PENERAPAN *PENETRATION TESTING* UNTUK MENGUJI KETAHANAN WEBSITE *SMART HEALTH* TERHADAP SERANGAN *BRUTE FORCE* DAN *DENIAL OF SERVICE (DOS)*

PROJEK

Sebagai Salah Satu Syarat untuk Menyelesaikan Studi di

Program Studi Teknik Komputer DIII

Oleh :

M SADDAM HAMIDIN

09030582226004

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

AGUSTUS 2025

HALAMAN PENGESAHAN

PROJEK

PENERAPAN *PENETRATION TESTING* UNTUK MENGUJI KETAHANAN WEBSITE *SMART HEALTH* TERHADAP SERANGAN *BRUTE FORCE* DAN *DENIAL OF SERVICE (DOS)*

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi D3 Teknik Komputer

Oleh:

M SADDAM HAMIDIN

09030582226004

Pembimbing 1	**: Huda Ubaya, M.T**
	NIP. 198106162012121003
Pembimbing 2	**: Adi Hermansyah, M.T.**
	NIP. 198904302024211001

Mengetahui

Koordinator Program Studi Teknik Komputer

Dr. Ir. Ahmad Heryanto, M.T.

198701222015041002

HALAMAN PERSETUJUAN

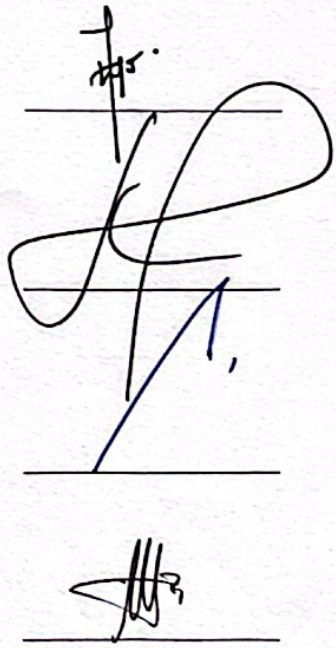
Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 28 Juli 2025

Tim Penguji :

1. **Ketua Sidang** : **Yoppy Sazaki, S.Si, M.T.**
2. **Pembimbing I** : **Huda Ubaya, M.T**
3. **Pembimbing II** : **Adi Hermansyah, M.T.**
4. **Penguji** : **Muhammad Ali Buchari, M.T.**



Mengetahui

Koordinator Program Studi Teknik Komputer

Dr. Ir. Ahmad Heryanto, M.T.

NIP 198701222015041002

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: M Saddam Hamidin
NIM	: 09030582226004
Program Studi	: Teknik Komputer
Jenjang	: DIII
Judul Projek	: Penerapan *Penetration Testing* untuk Menguji Ketahanan Website *Smart Health* Terhadap Serangan *Brute Force* dan *Denial of Service (DoS)*

Hasil Pengecekan Software iThenticate/Turnitin : 14%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil plagiat. Apabila ditemukan unsur plagiarisme dalam laporan projek ini, maka saya bersedia untuk menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Dengan pernyataan yang saya buat ini dengan sebenarnya dan tidak ada paksaan terhadap siapa pun.

Palembang, 05 Agustus 2025

M Saddam Hamidin
NIM 09040582226004

MOTTO DAN PERSEMBAHAN

MOTTO :

“Keberhasilan bukan milik dia yang pintar, melainkan milik mereka yang mau berusaha lebih keras dan tidak mudah menyerah”

Kupersembahkan kepada :

- *Kedua Orang Tua ku*
- *Dosen Pembimbing*
- *Teman Seperjuangan*
- *Almamaterku*

KATA PENGANTAR

Puji syukur penulis ucapkan Kepada Allah SWT, karena atas Rahmat-nya, Penulis dapat menyelesaikan laporan Proyek yang berjudul **"Penerapan *Penetration Testing* untuk Menguji Ketahanan Website *Smart Health* Terhadap Serangan *Brute Force* dan *Denial of Service (DoS)*"**. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, sangat sulit bagi penulis untuk menyelesaikan laporan Proyek ini. Pada kesempatan ini penulis ingin mengucapkan rasa syukur kepada Allah SWT. Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Projek ini. Oleh Karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terima kasih kepada yang terhormat.

1. Allah SWT atas berkat dan karunia-Nya, laporan proyek ini dapat terselesaikan.
2. Kepada kedua orang tua saya yang sudah mendidik dan membesarkan dengan penuh rasa kasih dan sayang serta memberikan dukungan, semangat dan jasa yang tidak terhitung sehingga saya sehat serta semangat dalam menjalankan setiap aktivitas.
3. Bapak Dr. Ir. Ahmad Heryanto., M.T. Selaku Koordinator Program Studi Teknik Komputer Universitas Sriwijaya.
4. Bapak Prof. Dr. Erwin, S. Si., M. Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Dosen Pembimbing 1, atas kesediaan memberikan masukan dan arahan dalam penyelesaian laporan projek ini.
6. Bapak Adi Hermansyah, M.T. selaku Dosen Pembimbing 2, atas kesediaan memberikan masukan dan arahan dalam penyelesaian laporan proyek ini.
7. Seluruh Dosen Program Studi Teknik Komputer Universitas Sriwijaya
8. Kakak-Kakak yang membantu penulis dalam menyelesaikan proyek ini yaitu kakak Andrian, Arman, dan Bagas
9. Dan juga teman terdekat seperjuangan saya yang telah banyak sekali

membantu dan memberikan dukungan serta doa dalam menyelesaikan laporan projek ini yaitu Rinda Ambarwati Putri.

10. Rekan- rekan penulis yang selalu memberikan suasana yang ramah dan juga memberikan dukungan serta semangat.

Saya berharap Allah SWT selalu memberikan semua kemudahan serta kelancaran dalam penyelesaian proyek ini, Laporan ini saya tulis dengan sebaik mungkin. Penulis menyadari bahwa laporan ini memiliki banyak sekali kekurangan, Oleh karena itu, kritik maupun saran selalu penulis harapkan dalam penyempurnaan proyek ini. Penulis berharap agar Laporan Tugas Akhir ini dapat bermanfaat untuk semua pihak-pihak yang membutuhkan dan semoga laporan ini membawa manfaat.

Palembang, 05 Agustus 2025

Penulis

M Saddam Hamidin

NIM. 09030582226004

PENERAPAN *PENETRATION TESTING* UNTUK MENGUJI KETAHANAN WEBSITE *SMART HEALTH* TERHADAP SERANGAN *BRUTE FORCE* DAN *DENIAL OF SERVICE (DOS)*

Oleh :

M Saddam Hamidin (09030582226004)

Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: sadamhamidin@gmail.com

Abstrak

Pemanfaatan teknologi digital dalam bidang kesehatan semakin berkembang, salah satunya melalui platform website *Smart Health* yang menyediakan layanan informasi dan konsultasi medis secara daring. Dengan meningkatnya penggunaan sistem berbasis web, risiko terhadap serangan siber juga semakin tinggi. Dua serangan yang umum terjadi adalah *Brute Force*, yang bertujuan untuk membobol kredensial pengguna dengan mencoba berbagai kombinasi kata sandi, serta *Denial of Service* (*DoS*), yang bertujuan melumpuhkan sistem dengan membanjiri server menggunakan permintaan secara berlebihan. Penelitian ini dilakukan menguji ketahanan website *Smart Health* terhadap kedua jenis serangan tersebut Pengujian dilakukan secara langsung terhadap sistem dengan cara melakukan simulasi serangan *Brute Force* pada halaman login dan serangan *DoS* terhadap server layanan. Dalam prosesnya, pengamatan dilakukan terhadap perilaku sistem saat menerima serangan, termasuk dampak pada performa, respon server, dan potensi terjadinya gangguan layanan. Pengujian dilakukan dalam lingkungan yang aman tidak mengganggu sistem produksi. Hasil dari pengujian menunjukkan bahwa sistem belum sepenuhnya aman terhadap serangan *Brute Force* karena tidak adanya fitur pengaman tambahan seperti pembatasan percobaan *login*, sistem juga menunjukkan penurunan performa yang signifikan saat menerima serangan *DoS* secara terus menerus, yang dapat mengakibatkan tidak tersedianya layanan untuk pengguna. Temuan ini mengindikasikan bahwa perlu adanya peningkatan mekanisme keamanan untuk melindungi layanan web dari ancaman serangan siber.

Kata Kunci : *Smart Health*, *Brute Force*, *DoS*, Keamanan Website, Pengujian Keamanan

IMPLEMENTATION OF PENETRATION TESTING TO TEST THE RESISTANCE OF SMART HEALTH WEBSITES AGAINST BRUTE FORCE ATTACKS AND DENIAL OF SERVICE (DOS)

By :

M Saddam Hamidin (09030582226004)

Diploma Program in Computer Engineering, Faculty of Computer Science

Email: sadamhamidin@gmail.com

Abstract

The use of digital technology in the healthcare sector is rapidly expanding, including through platforms such as the Smart Health website, which provides online medical information and consultation services. As web-based systems become more widespread, the risk of cyberattack also increases. Two common types of attack are Brute Force, which attempts to crack user credentials by trying numerous password combinations, and Denial of Service (DoS), which aims to disrupt systems by overwhelming servers with excessive request. This study aims to evaluate the resilience of the Smart Health website against these two types of attacks. The testing was conducted directly on the system by simulating Brute Force attacks on the login page and DoS attacks on the server. Observations focused on how the system behaves under attack, including impacts on performance, server response, and potential service disruption. The testing was carried out in a safe environment without affecting the live system. The results indicate that the system is still vulnerable to Brute Force attacks due to the absence of additional security features such as login attempt limits. Furthermore, the system experienced significant performance degradation during continuous DoS attacks, which could lead to service unavailability. These findings highlight the need to enhance security mechanisms to protect web services from cyber threats.

Keywords : Smart Health, Brute Force, DoS, Website Security, Security Testing

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, penggunaan sistem berbasis web sangat penting dalam mendukung layanan kesehatan digital, seperti platform *Smart Health* yang menyediakan layanan administrasi dan interaksi antara pasien dengan tenaga medis. Namun, kemajuan teknologi ini juga membawa risiko keamanan yang signifikan, termasuk serangan siber yang dapa mengancam keberlangsungan dan kerahasiaan data. Platform ini bertujuan untuk memudahkan akses ke layanan perawatan kesehatan dengan menawarkan berbagai fitur termasuk manajemen data pasien, penjadwalan, dan penyimpanan digital catatan medis. Namun, kemajuan ini juga membawa tantangan baru, terutama dalam hal keamanan data pengguna. Situs *web Smart Health* menyimpan informasi sensitif, termasuk data pribadi pasien dan informasi medis. Oleh karena itu, memastikan keamanan sistem menjadi prioritas utama untuk mencegah akses tidak sah dan potensi kebocoran data yang dapat membahayakan pengguna. Salah satu pengujian keamanan sistem Kecanggihan teknologi ini tidak serta membawa dampak positif saja. Melainkan juga membawa dampak negatif berupa tindakan kejahatan siber yang merugikan pengguna jaringan. Tindakan kejahatan siber tersebut biasanya dilakukan oleh individu atau kelompok yang sering disebut peretas[1].

Namun demikian, keberadaan sistem informasi yang terhubung ke jaringan tidak terlepas dari berbagai ancaman keamanan siber, Website yang memiliki sistem *login* dan layanan berbasis jaringan sangat rentan terhadap berbagai jenis serangan, terutama serangan *Brute Force* dan serangan *Denial of Service (DoS).* Kedua jenis serangan ini tergolong umum dalam ancaman siber saat ini dan berpotensi besar menimbulkan dampak yang merugikan bagi institusi, khususnya yang bergerak di bidang kesehatan. Oleh karena itu dibutuhkan perlindungan keamanan terhadap data-data bagi pengguna

platform tersebut, atau bahkan gangguan total terhadap layanan. Beberapa jenis serangan yang umum terjadi pada sistem berbasis web, Kedua serangan ini berbeda dari segi tujuan dan mekanisme, namun sama-sama dapat menimbulkan dampak serius terhadap kelangsungan layanan[2].

Serangan *Brute Force* merupakan salah satu bentuk serangan siber yang paling dasar namun tetap menjadi salah satu yang paling efektif dalam menargetkan sistem autentikasi pada aplikasi web. Serangan ini dilakukan dengan cara mencoba semua kemungkinan kombinasi *username* dan *password* secara berulang-ulang hingga penyerang berhasil menemukan kredensial yang benar untuk masuk ke dalam sistem. Teknik brute force bekerja berdasarkan prinsip *trial-and-error*, di mana sistem *login* diserang secara otomatis dengan memanfaatkan *tools* atau skrip khusus yang dapat mengirimkan ratusan bahkan ribuan permintaan *login* dalam waktu yang singkat. Dalam konteks aplikasi *Smart Health*, yang merupakan platform digital berbasis web untuk pelayanan kesehatan, keberhasilan serangan *Brute Force* dapat menyebabkan kebocoran data pribadi pasien, manipulasi informasi medis, hingga pengambilan alih akun yang dapat berdampak sangat serius terhadap privasi dan keamanan data kesehatan[3].

Pada sisi lain, *Denial of Service* (*DoS*) merupakan salah satu jenis serangan siber yang bertujuan untuk membuat suatu layanan sistem, atau jaringan tidak dapat diakses oleh pengguna yang sah. Serangan ini dilakukan dengan cara membanjiri sistem target menggunakan lalu lintas data atau permintaan dalam jumlah besar secara terus-menerus, sehingga sumber sistem seperti CPU, memori, atau *bandwidth* menjadi kelebihan beban. Akibatnya, sistem menjadi lambat merespons atau bahkan tidak dapat di akses sama sekali. Meskipun serangan ini tidak secara langsung mencuri atau merusak data, dampaknya sangat signifikan karena mengganggu ketersediaan layanan, yang merupakan salah satu aspek penting dalam keamanan informasi. Kedua jenis serangan tersebut menunjukkan bahwa aspek keamanan informasi (*Information Security*) harus menjadi prioritas utama dalam pengembangan dan pengelolaan layanan berbasis web. Keamanan informasi tidak hanya mencakup perlindungan terhadap data dari pencurian

atau modifikasi, tetapi juga menjamin bahwa Sistem tetap tersedia (*availability*), akurat (*integrity*), dan hanya dapat diakses oleh pihak yang berwenang (*confidentiality*). Dalam praktiknya, banyak organisasi belum sepenuhnya sepenuhnya menyadari kerentanan yang ada di dalam sistem mereka, atau tidak mengetahui seberapa kuat sistem mereka bertahan terhadap serangan siber nyata[4].

Melihat maraknya ancaman tersebut, diperlukan suatu metode sistematis untuk menguji ketahanan dan kerentanan dari sistem informasi, salah satunya melalui penerapan *Penetration Testing. Penetration Testing* adalah proses pengujian keamanan suatu sistem dengan melakukan simulasi serangan nyata guna menemukan kelemahan sistem sebelum disalahgunakan oleh pihak yang tidak bertanggung jawab. Metode ini memungkinkan pengembang sistem dan administrator jaringan untuk memahami titik-titik lemah dalam sistem serta mengambil tindakan pencegahan atau perbaikan secara proaktif[5].

Berdasarkan latar belakang tersebut, maka penelitian ini dilakukan untuk menguji ketahanan website *Smart Health* terhadap dua jenis serangan siber yaitu *Brute Force* dan *DoS*. Dengan cara melakukan simulasi langsung dalam lingkungan pengujian yang aman. Penelitian ini bertujuan untuk memberikan gambaran nyata mengenai seberapa besar risiko yang dihadapi oleh sistem *Smart Health*, serta menyediakan data awal yang dapat di gunakan sebagai dasar dalam pengambilan keputusan strategis untuk memperkuat sistem keamanan ke depannya. Dengan adanya pengujian ini, diharapkan pihak pengelola website *Smart Health* lebih memahami kelemahan sistem yang mereka miliki dan segera mengambil langkah-langkah yang diperlukan untuk meningkatkan perlindungan sistem, sehingga dapat menjamin keamanan data pasien.

Berdasarkan dari permasalahan diatas tersebut, penulis ingin mengangkat permasalahan ini dan menjadikan sebagai fokus penelitian dalam proyek penyusunan. Tugas Akhir dengan judul **"PENERAPAN *PENETRATION TESTING* UNTUK MENGUJI KETAHANAN WEBSITE *SMART HEALTH* TERHADAP SERANGAN *BRUTE FORCE* DAN *DENIAL OF SERVICE* (*DOS*)"**.

1.2 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, adapun rumusan masalah dalam penyusunan proyek ini sebagai berikut:

1. Bagaimana cara mengimplementasikan serangan *Brute Force* dan *Denial of Service (DoS)* terhadap website *Smart Health* yang menjadi targetkan pengujian?
2. Sejauh mana efektivitas penerapan *Penetration Testing* pada website *Smart Health*?
3. Apa kelemahan sistem website *Smart Health* berdasarkan hasil pengujian yang dilakukan?

1.3 Tujuan

Berdasarkan penjelasan pada latar belakang dan rumusan masalah yang sudah diuraikan. Adapun Tujuan dari penelitian dalam penyusunan proyek sebagai berikut:

1. Untuk mengetahui dan menjelaskan langkah-langkah implementasi serangan *Brute Force* dan *Denial of Service (DoS)* terhadap website *Smart Health* sebagai target pengujian.
2. Untuk mengevaluasi efektivitas penerapan metode *Penetration Testing* pada website *Smart Health.*
3. Untuk mengidentifikasi celah keamanan dan menganalisis kelemahan sistem keamanan pada website *Smart Health* berdasarkan hasil pengujian yang dilakukan.

1.4 Manfaat

Berdasarkan pada tujuan dalam penyusunan proyek. Maka manfaat dari pengujian ini sebagai berikut

1. Memberikan informasi yang berguna mengenai celah keamanan yang terdapat pada website *Smart Health*, sehingga dapat dijadikan dasar dalam perbaikan dan peningkatan sistem keamanan.
2. Memberikan gambaran nyata tentang potensi risiko keamanan siber yang dapat terjadi pada sistem website, sehingga dapat mendorong implementasi kebijakan keamanan yang lebih baik.
3. Menjadi referensi atau bahan pembelajaran bagi mahasiswa lainnya dalam

memahami penerapan *Penetration Testing* serta teknik serangan *Brute Force* dan *Denial of Service* dalam pengujian keamanan web.

1.5 Batasan Masalah

Pada penyusunan proyek ini memiliki batasan masalah, sebagai berikut:

1. Penelitian ini hanya memfokuskan pengujian terhadap dua jenis serangan siber yaitu *Brute Force Attack* dan *Denial of Service* (*DoS*) *Attack*.
2. Pengujian ini hanya dilakukan pada website *Smart Health*, khususnya pada fitur *login* untuk serangan *Brute Force*, dan kestabilan server untuk serangan *DoS*
3. Penelitian ini hanya berfokus pada identifikasi kerentanan.

1.6 Metode Penelitian

Dalam perancangan yang dilakukan pada proyek ini , Adapun beberapa metode penelitian yang akan digunakan, antara lain :

a. Metode Literatur

Metode Literatur ini dilakukan dengan mencari berbagai informasi dari berbagai sumber, seperti buku, artikel, jurnal, serta dokumen yang sesuai dengan judul "Penerapan *Penetration Testing* untuk Menguji Ketahanan Website *Smart Health* Terhadap Serangan *Brute Force* dan *Denial of Service (DoS)*" sebagai acuan dalam pemahaman pada konsep proyek yang akan dilakukan.

b. Metode Observasi

Pada proyek ini, metode observasi digunakan untuk mengamati dan menganalisis sistem website *Smart Health* yang akan diuji. Observasi dilakukan secara langsung terhadap situs tersebut dengan memperhatikan aspek-aspek yang dapat mempengaruhi kerentanannya, seperti mekanisme *login*, pengaturan server, dan *respons* sistem terhadap trafik tinggi serta digunakan untuk mengidentifikasi potensi celah keamanan yang mungkin tidak terlihat dalam dokumentasi. Hasil observasi ini menjadi dasar untuk menyusun rencana pengujian lebih lanjut, serta menentukan area yang perlu diuji secara mendalam.

c. Metode Konsultasi

Dalam proyek ini, pada metode konsultasi yaitu melakukan konsultasi

kepada dosen pembimbing. Dalam konsultasi ini, penulis mendapatkan masukan dan arahan terkait teknik-teknik yang tepat untuk menguji ketahanan website *Smart Health* serangan *Brute Force* dan *DoS*, konsultasi juga berguna untuk memastikan bahwa pengujian yang dilakukan sesuai dengan standar, serta dapat menghasilkan temuan yang valid dan bermanfaat.

d. Metode Implementasi dan Pengujian sistem Metode Implementasi

Metode implementasi digunakan untuk melaksanakan pengujian keamanan secara langsung pada website *Smart Health*. Dalam tahap ini, peneliti menerapkan teknik *Penetration Testing* sesuai dengan standar yang telah ditentukan berdasarkan hasil studi literatur dan konsultasi. Implementasi pengujian dilakukan untuk mengidentifikasi kerentanannya terhadap serangan *Brute Force* dan *DoS*. Pada pengujian *Brute Force,* peneliti akan mencoba untuk menebak kombinasi *username* dan *password* dengan berbagai cara. Sedangkan pada pengujian *DoS*, peneliti akan menguji sejauh mana website dapat bertahan ketika mendapatkan serangan trafik tinggi yang bertujuan untuk melumpuhkan server. Pengujian ini dilakukan dalam lingkungan yang aman untuk mencegah dampak negatif terhadap sistem yang diuji.

Metode pengujian sistem dilakukan untuk mengevaluasi performa dan ketahanan website *Smart Health* setelah diberi serangan. Dalam pengujian ini, peneliti akan mengukur sejauh mana sistem dapat mempertahankan dirinya dari serangan *Brute Force* dan *DoS*, serta mengevaluasi potensi dampak yang timbul jika serangan tersebut berhasil menembus sistem. Hasil pengujian ini akan digunakan untuk mengidentifikasi kelemahan dan memberikan gambaran mengenai seberapa efektif langkah-langkah pengamanan yang sudah diterapkan. Pengujian ini juga dilakukan untuk mengumpulkan data yang diperlukan sebagai bahan analisis.

1.7 Sistematika Penulisan

Dalam sistematika penulisan laporan ini, tersusun dari lima bab dengan masing-masing pokok pembahasan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini membahas penjelasan latar belakang dari penelitian proyek. Judul Proyek, Tujuan Proyek, Manfaat Proyek, Batasan masalah, Metode Penelitian Proyek, dan sistematika Penulisan Proyek.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai referensi atau teori-teori dasar dari penelitian seperti konsep-konsep yang dibahas serta penggabungan dari topik yang berkaitan dengan pengimplementasian proyek ini.

BAB III RANCANGAN PENELITIAN

Bab ini membahas tahapan perancangan serangan, dan menjelaskan langkah-langkah penelitian serangan yang akan diimplementasikan.

BAB IV HASIL DAN ANALISIS

Bab ini memaparkan hasil dari implementasi dan pengujian website *Smart Health* terhadap serangan *Brute Force* dan *DoS*, pada bab ini juga membahas kelemahan yang ditemukan.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan Kesimpulan dari hasil proyek dan memberi saran pengembang dalam implementasi website *Smart Health* terhadap serangan *Brute Force* dan *DoS.*

DAFAR PUSTAKA

[1] Wilkens, F. and Fischer, M., 2020. Awards Data-Driven Characterization of Brute-Force Attackers, IEEE Conference on Communications and Network Security (CNS)

[2] Zhang, S., Xie, X., and Xu, Y., 2020. A Brute-force Black-box Method to Attack Machine Learning-Based Systems in Cybersecurity. IEEE Access, 2:1-14

[3] Aljuhani, A., 2021. Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments. IEEE Access, 9:42236-42264

[4] Fachri, F. 2021. Optimizing Web Server Security for Brute Force Attacks using Penetration Testing. Journal of Information Science & Technology, 10(1): 55-58

[5] Alanda, A., Satria, D., Isthofa, M., Ardhana, A., Dahlan, A. and Mooduto, A. Informatics Virtualization Web Application Penetration Testing Using SQL Injection Attack. Journal of International on Informatics Visualization, 5(3): 320-326

[6] Grover, V, and Gagandeep. 2022. An Efficient Brute Force Attack Handling Techniques for Server Virtualization. Department of Computer Science, 1-6

[7] Zimmermann, V. and Gerber. N. 2021. The password is dead, long live the password. International Journal of Human-Computer Studies, 133(2020): 26-44

[8] Eipper, A. and Pöhn, D. 2024. How to Design a Blue Team Scenario for Beginners on the Example of Brute-Force Attacks on Authentications. Journal of Universita ̈t der Bundeswehr

[9] Li, L., Thakur, K., and Ali, M. L, 2020 Potential Development on Cyberattack and Prospect Analysis for Cybersecurity. 2020 Journal of IEEE, 22-26

[10] Liao S. 2020. A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments, in Proceedings - 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 64–71

[11] Eipper A. and Pöhn, D. 2024. How to Design a Blue Team Scenario for Beginners on the Example of Brute-Force Attacks on Authentications, 110-115

[12] Ferryansa, A., Budiono, and Almaarif, A. 2020. Analysis of USB Based Spying Method Using Arduino and Metasploit Framework in Windows Operating System . in 2020 3rd International Conference on Computer and Informatics Engineering, 437–442

[13] Harjono, E. B. 2020. Analysis and Implementation using Operating System on LSF methods dan Remaster. Journal Informatics Engeenering, 1(1): 25-26

[14] Wahid, A., Firdaus, M. E. and Parenreng, J. M. 2021. Implementation of

Wireshark and IPtables Firewall Collaboration to Improve Traffic Security on Network Systems. Internet of Things and Artificial Intelligence Journal, 1(4):249–264,

[15] Alanda, A., Satria, D., Isthofa, M., Ardhana, A., Dahlan, A. and Mooduto, A. Informatics Virtualization Web Application Penetration Testing Using SQL Injection Attack. Journal of International on Informatics Visualization, 5(3): 320-326

[16] Harjono, E. B. 2020. Analysis and Implementation using Operating System on LSF methods dan Remaster. Journal Informatics Engeenering, 1(1): 25-26

[17] Zhou, S., Liu, J., Hou, D., Zhong, X., and Zhang, Y. 2021. Autonomous penetration testing based on improved deep q-network. Applied Sciences (Switzerland), 11(19): 324-326

[18] Alanda, A., Satria, D., Isthofa, M., Ardhana, A., Dahlan, A., and Mooduto, A. 2021. Web Application Penetration Testing Using SQL Injection Attack. Internasional Journal on Informatics Visualization, 5(3):320-326

[19] Alkhwaja, I., Albugami., M., Alkhwaja, A., Alghamdi, M., Abahussain , h,M Alfawaz, F., Almurayh, F., and Min-Allah, N. 2023. Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. Journal of MDPI, 2-22

[20] Khaw, Y. M., Abiri, A., Jahromi, M. F. M., Arani, S., Sanner, D., Kundur., and Kassouf, M. 2021. A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays. IEEE Trans Smart Grid, 12(3): 2554–2565

[21] Li, L., Thakur, K., and Ali, M. L. 2020. Potential development on cyberattack and prospect analysis for cybersecurity. in IEMTRONICS 2020 - International IOT, Electronics and Mechatronics Conference, Proceedings, 236-245

[22] Luxemburk, J., Hynek, K., and Cejka, T. 2021. Detection of HTTPS Brute-Force Attacks with Packet-Level Feature Set. in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, 114–122

[23] Alkhwaja, I. 2023. Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. Applied Sciences (Switzerland), 13(10): 114-120

[24] Articel of Mikrotik » MikroTik RB941-2nD-TC hAP lite TC Router dan Panduan Pengguna Nirkabel.

[25] Chaudhary, S., O'Brien, A., and Xu, S. 2020. Automated Post-Breach Penetration Testing through Reinforcement Learning. IEEE Conference on Communications and Network Security (CNS).

[26] Sholihah, T. H., Waluyo, D., and Putro, T. G. S. 2025. The Impact of Big Data Analytics on Intelligence Gathering and Defence Decision Making. International Journal Of Humanities Education And Social Sciences (IJHESS), 4(5): 2051-2061.

[27] Gao, Y., Li, X., Peng, H., Fang, B., and Yu, P. S., 2020. HinCTI: A Cyber

Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE Trans Knowl Data Eng, 34(2): 708–722.

[28] Liu, S., Yu, Y., Hu, W., Peng, Y., and Yang, X. 2020., Intelligent Vulnerability Analysis for Connectivity and Critical-Area Integrity in IoV. IEEE Access 8: 114239–114248.

[29] Tariq, N., Khan, F. H., Moqurrab, S. H., and Srivastava, V., 2023. CAPTCHA Types and Breaking Techniques: Design Issues, Challenges, and Future Research Directions. ACM Comput, 00(000): 1-46

[30] OWASP., (2021). Brute Force Protection Cheat Sheet. OWASP Cheat Sheet Series.https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[31] Manoharan, M., 2020. API Rate Limiting Mechanisms in SaaS Applications: A Systematic Analysis of DDoS Protection Strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6): 1787-1798.

[32] Durmuskaya, M. E. and Bayrakli, S., 2025. Web Application Firewall Based on Machine Learning Models. PeerJ Computer Science, 1-30

[33] Hidayah, I., Munadi, R., and Irawati, I. D., 2019. Implementasi High-Availability Web Server Menggunakan Load Balancing as a Service pada Openstack Cloud. e-Proceeding of Engineering, 6(3): ISSN : 2355-9365.

[34] Heiding, F., Omer, M.A., Wallstrom, A., and Lagerstrom, R., 2020. Securing IoT Devices using Geographic and Continuous Login Blocking: A Honeypot Study. International Conference on Information Systems Security and Privacy, 424-430.

[35] Nachan, H., Poddar, D., Sarode, S., Kumhar, P., and Birla, S., 2021. Intrusion Detection System: A Survey. International Journal of Engineering Research & Technology (IJERT), 10(5): 1036–1047.