ANALISIS IMPLEMENTASI HONEYPOT DAN IDS PADA JARINGAN HOTSPOT SEBAGAI PENUNJANG KEAMANAN JARINGAN DI KOPKAR BGA DENGAN MENGGUNAKAN HONEYD DAN SNORT

TUGAS AKHIR

Dian Lestari
41520110104

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

ANALISIS IMPLEMENTASI HONEYPOT DAN IDS PADA JARINGAN HOTSPOT SEBAGAI PENUNJANG KEAMANAN JARINGAN DI KOPKAR BGA DENGAN MENGGUNAKAN HONEYD DAN SNORT

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Dian Lestari
41520110104

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

LEMBAR PERNYATAAN ORISINALITAS

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	: 41520110104
Nama	: Dian Lestari
Judul Tugas Akhir	: Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 24 Agustus 2022

Dian Lestari

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Dian Lestari
NIM	:	41520110104
Judul Tugas Akhir	:	Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 24 Agustus 2022

Dian Lestari

SURAT PERNYATAAN LUARAN TUGAS AKHIR

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Dian Lestari
NIM	:	41520110104
Judul Tugas Akhir	:	Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	
		Jurnal Nasional Terakreditasi	Sinta 3		
		Jurnal International Tidak Bereputasi			
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Inovtek Polbeng - Seri Informatika		
		ISSN	: 2527-9866		
		Link Jurnal	: http://ejournal.polbeng.ac.id/index.php/ISI		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 24 Agustus 2022

Dian Lestari

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41520110104
Nama	:	Dian Lestari
Judul Tugas Akhir	:	Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 11 Agustus 2022

(Dr. Leonard Goeirmanto)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41520110104
Nama	:	Dian Lestari
Judul Tugas Akhir	:	Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 22 Agustus 2022

(Aris Cherid, SE, MTI)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41520110104
Nama	:	Dian Lestari
Judul Tugas Akhir	:	Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 13 Agustus 2022

(Dwi Anindyani Rocmah,ST,MTI)

LEMBAR PENGESAHAN

NIM	:	41520110104
Nama	:	Dian Lestari
Judul Tugas Akhir	:	Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 24 Agustus 2022

Menyetujui,

(Harni Kusniyati, M.Kom)
Dosen Pembimbing

Mengetahui,

(Wawan Gunawan, S.Kom, MT)	(Ir. Emil R. Kaburuan, Ph.D., IPM.)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah SWT karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan penyusunan Tugas Akhir ini yang berjudul : "ANALISIS IMPLEMENTASI HONEYPOT DAN IDS PADA JARINGAN HOTSPOT SEBAGAI PENUNJANG KEAMANAN JARINGAN DI KOPKAR BGA DENGAN MENGGUNAKAN HONEYD DAN SNORT" tepat pada waktunya.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, penulisan laporan tugas akhir ini tidak dapat diselesaikan. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Keluarga yang selalu memberikan *support* dan mendoakan penulis.
2. Ibu Harni Kusniyati, M.Kom selaku dosen pembimbing Tugas Akhir Teknik Informatika.
3. Bapak Emil R. Kaburuan, Ph.D selaku Ketua Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Mercu Buana.
4. Seluruh Dosen Universitas Mercu Buana Fasilkom
5. Rekan kerja di Koperasi Karyawan BGA yang sudah memberikan *support* kepada penulis
6. Teman – teman Mahasiswa/wi Universitas Mercu Buana

Akhir kata, penulis berharap Laporan Tugas Akhir ini dapat bermanfaat bagi Kopkar BGA dan pembaca pada umumnya.

Jakarta, 24 Agustus 2022

Dian Lestari

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

NASKAH JURNAL

Analisis Implementasi Honeypot Dan Ids Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan Di Kopkar Bga Dengan Menggunakan Honeyd Dan Snort

Dian Lestari[1], Harni Kusniyati[2]
Universitas Mercu Buana, Jakarta
Jl. Raya, RT.4/RW.1, Meruya Sel., Kec. Kembangan, Jakarta, Daerah Khusus Ibukota Jakarta 11650
Emali : 41520110104@student.mercubuana.ac.id[1], harni.kusniyati@mercubuana.ac.id[2]

Abstrack - In the current era of digitalization, business processes are developing very rapidly because all business activities can be carried out more easily by utilizing the internet network for data exchange processes. The ease and speed of sending data between distant places is now relatively easy with the ease of accessing the internet. But behind the convenience felt when users take advantage of wireless network facilities or hotspots without realizing there is a security threat that may occur. ut behind the convenience felt when users take advantage of wireless network facilities or hotspots without realizing there is a security threat that may occur. The threat that arises is cybercrime or illegal acts committed by criminals using computer technology and internet networks to attack the victim's information system. Therefore, it is necessary to protect the company's network system to avoid these cybercrime attacks. n this study the authors conducted a trial and analysis of the use of Honeypot (Honeyd) and Intrusion Detection System (Snort) to protect a network system from cybercrime attacks. In this study, three types of attack testing were carried out in the form of Scanning Attack, Denial of Service / DoS and Malware. The results of these tests, the use of Honeyd and Snort is able to secure the network because it is able to detect attacker data traffic.

Keywords - *Honeypot, Intrusion Detection System, Scanning Attack, Dos, Malware*.

Intisari - Pada era digitalisasi saat ini, proses bisnis mengalami perkembangan yang sangat pesat karena segala aktifitas bisnis dapat dilakukan lebih mudah dengan memanfaatkan jaringan internet untuk proses pertukaran data. Kemudahan dan kecepatan mengirimkan data antar tempat yang berjauhan saat ini telah relatif terpenuhi dengan adanya kemudahan dalam melakukan akses internet. Namun dibalik kemudahan yang dirasakan ketika pengguna memanfaatkan fasilitas jaringan wireless atau hotspot tanpa disadari terdapat suatu ancaman kemanan yang memungkinkan terjadi. Ancaman yang timbul adalah cybercrime atau tindakan ilegal yang dilakukan pelaku kejahatan dengan menggunakan teknologi komputer dan jaringan internet untuk menyerang sistem informasi korban. Maka dari itu diperlukan perlindungan terhadap sistem jaringan perusahaan untuk menghindari serangan cybercrime tersebut. Dalam penelitian ini penulis melakukan uji coba dan analisis penggunaan Honeypot (Honeyd) dan Intrusion Detection System (Snort) untuk melindungi

sebuah sistem jaringan dari serangan cybercrime. Dalam penelitian ini dilakukan tiga jenis pengujian serangan berupa Scanning Attack, Denial of Service /DoS dan Malware. Hasil dari pengujian tersebut, penggunaan Honeyd dan Snort mampu mengamankan jaringan karena mampu untuk mendeteksi lalulintas data penyerang.
.

Kata Kunci – Honeypot, *Intrusion Detection System*, *Scanning Attack*, *Dos*, Malware .

PENDAHULUAN

Pada era digitalisasi saat ini, penggunaan jaringan komputer menjadi hal yang sangat dibutuhkan dalam suatu institusi atau perusahaan pada saat ini [1], proses bisnis mengalami perkembangan yang pesat karena segala aktifitas bisnis dapat dilakukan lebih mudah karena memanfaatkan jaringan internet untuk proses pertukaran data [2] Namun pemanfaatan jaringan internet justru menjadi ancaman bagi tindak kejahatan *cybercrime*, *cybercrime* adalah kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan [3]. Pelaku kejahatan *cybercrime* umumnya disebut sebagai *hacker*.

Berdasarkan sudut pandang hukum di Indonesia, dapat diketahui bahwa pencurian atau penggunaan data yang bukan merupakan hak miliknya merupakan suatu kejahatan, karena tindakan tersebut dapat merugikan bisnis. Salah satu perusahaan yang memiliki data penting adalah Koperasi Karyawan BGA (Kopkar BGA). Kopkar BGA didirikan bertujuan untuk meningkatkan kesejahteraan dan taraf hidup para karyawan dan masyarakat, untuk mencapai tujuan tersebut Kopkar BGA menjalankan kegiatan usaha seperti usaha simpan pinjam, pengadaan barang dan jasa umum, agribisnis dan unit pelayanan sembako (UPS) [4].

Salah satu masalah keamanan yang cukup signifikan pada jaringan adalah masuknya user dan program (misalnya : *worm, trojan horse*, virus) yang mengganggu kinerja sistem . Untuk itu diperlukan cara untuk menjaga sekuriti sistem. Salah satunya dengan membangun peringatan dini yang disebut deteksi intrusi /penyusupan (*intrusion detection*). Jenis serangan yang sering dilakukan yaitu *scanning*, DdoS (*Denial of Service Attacks*), serta serangan *malware*. Untuk itu diperlukan sistem yang dapat mendeteksi serangan serta menjebak penyerang yang akan melakukan penyerangan dengan metode serangan yang disebutkan sebelumnya. Salah satu metode yang dapat meningkatkan keamanan jaringan adalah *honeypot. Honeypot* adalah suatu mekanisme pertahanan yang bekerja dengan menjadi duplikasi layanan palsu dari server yang dijaga, telah dikembangkan secara *open source* dan dapat diunduh oleh calon pemakainya tanpa dipungut biaya apapun.

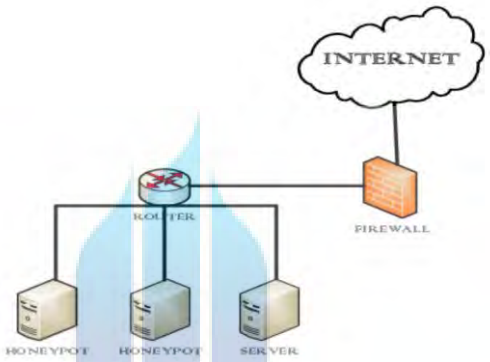
Sistem *Honeypot* dapat di kolaborasikan dengan *Intrusion Detection System* (IDS) seperti *Snort*. *Snort* merupakan sistem pencegahan dan deteksi intrusi jaringan bersifat open source dengan berbasis aturan (*rule-driven*) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan atau *alert* ketika ancaman terdeteksi [5]. Dengan melakukan kolaborasi antara *Honeypot* dan IDS, maka perusahaan dapat mendeteksi dan mencegah penyerangan yang dilakukan.

SIGNIFIKANSI STUDI

A. Honeypot

Honeypot adalah suatu mekanisme pertahanan yang bekerja dengan menjadi duplikasi layanan palsu dari server yang dijaga, telah dikembangkan secara open source dan dapat diunduh oleh calon pemakainya tanpa dipungut biaya apapun. Honeypot menggeser firewall sebagai proteksi terluar apabila biaya merupakan aspek yang dipertimbangkan dalam mengamankan server jaringan [6].

Aplikasi honeypot berjalan di server yang nantinya dapat menyembunyikan service port SSH asli yang biasa diakses dan diserang oleh penyerang dan juga membuat service port SSH palsu yang mampu menipu dan memantau penyerang yang mengancam pada server. Sehingga dengan honeypot, server dapat terhindar dan aman dari serangan yang dilakukan oleh penyerang [7].



Gambar 1. Arsitektur Honeypot

Terdapat tiga jenis layanan honeypot yang dapat disesuaikan dengan potensi ancaman yang diterima server, dan pemakai diberikan fleksibilitas untuk memilih salah satu dari ketiga layanan ini untuk dipergunakan didalam sistem jaringannya, yaitu [8]:

1. *Low interaction honeypot*

   Low Interaction Honeypot merupakan layanan pertama dalam honeypot dimana Honeypot akan menciptakan server tiruan dan pengelola jaringan selaku pemilik server masih memiliki kendali penuh untuk mengawasi kegiatan penyusupan yang terjadi.

2. *Medium interaction honeypot*

   Medium Interaction Honeypot merupakan layanan kedua dalam honeypot dimana sebuah sistem operasi palsu dibuat untuk menjebak attacker. Pada layanan ini beberapa perintah honeypot akan dilewatkan oleh sistem, sebagai gantinya setiap informasi dari attacker akan direkam dan dapat dievaluasi oleh pihak pengelola jaringan. Salah satu yang menyediakan layanan ini adalah *Cowrie.*

3. *High interaction honeypot*

   High Interaction Honeypot merupakan layanan ketiga dalam honeypot dimana pengelola jaringan tidak lagi perlu mengawasi kegiatan penyusupan karena server asli telah direplikasi secara keseluruhan, sehingga attacker

dipersilakan menyerang server replikasi yang diisikan informasi palsu, sehingga attacker merasa puas telah mendapatkan informasi secara ilegal, padahal server yang sebenarnya masih aman tanpa tersentuh sedikitpun.

Penelitian ini menerapkan *honeypot low interaction* karena kelebihan *honeypot low interaction* diantaranya adalah memberikan pengalaman yang baik bagi yang belum berpengalaman dan masih dalam tahap pembelajaran membangun honeypot. Honeypot low interaction memiliki beberapa kekurangan diantaranya [9]:

1. log yang dihasilkan sangat terbatas,
2. Kemampuan untuk menangkap serangan sudah diketahui sebelumnya,
3. dan *honeypot low interaction* mudah terdeteksi oleh penyerang yang sudah profesional.

B. Honeyd

Honeyd merupakan suatu program komputer yang bersifat open source. Cara kerja honeyd memungkinkan pengguna untuk membuat dan menjalankan beberapa virtual host dalam jaringan komputer. Dari virtual host tersebut pengguna dapat mensimulasikan suatu konfigurasi jaringan komputer untuk meniru beberapa jenis server [8]. Honeyd termasuk kedalam jenis low interaction honeypot. Low interaction honeypot merupakan jenis honeypot yang memiliki karakteristik lebih mudah dan cepat untuk diterapkan, hal tersebut dikarenakan honeypot jenis ini hanya menyediakan tiruan dari layanan tertentu saja. Dan honeypot jenis low interaction tidak terdapat sistem operasi nyata yang dimanfaatkan sebagai tempat operasi penyerangan[8].

Meskipun perangkat lunak Honeyd juga dapat dikonfigurasi untuk mencatat aktivitas penyerang, namun perangkat lunak Snort Intrusion detection system digunakan untuk mencatat aktivitas ini karena menyediakan analisis yang lebih kuat dan kategorisasi tanda tangan aktivitas penyerang.

C. Intrusion Detection System

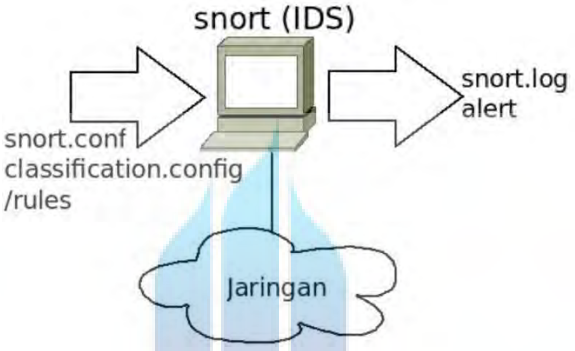
Secara umum, *intrusion* dapat dikatakan sebagai akses tidak sah ke properti atau area seseorang, tetapi jika menyangkut ilmu komputer, itu adalah tindakan untuk mengkompromikan tujuan keamanan jaringan komputer dasar yaitu. kerahasiaan, integritas, dan privasi [10]. Sedangkan Intrusion Detection adalah proses pemantauan peristiwa yang terjadi di sistem komputer atau jaringan dan menganalisisnya untuk tanda-tanda kemungkinan insiden ancaman dan pelanggaran praktik keamanan komputer, kebijakan penggunaan yang dapat diterima, atau kebijakan keamanan standar [10].

D. Snort

Snort merupakan salah satu alat pada IDS dengan komunitas open source, sehingga Snort merupakan alat yang disukai untuk melindungi keamanan jaringan komputer [7]. Snort adalah sistem pencegahan dan deteksi intrusi jaringan bersifat open source dengan berbasis aturan (rule-driven) yang digunakan untuk memantau

lalu lintas jaringan secara pasif dan memberikan peringatan atau alert ketika ancaman terdeteksi.

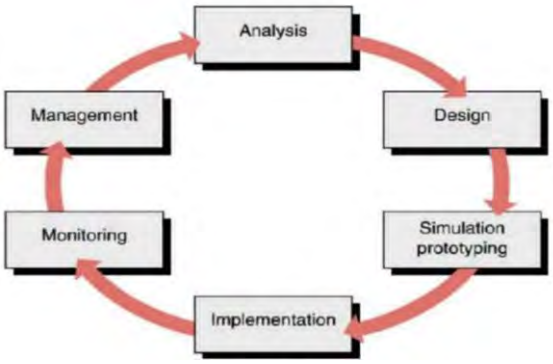
Kelebihan *Snort* terletak pada pembentukan *rules*. *Rules* dapat dibuat/dirancang untuk memblokir lalu lintas atau hanya mengirim peringatan, peringatan dapat dicatat ke file log, dapat dikirim ke konsol atau ditampilkan di layar. *Snort* dapat dikonfigurasi untuk mengirim email ke seseorang atau untuk login ke database. Berbagai pilihan dapat digunakan untuk pembentukan setiap *rules*. *Snort* pada dasarnya bekerja pada tiga mode: mode *Sniffer*, mode *Packet logger* dan mode *NIDS*. Snort dapat dijalankan sebagai mode *packet sniffer* dari baris perintah yang hanya melihat informasi header dan mencetak detailnya di layar. Mode ini dapat digunakan sebagai mode pencatat paket, yang mengambil setiap paket dan memasukkannya ke dalam file log yang berada di direktori *root*. File dapat dilihat nanti menggunakan Snort atau tcpdump. Mode ini untuk digunakan nanti seolah-olah seseorang ingin melihat paket yang diambil nanti [11].



Gambar 2. Arsitektur Snort

E. Metode Penelitian

Penelitian ini merupakan penelitian kuantiatif, dengan jenis penelitian *Network Development Life Cycle (NDLC)* dimana metode ini adalah sebuah metode yang bergantung pada proses pengembangan sebelumnya seperti perencanaan analisa bisnis strategis, design jaringan dengan topologi, simulasi dan prototyping, implementasi, monitoring jarigan yang sudah dibangun lalu melakukan pengaturan dan pemantauan jaringan [12]. Pada penelitian ini penulis mengembangkan sebuah sistem adalah pengembangan jaringan keamanan milik Kopkar BGA. Berikut merupakan tahapan dari metode NDLC sebagai berikut [13] :



Gambar 3. *Network Development Life Cycle (NDLC)*

F. Penelitian Terkait

Implementasi dari Honeypot dan IDS sebagai salah satu alternatif untuk mengamankan jaringan telah dipakai dan dibuktikan oleh beberapa penelitian yang telah berhasil dilakukan sebelum – sebelumnya. Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik Uniks Menggunakan Dionaea Sebagai Keamanan Jaringan [14]. Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware [15]. *Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual Honeypot Approach* [16]. Implementasi Low Interaction Honeypot Untuk Peningkatan Keamanan Server dan Analisa Serangan Pada Protokol SSH [7]

TABEL I
PERBANDINGAN DENGAN PENELITIAN SEBELUMNYA

No	Nama Penelitian	Judul	Metode Penelitian	Hasil Penelitian	Perbedaan
1	Dian Lestari, Harni Kusniayati (2022)	Analisis Implementasi Honeypot Dan IDS Pada Jaringan Hotspot Sebagai Penunjang Keamanan Jaringan di Kopkar BGA dengan Menggunakan Honeyd Dan Snort	Implementasi Low Interaction Honeypot menggunakan Honeyd dan Intrusion Detection System menggunakan Snort	Penggunaan Honeyd dapat menghindari serangan pada server dan Snort dapat membantu mendeteksi lalulintas data penyerang	Dapat mengelabui penyerang yang menggunakan server Honeyd dan mendeteksi lalulintas penyerang sehingga dapat diketahui sumber penyerangan yang dilakukan
2	Naufal Arkaan, Dolly Virgian Shaka Yudha Sakti (2019)	Implementasi Low Interaction Honeypot Untuk Peningkatan Keamanan Server dan Analisa Serangan Pada Protokol SSH	Implementasi Low Interaction Honeypot pada server menggunakan SHH server palsu	Honeypot yang dibuat menggunakan SSH server palsu atau SSH tiruan dapat mengelabui penyerang sehingga penyerang tidak menyerang SSH server yang asli.	Dapat mengelabui penyerang menggunakan SSH server palsu yang telah dibuat.

Dari tabel perbandingan penelitian diatas, penggunaan Low Interaction Honeypot pada kedua penelitian tersebut akan menciptakan server tiruan dan pengelola jaringan selaku pemilik server masih memiliki kendali penuh untuk mengawasi kegiatan penyusupan yang terjadi. Meskipun perangkat lunak Honeyd juga dapat dikonfigurasi untuk mencatat aktivitas penyerang, namun dalam penelitian ini penulis menggunakan perangkat lunak Snort Intrusion Detection System untuk mencatat aktivitas ini karena menyediakan analisis yang lebih kuat dan kategorisasi tanda tangan aktivitas penyerang. Snort adalah sistem pencegahan dan deteksi intrusi jaringan bersifat open source dengan berbasis aturan (rule-driven) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan atau alert ketika ancaman terdeteksi.

HASIL DAN PEMBAHASAN

A. Instalasi dan Konfigurasi Prangkat Lunak

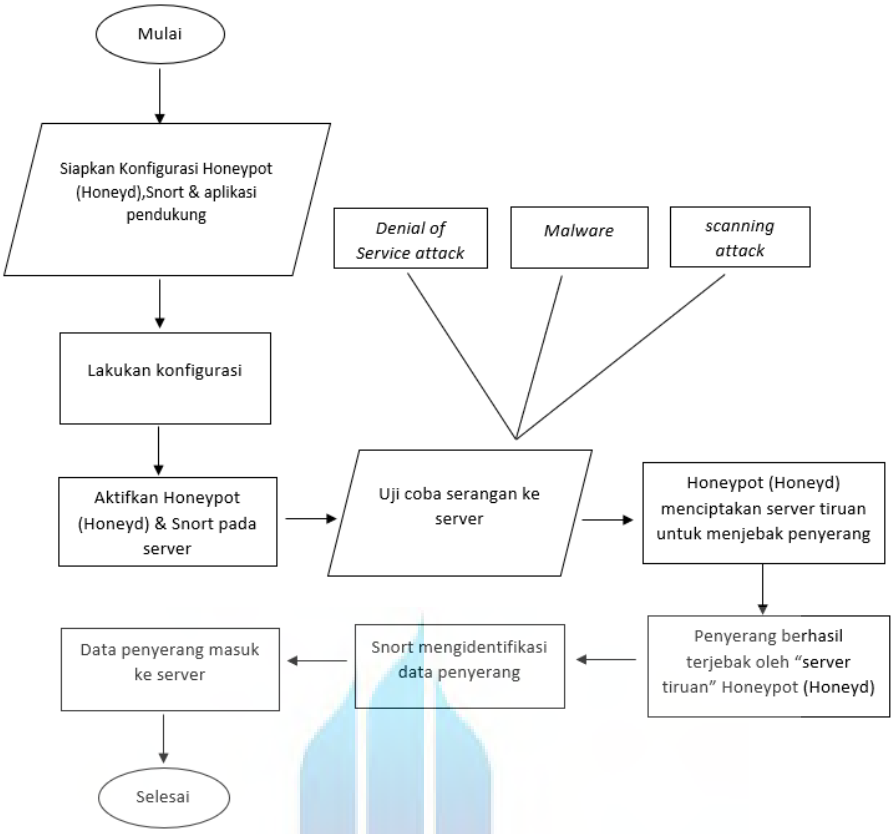
Proses instalasi sistem operasi disertai dengan konfigurasi jaringan (konfigurasi IP address, *subnet mask*) pada PC Server Honeypot, PC server IDS dan PC Attacker mutlak dilakukan agar penulis dapat melakukan implementasi, simulasi dan analisis pada penelitian ini. Instalasi ini nantinya dilakukan dalam sebuah perangkat lunak virtual dan kedua sistem operasi harus bisa saling terhubung dalam sebuah jaringan LAN atau HOTSPOT agar dapat saling berkomunikasi dalam sebuah jaringan virtual host. Dengan demikian dalam mengimplementasi / mensimulasikan penelitian ini dapat digambarkan spesifikasi perangkat keras dan perangkat lunak pada tabel berikut.

TABEL III
SPESIFIKASI PERANGKAT IMPLEMENTASI

Posisi	Sistem Operasi	IP Address	Tool/Command Pengujian
Server Honeypot	Ubuntu Server	192.168.72.131/24	Honeyd
PC-IDS	Ubuntu	192.168.43.163/24	Snort
PC-Attacker	Ubuntu	192.168.43.3/24 192.168.72.1/24	nmap, DoS, Malware

B. Ranangan Pengujian

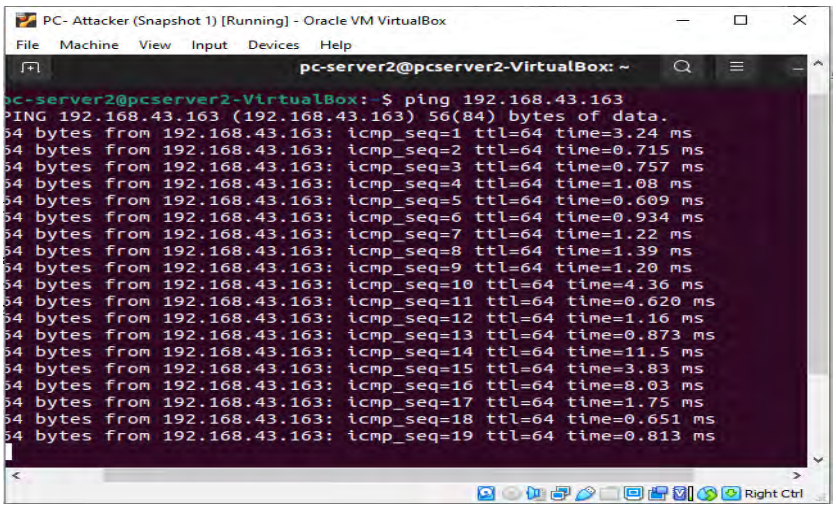
Pengujian dilakukan bertujuan untuk mengetahui seberapa suskes sistem dapat mendeteksi beberapa serangan yang dilakukan. Pada penelitian ini simulasi pengujian penyerangan dilakukan menggunakan ubuntu versi 22.4.05 64bit setelah honeyd dan snort selesai diimplementasikan. Berikut dibawah ini adalah skema gambaran alur skenario sistem pengujian.



Gambar 4. Flowchart Sistem Pengujian

C. Simulasi Pengujian Ping

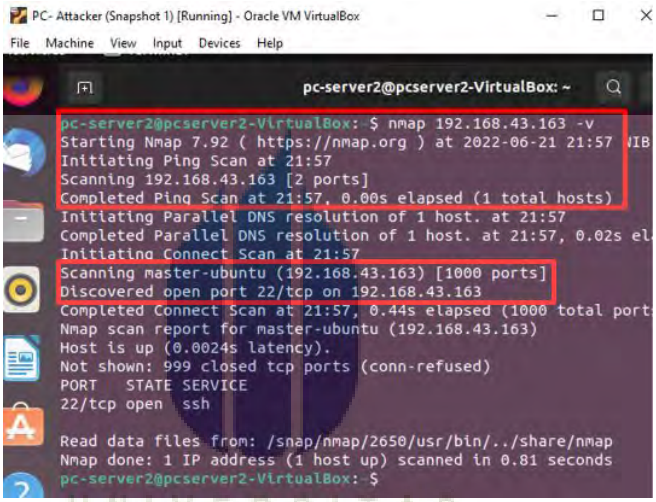
Ping adalah sebuah program yang digunakan untuk memeriksa induktivitas jaringan berbasis teknologi (TCP/IP). Dengan menggunakan program ini, dapat diuji apakah sebuah komputer terhubung dengan komputer lainnya. Hal ini dilakukan dengan mengirimkan sebuah paket kepada alamat ip yang hendak diuji coba konektivitasnya dan menunggu respon IP. Client akan melakukan ping pada komputer server dengan memasukkan perintah ping 192.168.43.163.



Gambar 5. Tampilan Pengujian Ping IP

D. Simlulasi Pengujian Tahap 1 (*Scanning Attack*)

Pengujian ini dilakukan dengan melakukan nmap port scan dengan menggunakan perintah nmap. Informasi yang diinginkan adalah port – port yang terbuka pada server, sistem operasi, dan versi sistem operasi dari server. Proses port scan dilakukan dengan teknik nmaping, dimana server hanya akan memberikan reply terhadap paket data yang dikirimkan client. Pihak penyerang dalam simulasi ini adalah komputer client dengan IP Address 192.168.43.3 dengan target server dengan IP address 192.168.43.163 untuk server 1 dan IP address 192.168.73.131 untuk server 2.



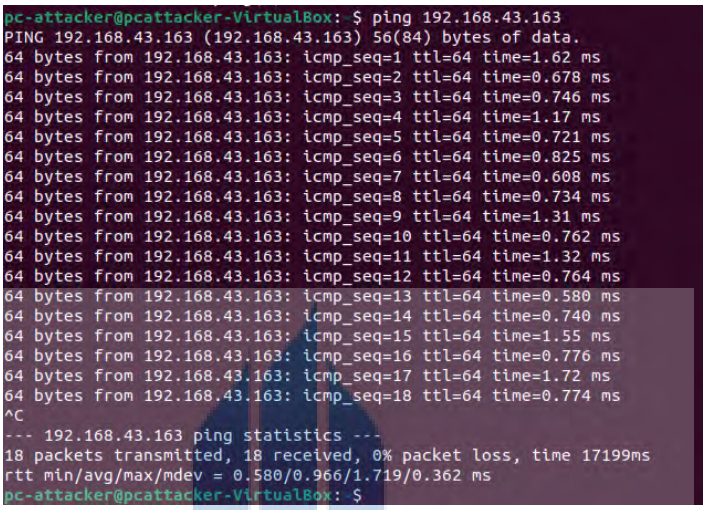
Gambar 6. Melakukan Port Scanning ke Server 1

Pada gambar diatas merupakan hasil port scanning yang dilakukan melalui PC-Attacker. Dari hasil ini diketahui port yang terbuka yakni port 22, atau bisa juga attacker melakukan ping manual ke IP address komputer server 1 melalui command prompt (shell) # ping 192.168.43.163, sedangkan untuk komputer server 2 #ping 192.168.72.131 sebagai berikut.

Gambar 7. Melakukan Port Scanning ke Server 2 (*honeyd*)

E. Simulasi Pengujian Tahap 2 (*Denial of Service /DoS*)

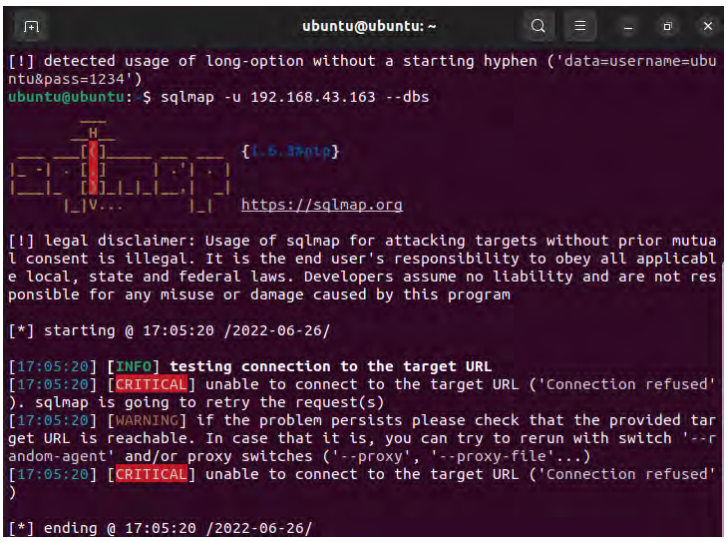
Pengujian ini peyerangan DoS (denial of service) yakni penyerangan dengan mencoba membanjiri (flood) jaringan sehingga lalu lintas pada jaringan menjadi lambat, akses ke layanan server menjadi terhambat, dengan cara mamasukkan perintah ping ke ip address tujuan sasaran, sebagai contoh **Ping 192.168.43.163 -t**



Gambar 8. Proses penyerangan *Denial of Service* ke IP Server 1

F. Simulasi Pengujian Tahap 3 (Malware)

Pengujian ketiga ini yang akan dilakukan adalah serangan malware, penulis menggunakan seragan malware jenis SQL Injection. Dengan perintah :
#sqlmap -u (IP sasaran) yaitu 192.168.43.163 sebagai (server 1) dan 192.168.72.1 sebagai (server 2) –dbs.



Gambar 9. Proses penyerangan Malware ke IP Server 1

KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan hasil penelitian ini adalah sebagai berikut :

1. Berdasarkan hasil pengujian yang dilakukan pada penelitian diatas dapat disimpulkan bahwa honeyd dan snort dapat diimplementasikan sebagai Intrusion Detection System (IDS) pada sistem operasi Ubuntu 22.04 LTS Linux untuk mendeteksi serangan berupa ping, NMAP portscan (Scanning), Denial of Service (DoS) dan Malware.
2. Hasil Analisis yang didapat dalam proses pengujian ping, didapat berupa informasi dari client yang melakukan ping pada server IDS. Nmap port scan yang dilakukan juga dideteksi oleh Snort IDS. Pengujian dengan DoS yang dilakukan juga sudah diberikan pendeteksian intrusi berupa peringatan yang yang dapat mendeteksi port yang terbuka yang disusupi oleh penyerang. begitu juga dengan malware.
3. Honeypot (honeyd) dan Snort dapat memberikan peringatan adanya sebuah serangan keamanan, sehingga dapat meningkatkan keamanan jaringan. Dapat atau tidaknya sebuah serangan terdeteksi oleh honeyd dan Snort IDS tergantung dari ada tidaknya rule dengan jenis signature pada sebuah pola serangan.
4. Honeyd dan Snort dapat dengan mudah diinstal dan dikonfigurasi pada sistem operasi apa saja, termasuk Linux yang digunakan pada penelitian ini.
5. Dari hasil pengujian sistem keamanan menggunakan honeyd dan snort cukup membantu dalam mengamankan jaringan karena mampu untuk mendeteksi lalulintas data penyerang.

REFERENSI

[1] I. I. Muwajihan and D. Jatikusumo, “Perancangan Jaringan Ethernet Link Dengan Menggunakan Teknologi Link Aggregation Dan Auto Failover,” 2021.

[2] A. Delfiantrisno and S. Sroyer, “ANALISIS POTENSI PEMANFAATAN TEKNOLOGI INTERNET DALAM MENUNJANG KEHIDUPAN SOSIAL EKONOMI MASYARAKAT KABUPATEN MIMIKA,” *Jurnal Kritis*, vol. Vol 4 No 1, pp. 1–17, 2020.

[3] A. G. Gani, “Cybercrime (Kejahatan Berbasis Komputer),” *Jurnal sistem Informasi*, vol. 5, no. 1, pp. 16–29, 2018.

[4] P. Kusmiarti, “Analisis Swot Pada Koperasi Karyawan Pt Bumitama Gunajaya Agro,” *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 1, no. 3, pp. 197–206, 2020, doi: 10.31933/jemsi.v1i3.90.

[5] A. R. Gunawan, N. P. Sastra, and D. M. Wiharta, “Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware,” *Majalah Ilmiah Teknologi Elektro*, vol. 20, no. 1, p. 81, 2021, doi: 10.24843/mite.2021.v20i01.p09.

[6] A. W. Sulaksono and E. C. Suharyanto, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. Vol. 5 No. 1, pp. 1–7, 2020.

[7] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 5, no. 2, pp. 112–120, Sep. 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.

[8] W. A. Sulaksono and C. E. Suharyanto, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 1, pp. 90–95, 2020.

[9] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.

[10] A. Tasneem, A. Kumar, and S. Sharma, "Intrusion Detection Prevention System using SNORT," *International Journal of Computer Applications*, vol. 181, no. 32, pp. 21–24, Dec. 2018, doi: 10.5120/ijca2018918280.

[11] A. Tasneem, A. Kumar, and S. Sharma, "Intrusion Detection Prevention System using SNORT," *International Journal of Computer Applications*, vol. 181, no. 32, pp. 21–24, 2018, doi: 10.5120/ijca2018918280.

[12] A. Nugroho and B. Yuliadi, "Sharing Printer Beda Network Menggunakan Jaringan Ad Hoc Dengan Aplikasi Mars Wifi Dan Static Routing Protocol," vol. 3, no. 2, 2018.

[13] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *Mahasiswa Bina Insani*, vol. 4, no. 1, pp. 1–10, 2019.

[14] R. Dermawati and M. H. Siregar, "IMPLEMENTASI HONEYPOT PADA JARINGAN INTERNET LABOR FAKULTAS TEKNIK UNIKS MENGGUNAKAN DIONAEA SEBAGAI KEAMANAN JARINGAN," *Jurnal Ilmiah Edutic*, vol. /Vol.7, No.1, pp. 1–11, 2020.

[15] A. R. Gunawan, N. P. Sastra, and D. M. Wiharta, "Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware," *Majalah Ilmiah Teknologi Elektro*, vol. 20, no. 1, p. 81, Mar. 2021, doi: 10.24843/mite.2021.v20i01.p09.

[16] O. Shobayo and M. Rodrigues, "Design and Implementation of a low-cost low-interaction IDS/IPS System using Virtual Honeypot Approach. Automated irrigation system using solar power View project New JPEG algorithm used for 3D Mesh Reconstruction View project Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual Honeypot Approach," 2017. [Online]. Available: https://www.researchgate.net/publication/327246920

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada Tim *Jurnal Informatika Polbeng* yang telah meluangkan waktu untuk membuat template ini.

KERTAS KERJA

Ringkasan

Berdasarkan sudut pandang hukum di Indonesia, dapat diketahui bahwa pencurian atau penggunaan data yang bukan merupakan hak miliknya merupakan suatu kejahatan, karena tindakan tersebut dapat merugikan bisnis. Salah satu perusahaan yang memiliki data penting adalah Koperasi Karyawan BGA (Kopkar BGA). Kopkar BGA menjalankan kegiatan usaha seperti usaha simpan pinjam, pengadaan barang dan jasa umum, agribisnis dan unit pelayanan sembako (UPS).

Pada Kopkar BGA yang saat ini sedang mengembangkan unit-unit bisnisnya maka diperlukan sistem keamanan jaringan untuk melindungi data-data yang tersimpan seperti data pribadi anggota, data mengenai usaha simpan pinjam, data produk sembako, dan lainnya dari masalah keamanan jaringan. Salah satu masalah keamanan yang cukup signifikan pada jaringan adalah masuknya user dan program yang mengganggu kinerja sistem . Untuk itu diperlukan cara untuk menjaga sekuriti sistem. Salah satunya dengan membangun peringatan dini yang disebut deteksi intrusi /penyusupan (*intrusion detection*). Jenis serangan yang sering dilakukan yaitu *scanning*, DdoS (*Denial of Service Attacks*), serta serangan *malware*. Salah satu metode yang dapat meningkatkan keamanan jaringan adalah *honeypot. Honeypot* adalah suatu mekanisme pertahanan yang bekerja dengan menjadi duplikasi layanan palsu dari server yang dijaga. Dengan menggunakan sistem *Honeypot*, maka penyerang akan dikelabui karena akan diarahkan menyerang server palsu dari *honeypot*.

Sistem *Honeypot* dapat di kolaborasikan dengan *Intrusion Detection System* (IDS) seperti *Snort*. *Snort* merupakan sistem pencegahan dan deteksi intrusi jaringan bersifat open source dengan berbasis aturan (*rule-driven*) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan atau *alert* ketika ancaman terdeteksi.