LAPORAN PRAKTIK KEINSIYURAN

AUDIT KEAMANAN JARINGAN DAN PENILAIAN KERENTANAN (VULNERABILITY ASSESSMENT) DI RUMAH SAKIT UNIVERSITAS INDONESIA

PERIODE: FEBRUARI 2024 – AGUSTUS 2024

AHMAD FIRDAUSI

52524110017

PEMBIMBING KAMPUS

Ir. Saiful Hendra. S.T., M.T., IPM

PEMBIMBING LAPANGAN

Prof. Dr. Ir. Setiyo Budiyanto.,ST., MT., IPU., Asean-Eng.,APEC-Eng

PROGRAM STUDI PROGRAM PROFESI INSINYUR
FAKULTAS TEKNIK
UNIVERSITAS MERCU BUANA
JAKARTA
2025

HALAMAN PENGESAHAN
LAPORAN PRAKTIK KEINSINYURAN

AUDIT KEAMANAN JARINGAN DAN PENILAIAN KERENTANAN (VULNERABILITY ASSESSMENT)

Disusun oleh:

AHMAD FIRDAUSI
52524110017

Telah disetujui oleh:

Dosen Pembimbing	Pembimbing Lapangan
Ir. Saiful Hendra, S.T., M.T., IPM. ASEAN Eng	Prof. Dr. Ir. Setiyo Budiyanto.,ST., MT., IPU., Asean-Eng.,APEC-Eng

Mengetahui

Dekan Fakultas Teknik	Ketua Program Studi Program Profesi Insinyur
Dr. Zulfa Fitri Ikatrinasari, M.T.	Ir. Imbuh Rochmad, S.T., M.T., IPM., ASEAN Eng., ACPE.

HALAMAN PERNYATAAN

Dengan ini saya menyatakan bahwa dalam mengerjakan dan Praktik Keinsinyuran ini saya tidak melakukan pemalsuan data dan semua materi dalam laporan ini merupakan hasil karya saya sendiri, kecuali yang secara tertulis diacu dalam naskah dan disebutkan sumbernya dalam Daftar Pustaka. Jika di kemudian hari terbukti tidak sesuai dengan pernyataan ini, maka saya bersedia menerima sanksi sesuai ketentuan.

Jakarta, 25 Juli 2025

Ahmad Firdausi
52524110017

ABSTRAK

Tujuan dari penelitian ini adalah untuk mengevaluasi keamanan jaringan di lingkungan rumah sakit melalui audit menyeluruh yang mencakup pemindaian dan analisis data untuk memastikan kelemahan keamanan jaringan yang ada. Selain itu, tujuan penelitian ini adalah untuk mengkategorikan dan mengklasifikasikan berbagai jenis kerentanan yang terkait dengan tingkat keparahan dan jenis ancaman yang dihadapi. Ini dilakukan untuk membantu kami menentukan langkah-langkah yang paling mendesak yang harus diambil oleh rumah sakit untuk mengurangi ancaman tersebut. Hasil audit ini menghasilkan rekomendasi yang disesuaikan untuk rumah sakit tertentu dengan menerapkan protokol keamanan jaringan terbaik. Banyak pihak menganggap penelitian ini penting. Hasil penelitian ini dapat memberikan wawasan yang lebih mendalam tentang kondisi keamanan jaringan rumah sakit yang diteliti. Informasi ini dapat membantu para peneliti membuat strategi yang lebih baik untuk mengurangi risiko serangan siber terhadap aset digital mereka. Dari perspektif akademis dan penelitian, temuan ini memperluas penelitian tentang metode dan penilaian kerentanan dalam keamanan siber kontemporer. Hasil ini dapat digunakan sebagai dasar untuk penelitian terkait. Studi ini juga dapat digunakan oleh rumah sakit lain dan masyarakat umum untuk membantu mereka melakukan audit keamanan jaringan dan memahami pentingnya perlindungan digital.

Hasil penelitian menunjukkan bahwa tindakan yang direkomendasikan telah meningkatkan keamanan jaringan secara substansial. Pembaruan sistem yang jarang, konfigurasi firewall yang buruk, dan kurangnya autentikasi multifaktor (MFA) yang digunakan dalam sistem autentikasi semuanya telah diatasi. Pembaruan sistem rutin, penegakan aturan firewall, dan penerapan MFA telah meningkatkan keamanan data. Selain itu, pembaruan firmware untuk perangkat IoT dan penerapan enkripsi AES 256 untuk komunikasi jaringan juga telah meningkatkan keamanan data. Penelitian ini juga menunjukkan bahwa mencatat kerugian finansial dan memperbarui dokumen respons insiden penting untuk penanganan ancaman yang lebih akurat dan efektif.

Singkatnya, audit keamanan berkala yang diusulkan dalam studi ini akan memungkinkan rumah sakit untuk mengikuti standar keamanan yang tinggi dan

meningkatkan keamanan berkelanjutan seiring dengan kemajuan teknologi digital. Rumah sakit juga akan lebih siap untuk mengenali dan mengatasi ancaman siber di masa mendatang dengan kebijakan audit yang konsisten.

Kata kunci : Audit keamanan; Kerentanan jaringan; Keamanan jaringan; Mitigasi risiko; Manajemen insiden; Kebijakan audit.

ABSTRACT

This study aimed to evaluate network security in a hospital environment through a comprehensive audit that included scanning and data analysis to determine the existing network security weaknesses. In addition, this study aimed to categorize and classify the various types of vulnerabilities related to the severity and type of threats faced. This was done to help us determine the most urgent steps that the hospital should take to mitigate the threats. This audit resulted in recommendations tailored to a specific hospital by implementing the best network security protocols.

Many parties consider this study important. The results of this study can provide deeper insight into the state of the network security of the hospital studied. This information can help researchers create better strategies to reduce the risk of cyberattacks on their digital assets. From an academic and research perspective, these findings expand the research on methods and vulnerability assessments in contemporary cybersecurity. These results can be used as a basis for related research. Other hospitals and the general public can also use this study to help them conduct network security audits and understand the importance of digital protection.

The study results showed that the recommended actions have substantially improved network security. Infrequent system updates, poor firewall configuration, and lack of multifactor authentication (MFA) used in authentication systems were all addressed. Regular system updates, firewall rule enforcement, and MFA implementation have improved data security. Additionally, firmware updates for IoT devices and the implementation of AES 256 encryption for network communications have also improved data security. The study also showed that recording financial losses and updating incident response documents are essential for more accurate and effective threat response.

In summary, the periodic security audits proposed in this study will enable hospitals to adhere to high-security standards and improve ongoing security as digital technologies advance. Hospitals will also be better prepared to recognize and address future cyber threats with consistent audit policies.

Keywords: *Security audit; Network vulnerability; Network security; Risk mitigation; Incident management; Audit policy.*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT karena atas rahmat-Nya, Laporan Praktik Keinsiyuran ini dapat diselesaikan dengan judul **"Audit Keamanan Jaringan Dan Penilaian Kerentanan (Vulnerability Assessment) Di Rumah Sakit Universitas Indonesia Periode: Februari 2024 – Agustus 2024".**

Penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, bimbingan, dan motivasi selama proses penulisan laporan ini.

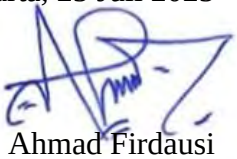
Terima kasih yang tak terhingga kepada Bapak Dosen Pembimbing Kampus Bapak Ir. Saiful Hendra. S.T., M.T., IPM. Serta Bapak Pembimbing Lapangan Prof. Dr. Ir. Setiyo Budiyanto.,ST., MT., IPM., Asean-Eng.,APEC-Eng. yang telah memberikan arahan, masukan, dan bimbingan yang sangat berharga. Terima kasih atas kesabaran dan dukungan yang diberikan dalam memandu penulisan laporan ini.

Tak lupa juga untuk mengucapkan terima kasih kepada Ketua Program Studi Profesi Insiyur Bapak Ir. Imbuh Rochmad, S.T., M.T., Ipm., Asean Eng., Acpe. Dan semua dosen, tenaga pendidik di Program Studi Profesi Insiyur yang telah memberikan ilmu, pemahaman, serta wawasan yang sangat berharga bagi penulis selama menempuh studi.

Penulis juga ingin mengungkapkan rasa terima kasih kepada keluarga atas doa dan supportnya selama penyusunan Laporan ini.

Akhir kata, semoga laporan ini dapat memberikan manfaat dan kontribusi yang positif dalam pengembangan ilmu pengetahuan, khususnya di bidang Teknik Elektro.

Jakarta, 25 Juli 2025



Ahmad Firdausi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL