temuan ke konteks lain memerlukan penelitian lanjutan yang mencakup replikasi pada minimal dua *server* produksi sejenis untuk validasi eksternal; (2) rentang waktu antara *pre-test* dan *post-test* (26 hari) relatif singkat untuk mendeteksi efek yang signifikan secara statistik pada perubahan konfigurasi berskala kecil, sebagaimana ditunjukkan oleh hasil uji dua proporsi (p = 0,076); periode observasi yang lebih panjang direkomendasikan untuk penelitian lanjutan guna memperoleh kesimpulan kausal yang lebih kuat; (3) uji signifikansi yang digunakan (*two-proportion z-test* dan *Chi-square test*) menggunakan data agregat, bukan data berpasangan per-kontrol, karena keterbatasan dokumentasi status per-kontrol pada beberapa titik waktu; uji McNemar yang lebih sesuai untuk data biner berpasangan menjadi rekomendasi metodologis untuk penelitian selanjutnya; dan (4) periode pengamatan *security alert* terperinci (24 jam per titik) relatif singkat untuk menangkap pola serangan yang sepenuhnya representatif;

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

penelitian lanjutan disarankan menggunakan periode observasi yang lebih panjang disertai uji korelasi formal untuk memperkuat validitas kausal antara *hardening* dan aktivitas serangan.

Sebagai tindak lanjut atas kontrol yang belum terpenuhi, direkomendasikan penjadwalan *maintenance window* khusus (idealnya pada periode libur sekolah) untuk melakukan pemisahan partisi sistem `(/tmp, /var, /home, /var/log, /var/log/audit)` secara bertahap, dikoordinasikan dengan pihak manajemen SMKN 5 Batam dan tim pengelola infrastruktur MySkanema, guna meminimalkan risiko gangguan layanan selama proses migrasi partisi berlangsung.

6. CONCLUSION

Penelitian ini berhasil menerapkan *hardening* CIS Benchmark Level 1 pada *server* produksi aktif Ubuntu 22.04 LTS milik SMKN 5 Batam yang menjalankan aplikasi Myskanema, divalidasi menggunakan Wazuh SCA, mencakup enam area: SSH *security*, kebijakan kata sandi, *permission* file sistem, *firewall* UFW, penonaktifan layanan tidak diperlukan, dan pemasangan *Fail2Ban*.

Compliance score meningkat dari 48,3% menjadi 57,0% dalam rentang waktu 26 hari (19 Mei–14 Juni 2026), dengan 18 kontrol yang sebelumnya gagal berhasil diperbaiki, meskipun peningkatan ini belum signifikan secara statistik pada rentang waktu tersebut (p = 0,076). Target fungsional >80% yang ditetapkan pada sub-bab 3.2 tidak tercapai. Analisis akar masalah menunjukkan bahwa sebagian besar dari 83 kontrol yang masih gagal memerlukan perubahan arsitektur signifikan — khususnya pemisahan partisi sistem `(/tmp, /var, /home, /var/log, /var/log/audit)` — yang membutuhkan *maintenance window* 12–24 jam dan tidak dapat dilakukan tanpa mengganggu layanan produksi aktif yang digunakan sekolah setiap hari. Kesenjangan antara target dan hasil ini mengindikasikan bahwa target 80% yang ditetapkan di awal penelitian kurang mempertimbangkan batasan operasional *server* produksi tanpa jendela pemeliharaan, dan menjadi catatan penting untuk perumusan target yang lebih realistis pada penelitian sejenis di masa mendatang. Volume *security alert*s menunjukkan variabilitas yang lebih dipengaruhi fluktuasi serangan eksternal harian dibanding efek *hardening* secara langsung, sehingga indikator efektivitas yang lebih dapat diandalkan adalah keberhasilan *Fail2Ban* memblokir 4 IP penyerang serta tidak ditemukannya *alert* level kritis selama pengujian. Performa sistem tetap stabil (CPU 1,5%, latensi 0,048 ms), jauh di bawah ambang batas yang ditetapkan, sehingga *hardening* tidak mengganggu stabilitas layanan Myskanema.

Dari tiga tujuan penelitian yang ditetapkan, tujuan implementasi *hardening* dan validasi menggunakan Wazuh SCA tercapai sepenuhnya. Tujuan ketiga, yaitu analisis efektivitas *hardening*, tercapai sebagian — dari tiga indikator yang digunakan (*compliance score*, penggunaan CPU, dan latensi jaringan), dua indikator (CPU dan latensi) memenuhi target, sementara *compliance score* belum mencapai target fungsional >80% yang ditetapkan di awal.

Untuk pengembangan lebih lanjut, kontrol CIS yang belum terpenuhi disarankan dikaji dan diterapkan bertahap saat jendela pemeliharaan tersedia. Pemantauan melalui Wazuh yang telah terpasang dapat dimanfaatkan SMKN 5 Batam secara berkelanjutan, sehingga manfaat penelitian ini tidak terbatas pada periode pengujian saja.

REFERENCES

[1] "Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara RI Tahun 2022 Nomor 196. Jakarta: Sekretariat Negara, 2022."

[2] "BSSN Catat 3,64 Miliar Serangan Siber Selama Januari-Juli 2025 - Teknologi." Accessed: Dec. 19, 2025. [Online]. Available: https://www.bloombergtechnoz.com/detail-news/88672/bssn-catat-3-64-miliar-serangan-siber-selama-januari-juli-2025

[3] "Security Configuration Assessment - Capabilities · Wazuh documentation." Accessed: Oct. 13, 2025. [Online]. Available: https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/index.html

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

[4] A. Sholihin and M. Salman, "OSCAT: A Comprehensive Tool for Automated CIS Benchmark Auditing," 2025. [Online]. Available: https://ajesh.ph/index.php/gp
[5] S. Dixit and P. Tripathi, "Strengthening Cybersecurity with Wazuh: Log-Based Threat Detection for a Resilient Digital World," *International Journal of Advanced Research in Computer and Communication Engineering Impact Factor*, vol. 8, no. 1, 2025, doi: 10.17148/IJARCCE.2025.14162.
[6] O. Mitchell and C. Osazuwa, "Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature," 2023.
[7] M. Alshar'e, "CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001," *Applied computing Journal*, pp. 245–255, Feb. 2023, doi: 10.52098/acj.202364.
[8] P. Subedi, "Evaluating Compliance Frameworks for Cloud Security: A Case Study on AWS Security Best Practices."
[9] O. Vakhula, Y. Kurii, I. Opirskyy, and V. Susukailo, "Security-as-Code Concept for Fulfilling ISO/IEC 27001:2022 Requirements."
[10] S. W. A. Hamdani *et al.*, "Cybersecurity Standards in the Context of Operating System," Apr. 30, 2022, *Association for Computing Machinery*. doi: 10.1145/3442480.
[11] B. Irawan, K. N. Sheha, M. Rahaman, N. Erzed, and A. Herwanto, "Evaluating the Effectiveness of Center of Internet Security Benchmark for Hardening Linux Servers Against Cyber Attacks", [Online]. Available: http://ijsr.internationaljournallabs.com/index.php/ijsr
[12] "CIS Ubuntu Linux 22.04 LTS v2.0.0 L1 Server | Tenable®." Accessed: Oct. 18, 2025. [Online]. Available: https://www.tenable.com/audits/CIS_Ubuntu_Linux_22.04_LTS_v2.0.0_L1_Server
[13] S. Sutton, V. Bungei, X. Wang, J. Frank, and E. Djan, "Teaching Endpoint Protection through Wazuh: A Project-Based Approach to Cybersecurity Education," 2026. [Online]. Available: www.cisse.info
[14] "D. C. Montgomery and G. C. Runger, Applied Statistics and Probability for Engineers, 7th ed. Hoboken, NJ, USA: John Wiley & Sons, 2018."
[15] "R. E. Walpole, R. H. Myers, S. L. Myers, and K. Ye, Probability & Statistics for Engineers & Scientists, 9th ed. Boston, MA, USA: Pearson Education, 2012.".
[16] "Automating Linux endpoint hardening with Wazuh | Wazuh." Accessed: Jun. 18, 2026. [Online]. Available: https://wazuh.com/blog/automating-linux-endpoint-hardening-with-wazuh/

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

LAMPIRAN C — DATA MENTAH HASIL PEMINDAIAN WAZUH SCA

Lampiran ini memuat data mentah hasil ekspor Wazuh *Security Configuration Assessment* (SCA) yang digunakan sebagai dasar perhitungan *compliance score* pada Bab 4. Data diekstraksi melalui modul *Configuration Assessment* → *Events* pada *platform* Wazuh, dengan metadata *agent* (*agent*.name, *agent*.id, *agent*.ip) yang telah diverifikasi identik pada kedua titik pengukuran.

C1. Data *Pre-test* — 19 Mei 2026

Agent: skanema | Agent ID: 001 | IP: 103.156.57.230 | Policy: CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0 | Waktu pemindaian: 19 Mei 2026, 09:58 WIB
Ringkasan: Passed = 100, Failed = 97, Not Applicable = 10, Total = 207, *Compliance score* = 48.3%

No	Judul Kontrol (CIS Benchmark)	Hasil
1	Ensure /dev/shm is a separate partition.	Passed
2	Ensure /etc/shadow password fields are not empty.	Passed
3	Ensure /tmp is a separate partition.	Failed
4	Ensure AIDE is installed.	Failed
5	Ensure AppArmor is enabled in the bootloader configuration.	Failed
6	Ensure AppArmor is installed.	Failed
7	Ensure Automatic Error Reporting is not enabled.	Failed
8	Ensure GDM is removed.	Passed
9	Ensure IPv6 status is identified.	Passed
10	Ensure NIS Client is not installed.	Passed
11	Ensure X window *server* services are not in use.	Passed
12	Ensure a nftables table exists.	Passed
13	Ensure access to /etc/issue is configured.	Passed
14	Ensure access to /etc/issue.net is configured.	Passed
15	Ensure access to /etc/motd is configured.	Passed
16	Ensure access to bootloader config is configured.	Failed
17	Ensure access to the su command is restricted.	Failed
18	Ensure accounts in /etc/passwd use shadowed passwords.	Passed
19	Ensure actions as another user are always logged.	Failed
20	Ensure all groups in /etc/passwd exist in /etc/group.	Passed
21	Ensure audit configuration files group owner is configured.	Passed
22	Ensure audit configuration files mode is configured.	Passed
23	Ensure audit configuration files owner is configured.	Passed
24	Ensure audit log files group owner is configured.	Passed
25	Ensure audit log storage size is configured.	Passed
26	Ensure audit logs are not automatically deleted.	Failed
27	Ensure audit tools group owner is configured.	Passed
28	Ensure audit tools mode is configured.	Passed
29	Ensure audit tools owner is configured.	Passed
30	Ensure audit_backlog_limit is sufficient.	Failed
31	Ensure auditd packages are installed.	Failed
32	Ensure auditd service is enabled and active.	Passed
33	Ensure auditing for processes that start prior to auditd is enabled.	Passed
34	Ensure autofs services are not in use.	Passed
35	Ensure avahi daemon services are not in use.	Passed
36	Ensure bluetooth services are not in use.	Passed
37	Ensure bootloader password is set.	Failed
38	Ensure changes to system administration scope (sudoers) is collected.	Failed
39	Ensure chrony is enabled and running.	Failed
40	Ensure chrony is running as user _chrony.	Not Applicable
41	Ensure cron daemon is enabled and active.	Passed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
42	Ensure cryptographic mechanisms are used to protect the integrity of audit tools.	Not Applicable
43	Ensure default user umask is configured.	Passed
44	Ensure dhcp *server* services are not in use.	Passed
45	Ensure dns *server* services are not in use.	Passed
46	Ensure dnsmasq services are not in use.	Passed
47	Ensure events that modify date and time information are collected.	Failed
48	Ensure events that modify the system's Mandatory Access Controls are collected.	Failed
49	Ensure events that modify the system's network environment are collected.	Failed
50	Ensure events that modify user/group information are collected.	Failed
51	Ensure filesystem integrity is regularly checked.	Failed
52	Ensure ftp client is not installed.	Failed
53	Ensure ftp *server* services are not in use.	Passed
54	Ensure group root is the only GID 0 group.	Passed
55	Ensure inactive password lock is configured.	Failed
56	Ensure ip6tables default deny firewall policy.	Failed
57	Ensure ip6tables loopback traffic is configured.	Failed
58	Ensure iptables default deny firewall policy.	Failed
59	Ensure iptables loopback traffic is configured.	Failed
60	Ensure iptables packages are installed.	Failed
61	Ensure iptables-persistent is not installed with ufw.	Passed
62	Ensure journald Compress is configured.	Not Applicable
63	Ensure journald ForwardToSyslog is disabled.	Not Applicable
64	Ensure journald Storage is configured.	Not Applicable
65	Ensure journald service is enabled and active.	Passed
66	Ensure ldap client is not installed.	Passed
67	Ensure ldap *server* services are not in use.	Passed
68	Ensure libpam-pwquality is installed.	Passed
69	Ensure local *login* warning banner is configured properly.	Failed
70	Ensure *login* and logout events are collected.	Failed
71	Ensure mail transfer *agent* is configured for local-only mode.	Passed
72	Ensure message access *server* services are not in use.	Passed
73	Ensure message of the day is configured properly.	Passed
74	Ensure minimum password age is configured.	Failed
75	Ensure minimum password length is configured.	Passed
76	Ensure network file system services are not in use.	Passed
77	Ensure nftables base chains exist.	Passed
78	Ensure nftables default deny firewall policy.	Passed
79	Ensure nftables is installed.	Passed
80	Ensure nftables is not installed with iptables.	Failed
81	Ensure nftables service is enabled.	Failed
82	Ensure nis *server* services are not in use.	Passed
83	Ensure nodev option set on /dev/shm partition.	Passed
84	Ensure nodev option set on /home partition.	Failed
85	Ensure nodev option set on /tmp partition.	Failed
86	Ensure nodev option set on /var partition.	Failed
87	Ensure nodev option set on /var/log partition.	Failed
88	Ensure nodev option set on /var/log/audit partition.	Failed
89	Ensure nodev option set on /var/tmp partition.	Failed
90	Ensure noexec option set on /dev/shm partition.	Failed
91	Ensure noexec option set on /tmp partition.	Failed
92	Ensure noexec option set on /var/log partition.	Failed
93	Ensure noexec option set on /var/log/audit partition.	Failed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
94	Ensure noexec option set on /var/tmp partition.	Failed
95	Ensure no*login* is not listed in /etc/shells.	Passed
96	Ensure nosuid option set on /dev/shm partition.	Passed
97	Ensure nosuid option set on /home partition.	Failed
98	Ensure nosuid option set on /tmp partition.	Failed
99	Ensure nosuid option set on /var partition.	Failed
100	Ensure nosuid option set on /var/log partition.	Failed
101	Ensure nosuid option set on /var/log/audit partition.	Failed
102	Ensure nosuid option set on /var/tmp partition.	Failed
103	Ensure pam_faillock module is enabled.	Failed
104	Ensure pam_pwhistory includes use_authtok.	Failed
105	Ensure pam_pwhistory module is enabled.	Failed
106	Ensure pam_pwquality module is enabled.	Passed
107	Ensure pam_unix does not include nullok.	Failed
108	Ensure pam_unix does not include remember.	Passed
109	Ensure pam_unix includes a strong password hashing algorithm.	Passed
110	Ensure pam_unix includes use_authtok.	Passed
111	Ensure pam_unix module is enabled.	Passed
112	Ensure password complexity is configured.	Not Applicable
113	Ensure password dictionary check is enabled.	Failed
114	Ensure password expiration is configured.	Failed
115	Ensure password expiration warning days is configured.	Passed
116	Ensure password failed attempts lockout includes root account.	Passed
117	Ensure password failed attempts lockout is configured.	Passed
118	Ensure password history is enforced for the root user.	Failed
119	Ensure password history remember is configured.	Failed
120	Ensure password maximum sequential characters is configured.	Not Applicable
121	Ensure password number of changed characters is configured.	Passed
122	Ensure password quality checking is enforced.	Failed
123	Ensure password quality is enforced for the root user.	Not Applicable
124	Ensure password same consecutive characters is configured.	Not Applicable
125	Ensure password unlock time is configured.	Passed
126	Ensure permissions on /etc/cron.d are configured.	Failed
127	Ensure permissions on /etc/cron.daily are configured.	Failed
128	Ensure permissions on /etc/cron.hourly are configured.	Failed
129	Ensure permissions on /etc/cron.monthly are configured.	Failed
130	Ensure permissions on /etc/cron.weekly are configured.	Failed
131	Ensure permissions on /etc/crontab are configured.	Failed
132	Ensure permissions on /etc/group are configured.	Passed
133	Ensure permissions on /etc/group- are configured.	Passed
134	Ensure permissions on /etc/gshadow are configured.	Failed
135	Ensure permissions on /etc/gshadow- are configured.	Failed
136	Ensure permissions on /etc/passwd are configured.	Passed
137	Ensure permissions on /etc/passwd- are configured.	Passed
138	Ensure permissions on /etc/security/opasswd are configured.	Failed
139	Ensure permissions on /etc/shadow are configured.	Failed
140	Ensure permissions on /etc/shadow- are configured.	Failed
141	Ensure permissions on /etc/shells are configured.	Failed
142	Ensure permissions on /etc/ssh/sshd_config are configured.	Failed
143	Ensure permissions on SSH public host key files are configured.	Passed
144	Ensure prelink is not installed.	Passed
145	Ensure print *server* services are not in use.	Passed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
146	Ensure re-authentication for privilege escalation is not disabled globally.	Passed
147	Ensure remote *login* warning banner is configured properly.	Passed
148	Ensure root is the only GID 0 account.	Passed
149	Ensure root is the only UID 0 account.	Passed
150	Ensure root password is set.	Passed
151	Ensure root user umask is configured.	Passed
152	Ensure rpcbind services are not in use.	Passed
153	Ensure rsh client is not installed.	Passed
154	Ensure rsync services are not in use.	Failed
155	Ensure samba file *server* services are not in use.	Passed
156	Ensure separate partition exists for /home.	Failed
157	Ensure separate partition exists for /var.	Failed
158	Ensure separate partition exists for /var/log.	Failed
159	Ensure separate partition exists for /var/log/audit.	Failed
160	Ensure separate partition exists for /var/tmp.	Failed
161	Ensure session initiation information is collected.	Failed
162	Ensure snmp services are not in use.	Passed
163	Ensure sshd Banner is configured.	Failed
164	Ensure sshd Ciphers are configured.	Passed
165	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured.	Failed
166	Ensure sshd DisableForwarding is enabled.	Failed
167	Ensure sshd GSSAPIAuthentication is disabled.	Passed
168	Ensure sshd HostbasedAuthentication is disabled.	Passed
169	Ensure sshd IgnoreRhosts is enabled.	Passed
170	Ensure sshd KexAlgorithms is configured.	Passed
171	Ensure sshd LogLevel is configured.	Passed
172	Ensure sshd *Login*GraceTime is configured.	Failed
173	Ensure sshd MACs are configured.	Failed
174	Ensure sshd MaxAuthTries is configured.	Failed
175	Ensure sshd MaxSessions is configured.	Passed
176	Ensure sshd MaxStartups is configured.	Failed
177	Ensure sshd PermitEmptyPasswords is disabled.	Passed
178	Ensure sshd PermitRoot*Login* is disabled.	Passed
179	Ensure sshd PermitUserEnvironment is disabled.	Passed
180	Ensure sshd UsePAM is enabled.	Passed
181	Ensure sshd access is configured.	Failed
182	Ensure strong password hashing algorithm is configured.	Passed
183	Ensure sudo authentication timeout is configured correctly.	Passed
184	Ensure sudo commands use pty.	Passed
185	Ensure sudo is installed.	Passed
186	Ensure sudo log file exists.	Failed
187	Ensure system is disabled when audit logs are full.	Failed
188	Ensure system warns when audit logs are low on space.	Failed
189	Ensure systemd-journal-remote authentication is configured.	Not Applicable
190	Ensure systemd-journal-remote is installed.	Failed
191	Ensure systemd-journal-remote service is not in use.	Passed
192	Ensure systemd-journal-upload is enabled and active.	Failed
193	Ensure systemd-timesyncd is enabled and running.	Passed
194	Ensure talk client is not installed.	Passed
195	Ensure telnet client is not installed.	Failed
196	Ensure tftp *server* services are not in use.	Passed
197	Ensure the audit configuration is immutable.	Failed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
198	Ensure ufw default deny firewall policy.	Failed
199	Ensure ufw is installed.	Passed
200	Ensure ufw is uninstalled or disabled with iptables.	Failed
201	Ensure ufw is uninstalled or disabled with nftables.	Failed
202	Ensure ufw loopback traffic is configured.	Failed
203	Ensure ufw service is enabled.	Passed
204	Ensure users must provide password for privilege escalation.	Passed
205	Ensure web proxy *server* services are not in use.	Passed
206	Ensure web *server* services are not in use.	Failed
207	Ensure xinetd services are not in use.	Passed

C2. Data *Post-test* — 14 Juni 2026
Agent: skanema | Agent ID: 001 | IP: 103.156.57.230 | Policy: CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0 | Status terakhir tiap kontrol per 14 Juni 2026, 05:27 WIB (diambil dari status terbaru pada rentang data historis)
Ringkasan: Passed = 118, Failed = 83, Not Applicable = 6, Total = 207, *Compliance score* = 57.0%

No	Judul Kontrol (CIS Benchmark)	Hasil
1	Ensure /dev/shm is a separate partition.	Passed
2	Ensure /etc/shadow password fields are not empty.	Passed
3	Ensure /tmp is a separate partition.	Failed
4	Ensure AIDE is installed.	Failed
5	Ensure AppArmor is enabled in the bootloader configuration.	Failed
6	Ensure AppArmor is installed.	Failed
7	Ensure Automatic Error Reporting is not enabled.	Failed
8	Ensure GDM is removed.	Passed
9	Ensure IPv6 status is identified.	Passed
10	Ensure NIS Client is not installed.	Passed
11	Ensure X window *server* services are not in use.	Passed
12	Ensure a nftables table exists.	Passed
13	Ensure access to /etc/issue is configured.	Passed
14	Ensure access to /etc/issue.net is configured.	Passed
15	Ensure access to /etc/motd is configured.	Passed
16	Ensure access to bootloader config is configured.	Failed
17	Ensure access to the su command is restricted.	Failed
18	Ensure accounts in /etc/passwd use shadowed passwords.	Passed
19	Ensure actions as another user are always logged.	Failed
20	Ensure all groups in /etc/passwd exist in /etc/group.	Passed
21	Ensure audit configuration files group owner is configured.	Passed
22	Ensure audit configuration files mode is configured.	Passed
23	Ensure audit configuration files owner is configured.	Passed
24	Ensure audit log files group owner is configured.	Passed
25	Ensure audit log storage size is configured.	Passed
26	Ensure audit logs are not automatically deleted.	Failed
27	Ensure audit tools group owner is configured.	Passed
28	Ensure audit tools mode is configured.	Passed
29	Ensure audit tools owner is configured.	Passed
30	Ensure audit_backlog_limit is sufficient.	Failed
31	Ensure auditd packages are installed.	Failed
32	Ensure auditd service is enabled and active.	Passed
33	Ensure auditing for processes that start prior to auditd is enabled.	Passed
34	Ensure autofs services are not in use.	Passed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
35	Ensure avahi daemon services are not in use.	Passed
36	Ensure bluetooth services are not in use.	Passed
37	Ensure bootloader password is set.	Failed
38	Ensure changes to system administration scope (sudoers) is collected.	Failed
39	Ensure chrony is enabled and running.	Failed
40	Ensure chrony is running as user _chrony.	Not Applicable
41	Ensure cron daemon is enabled and active.	Passed
42	Ensure cryptographic mechanisms are used to protect the integrity of audit tools.	Not Applicable
43	Ensure default user umask is configured.	Passed
44	Ensure dhcp *server* services are not in use.	Passed
45	Ensure dns *server* services are not in use.	Passed
46	Ensure dnsmasq services are not in use.	Passed
47	Ensure events that modify date and time information are collected.	Failed
48	Ensure events that modify the system's Mandatory Access Controls are collected.	Failed
49	Ensure events that modify the system's network environment are collected.	Failed
50	Ensure events that modify user/group information are collected.	Failed
51	Ensure filesystem integrity is regularly checked.	Failed
52	Ensure ftp client is not installed.	Passed
53	Ensure ftp *server* services are not in use.	Passed
54	Ensure group root is the only GID 0 group.	Passed
55	Ensure inactive password lock is configured.	Passed
56	Ensure ip6tables default deny firewall policy.	Passed
57	Ensure ip6tables loopback traffic is configured.	Failed
58	Ensure iptables default deny firewall policy.	Passed
59	Ensure iptables loopback traffic is configured.	Failed
60	Ensure iptables packages are installed.	Failed
61	Ensure iptables-persistent is not installed with ufw.	Passed
62	Ensure journald Compress is configured.	Not Applicable
63	Ensure journald ForwardToSyslog is disabled.	Not Applicable
64	Ensure journald Storage is configured.	Not Applicable
65	Ensure journald service is enabled and active.	Passed
66	Ensure ldap client is not installed.	Passed
67	Ensure ldap *server* services are not in use.	Passed
68	Ensure libpam-pwquality is installed.	Failed
69	Ensure local *login* warning banner is configured properly.	Failed
70	Ensure *login* and logout events are collected.	Failed
71	Ensure mail transfer *agent* is configured for local-only mode.	Passed
72	Ensure message access *server* services are not in use.	Passed
73	Ensure message of the day is configured properly.	Passed
74	Ensure minimum password age is configured.	Failed
75	Ensure minimum password length is configured.	Passed
76	Ensure network file system services are not in use.	Passed
77	Ensure nftables base chains exist.	Passed
78	Ensure nftables default deny firewall policy.	Passed
79	Ensure nftables is installed.	Passed
80	Ensure nftables is not installed with iptables.	Failed
81	Ensure nftables service is enabled.	Failed
82	Ensure nis *server* services are not in use.	Passed
83	Ensure nodev option set on /dev/shm partition.	Passed
84	Ensure nodev option set on /home partition.	Failed
85	Ensure nodev option set on /tmp partition.	Failed
86	Ensure nodev option set on /var partition.	Failed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
87	Ensure nodev option set on /var/log partition.	Failed
88	Ensure nodev option set on /var/log/audit partition.	Failed
89	Ensure nodev option set on /var/tmp partition.	Failed
90	Ensure noexec option set on /dev/shm partition.	Failed
91	Ensure noexec option set on /tmp partition.	Failed
92	Ensure noexec option set on /var/log partition.	Failed
93	Ensure noexec option set on /var/log/audit partition.	Failed
94	Ensure noexec option set on /var/tmp partition.	Failed
95	Ensure no*login* is not listed in /etc/shells.	Passed
96	Ensure nosuid option set on /dev/shm partition.	Passed
97	Ensure nosuid option set on /home partition.	Failed
98	Ensure nosuid option set on /tmp partition.	Failed
99	Ensure nosuid option set on /var partition.	Failed
100	Ensure nosuid option set on /var/log partition.	Failed
101	Ensure nosuid option set on /var/log/audit partition.	Failed
102	Ensure nosuid option set on /var/tmp partition.	Failed
103	Ensure pam_faillock module is enabled.	Passed
104	Ensure pam_pwhistory includes use_authtok.	Passed
105	Ensure pam_pwhistory module is enabled.	Passed
106	Ensure pam_pwquality module is enabled.	Passed
107	Ensure pam_unix does not include nullok.	Failed
108	Ensure pam_unix does not include remember.	Passed
109	Ensure pam_unix includes a strong password hashing algorithm.	Passed
110	Ensure pam_unix includes use_authtok.	Passed
111	Ensure pam_unix module is enabled.	Passed
112	Ensure password complexity is configured.	Passed
113	Ensure password dictionary check is enabled.	Failed
114	Ensure password expiration is configured.	Passed
115	Ensure password expiration warning days is configured.	Passed
116	Ensure password failed attempts lockout includes root account.	Passed
117	Ensure password failed attempts lockout is configured.	Passed
118	Ensure password history is enforced for the root user.	Failed
119	Ensure password history remember is configured.	Passed
120	Ensure password maximum sequential characters is configured.	Failed
121	Ensure password number of changed characters is configured.	Passed
122	Ensure password quality checking is enforced.	Failed
123	Ensure password quality is enforced for the root user.	Failed
124	Ensure password same consecutive characters is configured.	Failed
125	Ensure password unlock time is configured.	Passed
126	Ensure permissions on /etc/cron.d are configured.	Failed
127	Ensure permissions on /etc/cron.daily are configured.	Failed
128	Ensure permissions on /etc/cron.hourly are configured.	Failed
129	Ensure permissions on /etc/cron.monthly are configured.	Failed
130	Ensure permissions on /etc/cron.weekly are configured.	Failed
131	Ensure permissions on /etc/crontab are configured.	Failed
132	Ensure permissions on /etc/group are configured.	Passed
133	Ensure permissions on /etc/group- are configured.	Passed
134	Ensure permissions on /etc/gshadow are configured.	Failed
135	Ensure permissions on /etc/gshadow- are configured.	Failed
136	Ensure permissions on /etc/passwd are configured.	Passed
137	Ensure permissions on /etc/passwd- are configured.	Passed
138	Ensure permissions on /etc/security/opasswd are configured.	Failed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
139	Ensure permissions on /etc/shadow are configured.	Failed
140	Ensure permissions on /etc/shadow- are configured.	Failed
141	Ensure permissions on /etc/shells are configured.	Failed
142	Ensure permissions on /etc/ssh/sshd_config are configured.	Passed
143	Ensure permissions on SSH public host key files are configured.	Passed
144	Ensure prelink is not installed.	Passed
145	Ensure print *server* services are not in use.	Passed
146	Ensure re-authentication for privilege escalation is not disabled globally.	Passed
147	Ensure remote *login* warning banner is configured properly.	Passed
148	Ensure root is the only GID 0 account.	Passed
149	Ensure root is the only UID 0 account.	Passed
150	Ensure root password is set.	Passed
151	Ensure root user umask is configured.	Passed
152	Ensure rpcbind services are not in use.	Passed
153	Ensure rsh client is not installed.	Passed
154	Ensure rsync services are not in use.	Failed
155	Ensure samba file *server* services are not in use.	Passed
156	Ensure separate partition exists for /home.	Failed
157	Ensure separate partition exists for /var.	Failed
158	Ensure separate partition exists for /var/log.	Failed
159	Ensure separate partition exists for /var/log/audit.	Failed
160	Ensure separate partition exists for /var/tmp.	Failed
161	Ensure session initiation information is collected.	Failed
162	Ensure snmp services are not in use.	Passed
163	Ensure sshd Banner is configured.	Passed
164	Ensure sshd Ciphers are configured.	Passed
165	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured.	Passed
166	Ensure sshd DisableForwarding is enabled.	Failed
167	Ensure sshd GSSAPIAuthentication is disabled.	Passed
168	Ensure sshd HostbasedAuthentication is disabled.	Passed
169	Ensure sshd IgnoreRhosts is enabled.	Passed
170	Ensure sshd KexAlgorithms is configured.	Passed
171	Ensure sshd LogLevel is configured.	Passed
172	Ensure sshd *Login*GraceTime is configured.	Passed
173	Ensure sshd MACs are configured.	Failed
174	Ensure sshd MaxAuthTries is configured.	Passed
175	Ensure sshd MaxSessions is configured.	Passed
176	Ensure sshd MaxStartups is configured.	Failed
177	Ensure sshd PermitEmptyPasswords is disabled.	Passed
178	Ensure sshd PermitRoot*Login* is disabled.	Passed
179	Ensure sshd PermitUserEnvironment is disabled.	Passed
180	Ensure sshd UsePAM is enabled.	Passed
181	Ensure sshd access is configured.	Passed
182	Ensure strong password hashing algorithm is configured.	Passed
183	Ensure sudo authentication timeout is configured correctly.	Passed
184	Ensure sudo commands use pty.	Passed
185	Ensure sudo is installed.	Passed
186	Ensure sudo log file exists.	Failed
187	Ensure system is disabled when audit logs are full.	Failed
188	Ensure system warns when audit logs are low on space.	Failed
189	Ensure systemd-journal-remote authentication is configured.	Not Applicable
190	Ensure systemd-journal-remote is installed.	Failed

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

No	Judul Kontrol (CIS Benchmark)	Hasil
191	Ensure systemd-journal-remote service is not in use.	Passed
192	Ensure systemd-journal-upload is enabled and active.	Failed
193	Ensure systemd-timesyncd is enabled and running.	Passed
194	Ensure talk client is not installed.	Passed
195	Ensure telnet client is not installed.	Passed
196	Ensure tftp *server* services are not in use.	Passed
197	Ensure the audit configuration is immutable.	Failed
198	Ensure ufw default deny firewall policy.	Passed
199	Ensure ufw is installed.	Passed
200	Ensure ufw is uninstalled or disabled with iptables.	Failed
201	Ensure ufw is uninstalled or disabled with nftables.	Failed
202	Ensure ufw loopback traffic is configured.	Passed
203	Ensure ufw service is enabled.	Passed
204	Ensure users must provide password for privilege escalation.	Passed
205	Ensure web proxy *server* services are not in use.	Passed
206	Ensure web *server* services are not in use.	Failed
207	Ensure xinetd services are not in use.	Passed