46/S/TEKKOM-KCBR/PK.03.08/23/JANUARI/2025

IMPLEMENTASI HONEYPOT PADA SERVER UNTUK MENDETEKSI SERANGAN DOS

SKRIPSI

diajukan untuk memenuhi sebagian syarat

untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer

oleh

Fikri Rizalul Haq

NIM 2007056

PROGRAM STUDI TEKNIK KOMPUTER

KAMPUS UPI DI CIBIRU

UNIVERSITAS PENDIDIKAN INDONESIA

2025

HALAMAN HAK CIPTA

IMPLEMENTASI HONEYPOT PADA SERVER UNTUK MENDETEKSI SERANGAN DOS

Oleh
Fikri Rizalul Haq
NIM 2007056

Sebuah skripsi yang diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer

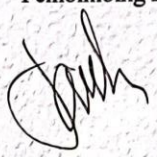
HALAMAN PENGESAHAN SKRIPSI

FIKRI RIZALUL HAQ

IMPLEMENTASI HONEYPOT PADA SERVER UNTUK MENDETEKSI SERANGAN DOS

disetujui dan disahkan oleh

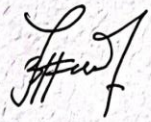
Pembimbing I



Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I.

NIP. 920200819940117101

Pembimbing II



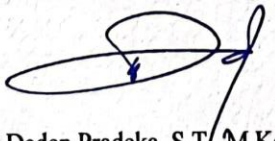
Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

Mengetahui,

Ketua Program Studi Teknik Komputer

Kampus UPI di Cibiru



Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Fikri Rizalul Haq

NIM : 2007056

Program Studi : Teknik Komputer

Dengan ini saya menyatakan bahwa skripsi dengan judul "Implementasi Honeypot pada Server untuk Mendeteksi Serangan DoS" ini beserta seluruh isinya adalah benar benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila dikemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Januari 2025

Yang membuat pernyataan

Fikri Rizalul Haq

NIM. 2007056

HALAMAN UCAPAN TERIMAKASIH

Segala puji dan syukur penulis panjatkan atas kehadirat Allah Swt, Tuhan semesta alam, yang selalu melimpahkan kasih sayang, rahmat, dan karunia-Nya kepada penulis. Tak lupa solawat serta salam, semoga selalu tercurahkan kepada Baginda Nabi Muhammad SAW, beserta para keluarga, sahabat, dan para pengikutnya hingga akhir zaman. Atas segala berkah dan pertolongan-Nya, penulis mampu menyelesaikan skripsi ini yang berjudul "Implementasi Honeypot Pada Server Untuk Mendeteksi Serangan DoS" dengan baik.

Dalam penyusunan skripsi ini, penulis banyak mendapat hambatan dan tantangan. Namun, dengan dukungan dari berbagai pihak, penulis dapat menyelesaikan skripsi ini dengan baik. Untuk itu, penulis ingin menyampaikan terima kasih kepada semua pihak yang telah memberikan bantuannya, terutama kepada yang terhormat:

1. Kedua orang tua, Bapak Engkus Kusmana dan Ibu Eti Nurhayati serta keluarga besar yang selalu memberi dukungan secara moral dan material, serta mengirimkan doa setiap hari agar saya dapat menyelesaikan skripsi ini, kasih sayang mereka yang tak terhingga semoga Allah SWT selalu menjaga kesehatan mereka.
2. Kakak saya, Zulfan Aulia dan Siti Yulianti atas segala doa dan dukungannya.
3. Bapak Deden Pradeka, S.T., M.Kom., selaku ketua program studi Teknik Komputer.
4. Bapak Muhammad Taufik, S.Tr.Kom., M.T.I. selaku dosen wali sekaligus dosen pembimbing pertama atas bimbingan, dukungan, dan ilmu yang telah bapak berikan selama proses penyusunan tugas akhir ini. Tanpa bimbingan dan saran dari bapak, saya mungkin tidak akan berhasil menuntaskan penelitian ini dengan sukses.
5. Bapak Dr. Eng. Munawir, S.Kom., M.T. selaku dosen pembimbing kedua atas bimbingan, dukungan, dan ilmu yang telah bapak berikan selama proses penyusunan tugas akhir ini.

6. Bapak dan Ibu Dosen Program Studi Teknik Komputer serta seluruh civitas akademika Universitas Pendidikan Indonesia yang telah memberikan segala kebaikan dan jasa selama masa perkuliahan. Semoga segala kebaikan dan jasa yang telah berikan mendapatkan balasan yang setimpal.
7. Teman-teman kost Letter-U Sultan Ichsanul Ghifari, Fanny Muhammad Fahmi Kamillah, Dimas Yuda Putra Aryanto, Satria Arya Respati, Tengku Juansyah, Hisyam Nugraha Solihin, Aldi Sidik Maulana, Muhammad Fajar, Abdi Surya Perdana, Deandy Zahran, Nazar Andrian F, Ardi Rahman Sidiq, M. Wirakusumah, Fasya Khalifa Ardi. Atas segala dukungan dan bantuan yang telah diberikan.
8. Teman-teman, seluruh mahasiswa Teknik Komputer Angkatan 2020, yang telah menjadi sahabat dan saudara selama masa perkuliahan ini. Terima kasih atas segala dukungan, kebersamaan, dan kenangan yang telah kita ciptakan bersama. Tanpa kalian, perjalanan ini tidak akan sama. Kalian adalah keluarga pilihan yang selalu ada dalam suka dan duka. Semoga persahabatan kita terus erat dan membawa kita ke masa depan yang gemilang. Terima kasih atas segalanya.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan, sehingga sangat diharapkan masukan dan kritik dari berbagai pihak untuk perbaikan di masa mendatang. Sekali lagi, saya mengucapkan terima kasih dan mohon maaf yang sebesar-besarnya jika terdapat kesalahan. Semoga penelitian ini memberikan manfaat bagi para pembaca.

IMPLEMENTASI HONEYPOT PADA SERVER UNTUK MENDETEKSI SERANGAN DOS

Fikri Rizalul Haq

2007056

ABSTRAK

Era digital telah merevolusi cara kita hidup, bekerja, dan berinteraksi. Internet, sebagai infrastruktur utama dalam dunia digital, telah menghubungkan miliaran orang dalam jaringan yang luas. Perkembangan pesat teknologi informasi dan komunikasi, seperti smartphone dan aplikasi pintar, semakin mempermudah akses kita terhadap informasi, memungkinkan kita untuk belajar, bekerja, dan bersosialisasi tanpa batasan waktu dan jarak. Namun, perkembangan ini juga membawa ancaman siber, seperti serangan *Denial of Service* (DoS) yang dapat melumpuhkan server dengan membanjiri lalu lintas data. Kurangnya sistem deteksi dini yang efektif membuat banyak server rentan, berpotensi menyebabkan gangguan operasional dan kerugian besar. Penelitian ini bertujuan untuk menganalisis serangan DoS terhadap kinerja server dengan menggunakan Honeypot Dionaea. Honeypot Dionaea digunakan untuk tindakan pencegahan awal terhadapa serangan DoS. Pada penelitian ini menggunakan metodologi *Design and Development (D&D),* dimana server akan menggunakan topologi start yang diintegrasikan menggunakan Honeypot Dionaea pengujian dilakukan dengan serangan DoS seperti TCP flood, HTTP flood, slowhttptest, menggunakan tools LOIC, Slowhttp, Slowloris. Dengan memanfaatkan Honeypot Dionaea, metode ini memungkinkan peneliti untuk menangkap aktivitas berbahaya secara *real-time*. Hasil pengujian IP private memiliki tingkat persentasi keberhasilan dari 5% sampai dengan 98%. Kemudian, hasil pengujian menggunakan IP publik memiliki persentase keberhasilan dari 6% sampai dengan 97% Penelitian ini menyimpulkan Dionaea efektif dalam mendeteksi serangan siber, dengan tingkat keberhasilan yang signifikan dalam menangkap koneksi mencurigakan dan waktu deteksi yang cepat, yang menunjukkan kemampuannya merespons serangan secara *real-time.*

Kata Kunci: Dionaea, DoS, Slowloris, Slow HTTP, Honeypot

IMPLEMENTATION OF HONEYPOT ON SERVER TO DETECT DOS ATTACKS

Fikri Rizalul Haq

2007056

ABSTRACT

The digital age has revolutionized the way we live, work and interact. The internet, as the main infrastructure in the digital world, has connected billions of people in a vast network. The rapid development of information and communication technology, such as smartphones and smart applications, has further facilitated our access to information, allowing us to learn, work, and socialize without time and distance limitations. However, these developments also bring cyber threats, such as Denial of Service (DoS) attacks that can cripple servers by flooding data traffic. The lack of an effective early detection system leaves many servers vulnerable, potentially causing operational disruptions and huge losses. This research aims to analyze DoS attacks on server performance using the Dionaea Honeypot. Dionaea Honeypot is used for early preventive measures against DoS attacks. In this study using the Design and Development (D&D) methodology, where the server will use a start topology that is integrated using the Dionaea Honeypot, testing is done with DoS attacks such as TCP flood, HTTP flood, Slowhttptest, using LOIC, Slowhttp, Slowloris tools. By utilizing the Dionaea Honeypot, this method allows researchers to capture malicious activity in real-time. Private IP test results have a success percentage rate of 5% to 98%. Then, the test results using public IPs have a percentage of success from 6% to 97%. This study concludes that Dionaea is effective in detecting cyberattacks, with a significant success rate in capturing suspicious connections and fast detection time, which shows its ability to respond to attacks in real-time.

Keyword: *Dionaea, DoS, Slowloris, Slow HTTP, Honeypot.*

DAFTAR ISI

HALAMAN HAK CIPTA ii
HALAMAN PENGESAHAN SKRIPSI iii
HALAMAN PERNYATAAN iv
HALAMAN UCAPAN TERIMAKASIH v
ABSTRAK vii
ABSTRACT viii
DAFTAR ISI ix
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR LAMPIRAN xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Penelitian 1
1.2 Rumusan Masalah Penelitian 4
1.3 Tujuan Penelitian 4
1.4 Manfaat Penelitian 4
1.4.1 Manfaat Teoritis 4
1.4.2 Manfaat Praktis 4
1.5 Batasan Penelitian 5
1.6 Struktur Organisasi Skripsi 5
BAB II KAJIAN PUSTAKA 6
2.1 Honeypot 6
2.1.1 Klasifikasi Honeypot 6
2.1.2 Honeypot Dionaea 7
2.2 Server 8
2.3 Keamanan Jaringan 9
2.4 Nmap 9
2.5 LOIC (Low Orbit Ion Canon) 10
2.6 Serangan Siber 11

2.6.1 Denial of Service (DoS) 11
2.6.2 Slow HTTP 12
2.6.3 Slowloris 12
2.7 Penelitian Terkait 13
BAB III METODE PENELITIAN 16
3.1 Metode Penelitian 16
3.2 Tahap Analisis 16
3.3 Tahap Desain 17
3.4 Tahap Pengembangan 20
3.5 Tahap Pengujian 21
3.6 Tahap Evaluasi 23
BAB IV TEMUAN DAN PEMBAHASAN 24
4.1 Hasil Penelitian 24
4.1.1 Implementasi Honeypot 24
4.1.1.1 Instalasi Dionaea 24
4.1.1.2 Tampilan Log Serangan 26
4.1.1.3 Port Scanning 27
4.1.1.4 Serangan Denial of Sevice (DoS) 29
4.2 Pembahasan Hasil Pengujian 31
4.2.1.1 Implementasi Honeypot Dionaea Menggunakan IP Private 32
4.2.1.2 Implementasi Honeypot Dionaea Menggunakan IP Publik 37
BAB V SIMPULAN, IMPLIKASI DAN REKOMENDASI 43
5.1 Simpulan 43
5.2 Implikasi 43
5.3 Rekomendasi 44
DAFTAR PUSTAKA 45
LAMPIRAN 49

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait 13

Tabel 4. 1 Hasil Pengujian IP Private 32

Tabel 4. 2 Hasil Pengujian TCP Flood (LOIC)..... 33

Tabel 4. 3 Hasil Pengujian HTTP Flood (LOIC) 34

Tabel 4. 4 Hasil Pengujian Slow HTTP 34

Tabel 4. 5 Hasil Pengujian Slowloris 35

Tabel 4. 6 Hasil Pengujian IP Publik 37

Tabel 4. 7 Hasil Pengujian TCP Flood (LOIC)..... 38

Tabel 4. 8 Hasil Pengujian HTTP Flood (LOIC) 39

Tabel 4. 9 Hasil Pengujian Slow HTTP 39

Tabel 4. 10 Hasil Pengujian Slowloris 40

DAFTAR GAMBAR

Gambar 1. 1 Grafik pengguna internet di Indonesia (Survei Internet APJII, 2024) 1

Gambar 1. 2 Top 10 Serangan Siber (Badan Siber dan Sandi Nasional, 2023)..... 2

Gambar 2.1 Hirarki Honeypot..... 8

Gambar 2.2 Tampilan LOIC 11

Gambar 3.1 Tahapan Metode Penelitian D&D 16

Gambar 3. 2 Topologi Jaringan..... 18

Gambar 3. 3 Cara Kerja Dionaea 19

Gambar 4. 1 Tampilan Dionaea.cfg 25

Gambar 4. 2 Tampilan log Dionaea bistreams..... 27

Gambar 4. 3 Tampilan log Dionaea JSON..... 27

Gambar 4. 4 Port scannig sebelum Dionaea dijalankan..... 28

Gambar 4. 5 Port scanning sesudah Dionaea dijalankan 28

Gambar 4. 6 Tampilan LOIC 29

Gambar 4. 7 Serangan Slowhttp..... 30

Gambar 4. 8 Serangan Slowloris..... 31

Gambar 4. 9 Tampilan Log DDoS Pada Format JSON 36

Gambar 4. 10 Tampilan Log DDoS Pada Bistreams 36

Gambar 4. 11 Tampilan Log Serangan pada JSON IP Publik 41

Gambar 4. 12 Tampilan Log DDoS Pada Bistreams IP Publik 41

DAFTAR LAMPIRAN

Lampiran 1. Tampilan web Dokumentasi Dionaea..... 49

Lampiran 2. Ujicoba Serangan IP *Private* 50

Lampiran 3. Ujicoba serangan IP publik..... 51

Lampiran 4. Tampilan Dionaea..... 52

Lampiran 5. Tampilan Menu Log JSON dan Bistreams..... 53

DAFTAR PUSTAKA

Al Fikri, K., & Djuniadi, D. (2021). Keamanan Jaringan Menggunakan Switch Port Security. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 5(2), 302-307.

Alieyan, K., Almomani, A., Anbar, M., Alauthman, M., Abdullah, R., & Gupta, B. B. (2021). *DNS rule-based schema to botnet detection. Enterprise Information Systems, 15*(4), 545-564.

Anwar, E., Lamada, M., & Zulhajji, Z. (2024). Network Security System Against Honeypot Based Packet Sniffing Attacks. *Pinisi Journal of Science and Technology, 1*(5), 15-29.

Aryanti, S., Khairil, & Aspriyono, H. (2023). Pengembangan Sistem Keamanan Jaringan Wifi Berbasis Mikrotik Menggunakan Metode Network Development Life Cycle (NDLC). *Teknosia, 17*(2), 88–95. https://doi.org/10.33369/teknosia.v17i2.31582

Auliafitri, D., RizkiSuro, E., Malik, M. R. M., & Setiawan, A. (2024). Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit. *Journal of Internet and Software Engineering, 1*(3), 12-12. https://doi.org/10.47134/pjise.v1i3.2620

Badan Siber dan Sandi Nasional. (2023). Lanskap Keamanan Siber Indonesia. https://educsirt.kemdikbud.go.id/portal/berita/197

Bowono, P., Setiawan, F., Christian, H. R., Sitorus, A. B., & Sinlae, F. (2024). Pelatihan Instalasi Sistem Operasi Komputer dengan VMWARE. *ARembeN:* Jurnal Pengabdian Multidisiplin, *2*(1), 1-8. https://doi.org/10.69688/aremben.v2i1.48

Cahyanto, T. A., Oktavianto, H., & Royan, A. W. (2016). Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia), 1*(2).

Cisar, P., & Pinter, R. (2019). Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences, 9*(4), 129-149. https://doi.org/10.24368/jates.v9i4.139

Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer, 7*(2),108-115. https://doi.org/10.30656/prosisko.v7i2.2522

Fadhol, M., & Marcus, R. D. (2023). Implementasi Honeypot Dionaea Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan. In *Seminar Nasional Sistem Informasi (SENASIF)* (Vol. 7, pp. 3807-3817).

Geges, S., & Wibisono, W. (2015). Pengembangan Pencegahan Serangan Distributed Denial of Service (DDoS) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle. *Jurnal Ilmiah Teknologi Informasi*, *13*(1), 53-67.

Haniyah, W., Hidayat, M. C., Putra, Z. F. I., Pertama, V. A., & Setiawan, A. (2024). A Simulasi Serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux. Journal of Internet and Software Engineering, 1(2), 8. https://doi.org/10.47134/pjise.v1i2.2654

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika: Jurnal Sistem Komputer*, *11*(1), 67-76.

Harsono, H. (2022). Faktor-Faktor Yang Mempengaruhi Sistem Informasi Berbasis Komputer: Sistem Operasi, Server, Dan Programmer (Literature Review Executive Support Sistem for Business). *Jurnal Manajemen Pendidikan Dan Ilmu Sosial*, *3*(2), 583-593. https://doi.org/10.38035/jmpis.v3i2.1121

Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S., & Buchanan, W. J. (2021). A Comparative Analysis of Honeypots on Different Cloud Platforms. *Sensors (Basel, Switzerland)*, *21*(7), 2433. https://doi.org/10.3390/s21072433

Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *TerAs Law Review: Jurnal Hukum Humaniter Dan HAM*, *3*(1), 11–22. https://doi.org/10.25105/teras-lrev.v3i1.10742

Mispriatin, M., Ginting, J. G. A., & Arifwidodo, B. (2022). Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan. *Prosiding Seminar Nasional Teknoka*, *6*, 170–178. Retrieved from https://journal.uhamka.ac.id/index.php/teknoka/article/view/10276

Mufti Prasetiyo, S., Gustiawan, R., Farhat, & Rizzel Albani, F. (2024). Penanganan Deadlock Yang Optimal Dalam Sistem Operasi Windows: Pencegahan, Identifikasi Penyebab, Dan Konsekuensi Deadlock. *Buletin Ilmiah Ilmu Komputer Dan Multimedia (BIIKMA)*, *2*(1), 60–64. Retrieved from http://jurnalmahasiswa.com/index.php/biikma/article/view/1030

Nurilahi, D. K., Munadi, R., Syahrial, S., & Bahri, A. L. (2022). Penerapan Metode NaÃ¯ ve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning. *ELKOMIKA: Jurnal Teknik Energi Elektrik,Teknik Telekomunikasi, & Teknik Elektronika, 10*(2), 309. http://dx.doi.org/10.26760/elkomika.v10i2.309

Putra, M. T. D., Pradana, H., Munawir, M., Pradeka, D., Yuniarti, A. R., & Sadik, J. (2024). Batiknet: Batik Classification-based Management Application for Inexperienced User. *JOIV: International Journal on Informatics Visualization, 8*(4), 2411-2418.

Ramli, H., & Alifsyah, M. Y. (2023). Analisis Keamanan Komputer Terhadap Serangan Distributed Denial of Service (DDOS). *Journal of Renewable Energy and Smart Device*, 25-30. https://doi.org/10.61220/joresd.v1i1.235

Richey, R.C., & Klein, J.D. (2007). Design and Development Research: Methods, Strategies, and Issues (1st ed.). Routledge. https://doi.org/10.4324/9780203826034

Ruswandi, K., Pohan, M. R. Z., Halim, K. V., & Neyman, S. N. (2024). Strategi Pencegahan Efektif terhadap Serangan DDoS Slowloris menggunakan Kali Linux dan Linux Mint *Journal of Technology and System Information,* 1(4), 11. https://doi.org/10.47134/jtsi.v1i4.2645

Safitrah, T., Sinaga, A. B. G., Alghifari, M., & Neyman, S. N. (2024). Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest. *Journal of Technology and System Information, 1*(4), 11-11. https://doi.org/10.47134/jtsi.v1i4.2663

Saptarianto, H., Deviani, S., Anah, S. I., & Noviyanti, I. (2024). Menghadapi Tantangan Era Digital, Strategi Integrasi Media Sosial, Literasi Digital dan Inovasi Bisnis. Jurnal Manuhara: Pusat Penelitian Ilmu Manajemen dan Bisnis, 2(3), 128-139.

Singh, C., & Jain, A. K. (2024). A Comprehensive Survey on DDoS Attacks Detection & Mitigation in SDN-IoT Network. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 100543.

Sumayyah, Z. I., Permana, S. D. S., Tsabit, M., & Setiawan, A. (2024). Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDoS) terhadap Website Ilegal dengan Kali Linux. Journal of Internet and Software Engineering, 1(2), 14. https://doi.org/10.47134/pjise.v1i2.2694

Survei Internet APJII 2024. Diambil 23 Januari 2025, dari http://survei.apjii.or.id/

Tarigan, B. M., Juliyanti, S., & Gustina, S. (2024, December). Implementasi dan Efektivitas Pengendalian Keamanan Jaringan Menggunakan Tools Honeypot KFSENSOR. In Prosiding Seminar Nasional Amikom Surakarta (Vol. 2, pp. 1164-1175).

Tati Ernawati, & Fikri Faiz Fadhlur Rachmat. (2021). Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 5(1), 180 - 186. https://doi.org/10.29207/resti.v5i1.282

Ubaidillah, U., Taryo, T., & Hindasyah, A. (2023). Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDoS) dan Malware. *JTIM: Jurnal Teknologi Informasi Dan Multimedia*, *5*(3), 208-217. https://doi.org/10.35746/jtim.v5i3.405

Wicaksono, A. I. H. (2018). *Mendeteksi Serangan Distributed Denial of Service (DDOS) Pada Jaringan Komputer* (Doctoral dissertation, Institut Teknologi Sepuluh Nopember).

Zen Munawar, & Novianti Indah Putri. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA|Jurnal Sistem Informasi Karya Anak Bangsa*, 2(01), 14–20. Retrieved from https://ejournal.unibba.ac.id/index.php/j-sika/article/view/275

Zidane, M. (2021). Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naive Bayes. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *6*(1), 172–180. Diambil dari https://j-ptiik.ub.ac.id/index.php/jptiik/article/view/10404