ANALISIS IMPLEMENTASI KERENTANAN WEBSITE LABORATORIUM JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER MENGGUNAKAN OPENVAS DAN ACUNETIX VULNERABILITY SCANNER

SKRIPSI

Muhammad Irfan **2007422022**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2024

ANALISIS IMPLEMENTASI KERENTANAN WEBSITE LABORATORIUM JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER MENGGUNAKAN OPENVAS DAN ACUNETIX VULNERABILITY SCANNER

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik

Muhammad Irfan **2007422022**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2024

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Irfan
NIM	: 2007422022
Jurusan/ProgramStudi	: T.Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul skripsi	: Analisis Implementasi Kerentanan Website Laboratorium Jurusan Teknik Informatika dan Komputer Menggunakan Openvas Dan Acunetix Vulnerbility Scanner

Menyatakan dengan sebenarnya bahwa skripsiini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 28 Juli 2024

Yang membuat pernyataan

(Muhammad Irfan)

NIM 2007422022

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Muhammad Irfan

NIM 2007422022

Program Studi : Teknik Multimedia Jaringan

Judul Skripsi :PENERAPAN ANALISIS IMPLEMENTASI KERENTANAN WEBSITE LABORATORIUM JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER MENGGUNAKAN *OPENVAS* DAN *ACUNETIX VULNERBILITY SCANNER*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Kamis

Tanggal 15, Bulan Agustus, Tahun 2024. dan dinyatakan **LULUS.**

Disahkan oleh		Tanda Tangan
Pembimbing I	:Ariawan Andi Suhanndana, S.Kom, M.T.I	(.....)
Penguji I	: Dr. Prihatin Oktivasari, S.Si., M.Si.	(.....)
Penguji II	: Iik Muhammad Malik, S.Kom. M.T	(.....)
Penguji III	: Asep Kurniawan, S.Pd., M.Kom.	(.....)

Mengetahui :

Jurusan Teknik Informatika dan Komputer Ketua

Dr., Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat dan sebagi salah satu syarat untuk mencapai gelar Sarjana Terapan di Politeknik Negeri Jakarta. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan laporan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Kepada kedua orang tua dan keluarga penulis yang selalu memberikan semangat, dukungan, doa, serta dukungan moral maupun materi yang tak terhingga sampai penulis bisa berada dititik ini.
2. Kepada Bapak Ariawan Andi Suhandana,S.Kom.,M.T.I selaku pembimbing penulis yang telah banyak membantu, mendukung dan memberi masukan serta saran kepada penulis selama pengerjaan skripsi ini hingga selesai.
3. .Kepada Bapak Iik Muhamad Malik Matin, S.Kom., M.T. selaku kepala Lab Cyber Security dan yang telah banyak membantu saya dalam menjalankan penelitian saya selama di ruang server.
4. Seluruh jajaran Dosen dan Staf Teknik Informatika dan Komputer Politeknik Negeri Jakarta.

Akhir kata, penulis berharap Allah SWT membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 26 Juli 2024

Muhammad Irfan

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama : Muhammad Irfan

NIM : 2007422022

Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul: **ANALISIS IMPLEMENTASI KERENTANAN WEBSITE LABORATORIUM JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER MENGGUNAKAN *OPENVAS* DAN *ACUNETIX VULNERBILITY SCANNER***.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih mediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 28 Agustus 2024

Muhammad Irfan

NIM 2007422017

Analisis Implementasi Kerentanan Website Laboratorium Jurusan Teknik Informatika dan Komputer Menggunakan Openvas dan Acunetix

ABSTRAK

Scanning Salah satu media untuk mengamankan jaringan komputer adalah menerapkan *Web Application Firewall* (WAF). Penggunaan website sudah lumrah dilakukan. Dengan jumlah penduduk Indonesia sebanyak 270 juta jiwa lebih tak heran penggunaan website dapat berjalan optimal dan banyak sekali pemanfaatannya. Namun, sayangnya banyaknya pengguna website di Indonesia berbanding lurus dengan ancaman sebuah perangkat terkena serangan DdoS. Selama Pandemi Covid-19 telah diberitakan Indonesia telah mengalami peningkatan serangan DDoS. Dengan memanfaatkan *OpenVas* dan Acunetix Vulnability Scanner sebagai *web application firewall* (WAF) yang kuat dapat memberikan perlindungan dari berbagai serangan terhadap aplikasi web dan memungkinkan pemantauan lalu lintas HTTP. Penelitian ini bertujuan untuk melakukan pengujian dan analisa sejauh mana keamanan website Laboratorium Jurusan TIK dan memberikan saran pemecahan masalah dari hasil analisa. *OpenVAS* membutuhkan waktu 12 menit untuk menyelesaikan pemindaian dan mendeteksi 7 kerentanan dengan tingkat keparahan medium, tanpa mendeteksi kerentanan high, low, atau informational. Di sisi lain, Acunetix menyelesaikan pemindaian dalam waktu yang lebih singkat, hanya 3 menit, dan mendeteksi 4 kerentanan medium, serta mengidentifikasi 3 kerentanan low dan 5 kerentanan informational,

Kata kunci: Network Forensic Investigation Framework, Web Applicatiom Firewall(WAF), Network Attack, Network Scanning, Acunetix Web Vulnerbility, OpenVas, Web Server

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Pendahuluan

Analisis Keamanan sistem pada industri 4.0 atau Revolusi Industri keempat merupakan istilah yang umum digunakan untuk tingkatan perkembangan industri teknologi di dunia. Pada tingkatan keempat ini, dunia memang fokus kepada teknologi-teknologi yang bersifat digital, oleh karena itu teknologi informasi sangat-sangat menjadi tumpuan untuk industri yang bertujuan untuk mempermudah dan mempercepat proses-proses untuk membuat produk. Pandemi Covid-19 secara tidak lansung mempercepat Revolusi Industri 4.0, dimana banyak kegitan dilakukan tidak dengan bertatap muka secara lansung, melainkan melalui pertemuan online melalui gadget masing-masing. Begitu juga dengan pencarian informasi, semua dilakukan dengan cepat melalui internet. Dengan faktor tersebut, banyak industri dan instansi berpacu untuk melakukan pembaharuan terhadap layanan informasi mereka yang agar pengiriman data dan informasi meningkat. Disamping keuntungan tersebut, tingkat resiko dan ancaman penyalahgunaan teknologi informasi juga menjadi semakin meningkat seiring kemajuan teknologi, penggunaan layanan *cloud* untuk menyimpan data juga telah menjadi hal umum (Indu, Anand, and Bhaskar 2018). Dengan jumlah data yang besar yang disimpan di *server* dan berbagai ancaman serangan cyber yang mungkin terjadi, penting untuk mempertimbangkan kerentanan yang ada. Kondisi ini dapat mengakibatkan pencurian data pribadi yang pada akhirnya menyebabkan kerugian finansial, kerusakan reputasi, dan pelanggaran privasi yang signifikan bagi individu (Nurul, Anggrainy, and Aprelyani 2022).

Internet merupakan kebutuhan yang sangat penting pada era digital seperti sekarang. Revolusi industri 4.0 mengharuskan setiap orang terhubung ke jaringan internet setiap saat untuk berkomunikasi. Institusi atau perusahaan menjadikan internet sebagai bagian dari infrastruktur untuk meningkatkan produktivitas karyawan dan perusahaan. Tingginya kebutuhan internet terkadang dimanfaatkan oleh pihak-pihak tertentu untuk serangan jaringan komputer. Serangan jaringan komputer

meningkat secara signifikan pada era digital seperti ini. Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat ada 88.414.296 serangan siber di Indonesia yang terjadi sejak 1 Januari hingga 12 April 2020. Pada Januari terpantau ada 25.224.811 serangan dan kemudian pada Februari terekam 29.188.645 serangan. Lalu, pada Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 tercatat ada 7.576.851 serangan (Iskandar, 2020). Para hacker tidak hanya menargetkan serangan untuk melumpuhkan jaringan komputer suatu perusahaan. Mereka juga berusaha untuk mencuri berbagai data dari server.

Pada saat ini perkembangan teknologi sangatlah pesat apalagi dengan didukungnya fasilitas internet yang sangat mumpuni. Perubahan yang sangat cepat, kadang kala meluputkan developer dalam melakukan pengujian terhadap aplikasi yang dibangun. Pengujian merupakan proses yang sangat penting didalam pengembangan perangkat lunak yang berkualitas tinggi, karena dari beberapa kesalahan yang dianggap tidak penting beresiko sangat berbahaya hal ini menjadi celah (vulnerability) bagi attacker untuk memanfaatkan informasi yang di curi Pengujian dan Analisis Keamanan Website Menggunakan *Acunetix Vulnerability Scanner* melalui serangan kepada aplikasi. Kebutuhan akan *vulnerability* assessment selama ini biasanya dipandang sebelah mata, karen hanya dianggap sebagai kegiatan formalitas dan sedikit orang yang melakukan kegiatan ini . Salah satu sistem yang umumnya menjadi sasaran hacker dan cracker adalah aplikasi berbasis website. Hal tersebut dikarenakan pemanfaatan aplikasi mengalami pertumbuhan yang sangat pesat saat ini. Serangan yang dilakukan dapat berupa *Cross Site Scripting* (XSS), *Cross Site Request Forgeri* (CSRF), *SQL injection* dan lain sebagainya . Serangan SQL injection merupakan sebuah aksi hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah SQL yang ada di memori aplikasi client dan mengekploitasi aplikasi menggunakanh basis dataPada laporan tersebut tercatat 1404 insiden penyerangan pada web yang menyebabkan 1315 di antaranya dikonfirmasi mengalami kebocoran data. Salah satu teknik yang digunakan yang disebutkan pada laporan tersebut adalah *Brute Force* (T1110). Percobaan *brute force* juga terjadi di Indonesia pada tahun 2021 lalu (Hafis, n.d.).

Selain *brute force*, serangan *Denial of Service* (DoS) juga disebutkan pada laporan ini. Terdapat kasus DoS yang berhasil dikonfirmasi sebanyak 6248 insiden dan serangan jenis ini selalu menjadi yang tertinggi setiap tahunnya pada laporan Verizon.

Beberapa faktor dari dari celah keamanan bisa terjadi karena kurangnya sistem pengamanan website dan kekeliruan *programmer* ketika melakukan coding . Salah satu cara untuk melakukan evaluasi keamanan website menggunakan perangkat lunak yang khusus dirancang untuk mengetahui kerentanan yang ada pada suatu sistem yaitu *Acunetix Vulnerability Scanner Pentest-tools.com,* vulnerability scanner, *OWASP ZAP* . Pengujian ini juga tidak terbatas pada aplikasi yang di kustom sendiri, aplikai *CMS* (Content Management System) seperti OJS juga menjadi target uji . Pengujian vulnerability dilakukan untuk pengukuran atau assessment yang mutlak dilakukan untuk mendapatkan peningkatan kualitas dan salah satu cara pengukuran terhadap keamanan sistem. Hasil dari assesment menjadi bahan pertimbangan bagi developer untuk mengambil tindakan pencegahan dan mengetahui cara kerja dari attackers .

Penelitian yang dilakukan ini berfokus dalam mengimplementasikan konsep Web Application Firewall (WAF) yang dikembangkan oleh *Trustwave's SpiderLabs. ModSecurity* memiliki bahasa pemrograman berbasis event yang kuat yang memberikan perlindungan dari berbagai serangan terhadap aplikasi web dan memungkinkan pemantauan lalu lintas HTTP. Berdasarkan hal tersebut, sangat dianjurkan untuk menerapkan analisis keamanan terhadap aplikasi yang bertujuan untuk meminimalisir terjadinya gangguan pada kinerja aplikasi berbasis web sehingga harus adanya evaluasi terhadap keamanan sistem aplikasi. Dengan adanya Analisis Keamanan Aplikasi Web Laboratorium Jurusan TIK dengan tujuan menemukan keretanan dan menguji pada aplikasi sehingga pemilik aplikasi web tersebut dapat memperbaiki dan meningkatkan keamanan dari sebuah aplikasi.

1.2 Rumusan Masalah

Beberapa rumusan masalah yang dapat menjadi dasar dalam penelitian ini diantaranya adalah:

a. Bagaimana *Scanning Vulnerbility* sistem keamanan Website Laboratorium Jurusan TIK dengan menggunakan *OpenVas* dan *Acunetix* dilakukan?
b. Bagaimana Analisis sistem keamanan Website Laboratorium Jurusan TIK dengan Menggunakan *OpenVas* dan *Acunnetix* dalam Melakukan *Scanning Vulnerability* ?
c. Apa saja Perbedaan yang didapatkan dalam mengimplementasikan *OpenVas* dan *Acunetix Vulnerability Scanner* dalam melakukan *Scanning Vulnerability?*

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang disusun agar ruang lingkup penelitian lebih terfokus, yang diantara lain adalah:

a. Penelitian ini mencakup implementasi Scanning keamanan Website Laboratorium Jurusan TIK yang menggunakan perangkat lunak OpenVas dan , dengan *Acunetix Vulnerability* fokus pada kerentanan terhadap website tersebut.
b. Penelitian ini membatasi ruang lingkupnya hanya pada Scanning keamanan Website Laboratorium Jurusan TIK dengan menggunakan OpenVas dan *Acunnetix Vulnerabillity*, dengan fokus pada deteksi kerentanan ke pada website.
c. Batasan masalah penelitian ini mencakup analisis efektivitas dan kinerja OpenVas dan *Acunetix Vulnerability* dalam mengatasi serangan yang ditujukan pada website Laboratorium Jurusan TIK.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah:

a. Menganalisis implementasi keamanan *Website* Laboratorium TIK yang melibatkan penggunaan Tools seperti *OpenVas* dan *Acunetix Vulnertability.*

b. Mengidentifikasi kerentanan keamanan yang ada pada aplikasi web, server, dan infrastruktur jaringan.

c. Menganalisis efisiensi dan akurasi deteksi yang disediakan oleh *OpenVas* dan *Acunetix Vulnerbility* terhadap serangan *Website.*

1.4.2 Manfaat

Manfaat yang diharapkan dalam keberhasilan penelitian ini adalah sebagai berikut:

a. Mengembangkan metodologi untuk menganalisis dan mengevaluasi sistem keamanan Website.

b. Memberikan wawasan mendalam tentang sistem keamanan Web Server padadalam mengetahui serangan Website.

c. Menyediakan rekomendasi dan saran praktis untuk meningkatkan efektivitas dan efisiensi sistem keamanan Website dengan memanfaatkan alat-alat OpenVas dan Acunetix.

d. Hasil penelitian ini diharapkan dapat memberikan informasi dan berfokus pada perbaikan kerentanan pada website.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan laporan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab I berisikan penjelasan mengenai latar belakang Analisis Implementasi Keamanan Website Laboratorium Jurusan Teknik Informatika dan Komputer Menggunakan OpenVas dan *Acunetix Vulnerability Scanner* Bagian ini juga memuat Batasan masalah penelitian, serta manfaat dari penelitian yang dilakukan.

BAB II TINJAUAN PUSTAKA

Bab II berisikan penjelasan mengenai landasan teori atau kajian ilmu yang berhubungan dengan berbagai pokok pikiran topik penyusunan skripsi ini yang relevan dari sumber yang valid.

BAB III METODE PENELITIAN

Bab III berisikan penjelasan mengenai rancangan penelitian yang akan dilakukan, Bagaimana melakukan-nya, mulai dari pengumpulan data, jadwal mulai penelitain, dan lain sebagainya.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan pembahasan mengenai proses Implementasi Scanning dan hasil, terhadap web application firewall .Pada bab ini juga berisikan hasil dari Scanning Vulnerbility serta dokumentasi Analisis data yang didapatkan.

BAB V PENUTUP

Bab ini berisikan kesimpulan berdasarkan uraian yang telah dipaparkan pada bab sebelumnya. Selain itu pada bab ini juga berisikan saran untuk pengembangan dan keamanan lebih lanjut terhadap Website yang telah diteliti.

BAB V
PENUTUP

5.1 Kesimpulan

Setelah dilakukannya penelitian implementasi Scanning Vulnerbility terhadap website Laboratorium JTK di politeknik negeri Jakarta dapat diperoleh kesimpulan sebagai berikut.

1. Hasil pemindaian kerentanan sistem keamanan website Laboratorium Jurusan TIK, dapat disimpulkan bahwa beberapa kerentanan tetap konsisten muncul pada ketiga pemindaian yang dilakukan pada tanggal 14 Juni, 20 Juli, dan 24 Juli 2024. Kerentanan seperti *"DCE/RPC and MSRPC Services Enumeration Reporting", "HTTP Debugging Methods (TRACE/TRACK) Enabled", "SSL/TLS: Certificate Expired", "SSL/TLS: Untrusted Certificate Authorities", "SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength", dan "SSL/TLS: Certificate Signed Using A Weak Signature Algorithm"* terus terdeteksi dengan tingkat keparahan medium. Pada pemindaian pertama, beberapa kerentanan tidak terdeteksi, tetapi muncul pada pemindaian kedua dan ketiga, seperti *"HTTP Debugging Methods (TRACE/TRACK) Enabled*" pada port 80/tcp. Nilai kerentanan juga konsisten, yang mengindikasikan bahwa tidak ada perbaikan yang dilakukan antara pemindaian tersebut.
2. Dari hasil analisis data pemindaian kerentanan sistem keamanan website Laboratorium Jurusan TIK yang ditampilkan pada tabel di atas, terlihat bahwa beberapa kerentanan tetap konsisten muncul dalam tiga kali pemindaian yang dilakukan pada tanggal 27 Juni, 16 Juli, dan 21 Juli 2024. Kerentanan yang memiliki tingkat keparahan medium dan nilai CVSS tinggi mencakup "Directory Listings", *"SSL/TLS Not Implemented", "Test CGI script leaking environment variables", dan "(Possible) Internal IP Address Disclosure"*, dengan nilai CVSS mencapai 6.9. Hal ini menunjukkan bahwa kelemahan-kelemahan ini memerlukan perhatian khusus dan tindakan perbaikan segera

3. hasil pemindaian menggunakan *OpenVAS* dan *Acunetix*, terlihat perbedaan signifikan dalam durasi pemindaian dan hasil yang diperoleh. *OpenVAS* membutuhkan waktu 12 menit untuk menyelesaikan pemindaian dan mendeteksi 7 kerentanan dengan tingkat keparahan medium, tanpa mendeteksi kerentanan high, low, atau informational. Di sisi lain, Acunetix menyelesaikan pemindaian dalam waktu yang lebih singkat, hanya 3 menit, dan mendeteksi 4 kerentanan medium, serta mengidentifikasi 3 kerentanan low dan 5 kerentanan informational, meskipun OpenVAS memerlukan waktu lebih lama, hasilnya lebih fokus pada kerentanan medium tanpa mendeteksi kerentanan lainnya. Acunetix, dengan waktu pemindaian yang lebih cepat, memberikan hasil yang lebih beragam termasuk kerentanan low dan informational, yang dapat memberikan gambaran lebih lengkap mengenai kondisi keamanan sistem.

5.2 Saran

Adapun Berdasarkan hasil penelitian dan kesimpulan, maka didapati saran yang dapat menjadi acuan pada penelitian selanjutnya berdasarkan hasil pemindaian kerentanan sistem keamanan pada website Laboratorium Jurusan TIK, disarankan agar penelitian selanjutnya lebih fokus pada analisis mendalam terhadap penyebab utama munculnya kerentanan yang konsisten terdeteksi pada ketiga pemindaian yang dilakukan, terutama yang berkaitan dengan layanan DCE/RPC dan MSRPC, metode debugging HTTP, serta masalah SSL/TLS. Selain itu, penelitian lanjutan dapat meneliti perbedaan efektivitas dan efisiensi antara alat pemindaian seperti OpenVAS dan Acunetix, dengan tujuan untuk mengidentifikasi alat yang paling sesuai untuk konteks tertentu dan memahami mengapa terdapat perbedaan dalam durasi dan hasil pemindaian. Penting juga untuk mengevaluasi kebijakan mitigasi dan langkah-langkah perbaikan yang perlu diimplementasikan untuk mengatasi kerentanan yang terdeteksi secara berulang, serta menyarankan tindakan yang lebih proaktif dalam pemantauan dan peningkatan keamanan sistem agar kerentanan dengan tingkat keparahan medium atau CVSS tinggi dapat segera diatasi.

DAFTAR PUSTAKA

Widodo, T., & Aji, A. S. (2022). Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS). JISKA (Jurnal Informatika Sunan Kalijaga), 7(1), 46-55.

Zain, A. R., Matin, I. M. M., & Kautsar, K. (2023, August). Analisis Implementasi Modsecurity dan Reverse Proxy Untuk Pencegahan Serangan Keamanan DDoS pada Web Server. In Seminar Nasional Inovasi Vokasi (Vol. 2, pp. 118-127).

Muharromin, M. (2023). Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache. JUPITER (Jurnal Penelitian Ilmu dan Teknik Komputer), 15(1b), 393-402.

Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi. Jurnal Teknologi Dan Sistem Informasi Bisnis, 6(1), 162-167.

Fitroh, Q. A., & Sugiantoro, B. (n.d.). Peran Ethical Hacking dalam Peran EthicalHacking dalam Memerangi Cyberthreats.

Zeebaree, S. R., Jacksi, K., & Zebari, R. R. (2020). Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers. Indones. J. Electr. Eng. Comput. Sci, 19(1), 510-517.

Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.

Idhom, M., Alit, R., & Fauzi, A. (2021, May). Implementation of Web Server Security Against Denial of Service (DoS) Attacks. In IOP Conference Series: Materials Science and Engineering (Vol. 1125, No. 1, p. 012037). IOP Publish

Khaliq, A., & Novida Sari, S. (2022). PEMANFAATAN KERANGKA

KERJA INVESTIGASI FORENSIK JARINGAN UNTUK IDENTIFIKASI SERANGAN JARINGAN MENGGUNAKAN SISTEM DETEKSI INTRUSI (IDS). Jurnal Nasional Teknologi Komputer, 2(3), 150–158. https://doi.org/10.61306/jnastek.v2i3.52

(View of Pemanfaatan Network Forensic Investigation Framework Untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS).Pdf, n.d.)

Wibowo, F., Harjono, H., & Wicaksono, A. P. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. Jurnal Informatika, 6(2), 212-217.

Astriani, T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar NIST 800-115. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8(4), 2041-2050.

Al Fajar, F. (2020). Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability. Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika, 3(2), 110-120.

Prasetyo, S. E., & Hassanah, N. (2021). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf. Jurnal Ilmiah Informatika, 9(02), 82-86.

Kestina, L., Yuhandri, Y., & Nurcahyo, G. W. (2023). Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci). INNOVATIVE: Journal Of Social Science Research, 3(4), 9192-9203.

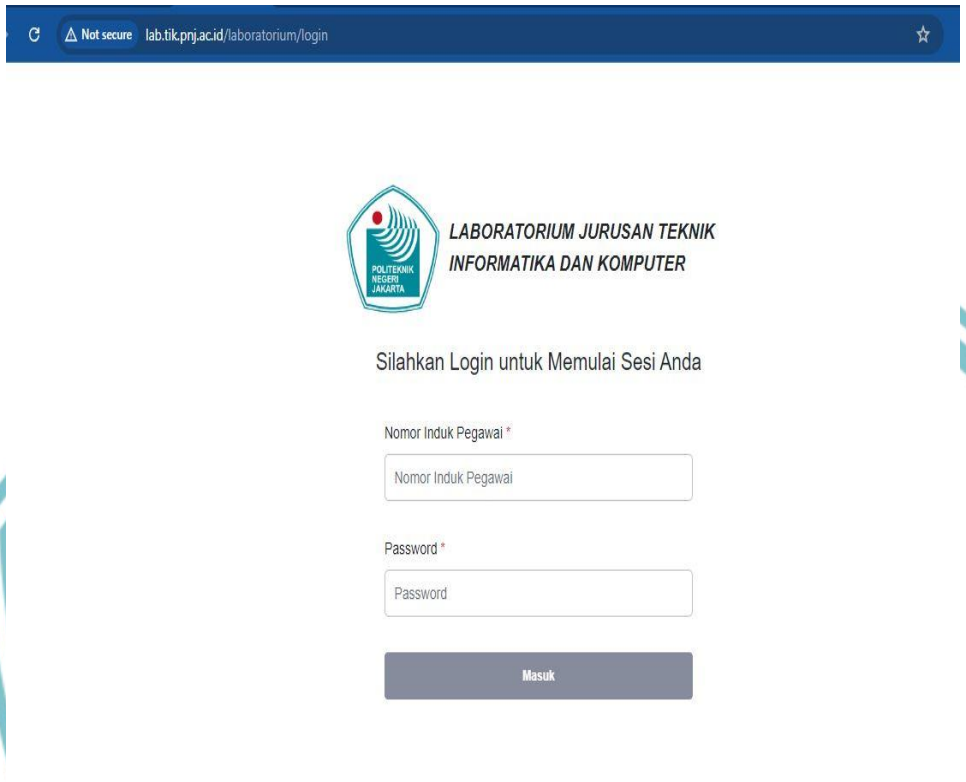
Armando, Y., & Rosalina, R. (2023). Penetration Testing Tangerang City Web Application With Implementing OWASP Top 10 Web Security Risks Framework. *JISA (Jurnal Informatika dan Sains)*, *6*(2), 105-109.

DAFTAR RIWAYAT HIDUP

Lahir di Jakarta, 24 April. Lulus dari SDN PUSPANEGARA 03 pada tahun 2014, SMPN 1 CITEUREUP pada tahun 2017, SMAN 4 CIBINONG pada tahun 2020 dan Diploma II program studi Network Administrator Professional di CCIT – FTUI pada tahun 2022. Saat ini sedang menempuh Pendidikan Diploma IV Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

LAMPIRAN

Lampiran 1 - Dasboard login Website

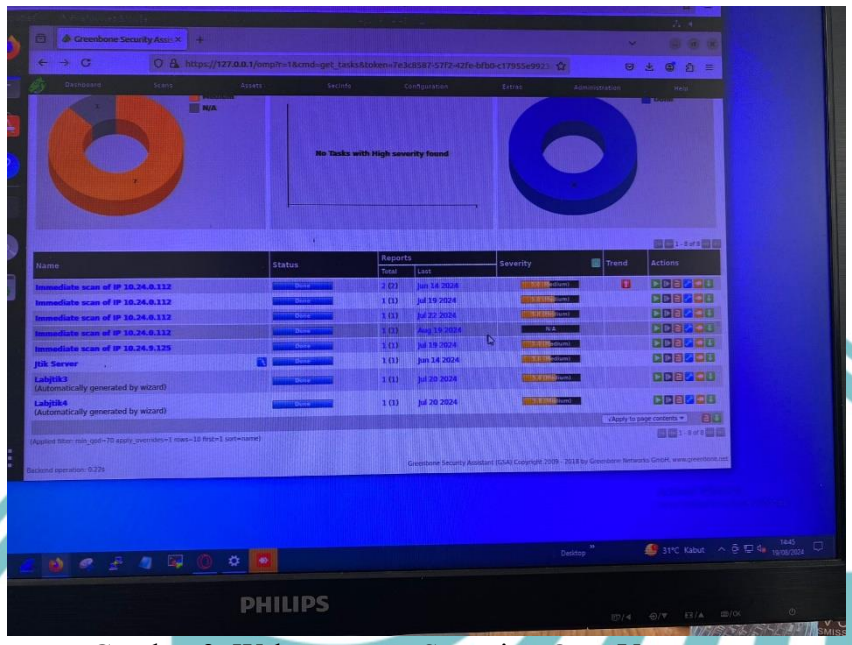


Gambar 1. Dasboard login Website

Lampiran 2 – Waktu Mengerjakan di Ruang Server

Gambar 1. Ruang Server

Lampiran 3 - (Scanning Openvas)



Gambar 3. Waktu proses Scanning OpenVas

Lampiran 4 - (Lanjutan)