BAB VI

PENUTUP

A. Kesimpulan

Berdasarkan hasil analisis yang telah dilakukan dalam penelitian yang berjudul "Analisis dan Implementasi Honeypot untuk Mendeteksi Serangan DoS (*Denial of Service*)", maka penulis menyimpulkan bahwa:

1. Serangan DoS bekerja dengan cara membanjiri traffic dengan ribuan packet data menggunakan DoS *tools* seperti LOIC dan slowloris, menuju sebuah situs web atau server. Dampak dari serangan DoS ini adalah situs web atau server tersebut akan menjadi lambat untuk merespon atau *down*, sehingga tidak dapat diakses oleh penggunanya.
2. Honeypot dapat diimplementasikan pada *device* yang menjadi situs web atau server yang rentan terkena serangan DoS. Honeypot dapat dijalankan melalui PenTBox, kemudian honeypot di*setting* untuk melindugi port – port tertentu dari *cyber attack*, seperti di*setting* untuk melindungi situs web pada port 80.
3. Honeypot dapat mendeteksi IP *address* dan port yang digunakan *attacker* beserta dengan waktu penyerangan yang tercatat dalam log honeypot. Honeypot dapat mengelabui *attacker* untuk melakukan serangan pada port – port yang sudah disiapkan sehingga port asli yang menyediakan *service* tetap aman. Honeypot mengatasi serangan DoS dengan mengurangi jumlah *packet* data yang masuk dengan mengirimkan *packet* dengan informasi "[TCP ZeroWindow]" yang membuat window pada TCP header menjadi 0 sehingga device yang telah diimplementasikan honeypot tidak bisa menerima kiriman packet data.

B. Saran

Saran yang dapat diberikan oleh penulis berdasarkan hasil analisis yang telah dilakukan yaitu antara lain:

1. Menutup *open port* dari *service* yang sudah tidak digunakan sehingga *attacker* tidak menggunakan celah tersebut untuk melakukan serangan.
2. Menambah *tools* keamanan DoS seperti WAF (*Web Application Firewall*) yang dijalankan bersamaan dengan honeypot sehingga *attacker* yang menyerang port yang asli dapat dihentikan oleh WAF.

DAFTAR PUSTAKA

[1] "Global Cyber Attacks Rise by 7% in Q1 2023 - Infosecurity Magazine." Accessed: May 21, 2023. [Online]. Available: https://www.infosecurity-magazine.com/news/global-cyber-attacks-rise-7-q1-2023/

[2] "DDoS threat report for 2023 Q1." Accessed: May 21, 2023. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2023-q1/

[3] "Serangan DDos Terhadap Situs DPR Halaman all - Kompasiana.com." Accessed: Dec. 07, 2023. [Online]. Available: https://www.kompasiana.com/natashaayuamanda/63312e5e4addee32e75503f2/serangan-ddos-terhadap-situs-dpr?page=all#section1

[4] "Honeypot Security: Types Of Honeypots, How Does It Works? & Applications In 2023 - Cybersecurity For Me." Accessed: May 22, 2023. [Online]. Available: https://cybersecurityforme.com/honeypot-security/

[5] "ANALISIS DAN IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER SKRIPSI," 2020.

[6] "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," 2020, doi: 10.30743/infotekjar.v5i1.2783.

[7] R. Dermawati and M. Hasim Siregar, "IMPLEMENTASI HONEYPOT PADA JARINGAN INTERNET LABOR FAKULTAS TEKNIK UNIKS MENGGUNAKAN DIONAEA SEBAGAI KEAMANAN JARINGAN," 2020.

[8] "Honeypot Menggunakan Honeyd Sebagai Solusi Keamanan Jaringan Dari Aktivitas Serangan," 2018.

[9] "ANALISA DAN IMPLEMENTASI HONEYPOT HONEYD PADA JARINGAN WIRELESS DI FAKULTAS TEKNIK UNIVERSITAS ISLAM KUANTAN SINGINGI," 2021.

[10] R. A. Kurniawan and R. Primananda, "Pengelompokan Serangan DoS pada Honeypot menggunakan Algoritma K-Means," 2023. [Online]. Available: http://j-ptiik.ub.ac.id

[11] "Penerapan Keamanan Jaringan Menggunakan Honeypot Snare & Tanner Berbasis Web Secara Low Interaction Pada Layanan Web Server," 2023.

[12] N. R. Rosyid *et al.*, "SISTEMASI: Jurnal Sistem Informasi Deteksi Malware pada Jaringan Lokal Berbasis Honeypot dan Yara Malware

Detection on Local Network based on Honeypot and Yara," 2023. [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[13] "Apa itu DDOS? Inilah Cara Mengatasinya." Accessed: Feb. 07, 2023. [Online]. Available: https://www.elitery.com/articles/apa-itu-ddos/

[14] "Pengertian DDOS dan Bagaimana Menanggulanginya - Niagahoster." Accessed: Feb. 07, 2023. [Online]. Available: https://www.niagahoster.co.id/blog/ddos-adalah/#Teknik_DDoS

[15] "DDOS: Pengertian, Cara Kerja, dan Cara Menghindarinya." Accessed: Feb. 07, 2023. [Online]. Available: https://makinrajin.com/blog/ddos-adalah/#1_Request_Flooding

[16] "Apa itu Syn Flood Attack dan Cara Mengatasinya – Rumahweb." Accessed: Feb. 07, 2023. [Online]. Available: https://www.rumahweb.com/journal/apa-itu-syn-flood-attack-adalah/

[17] "UDP flood DDoS attack | Cloudflare." Accessed: Feb. 07, 2023. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/udp-flood-ddos-attack/

[18] "What is an ICMP Flood Attack? | NETSCOUT." Accessed: Feb. 07, 2023. [Online]. Available: https://www.netscout.com/what-is-ddos/icmp-flood

[19] "What is Ping of Death (PoD) | DDoS Attack Glossary | Imperva." Accessed: Feb. 07, 2023. [Online]. Available: https://www.imperva.com/learn/ddos/ping-of-death/

[20] "Apa itu DDoS serta Cara Mengatasinya Dengan Tepat." Accessed: Feb. 07, 2023. [Online]. Available: https://www.cloudmatika.co.id/blog-detail/apa-itu-ddos

[21] "Pengertian, Fungsi, dan Contoh Software Honeypot." Accessed: Feb. 07, 2023. [Online]. Available: https://aliyhafiz.com/honeypot-adalah/

[22] "Honeypot: Server Untuk Mengelabui Serangan Hacker." Accessed: Feb. 07, 2023. [Online]. Available: https://www.dewaweb.com/blog/apa-itu-honeypot/

[23] "23 Software Honeypot Yang Digunakan Untuk Menjebak Hacker." Accessed: Feb. 07, 2023. [Online]. Available: https://aliyhafiz.com/23-software-honeypot-yang-digunakan-untuk-menjebak-hacker/

[24] "5 Fase Ethical Hacking dan Cyber Kill Chain | by Aurell Mayo | Medium." Accessed: Oct. 22, 2023. [Online]. Available: https://medium.com/@mayolv129/5-fase-ethical-hacking-dan-cyber-kill-chain-fb693e715adf

UNIVERSITAS ATMA JAYA YOGYAKARTA