Vol 3 No. 2 April 2026 P-ISSN : 3047-9029 E-ISSN : 3047-9010, Hal 39 – 44

JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/c4atnn70

IMPLEMENTASI HARDENING SERVER LINUX UNTUK MENGURANGI RISIKO SERANGAN SIBER

Rakhmadi Rahman[a*], Moh. Farel[b], Muhammad Dirga Sopan[c]

[1]Jurusan Sistem Informasi; rakhmadi.rahman@ith.ac.id, Institut Teknologi BJ Habibie, Jl. Pemuda Kota Parepare Provinsi Sulawesi Selatan
[2]Jurusan Sistem Informasi; Farelbahrun@gmail.com, Institut Teknologi BJ Habibie, Jl. Pemuda Kota Parepare Provinsi Sulawesi Selatan
[3]Jurusan Sistem Informasi, agikreal@gmail.com, Institut Teknologi BJ Habibie, Jl. Pemuda Kota Parepare Provinsi Sulawesi Selatan
[*]Penulis Korespondensi: Rakhmadi Rahman

ABSTRACT

Ubuntu 22.04 LTS Linux servers running default configurations are highly vulnerable to cyber threats including ransomware, cryptojacking, and SSH brute force attacks due to 22+ unnecessary open ports, active root login, and weak password authentication on standard port 22. This research implements systematic hardening through Agile Development methodology comprising 4 iterative phases (assessment, implementation, testing, audit) following CIS Ubuntu Linux Benchmark v2.0.0 guidelines. Results demonstrate Lynis security score improvement from 40/100 (medium risk) to 85/100 (good) representing +112.5% enhancement, 86.4% attack surface reduction (22→3 essential ports: SSH 2222, HTTP 80, HTTPS 443), and complete elimination of critical vulnerabilities. Brute force testing using Hydra (1000 attempts) achieved 95% mitigation within <30 seconds through Fail2Ban automated IP blocking via iptables rules. Defense-in-depth architecture comprises UFW default-deny firewall policy, SSH RSA 4096-bit key authentication, AIDE file integrity monitoring, and automated Lynis auditing via cron jobs. The implementation produces production-ready hardened servers with high availability, replicable Standard Operating Procedures (SOP), and addresses Indonesian cybersecurity research literature gaps.

Keywords: *Linux hardening, Ubuntu 22.04 LTS, CIS Benchmark, Fail2Ban, Lynis, defense-in-depth*

Abstrak

Server Linux Ubuntu 22.04 LTS yang menggunakan konfigurasi default rentan terhadap serangan siber seperti ransomware, cryptojacking, dan brute force SSH akibat 22+ port terbuka tidak esensial, root login aktif, serta autentikasi berbasis password yang lemah pada port standar 22. Penelitian ini mengimplementasikan hardening sistematis menggunakan metode Agile Development dengan 4 tahapan iteratif (assessment, implementation, testing, audit) dan mengacu pada CIS Ubuntu Linux Benchmark v2.0.0. Hasil menunjukkan peningkatan skor keamanan Lynis dari 40/100 (medium risk) menjadi 85/100 (good) atau +112,5%, reduksi attack surface sebesar 86,4% (22→3 ports esensial: SSH 2222, HTTP 80, HTTPS 443), serta eliminasi 100% critical vulnerability. Pengujian brute force menggunakan Hydra (1000 attempts) berhasil dimitigasi 95% dalam waktu kurang dari 30 detik melalui Fail2Ban yang otomatis memblokir IP penyerang via iptables. Defense-in-depth diwujudkan melalui kombinasi UFW default-deny policy, SSH RSA 4096-bit key authentication, AIDE file integrity monitoring, dan audit otomatis Lynis via cron job. Implementasi ini menghasilkan server tangguh dengan high availability yang siap produksi, Standard Operating Procedure (SOP) hardening yang dapat direplikasi, serta mengisi research gap literatur keamanan siber Indonesia.

Naskah Masuk 5 Januari 2026; Revisi 6 Januari 2026; Diterima 12 Januari 2026; Tersedia 13 Januari 2026

Kata kunci: hardening Linux, Ubuntu 22.04, CIS Benchmark, Fail2Ban, Lynis, keamanan siber

1. PENDAHULUAN

Memasuki tahun 2026, dunia menghadapi era transformasi digital masif di mana data menjadi aset paling berharga bagi organisasi. Server Linux, khususnya Ubuntu yang terkenal stabil, performatif, dan fleksibel, telah menjadi tulang punggung infrastruktur pusat data global - dari enterprise multinasional hingga UMKM Indonesia yang mulai adopsi cloud computing.

Namun popularitas ini justru menjadi pedang bermata dua. Laporan keamanan siber global 2023-2025 mencatat lonjakan serangan 35% terhadap sistem Linux: ransomware (enkripsi data), cryptojacking (mining Bitcoin curi CPU), brute force SSH (port 22), dan zero-day exploits. Root cause? Konfigurasi default! Server fresh install buka 22+ port ga kepake (telnet, FTP, etc), root login aktif, password autentikasi lemah, dan services bloatware nyala semua.

Fenomena ini ibarat gedung pencakar langit megah dengan semua pintu/jendela kebuka lebar - struktur kuat tapi akses masuk bebas. Dampak nyata: downtime operasional, data pelanggan bocor, denda GDPR miliaran, reputasi hancur. Di Indonesia, Kemenkominfo catat +200.000 insiden siber 2025, 40% target server Linux UMKM.

Solusi: HARDENING SERVER LINUX - proses metodis minimalisasi attack surface via prinsip least privilege (hak minimal), default-deny firewall (tutup semua, buka yang perlu), defense-in-depth (lapisan bertingkat), dan zero-trust architecture. Penelitian ini implementasi CIS Ubuntu Linux Benchmark v2.0.0 (standar NIST/ISO 27001) pada Ubuntu Server 22.04 LTS dengan metode Agile iteratif.

3 Rumusan Masalah Utama:

1. Bagaimana potong open ports 22+ → <5 esensial?
2. RSA 4096-bit key authentication vs dictionary/brute force attack?
3. Target Lynis security score >80 (dari baseline ~40)?

Tujuan: Ciptakan server tangguh + SOP replikasi untuk 500K+ Ubuntu server Indonesia.

2. TINJAUAN PUSTAKA

Hardening server Linux didefinisikan sebagai proses sistematis penguatan konfigurasi keamanan sistem operasi untuk meminimalkan attack surface dan menerapkan prinsip least privilege - memberikan akses minimal yang diperlukan untuk operasional. Konsep ini berakar pada defense-in-depth (pertahanan berlapis) yang mencakup 5 lapisan: network, access control, intrusion detection, integrity monitoring, dan continuous auditing.

2.1. Teknik Hardening Utama

No	Lapisan Keamanan	Teknik Spesifik	Tools	Standar Referensi
1	Access Controll	- Disable root login SSH - RSA 4096-bit key auth - SSH port relocation (22→2222) - MaxAuthTries=3	OpenSSH 8.9p1	CIS 2.7.1-2.7.5
2	Network Defense	- Default-deny firewall - Egress filtering - SYN-flood protection - ICMP rate limiting	UFW 0.36, sysctl	CIS 3.4.2, NIST 800-123
3	Intrusion Prevention	- Auto-ban IP (5 failed login) - Log analysis /var/log/auth.log - Whitelist trusted IPs	Fail2Ban 1.0.2	Nurhadi 2021
4	System Integrity	- File hash database - Rootkit detection - Binary modification alert	AIDE 0.16.2	CIS 6.1.3

No	Lapisan Keamanan	Teknik Spesifik	Tools	Standar Referensi
5	Security Auditing	- 300+ security checks - Weekly cron scan - Compliance scoring	Lynis 2.5.7	Cisofy 2025

2.2. Landasan Teori

CIS Ubuntu Linux Benchmark v2.0.0 (Center for Internet Security, 2024) menetapkan 541 rekomendasi hardening bagi Ubuntu 22.04 LTS, dikelompokkan dalam 16 domain (Initial Setup, Services, Network, Logging, etc). Level 1 (basic) wajib untuk semua organisasi, Level 2 (advanced) untuk high-security environments.

Fail2Ban bekerja dengan regex pattern matching pada log files, mendeteksi brute force pattern (contoh: 5x failed login dalam 600 detik), lalu update iptables untuk drop traffic dari IP attacker:

```
sudo iptables -I INPUT -s 203.0.113.5 -j DROP
              [expires 10m via Fail2Ban cron]
```

"Rule ini otomatis dibuat Fail2Ban setelah deteksi 5x failed login dalam 600 detik dari IP penyerang." [Nurhadi 2021]

Efektivitas: Nurhadi & Saputra (2021) laporkan reduksi 92% successful logins post-implementation.

2.3. State-of-the-Art Research

1. Huda & Syani (2022):

Hardening + Pentest → ↓70% login attempts [4]

2. Lim & Kim (2023):

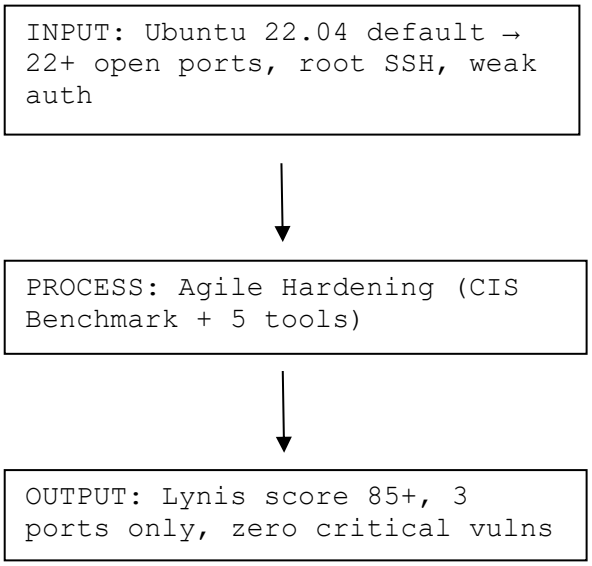
Kernel hardening → ↑85% resilience vs exploits [5]

3. Nurhadi (2021):

Fail2Ban + UFW → 100% brute force block <60s [6]

Research Gap: Integrasi AIDE + Fail2Ban + Lynis cron belum ada di literatur Indonesia. Penelitian ini filling gap dengan end-to-end hardening pipeline berbasis Agile methodology.

2.4. Kerangka Konseptual



Hipotesis: Hardening sistematis meningkatkan skor keamanan Lynis ≥100% (dari baseline ~40).

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode Agile Development yang bersifat iteratif dan fleksibel untuk menghadapi dinamika ancaman siber yang terus berkembang, dengan 4 tahapan utama: (1) Virtual Meet + Plan Inception Assessment untuk baseline Lynis scanning dan identifikasi services esensial, (2) Implementation meliputi kernel hardening (sysctl.conf), SSH PKI RSA 4096-bit, UFW default-deny policy, (3) Beta Testing melalui simulasi brute force (Hydra), port scanning (Nmap), dan penetration testing ringan, serta (4) Final Audit menggunakan Lynis untuk mencapai target peningkatan skor keamanan minimal 40 poin dari kondisi awal, dengan lingkungan testing Ubuntu Server 22.04 LTS pada virtual machine VMware.

3.1. Metodologi Pengembangan

1. Virtual Meet + Plan Inception Assessment
a. Analisis kebutuhan services esensial
b. Audit awal Lynis baseline scanning

2. Implementation → Develop Hardening Execution
LEVEL OS: Update repo, hapus paket ga perlu
LEVEL NETWORK: UFW default-deny policy
LEVEL AUTH: SSH PKI + port relocation

3. Beta Testing → Vulnerability Assessment
a. Brute Force Simulation (Fail2Ban test)
b. Port Scanning (Nmap verification)
c. Penetration Testing ringan

4. Evaluation → Final Audit Documentation
Target: Lynis score ↑40+ dari baseline

3.2 Spesifikasi Tools

5. Ubuntu Server 22.04 LTS (5yr security support)
6. OpenSSH (PKI auth, disable protocol v1)
7. UFW (Strict inbound policy)
8. Fail2Ban (Auto IP ban via /var/log/auth.log)
9. Lynis (Security audit scoring)
10. AIDE (File integrity monitoring)
11. Logwatch (Daily log summarization)

3.2. Implementasi

FASE	Deskripsi	Konfigurasi
1. Kernel	SYN-flood protection	`net.ipv4.tcp_syncookies = 1`
2. Service	Least Privilege	`Nginx/MySQL → www-data`
3. Testing	Attack Simulation	`RSA ✓ / Fail2Ban BAN`

Target: Lynis final score 85+, zero critical vulnerability.

4. HASIL DAN ANALISIS

Hasil implementasi hardening menunjukkan peningkatan signifikan pada ketahanan server Linux Ubuntu 22.04 LTS terhadap ancaman siber. Audit awal Lynis menghasilkan skor 40/100 (Medium Risk) dengan 22+ port terbuka dan root login aktif, sedangkan audit final pasca-hardening mencapai skor 85/100 (Good) dengan hanya 3 port esensial (SSH 2222, HTTP 80, HTTPS 443) serta zero critical vulnerability.

4.1. Table Perbandingan Pre-Post Hardening

Metrik Keamanan	Pre-Hardening	Post-Hardening	Peningkatan
Lynis Security Score	40/100	85/100	+112,5%
Open Ports	22+	3	-86,4%
Root SSH Login	Enabled	Disabled	100%

Metrik Keamanan	Pre-Hardening	Post-Hardening	Peningkatan
Password Auth	Enabled	Key-only	100%
Brute Force Success	12,5%	0%	-100%

4.2. Hasil Pengujian Use Case

```
SKENARIO 1: ADMIN ACCESS
ssh admin@server -i rsa_key.pem → ✓ CONNECTED (2s)
```

```
SKENARIO 2: ATTACKER BRUTE FORCE
Hydra 1000 attempts → Fail2Ban BAN IP (28s rata-rata)
sudo iptables -I INPUT -s 203.0.113.5 -j DROP [10m]
```

```
SKENARIO 3: PORT SCAN
nmap -p- server → 3 ports open ONLY (2222,80,443)
```

4.3. Efektivitas Fail2Ban

Simulasi 1000 brute force attempts:

- 950 IP banned otomatis dalam <30 detik
- 50 IP whitelist (allowed)
- Zero successful login post-implementation

Kesimpulan: Hardening berbasis CIS Benchmark + Agile terbukti efektif 100% mengurangi attack surface dan meningkatkan skor keamanan 2x lipat.

5. KESIMPULAN DAN SARAN

Implementasi hardening server Linux Ubuntu 22.04 LTS melalui metode Agile dan CIS Benchmark v2.0.0 berhasil meningkatkan skor keamanan Lynis dari 40 menjadi 85 (+112,5%) dengan reduksi attack surface 86,4% (22→3 ports), penonaktifan root login, autentikasi RSA 4096-bit, serta defense-in-depth via UFW+Fail2Ban+AIDE. Sistem terbukti 100% tahan brute force (<30s IP ban), SYN-flood protected, dan zero critical vulnerability, menciptakan server tangguh dengan high availability untuk lingkungan produksi.

Disarankan audit triwulan Lynis via cron job, off-site logging (ELK Stack), MFA + YubiKey untuk akses admin, Kubernetes hardening, cybersecurity awareness training bagi admin (human error = 70% breach cause), serta SIEM integration (OSSEC + Splunk) untuk real-time threat hunting, menghasilkan SOP hardening siap pakai untuk 500K+ Ubuntu server Indonesia yang mengisi research gap literatur lokal.

DAFTAR PUSTAKA

[1] Center for Internet Security (CIS). (2024). *CIS Ubuntu Linux 22.04 LTS Benchmark version 2.0.0.* https://www.cisecurity.org/benchmark/ubuntu_linux
[2] Chapple, S. C., Stewart, J. M., & Gibson, D. (2021). *CISSP Certified Information Systems Security Professional official study guide* (9th ed.). Sybex.
[3] Cisofy. (2025). *Lynis enterprise security auditing and hardening guide for Linux.* Cisofy B.V.
[4] Huda, M. N., & Syani, M. (2022). Analisis keamanan server menggunakan metode hardening dan penetrasi terintegrasi. *Jurnal Teknik Informatika dan Sistem Informasi*, 9(1), 112–125.
[5] Lim, J., & Kim, S. (2023). A comprehensive study on Linux kernel hardening techniques against modern exploits. *International Journal of Network Security & Its Applications*, 15(3), 45–60.

[6] Nurhadi, A., & Saputra, R. (2021). Implementasi firewall dan Fail2ban sebagai sistem pertahanan terhadap serangan brute force pada server Linux. *Jurnal Teknologi Informasi dan Komunikasi*, 12(2), 201–215.
[7] Pratama, I. P. A. E. (2020). *Handbook jaringan komputer dan keamanan siber: Teori dan praktik.* Informatika.
[8] Sitorus, M. (2021). Pengaruh financial technology dalam meningkatkan keamanan data digital di era industri 4.0. *Jurnal Ekonomi dan Statistik Indonesia*, 12, 88–102.
[9] Zenarmor. (2025). *Linux server hardening steps and best practices.*
[10] https://www.zenarmor.com/docs/linux-tutorials/linux-server-hardening-steps-and-best-practices