BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Dalam melakukan penelitian, literatur yang ada berupa karya tesis dan publikasi sebelumnya yang relevan dengan topik yang diteliti oleh penulis dalam rangka penyusunan Tugas Akhir ini. Berikut merupakan karya-karya ilmiah sebelumnya yang terkait dengan yang berkaitan:

Penelitian yang dilakukan oleh Arkaan, Naufal, dan Dolly Virgian Shaka Yudha Sakti (2019) menilai aktivitas penyerang di server, serta kemungkinan kredensial yang digunakan oleh penyerang, sehingga temuan serangan dapat digunakan sebagai pelajaran bagi administrator server untuk membuat server yang dikelola lebih aman. *Honeypot* berjalan di server dan dapat menyembunyikan *port* layanan SSH yang sebenarnya, yang sering dikunjungi dan ditargetkan oleh penyerang, serta membangun *port* layanan SSH palsu untuk mengelabui dan memantau penyerang yang membahayakan server [4].

Penelitian yang dilakukan oleh Mardiyanto, Bagus, Tutuk Indriyani, dan I Made Suartana (2016) mengkombinasikan honeyd dengan iptables, yang digunakan untuk menguji berbagai serangan di jaringan lokal, termasuk pemindaian host, DoS, dan Ddos. Honeyd mampu mengidentifikasi serangan yang dilakukan oleh Netscan android saat memindai host di jaringan dalam pengujian. Honeyd digunakan untuk membuat dan menjalankan host virtual di jaringan komputer, serta mendeteksi serangan oleh penyerang, saat dikonfigurasi. Untuk mencegah dan menghentikan serangan pada server menggunakan arsitektur sistem iptables yang sudah dikonfigurasi [5].

Penelitian yang dilakukan oleh Wirawan, M Arif, Imam Riadi, dan Sunardi (2016) CAIDA DDoS Attack 2007 dan data simulasi diri digunakan untuk mengumpulkan data pelatihan dan pengujian. Persentase rata-rata pengenalan tiga keadaan jaringan (normal, DDoS lamban, dan DDoS) adalah 90,52 persen dalam

pengujian menggunakan teknik analisis statistik log jaringan dengan fungsi jaringan saraf sebagai metode deteksi. Pengenalan metode baru untuk mendeteksi serangan DDoS dimaksudkan untuk menjadi pelengkap Intrusion Detection System (IDS) dalam hal mengantisipasi terjadinya serangan DDoS [6].

Penelitian yang dilakukan oleh Hudzaifah, A. Sularsa, and D. R. Suchendra (2018) membangun sistem monitoring *malicious traffic* di Jaringan dengan Maltrail. Dalam hal ini melakukan pembuatan topologi jaringan berdasarkan satu jaringan yang sama. Hasil pengujiannya untuk menemukan sebuah *malware* di dalam jaringan sehingga bisa terdeteksi oleh Maltrail [7].

Dari beberapa penelitian yang diuraikan di atas maka terdapat perbedaan dengan penelitian ini seperti subjek dan objek yang diteliti. Penulis pada penelitian ini mencoba mengkombinasikan dengan metode baru yaitu terkait HoneyPy dengan Maltrail menggunakan analisis deskriptif guna mendeteksi serangan dari DoS.

2.2 Dasar Teori

2.2.1 Insiden Keamanan Jaringan

Keamanan jaringan merupakan topik hangat saat ini, dan semakin berkembang. Kemajuan teknologi komputer memberikan banyak keuntungan, tetapi juga memiliki banyak kelemahan. Serangan terhadap sistem komputer yang terhubung ke internet adalah salah satunya. Banyak sistem atau jaringan komputer yang dirugikan atau diretas akibat serangan tersebut [8].

Keamanan jaringan komputer terdiri dari empat komponen utama: perangkat lunak, perangkat keras jaringan, layanan *Internet of Things*, dan sumber daya bersama. Keamanan jaringan komputer seperti yang didefinisikan oleh Organisasi Internasional untuk Standardisasi yang merupakan perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer dari kehancuran, perubahan atau lubang keamanan karena alasan yang tidak disengaja atau berbahaya sehingga sistem komputer dapat terus berfungsi dengan aman. terpercaya, dan layanan komputer juga tersedia secara berkala. Pengguna dapat membuat jaringan komunikasi menggunakan peralatan jaringan seperti *router, hub, switch*, dan kabel.

Jaringan komputer telah berkembang menjadi alat penting untuk komunikasi dan penyimpanan data dalam berbagai format dan lokasi. Berbagai penelitian telah menunjukkan bahwa sistem jaringan komputer sangat rentan terhadap beberapa serangan, dan keamanan jaringan meruapakan salah satu entitas paling dinamis untuk bisnis, dipengaruhi oleh perubahan tren teknologi dan pergeseran vektor ancaman dan aplikasi ancaman tingkat lanjut ke aplikasi yang lebih canggih [9].

Insiden keamanan jaringan merupakan serangan terhadap jaringan komputer yang memiliki pengaruh langsung atau tidak langsung terhadap keamanan sistem dan melanggar kebijakan keamanan sistem. *Probe, scan, account compromize, root compromize, packet sniffer, denial of service, exploitation of trust, malicious code,* dan *infrastructure attacks* merupakan contoh insiden. Berikut ini daftar beberapa jenis kejadian yang terjadi:

a) Probe

Adanya upaya tak terduga untuk mendapatkan akses ke sistem atau memperoleh informasi tentang sistem dapat digunakan untuk mengidentifikasi penyelidikan. Upaya untuk masuk ke akun yang tidak digunakan adalah salah satu contohnya. Probing ini dapat dibandingkan dengan mencoba memasuki ruangan dengan memeriksa apakah pintu terkunci atau tidak.

b) Scan

Scan merupakan eksekusi otomatis dari sejumlah besar tindakan probing. Tool dapat secara otomatis menentukan port mana yang terbuka di komputer lokal dan jauh, alamat IP saat ini, dan bahkan sistem operasi host target. NMAP adalah contoh alat pemindaian.

c) Account Compromise

Account Compromise mengacu pada penggunaan akun komputer secara tidak sah oleh seseorang yang bukan pemilik akun. Ketika akun diretas, data korban mungkin hilang atau rusak. Peristiwa pelanggaran akun mungkin memiliki konsekuensi lain, seperti terjadinya insiden *root compromise*, yang dapat mengakibatkan lebih banyak kerugian.

d) Root Compromise

Root Compromise identik dengan Account Compromise. Pengecualian bahwa akun digunakan secara teralarang yaitu akun dengan hak administrator sistem. Pada sistem berbasis UNIX, kata root mengacu pada akun pengguna dengan akses tidak terbatas. Penyerang yang berhasil menjalankan *root compromise* pada sistem korban memiliki kendali penuh atas sistem, termasuk kemampuan untuk meluncurkan aplikasi, mengubah kinerja sistem, dan menyembunyikan bukti intrusi.

e) Packet Sniffer

Packet Sniffer merupakan perangkat lunak dan perangkat keras yang mengumpulkan data saat melewati jaringan komputer. Tujuan dari packet sniffer untuk menempatkan kartu antarmuka jaringan (NIC), seperti Ethernet, ke dalam mode promiscuous sehingga dapat merekam semua lalu lintas jaringan. Mode promiscuous adalah konfigurasi jaringan di mana semua workstation di jaringan mendengar semua komunikasi, tidak hanya lalu lintas yang diarahkan ke mereka.

f) Denial Of Service (Dos)

Komputer dan database, serta layanan yang disediakan oleh organisasi pemilik jaringan merupakan sumber daya jaringan yang berharga. Mayoritas pengguna jaringan memanfaatkan layanan ini untuk membuat pekerjaan mereka lebih efisien. Jika layanan ini tidak tersedia karena alasan apa pun, pasti akan mengakibatkan hilangnya produktivitas.

g) Eksploitasi Terhadap Kepercayaan

Komputer dalam suatu jaringan seringkali memiliki hubungan kepercayaan satu sama lain. Sebelum menjalankan perintah, misalnya, komputer akan melalui kumpulan file yang mengidentifikasi komputer lain mana di jaringan yang diizinkan untuk menjalankan perintah. Jika penyerang dapat menyembunyikan identitas mereka dan tampaknya menggunakan komputer yang dapat dipercaya, penyerang akan dapat memperoleh akses tidak sah ke sistem lain.

h) Malicious Code

Malicious code adalah suatu program yang ketika dijalankan akan menyebabkan pengguna mengalami semacam hasil negatif. Trojan horse, virus, dan worm merupakan contoh program jahat. Setelah dijalankan, worm dapat menyalin dirinya sendiri dan menyebar sesuka hati tanpa perlu keterlibatan manusia.

2.2.2 DoS

Denial of Service (DoS) merupakan semacam serangan terhadap komputer atau server di jaringan internet yang menghabiskan sumber daya komputer hingga tidak dapat lagi menjalankan tugasnya dengan benar, mencegah pengguna lain mengakses layanan yang disediakan oleh komputer yang diserang. DoS pada penelitian ini menggunakan satu PC/Laptop untuk melakakukan serangan dengan bantuan *tools* seperti Virtual Box beserta OS Kali Linux.

Dalam serangan, penyerang akan berusaha untuk melarang pengguna mengakses sistem atau jaringan dengan menggunakan satu atau lebih metode berikut:

1. Membanjiri lalu lintas jaringan dengan volume data yang signifikan, sehingga tidak memungkinkan lalu lintas jaringan dari pengguna terdaftar untuk mencapai sistem.
2. Meningkatkan jumlah permintaan untuk layanan jaringan yang disediakan oleh host ke titik di mana permintaan dari pengguna terdaftar tidak dapat ditangani oleh layanan itu.
3. Mengubah informasi konfigurasi sistem atau bahkan merusak komponen pada server secara fisik untuk mengganggu komunikasi antara host dan klien yang terdaftar.

2.2.3 Server

Dalam jaringan komputer, server merupakan sistem komputer yang menawarkan berbagai layanan. Server dilengkapi dengan sistem operasi tertentu dan memiliki RAM yang cukup. Server juga dapat menjalankan aplikasi untuk mengelola akses dan sumber daya jaringan. *Server DHCP, server Mail, server HTTP, server FTP, dan server DNS* hanyalah beberapa contoh aplikasi server yang memanfaatkan arsitektur klien [10].

2.2.4 Honeypot

Honeypot merupakan perangkat keamanan rahasia yang digunakan untuk menarik penyusup untuk memberikan informasi sensitif. Untuk memastikan keberhasilan operasi, perlu untuk menyembunyikan identitasnya. Honeypot dimaksudkan untuk terlibat dengan penyerang untuk mempelajari lebih lanjut tentang mereka. Pada dasarnya, sebuah sistem yang dimaksudkan agar tampak seperti sistem aslinya untuk diserang dan belajar cara mengoperasikan atau menjebak penyerang [11].

a) Jenis Honeypot

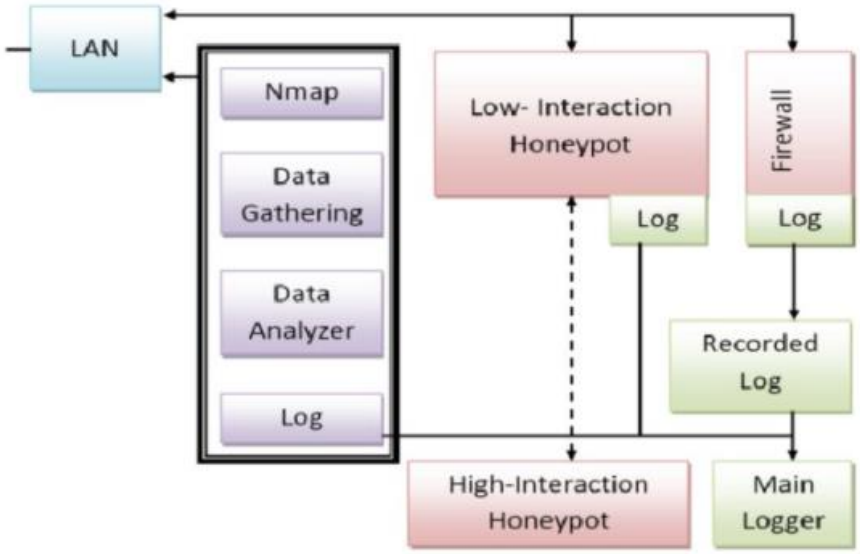
Perbedaan jenis honeypot ini berdasarkan *level of involvement* (tingkat keterlibatan). *Level of involvement* membedakan derajat interaksi penyerang dengan sistem honeypot. Terdiri dari 2 jenis yaitu:

1. Low Interaction Honeypot (LIH)

   Ini hanya meniru sejumlah layanan. Memasang listener pada port merupakan cara termudah untuk membuat layanan ini. Tidak ada sistem operasi asli di *Low Interaction Honeypot* untuk digunakan penyerang sebagai basis operasi. Karena kompleksitas sistem operasi telah berkurang, ini akan dapat sangat meminimalkan risiko. Honeypot dengan Interaksi Rendah mirip dengan koneksi satu arah.

2. High Interaction Honeypot (HIH)

   Menyediakan sistem yang lengkap untuk berinteraksi. Artinya honeypot dengan tingkat interaktivitas yang tinggi tidak hanya mereplikasi layanan, fungsi, atau sistem operasi. Honeypot semacam ini mensimulasikan sistem dan layanan dunia nyata. Akibatnya, penyerang memiliki kendali penuh atas sistem honeypot. HIHAT adalah contoh aplikasi web honeypot dengan tingkat interaksi yang tinggi. HIHAT mengubah aplikasi PHP menjadi honeypot dengan interaksi tinggi [12].



Gambar 2.1 Alur Perbedaan LIH dan HIH

Alur perbedaannya pada letak tingkat keterlibatan pada sistem keamanannya, pada *Low Interaction Honeypot* hanya akan mengemulasikan sebagian service, sedangkan *High Interaction Honeypot* akan menggunakan keseluruhan dari *resource* sistem dimana *Honeypot* dibuat persis dengan sistem yang asli atau nyata dan juga menjadi keseluruhan pada sistem operasi seperti pada gambar 2.1.

2.2.5 HoneyPy

HoneyPy memiliki plugin yang disertakan. Fungsionalitas plugin menentukan jumlah keterlibatan. Lebih banyak interaktivitas dapat dicapai dengan membuat plugin yang mensimulasikan layanan berbasis UDP atau TCP. Secara default, setiap tindakan direkam dalam file. HoneyPy merupakan aplikasi honeypot kecil terbaru yang dapat diunduh dari github dan digunakan di komputer Linux atau Windows, akan digunakan dalam penelitian ini. Tujuan utama Honeypy yaitu mengirim data log kembali ke situs web HoneyPy. HoneyPy dikembangkan dengan Python dan dirancang agar mudah dipasang dan digunakan, dengan kemampuan untuk menambahkan plugin dan menjalankan logger dengan pengaturan khusus [13].

2.2.6 Maltrail

Maltrail merupakan sistem deteksi lalu lintas berbahaya yang menggunakan daftar hitam yang dapat diakses publik dari jalur berbahaya dan umumnya mencurigakan, serta jejak statis dari laporan anti-virus yang berbeda dan daftar yang ditentukan pengguna khusus, di mana jejak tersebut dapat berkisar dari nama domain hingga alamat IP [7].

2.2.7 VirtualBox

VirtualBox merupakan program open source terkait virtualisasi. Virtualisasi yaitu teknologi yang memungkinkan untuk membangun komputer PC virtual yang dapat berfungsi secara independen dari sistem operasi. Komputer host mensimulasikan semua jenis perangkat keras yang terkait dengan mesin virtual. Jika seseorang ingin menguji dan meniru instalasi sistem tanpa kehilangan sistem yang ada, kemampuan ini sangat penting. Tampaknya kita dapat memiliki beberapa jenis perangkat PC dengan beberapa sistem operasi yang memanfaatkan VirtualBox tanpa harus memiliki peralatan yang sebenarnya [14].

2.2.8 Linux

Linux merupakan sistem operasi berbasis Unix yang tersedia secara bebas untuk umum dan diatur oleh GNU General Public License (GPL). Linux open-source ditawarkan dalam sejumlah distribusi, yang masing-masing mencakup satu set paket perangkat lunak yang dapat diinstal. Sangat penting untuk menjaga agar paket-paket ini tetap mutakhir untuk memanfaatkan fitur-fitur baru, perbaikan bug, dan patch keamanan [15]. Linux dikenal karena sistem operasinya yang dirancang terutama untuk server, serta keamanan akses data, sehingga masih dianggap sebagai sistem operasi yang mampu menembus dan melindungi jaringan. Berikut ini adalah sistem operasi yang digunakan dalam penelitian ini:

a) Kali Linux

Kali Linux adalah sistem operasi berbasis Debian yang dibangun oleh Offensive Security sebagai pengganti BackTrack, distribusi Linux perusahaan induknya. Perangkat lunak pengujian penetrasi untuk komputer. Dan juga sistem operasi open source yang tersedia secara bebas untuk umum dan dirancang untuk berbagai aktivitas

keamanan informasi seperti pengujian penetrasi, penelitian keamanan, forensik komputer, dan rekayasa balik. Ada juga berbagai alat di Kali Linux yang dapat digunakan untuk pengujian dalam penelitian keamanan [16]. Dalam hal ini peneliti menggunakan Kali Linux untuk melakukan simulasi serangan terhadap server.

b) CentOs

CentOS merupakan sistem operasi gratis berdasarkan kernel Linux yang pertama kali diterbitkan pada Mei 2004. RHEL adalah tempat CentOS dimulai. "Gregory Kurtzer" menciptakan CentOS, yang pertama kali dirilis sebagai build CAOS. Platform pengembangan yang merupakan salah satu distribusi terbaik dan paling kuat yang tersedia. Ini adalah proyek perangkat lunak bebas berbasis komunitas yang bertujuan untuk menciptakan fondasi yang stabil bagi komunitas open source untuk berkembang. Dan juga mencakup beberapa peningkatan keamanan tingkat perusahaan serta menjadikannya solusi yang fantastis untuk aplikasi apa pun [17]. Pada penelitian ini CentOs8 menjadi server tambahan yang berguna untuk dilakukannya sebuah uji coba serangan.

c) Linux Mint

Linux Mint merupakan distribusi berbasis Ubuntu dengan tujuan memberikan pengalaman desktop tradisional dengan berbagai alat yang berguna, unik dan kemampuan multimedia out-of-the-box. Desktop dan menu yang dipesan lebih dahulu, serta berbagai alat konfigurasi unik dan antarmuka instalasi paket berbasis web, semuanya disertakan. Repositori perangkat lunak Ubuntu kompatibel dengan Linux Mint [18]. Pada penelitian ini Linux Mint digunakan sebagai server utama dengan menerapkan sistem HoneyPy dan Maltrail.