INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 243-246, ISSN: 3123-5573 (Online)

Analisis Kerentanan Sistem Jaringan Kampus Menggunakan *Vulnerability Assessment Tools*

Rakhmadi Rahman[1],Muh Ariel Anugrah[2], Afrilia Dian Triutami[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie
E-mail: adaith@ith.ac.id

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:
Network Security, Vulnerability Assessment, Nessus, Risk Analysis, Risk Assessment

ABSTRACT

Network security in a campus environment is a critical aspect due to the increasing dependence of academic and administrative services on network infrastructure. Network complexity combined with limited periodic security evaluations may result in vulnerabilities that are not immediately detected. This study aims to analyze the security condition of a campus network system using a vulnerability assessment approach based on the Nessus Essentials tool. The research employs a descriptive method consisting of system observation, vulnerability scanning, and risk analysis based on severity classification. The results indicate that the analyzed network contains vulnerabilities with varying levels of severity, predominantly categorized as low and informational, which reflect configuration weaknesses and service information exposure. Although no critical vulnerabilities were identified, these findings may still contribute to potential security risks if not managed continuously. This study demonstrates that vulnerability assessment can serve as an effective initial preventive approach for systematic campus network security evaluation.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
Network Security, Vulnerability Assessment, Nessus, Risk Analysis, Risk Assessment)

ABSTRAK

Keamanan sistem jaringan kampus merupakan aspek kritis seiring meningkatnya ketergantungan layanan akademik dan administrasi terhadap infrastruktur jaringan. Kompleksitas jaringan serta keterbatasan evaluasi keamanan berkala berpotensi menimbulkan kerentanan yang tidak teridentifikasi secara langsung. Penelitian ini bertujuan untuk menganalisis kondisi keamanan sistem jaringan kampus menggunakan pendekatan vulnerability assessment berbasis tools Nessus Essentials. Metode penelitian bersifat deskriptif dengan tahapan observasi sistem, pemindaian kerentanan, serta analisis tingkat risiko berdasarkan klasifikasi severity. Hasil penelitian menunjukkan bahwa sistem jaringan memiliki sejumlah kerentanan dengan tingkat keparahan yang bervariasi, didominasi oleh kategori low dan informational, yang mengindikasikan kelemahan konfigurasi serta keterbukaan informasi layanan. Meskipun tidak ditemukan kerentanan kritis, keberadaan temuan tersebut tetap berpotensi meningkatkan risiko keamanan apabila tidak dikelola secara berkelanjutan. Penelitian ini menegaskan bahwa vulnerability assessment dapat digunakan sebagai langkah preventif awal dalam evaluasi keamanan jaringan kampus secara sistematis dan terukur.

Corresponding Author:
Rakhmadi Rahman
Institut Teknologi Bacharuddin Jusuf Habibie
E-mail: adaith@ith.ac.id

PENDAHULUAN

Perkembangan teknologi informasi mendorong institusi pendidikan tinggi untuk mengandalkan sistem jaringan dalam mendukung aktivitas akademik dan administrasi. Kondisi ini menyebabkan keamanan jaringan menjadi faktor strategis yang berpengaruh langsung terhadap keberlangsungan layanan. Infrastruktur jaringan yang terus berkembang sering kali tidak diimbangi dengan evaluasi keamanan yang terstruktur, sehingga berpotensi menimbulkan celah keamanan.Kerentanan sistem jaringan umumnya tidak langsung terdeteksi karena tidak selalu berdampak pada gangguan operasional secara langsung. Tanpa mekanisme evaluasi keamanan yang sistematis, kerentanan tersebut dapat berkembang menjadi risiko yang berdampak pada kebocoran data dan gangguan layanan. Oleh karena itu, diperlukan pendekatan yang mampu memberikan gambaran awal kondisi keamanan jaringan secara menyeluruh.

Vulnerability assessment merupakan pendekatan yang digunakan untuk mengidentifikasi dan mengevaluasi potensi kerentanan sistem tanpa melakukan eksploitasi aktif. Pendekatan ini relevan diterapkan pada lingkungan kampus karena mempertimbangkan aspek etika dan keberlangsungan operasional. Penelitian ini difokuskan pada analisis kerentanan sistem jaringan kampus menggunakan vulnerability assessment tools guna memperoleh gambaran tingkat risiko keamanan jaringan. Berbeda dengan penetration testing yang berfokus pada eksploitasi kerentanan, penelitian ini menitikberatkan pada evaluasi awal kondisi keamanan jaringan sebagai dasar manajemen risiko. Dengan pendekatan ini, penelitian diharapkan dapat memberikan gambaran objektif mengenai tingkat kerentanan sistem jaringan kampus tanpa mengganggu operasional sistem yang sedang berjalan.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif untuk memperoleh gambaran awal kondisi keamanan sistem jaringan kampus. Objek penelitian adalah sistem jaringan kampus yang dianalisis dari sisi keamanan jaringan. Pengumpulan data dilakukan melalui observasi sistem, studi literatur, serta pemindaian kerentanan menggunakan Nessus Essentials.

Proses vulnerability assessment dilakukan dengan metode unauthenticated basic network scan terhadap host dalam satu segmen jaringan. Pendekatan unauthenticated dipilih untuk mensimulasikan sudut pandang penyerang eksternal serta menjaga aspek etika dan keberlangsungan operasional sistem. Hasil pemindaian dianalisis berdasarkan klasifikasi tingkat keparahan (critical, high, medium, low, dan informational) yang disediakan oleh tools. Penelitian ini tidak mencakup eksploitasi kerentanan maupun penetration testing, sehingga analisis difokuskan pada identifikasi dan klasifikasi risiko keamanan jaringan.

HASIL DAN PEMBAHASAN

Hasil pemindaian menunjukkan bahwa sistem jaringan yang dianalisis memiliki sejumlah kerentanan dengan tingkat keparahan yang berbeda. Mayoritas temuan berada pada kategori low dan informational, yang mengindikasikan adanya layanan terbuka serta informasi sistem yang dapat diakses dari sisi jaringan. Meskipun tidak ditemukan kerentanan dengan tingkat critical, keberadaan kerentanan tingkat rendah tetap menunjukkan bahwa sistem jaringan belum sepenuhnya optimal dari sisi keamanan. Kerentanan tersebut dapat menjadi titik awal eskalasi risiko apabila dikombinasikan dengan kesalahan konfigurasi lain atau kelalaian pengelolaan jaringan. Temuan ini menegaskan pentingnya evaluasi keamanan jaringan secara berkala sebagai bagian dari manajemen risiko keamanan informasi..

Dominasi temuan dengan tingkat keparahan low dan informational menunjukkan bahwa sistem jaringan tidak berada pada kondisi kritis, namun masih memiliki kelemahan pada aspek konfigurasi dan keterbukaan informasi layanan. Kerentanan jenis ini sering kali menjadi tahap awal dalam rantai serangan (attack chain) apabila dikombinasikan dengan kesalahan konfigurasi lanjutan atau kelalaian pengelolaan sistem. Oleh karena itu, meskipun tidak bersifat kritis, temuan tersebut tetap memiliki implikasi terhadap manajemen risiko keamanan jaringan dan perlu mendapatkan perhatian dalam pengelolaan keamanan jangka panjang.

KESIMPULAN

Penelitian ini menunjukkan bahwa vulnerability assessment tools mampu memberikan gambaran awal kondisi keamanan sistem jaringan kampus secara sistematis. Hasil analisis kerentanan menunjukkan variasi tingkat keparahan yang didominasi oleh kategori low dan informational, yang mengindikasikan adanya kelemahan konfigurasi dan keterbukaan informasi layanan. Pendekatan vulnerability assessment terbukti relevan sebagai langkah preventif awal dalam evaluasi keamanan jaringan tanpa mengganggu operasional sistem.

DAFTAR PUSTAKA

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Waltham, MA: Syngress.

Behl, A., & Behl, K. (2017). *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford: Oxford University Press.

ENISA. (2016). *Vulnerability Assessment and Risk Management*. European Union Agency for Cybersecurity.

Kizza, J. M. (2015). *Guide to Computer Network Security*. London: Springer.

NIST. (2012). *Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1)*. National Institute of Standards and Technology.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.

Stallings, W. (2018). *Network Security Essentials: Applications and Standards*. Boston: Pearson Education.

Tenable, Inc. (2023). *Nessus Essentials User Guide*. Tenable Network Security.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security*. Boston: Cengage Learning.