UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

Implementasi Deteksi Serangan DoS Real-Time dan Mitigasi Otomatis pada Server VPS Berbasis C

Oleh:

Saputra Budianto,

Hamzah Setiwan

Informatika

Universitas Muhammadiyah Sidoarjo

Juli, 2025

Pendahuluan

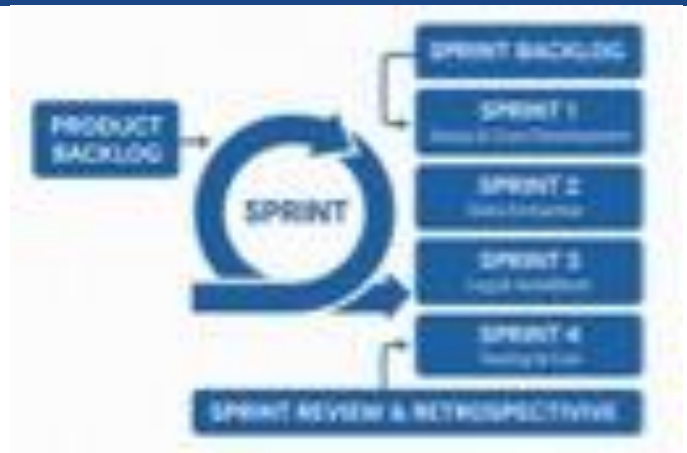
Di era dunia serba dengan kemudahan untuk berkomunikasi satu sama lain, menciptakan peluang bagi para pelaku kejahatan untuk melakukan tindakan kejahatan cyber, salah satunya adalah teknik serangan DoS (*Denial of Service*). Pada dasarnya, serangan DoS dilakukan oleh penyerang untuk melumpuhkan sistem target dengan menghabiskan sumber daya yang dimiliki oleh target.

Pertanyaan Penelitian (Rumusan Masalah)

1. Bagaimana cara mengimplementasikan sistem deteksi *real-time* untuk serangan *DoS* pada *Server VPS* berbasis C agar dapat mengenali lalu lintas mencurigakan?

2. Bagaimana mekanisme mitigasi otomatis yang dapat diterapkan pada *Sever VPS* berbasis C untuk mengurangi dampak serangan *DoS* tanpa mengganggu kinerja layanan?

Metode Agile Scrum



Scrum merupakan metodologi yang digunakan dalam pengembangan sistem, yang diadaptasi dari metode agile, yang digunakan untuk mengelola dan mengendalikan proses perubahan system. Dalam penelitian ini, Scrum digunakan untuk memitigasi dan mendeteksi serangan DoS pada Server VPS secara Real-Time dan Otomatis menggunakan Bahasa pemorgraman C.

Hasil

Pada gambar tersebut merupakan hasil dari DoS Attacking menggunakan tool PeInfo yang dibuat oleh penulis dengan sasaran Server tanpa dilindungi oleh DoS Attack Defender Tool yang dibuat oleh penulis.

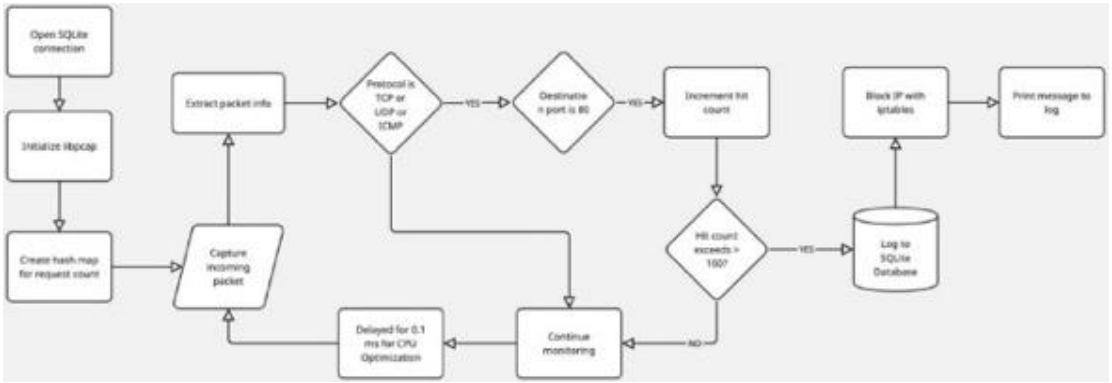
Hasil

Pada gambar tersebut merupakan hasil dari DoS Attacking menggunakan tool PeInfo yang dibuat oleh penulis dengan sasaran Server yang dilindungi oleh DoS Attack Defender Tool yang dibuat oleh penulis.

Pembahasan

Dalam mengembangkan penelitian ini metodologi Agile Scrum diadopsi karena ketersediaannya di lapangan. Pendekatan ini harus dipilih untuk memastikan fleksibilitas anggota sambil mempertahankan pendekatan iteratif dan inkremental. Pemrosesan sistem diperlukan untuk mendukung proses rantai pasokan secara real-time dan efisien.

Pembahasan



Peneliti memiliki produk seperti membuat paket data menggunakan libpcap, membuat paket data untuk IP, port, dan protokol, mengembangkan sistem validasi berbasis batas paket, mengakses SQLite, mengimplementasikan firewall dengan iptables, dan meningkatkan log tingkat sistem. Penundaan ini menyebabkan beberapa sprint dengan banyak tantangan.

Pembahasan

Sebelum membahas fungsi dan kegunaan dari kode yang telah dibuat oleh penulis, Langkah awal clone terlebih dahulu 2 repository penulis yang telah dipublikasikan ke platform Github. dengan cara membuka terminal. Berikut merupakan url github Tool DoS Attack Defender dan Tool DoS Attack yang telah dikembangkan penulis. Ikuti perintah berikut untuk dapat mengkloning sebuah repository github, pastikan sudah install github terlebih dahulu di komputer masing masing. Buka aplikasi Terminal dan beri perinta sebagai berikut

git clone https://github.com/craftgirlsss/DoS-Attack-Defender

git clone https://github.com/craftgirlsss/DoS-Attack-Tool

Temuan Penting Penelitian

Deteksi Serangan DoS Dapat Dilakukan Secara Real-Time Menggunakan Bahasa C

Sistem mampu memonitor trafik secara langsung melalui socket programming dan mendeteksi pola serangan seperti tingginya jumlah koneksi dari IP yang sama dalam waktu singkat, atau permintaan berulang terhadap port/layanan tertentu.

Manfaat Penelitian

Meningkatkan Keamanan Server VPS

- **Deteksi serangan DoS secara real-time** memungkinkan sistem mengenali ancaman sebelum dampaknya terlalu besar.
- **Mitigasi otomatis** mempercepat respons terhadap serangan tanpa intervensi manual, sehingga server tetap bisa berjalan normal atau cepat pulih.

Referensi

[1] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, “Distributed reflection denial of service attack: A critical review,” Dec. 01, 2021, *Institute of Advanced Engineering and Science*. doi: 10.11591/ijece.v11i6.pp5327-5341.

[2] P. Simarmata, N. F. Saragih, I. K. Jaya, and H. Artikel, “Deteksi Serangan DDOS Pada VPS Menggunakan Metode Deep Neural Network,” 2023. [Online]. Available: http://ojs.fikom-methodist.net/index.php/methotika

[3] R. Sommese *et al.*, “Investigating the impact of DDoS attacks on DNS infrastructure,” in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, Association for Computing Machinery, Oct. 2022, pp. 51–64. doi: 10.1145/3517745.3561458.

[4] U. Kingsley and J. Sonia, “Analysis of Linux Kernel Iptables for Mitigating DDOS Attacks; A Component-Based Approach,” *International Journal of Computer Science and Mathematical Theory*, 2021, doi: 10.56201/ijcsmt.v9.no4.2023.pg12.22.

[5] L. D. Garcia, “REAL-TIME NETWORK SIMULATIONS FOR ML/DL DDOS DETECTION USING DOCKER,” 2024.

[6] D. Lincopinis, B. B. Chavez, T. Angelo, J. Gitalan, and D. R. Lincopinis, “C Programming Language: A Review,” *Journal of Universal Computer Science*, vol. 27, no. 1, 2021, doi: 10.3897/jucs.

[7] A. Alsabeh, J. Khoury, E. Kfoury, J. Crichigno, and E. Bou-Harb, “A Survey on Security Applications of P4 Programmable Switches and a STRIDE-based Vulnerability Assessment,” 2022. [Online]. Available: https://www.elsevier.com/open-access/userlicense/1.0/

[8] W. Chrisdianto and S. A. Putri, “PENGEMBANGAN SISTEM MANAJEMEN TEMA WEBSITE BERBASIS METODE AGILE SCRUM.”

[9] A. C. Sassa, I. Alves De Almeida, T. Nakagomi, F. Pereira, and M. Silva De Oliveira, “Scrum: A Systematic Literature Review.” [Online]. Available: www.ijacsa.thesai.org

[10] D. J. K. Putra and P. F. Tanaem, “Perancangan Aplikasi Pembukuan Menggunakan Metode Agile Scrum,” *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 3, Dec. 2022, doi: 10.28932/jutisi.v8i3.5060.

[11] O. C. Resmi Rachmawati, Deyana Kusuma Wardani, Wifda Muna Fatihia, Arna Fariza, and Hestiasari Rante, “Implementing Agile Scrum Methodology in The Development of SICITRA Mobile Application,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 1, pp. 41–50, Feb. 2023, doi: 10.29207/resti.v7i1.4688.

[12] N. Rizky *et al.*, “Analisis Kebutuhan Sistem Informasi Manajemen Kegiatan Kemahasiswaan STIKI Malang Menggunakan Agile Requirements Engineering,” *J-Intech : Journal of Information and Technology*, vol. 10, no. 1, pp. 21–29, 2022, doi: 10.32664/j-intech.v10i01.

[13] N. Edrina Christine *et al.*, “PENERAPAN METODE AGILE SCRUM PADA SISTEM E-POSYANDU BERBASIS WEB,” 2024.

[14] S. Hartono and K. Khotimah, “DETEKSI DAN MITIGASI SERANGAN BACKDOOR MENGGUNAKAN PYTHON WATCHDOG.”

[15] P. Szynkiewicz, “Signature-Based Detection of Botnet DDoS Attacks,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13300 LNCS, Springer Science and Business Media Deutschland GmbH, 2022, pp. 120–135. doi: 10.1007/978-3-031-04036-8_6.

[16] D. Said, “Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid,” *Energies (Basel)*, vol. 16, no. 8, Apr. 2023, doi: 10.3390/en16083572.

[17] “Naskah Publikasi_L200180128”.

[18] M. Hamidouche, B. F. Demissie, and B. Cherif, “Real-time Threat Detection Strategies for Resource-constrained Devices,” Mar. 2024, [Online]. Available: http://arxiv.org/abs/2403.15078

[19] F. Panduardi, H. Yuliandoko, and A. Priyo Utomo, “Network Security Using Honeypot and Attack Detection with Android Application,” *Indonesian Journal of EngineeringResearch*, vol. 2, no. 2, pp. 53–60, 2021, doi: 10.11594/ijer.02.02.04.

[20] H. Setiawan, W. Sulistyo, F. Teknologi Informasi, and U. Kristen Satya Wacana, “SIEM (Security Information Event Management) Model for Malware Attack Detection Using Suricata and Evebox,” *International Journal of Engineering*, vol. 5, no. 2, 2023.


UMSIDA
DARI SINI PENCERAHAN BERSEMI