AnoaTIK: Jurnal Teknologi Informasi dan Komputer e-ISSN: **2987-7652**
Vol. 1, No. 2, Desember 2023 *Hal. 68-70*

PENERAPAN SISTEM KEAMANAN IDS PADA JARINGAN NIRKABEL (HOTSPOT)

Andi Muhammad Nur Hidayat[1], Leniawati[2]

[1,2]Fakultas Sains dan Teknologi Universitas Islam Negeri Alauddin Makassar
Email: [1]andi.nurhidayat@uin-alauddin.ac.id, [2]60200118010@uin-alauddin.ac.id

Abstrak

Infrastruktur Jaringan Nirkabel memiliki satu masalah besar, terutama yang membuka akses untuk umum, seperti hotspot adalah masalah keamanannya, dimana banyak terjadi penyerangan oleh satu atau beberapa orang penyerang (attacker) baik pada server penyedia hotspot atau pengguna. Dengan demikian dibutuhkan suatu taktik atau teknik pengamanan guna menanggulangi masalah tersebut. Subyek penelitian ini adalah penerapan sistem keamanan jaringan nirkabel hotspot. Metode yang digunakan dalam penelitian ini adalah Studi Pustaka (Library Research) dan observasi yaitu melakukan pengamatan secara lagsung terhadap jaringan hospot di Cafe Atrium. Analisis dilakukan untuk mendapatkan hasil serta data yang bisa dijadikan sebagai acuan guna menerapkan suatu sistem keamanan jaringan hotspot berbasis honeypot dan snort. Sistem hasil implementasi diuji dengan dua metode yaitu Alpha Test dan Beta test. Hasil penelitian ini adalah kombinasi antara Honeypot dan IDS dengan Honeyd dan Snort ini memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditujukan ke jaringan hotspot.

Kata kunci: *Sistem Keamanan, Honeypot, IDS, Jaringan Nirkabel, Hotspot*

IMPLEMENTATION OF IDS SECURITY SYSTEM ON WIRELESS NETWORK (HOTSPOT)

Abstract

This res The Wireless Network Infrastructure has a significant issue, especially when providing public access, such as hotspots, which is a security concern. There are frequent attacks by one or multiple attackers, either targeting the hotspot provider's server or the users. Therefore, a security tactic or technique is required to address this issue. The subject of this research is the implementation of a security system for wireless network hotspots. The methods used in this study are Literature Review and observation, which involves direct observation of the hotspot network at Cafe Atrium. An analysis is conducted to obtain results and data that can serve as a reference for implementing a security system for hotspot networks based on honeypot and snort. The implemented system is tested using two methods: Alpha Test and Beta Test. The result of this research is a combination of Honeypot and IDS with Honeyd and Snort, providing a multi-layered security system that deceives and detects attacks targeting the hotspot network.

Keywords: *security system, Honeypot, IDS, wireless network, Hotspot*

1. PENDAHULUAN

Honeypot adalah sebuah sistem atau komputer yang sengaja digunakan sebagai umpan menjadi sasaran serangan penyerang. Komputer digunakan serangan dilakukan oleh penyerang dengan cara membobol server itu (Aidin et al., 2016). Honeypot akan memberikan data palsu jika terjadi sesuatu yang aneh masuk ke sistem atau server. Secara teori, honeypot tidak akan mencatat lalu lintas apa yang sah. Oleh karena itu, kita melihat apa yang berinteraksi dengan honeypot tersebut. Pengguna yang menggunakan sumber daya sistem digunakan secara ilegal. Karena itu Honeypot tampaknya merupakan sistem yang berhasil disusupi oleh penyerang. Penyerang tidak memasuki sistem sebenarnya melainkan sistem palsu.

Salah satu software honeypot yang terkenal dan banyak digunakan adalah Honeyd.

Ini akan menjebak penyerang dengan membuat server palsu dengan berbagai jenis sistem operasi seperti Windows, Linux, Unix, Mac Os dan bahkan Cisco.

router dengan layanan bersama seperti FTP, Web, server, dll. Satu dari keuntungan Honeyd adalah ia mengemulasi banyak server dan layanan palsu

hanya di satu komputer atau server untuk menghemat sumber daya, (Agustino et al., 2017).

Sistem keamanan firewall tidak cukup untuk memitigasi kejadian ini serangan pada jaringan komputer. Banyak serangan terjadi secara online Komputer dapat dideteksi setelah kejadian aneh terjadi di jaringan. Admin tidak bisa mengetahui secara pasti apa yang terjadi, jadi perlu waktu lama untuk menguji sistem untuk mengetahuinya masalah terjadi, (Zickuhr, 2016).

Untuk mengatasi permasalahan tersebut diperlukan suatu tool yang dapat mendeteksi lebih awal penyusup atau aktivitas berbahaya secara online. Sistem deteksi intrusi adalah solusi yang sangat sesuai untuk kebutuhan.

Salah satu IDS (Intrusion Detection System) yang sangat populer di bidang keamanan itu Mendengus, (Fachri & Harahap, 2020). Snort pertama kali dibuat dan dikembangkan oleh Martin Roesh di situs pada bulan November 1998, kemudian menjadi proyek Open Source. Bahkan di situs resminya www.snort.org resmi mereka berani mengklaim sebagai standar "intrussion/ detection/prevention". Snort adalah IDS yang sangat populer dan cukup kuat.

2. METODE PENELITIAN

2.1. Subjek Penelitian

Topik penelitian yang akan diangkat pada tugas akhir ini adalah “Aplikasi Sistem keamanan Honeypot dan IDS di jaringan nirkabel (Hotpsot)” dengan penelitian kasus di cyber Cafe Atrium, diharapkan ada sistem keamanan Jaringan hotspot berupa Honeyd dan Snort ini akan mengurangi resiko serangan, untuk server dan pengguna.

2.2. Metode Pengumpulan Data

Metode yang digunakan dimaksud- kan untuk memberikan hasil penelitian dan analisis yang lebih mendalam. Target dan data yang diperoleh lebih akurat, (Nadialista Kurniawan, 2021). Kelengkapan data yang diperoleh dimungkinkan berkontribusi dalam proses penulisan penelitian ini diperlukan untuk pengumpulan data yang terdiri dari:

a) Study Pustaka

Metode pengumpulan data didasarkan pada pembacaan literatur buku, majalah atau artikel yang dimaksudkan untuk mengumpulkan konsep-konsep teoritis berkaitan dengan masalah yang ingin diteliti, mencari sumber data di internet dan perpustakaan, (Darmalaksana, 2020).

b) Metode Observasi

Pengumpulan data dengan observasi langsung terhadap subjek penelitian memperoleh informasi yang akurat dan sistematis, (Fachri & Harahap, 2020). Meliputi instalasi, konfigurasi, alat yang digunakan dan menguji koneksi Internet.

3. HASIL DAN PEMBAHASAN

3.1. Hasil

Berdasarkan penelitian yang disebutkan pada subbab 4 di atas, diperoleh hasil berupa file log aktivitas penyerang yang disimpan Honeyd di direktori /var/log/honeyd/. Setiap kali ada akses ke mesin virtual (server palsu) di alamat IP 192.168.1.100 -192.168.1.105, ini segera dicatat di file log. Setiap aktivitas yang menyerang hotspot, terutama server jahat, akan dicatat oleh Honeyd berdasarkan jenis server jahat tersebut.

Proses pengemulsi server palsu dari Honeyd dan Farpd serta jenis layanan yang mereka sediakan serta isi file log yang dihasilkan akan dijelaskan pada subbagian berikut. Ingat formulir layanan berfungsi serupa dengan layanan aslinya.

3.2. Pembahasan

3.2.1. Akses Hotspot

Akses ke hotspot yang dikonfigurasi pada hotspot ini gratis sehingga setiap pengguna atau penyerang dapat langsung terhubung ke hotspot tanpa otentikasi apa pun seperti nama pengguna atau kata sandi, (Danang & Setiawan, 2022). Karena fokus utama penelitian ini adalah pada honeypot dan kredensial, maka tidak digunakan sistem autentikasi atau sistem pemfilteran MAC, namun lebih baik digunakan pada hotspot untuk alasan keamanan.

Bagi user ataupun penyerang disediakan alamat ip 192.168.1.10 samapai dengan 192.168.1.29. Karena alokasi alamat ip sudah di buat dhcp pada server yang bersifat dinamis.

3.2.2. Prinsip kerja Honeyd

Honeyd menjadi aktif ketika menerima probe atau koneksi dari satu atau lebih server palsu dimana server tersebut berada dalam profil Honeyd. Setelah mengidentifikasi dirinya sebagai server palsu yang mungkin menjadi korban penyerang, Honeyd mulai berinteraksi dengan penyerang. Setelah penyerang puas Jika Anda menyerang server palsu dan kehilangan koneksi, layanan emulasi server palsu tersebut tidak akan langsung berhenti. Honeyd akan menunggu koneksi lain. Honeyd dapat berinteraksi dengan beberapa penyerang secara bersamaan dengan mensimulasikan layanan server palsu, (Syaimi et al., 2013).

Untuk bisa melihat IP Address tersebut, Honeyd membutuhkan bantuan fitur ARP spoofing yang biasanya disediakan oleh layanan arpd atau farpd di Ubuntu 10.04. Spoofing ARP (spoofing) terjadi ketika alamat IP pengguna yang tidak ada (perangkat IP tidak aktif/tidak digunakan) dikaitkan (dikonfirmasi) dengan alamat MAC server honeypot. Hasilnya, paket data terkirim ke honeypot.

4. KESIMPULAN

Berdasarkan pengujian dan analisis data yang dilakukan pada pencarian Honeypot dan Snort sebagai monitor penyerang untuk jaringan nirkabel hotpsot, dapat disimpulkan bahwa adalah:

a) Honeypot adalah suatu sistem komputer atau server yang sengaja dikorbankan untuk menjadi sasaran penyerang, melayani setiap serangan yang dilakukan penyerang dengan setiap intrusi terhadap mesin pemiliknya. Server backend menipu atau memberikan data palsu jika aktor jahat menyusup ke sistem atau server backend. Oleh karena itu, honeypot nampaknya merupakan sistem yang berhasil ditembus oleh penyerang yang memasuki bukan sistem asli melainkan sistem palsu.
b) Penerapan Honeypot Honeyd pada jaringan titik akses nirkabel, yang saat ini berkembang pesat, akan menambah kesulitan bagi penyerang yang mencoba melakukan serangan.
c) Honeypot akan mencatat aktivitas penyerang yang menyerang server palsu yang menyediakan layanan serupa ke server utama dalam bentuk file log.
d) Snort memberikan rekaman trafik yang janggal atau mencurigakan ke server dalam bentuk file log atau alert.
e) Kombinasi Honeypot dan IDS dengan Honeyd dan Snort memberikan sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang menarget- kan jaringan hotspot.

5. DAFTAR PUSTAKA

[1] Agustino, D. P., Priyoatmojo, Y., & Safitri, N. W. W. (2017). Implementasi Honeypot Sebagai Pendeteksi Serangan dan Melindungi Layanan Cloud Computing. *E-Proceedings KNS&I STIKOM Bali*, 196–201. https://knsi.stikombali.ac.id/index.php/eproceedings/article/view/37

[2] Aidin, L. P., Nasution, S. M., & Azmi, F. (2016). Implementasi High Interaction Honeypot Pada Implementation of High Interaction Honeypot. *E-Proceeding of Engineering*, *3*(2), 2172–2178.

[3] Danang, & Setiawan, K. (2022). Pengaturan Billing Hotspot Pada Sistem Jaringan Rt/Rw Net Dengan Mikrotik Router Os. *Jurnal Publikasi Teknik Informatika*, *1*(1), 12–22.

[4] Darmalaksana, W. (2020). Metode Penelitian Kualitatif Studi Pustaka dan Studi Lapangan. *Pre-Print Digital Library UIN Sunan Gunung Djati Bandung*, 1–6.

[5] Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *Jurnal Media Informatika Budidarma*, *4*(2),413. https://doi.org/10.30865/ mib.v4i2.2037

[6] Nadialista Kurniawan, R. A. (2021). No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title. *Industry and Higher Education*, *3*(1), 1689–1699. http://journal.unilak.ac.id/index.php/JIEB/article/view/3845%0Ahttp://dspace.uc.ac.id/handle/123456789/1288

[7] Syaimi, A., Utami, P., Lidyawati, L., & Ramadhan, Z. (2013). Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd. *Jurnal Reka Elkomika ©TeknikElektro | Itenas Jurnal Online Institut Teknologi Nasional Jurnal Reka Elkomika*, *1*(4), 2337–2439.

[8] Zickuhr, B. K. M. (2016). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*. *IV*(June), 182–192.