ANALISIS METODE VULNERABILITY SCANNING DAN PERBANDINGAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE

Skripsi

Diajukan Untuk Memenuhi Persyaratan

Guna Meraih Gelar Sarjana Informatika

Universitas Muhammadiyah Malang

Dhana Agustya Putra Sasongko

201910370311357

Bidang Minat

Sistem Keamanan Jaringan

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2024

LEMBAR PERSETUJUAN

ANALISIS METODE VULNERABILITY SCANNING DAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *22 November 2024*

Dosen Pembimbing 1	Dosen Pembimbing 2
Luqman Hakim S.Kom., M.Kom.	**-**
NIP. 10819030658PNS.	**NIP.**

LEMBAR PENGESAHAN

ANALISIS METODE VULNERABILITY SCANNING DAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

DHANA AGUSTYA PUTRA SASONGKO

201910370311357

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 22 November 2024

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Diah Risqiwati ST., MT.	**Ir. Wildan Suharso S.Kom., M.Kom**
NIP. 10814100545PNS.	**NIP. 10817030596PNS.**

Mengetahui,
Ketua Jurusan Informatika

Fajar Calih Wasis Wicaksono S.kom. M.Cs.
NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : DHANA AGUSTYA PUTRA SASONGKO

NIM : 201910370311357

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"ANALISIS METODE VULNERABILITY SCANNING DAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Luqman Hakim S.Kom., M.Kom.

Malang, 22 November 2024
Membuat Pernyataan

DHANA AGUSTYA PUTRA SASONGKO

ABSTRAK

Kemajuan teknologi jaringan, termasuk internet, telah mendorong perkembangan website sebagai wadah informasi yang mudah diakses dan digunakan untuk berbagai aktivitas. Namun, peningkatan jumlah website juga membuka peluang bagi hacker dan cracker untuk mengeksploitasi kerentanan sistem keamanan, seperti pencurian data dan serangan sistem. Berbagai metode pengujian keamanan, seperti white box dan black box testing, digunakan untuk mendeteksi kerentanan pada aplikasi web. Salah satu teknologi keamanan yang banyak digunakan adalah Intrusion Detection System (IDS) berbasis Snort, yang memiliki kemampuan mendeteksi ancaman dengan ribuan aturan keamanan. Penelitian ini bertujuan untuk mengembangkan sistem keamanan berbasis Snort melalui pengujian menggunakan metode Vulnerability Scanning dan Penetration Testing. Dengan menganalisis hasil identifikasi terhadap berbagai pola serangan, penelitian ini diharapkan dapat meningkatkan kemampuan Snort dalam mendeteksi serangan secara lebih mendetail dan memberikan kontribusi terhadap perancangan sistem keamanan website yang lebih stabil dan efektif.

Kata Kunci: Keamanan Website, Snort, Intrusion Detection System (IDS), Vulnerability Scanning, Penetration Testing, Kerentanan Aplikasi Web.

ABSTRACT

The advancement of network technology, including the internet, has driven the rapid growth of websites as accessible platforms for information and various activities. However, the increasing number of websites also presents opportunities for hackers and crackers to exploit system vulnerabilities, such as data theft and system attacks. Various security testing methods, including white box and black box testing, are utilized to detect vulnerabilities in web applications. One widely used security technology is the Snort-based Intrusion Detection System (IDS), known for its ability to detect threats using thousands of security rules. This study aims to enhance the Snort-based security system through testing methods such as Vulnerability Scanning and Penetration Testing. By analyzing the identification results against various attack patterns, this research seeks to improve Snort's capability in detecting attacks more comprehensively and contribute to designing a more stable and effective web security system.

Keywords: Website Security, Snort, Intrusion Detection System (IDS), Vulnerability Scanning, Penetration Testing, Web Application Vulnerabilities.

KATA PENGANTAR

Dengan memanjatkan puji syukur ke hadirat Allah SWT atas limpahan rahmat dan hidayah-Nya, sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul:

"ANALISIS METODE VULNERABILITY SCANNING DAN PERBANDINGAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE"

Di dalam tulisan ini disajikan pokok-pokok bahasan yang meliputi teori dasar mengenai teknologi jaringan dan sistem keamanan, analisis kerentanan aplikasi web, metode pengujian keamanan menggunakan Snort, serta pengujian menggunakan metode vulnerability scanning dan penetration testing untuk mengidentifikasi dan mengatasi ancaman terhadap keamanan website. Penelitian ini bertujuan untuk memberikan solusi dalam meningkatkan keamanan website melalui teknologi IDS berbasis Snort.

Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu, peneliti mengharapkan saran yang membangun agar tulisan ini bermanfaat bagi perkembangan ilmu pengetahuan, khususnya dalam bidang keamanan jaringan dan aplikasi web.

Malang, 07 Desember 2024

Dhana Agustya Putra Sasongko

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

[1]. Dar, M. H., & Harahap, S. Z. (2017). IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER. JURNAL INFORMATIKA, 6(3), 14–23. https://doi.org/10.36987/informatika.v6i3.1619

[2]. Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. JURNAL MEDIA INFORMATIKA BUDIDARMA, 4(2), 413. https://doi.org/10.30865/mib.v4i2.2037

[3]. Hafiz, A., Kurniawan, T., Sivi, N. A., Ikhsan, F. K., & Andhika, P. (2020). ANALISIS CELAH KEAMANAN JARINGAN DAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM. Jurnal Informasi Dan Komputer, 8(2), 59–66. https://doi.org/10.35959/jik.v8i2.185

[4]. Lukman, L., & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. Respati, 15(2), 6. https://doi.org/10.35842/jtir.v15i2.343

[5]. Prasetyo, H. (2016). Analisa Keamanan Web Server Menggunakan Web Application Firewall Modsecurity

[6]. Arman, M., & Rachmat, N. (2020). IMPLEMENTASI SISTEM KEAMANAN WEB MENGGUNAKAN PFSENSE. Jusikom : Jurnal Sistem Komputer Musirawas, 5(1), 13-23. https://doi.org/10.32767/jusikom.v5i1.752

[7]. Hassan, Z., Shahzeb, Odarchenko, R., Gnatyuk, S., Zaman, A., & Shah, M (2018). Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems. 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), 238-288. https://doi.org/10.1109/MSNMC.2018.8576287

[8]. Purba, W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. AITI, 17(2), 143-158. https://doi.org/10.24246/aiti.v17i2.143-158

[9]. Mutaqin, A. (2016). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 4(1).

[10]. Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort. Jurnal Sisfokom (Sistem Informasi dan Komputer), 9(1), 97-101. https://doi.org/10.32736/sisfokom.v9i1.770

[11]. F. R. Muñoz et al. (2016). Analyzing the traffic of penetration testing tools with an IDS. J Supercomput. DOI: 10.1007/s11227-016-1920-7

[12]. Yuma, M., & Vitaly K. (2015). Evaluation of Web Vulnerability Scanners. IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 24-26. DOI: 10.1109/IDAACS.2015.7340766

[13]. Helenius, M., &Vallius, M. (2022). REST API SECURITY: TESTING AND ANALYSIS. Tampere University

Lampiran

Video Dokumentasi :
https://drive.google.com/drive/folders/14BWcpiy_MJFiKPvOXomGHzf5H8yasxdL?usp=sharing

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **DHANA AGUSTYA PUTRA SASONGKO**

NIM : **201910370311357**

Judul TA : **ANALISIS METODE VULNERABILITY SCANNING DAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	28 %
2.	Bab 2 – Daftar Pustaka	25 %	8 %
3.	Bab 3 – Analisis dan Perancangan	25 %	13 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	0 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	11 %
6.	Makalah Tugas Akhir	20%	20 %

**) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)*

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

(.....)