BAB II

TINJAUAN PUSTAKA

2.1 TINJAUAN PUSTAKA

Pada kaian pustak ini menjadi salah satu acuan bagi penulis dalam melakukan penelitian sehingga dapat menjadi studi literatur dalam mengkaji sebuah penelitian yang dilakukan. Penulis memiliki perbedaan dalam melakukan penelitian ini terhadap penelitian yang sebelumnya dan tidak terlepas dari topik penelitian yang menangani penerapan keamanan jaringan, Firewall, Intrusion Prevention system (IPS) dan Honeypot. Berikut merupakan kajian pustaka yang berisi penelitian yang sebelumnya terkait dengan penelitian yang dilakukan penulis:

Pada penelitian sebelumnya yang berjudul "*Penerapan Keamanan Jqringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware*". Oleh Agus Riki Gunawan, Nyoman Putra Sastra, Dewa Made Wiharta. Tujuan dari penelitian ini yaitu menggunakan sistem *snort* dan *honeypot* untuk memonitoring terjadinya serangan terhadap *malware* dan attacker yang masuk pada jaringan kampus Universitas Udayana. Dari penelitian yang dilakukan peneliti mendapatkan hasil bahwa sistem snort dapat mendeteksi 250.519 data dengan 22 atribut layanan dan dibagi berdasarkan jam kerja dan jam tidak kerja.*Honeypot* dapat mencegah 248.574 data serangan dengan 11 atribut, yang setiap atributnya dapat mendeteksi IP penyerang dengan tanggal penyerangan. System snort dan honeypot dapat dijalankan pada background server agar tidak membebani kinerja dan performa dari server jaringan. Dengan penerapan system snort dan honeypot dapat memberikan keamanan berlapis selama 24 jam secara otomatis dan dapat dipantau secara berkala, sehingga dapat diaplikasikan pada jaringan yang lebih besar.[9]

Penelitian tahun 2018 yang berjudul "*Analisis Network Security Snort Menggunakan Metode Intruction Detection System (IDS) Untuk Optimasi Keamanan Jaringan Komputer*" Oleh Parnigotan Panggabean,

S.Kom., M.Kom yang tujuan untuk penerapan sistem keamanan jaringan komputer menggunakan *Snort* untuk mendeteksi serangan *Denial of Service* (DoS) pada jaringan internal maupun external.Penelitian ini pengujiannya memakai tiga metode menurut keamanan snort yaitu menggunakan keamanan sistem snort terhadap agresi DoS metode *Transmission Control Protocol* (TCP), User Data Protocol (UDP), & *Hypertext Transfer Protocol* (HTTP). Untuk metode penyerangan *Denial of Service* memakai LOIC. Pada penelitian ini metode Intrusion Detection System bisa mengoptimalkan taraf keamanan jaringan personal komputer melalui pendeteksian agresi sebagai akibatnya administrator jaringan bisa melakukan tindakan pencegahan. Hasil menurut pengujian Snort bisa mendeteksi agresi DoS menggunakan memakai metode protokol TCP, UDP, & HTTP menggunakan menangkap ip address penyerang yg membentuk respon & CPU personal komputer menyebabkan overload[10]

Penelitian pada tahun 2017 yang berjudul *"Perancangan Analisis Keamanan Jaringan Nirkabel Dari DDoS (Distributed Denial Of Service) Berbasis Honeypot"*. Oleh Sutarti dan Khairunnisa.Tujuan dari penelitian untuk memungkinkan administrator jaringan untuk mendeteksi lalu lintas berbahaya. Metode serangan yang digunakan adalah spam, malware, serangan DDoS, scammer, dan virus. Hasil dari sistem honeypot membuat tugas deteksi lebih mudah, lebih efektif dan lebih murah. Kelemahan dari honeypots adalah bahwa sistem hanya menangkap aktivitas yang diarahkan pada sistem produk dan tidak mencegat serangan pada sistem lain.[11]

Penelitian pada tahun 2019 yang berjudul *"Sistem monitoring Serangan Jaringan Komputer Berbasis web Service Menggunakan Honeypot Sebagai Intusion Prevention system"* Oleh Indah Sari, Muh Yamin, LM. Fid Aksara.Penelitian ini dengan tujuan untuk melakukan monitoring terhadap aktivitas penyerang yang dapat ditampilkan pada web Service. Penelitian ini menggunakan metode Intrusion Prevention System (IPS) untuk mencegah terjadinya serangan. Penelitian ini juga menggunakan Honeypot yang digunakn untuk memperoleh informasi-

informasi dari kegiatan penyerang, serta mengetahui metode yang digunakan penyerang. Hasil dari penelitian ini didapatkan bahwa pembuatan sistem monitoring serangan jaringan komputer berbasis web Service menggunakan Honeypot sebagai IPS berhasil diterapkan dengan menerima serangan yang masuk melalui port TCP adalah sebanyak 33,96%, dan ICMP 32,07%.[12]

Penelitian pada tahun 2019 yang berjudul *"Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery"* Oleh Alja Aminto, Wiwin Sulistyo.Penelitian ini bertujuan untuk menerapkan sistem keamanan jaringan berbasis IPS menggunakan snort dan honeypot artillery yang bisa membantu administrator jaringan dalam mengamankan sistem jaringan (lokal/internet) yang digunakan dari ancaman pencurian dan perusakan data serta dapat mengetahui jenis-jenis serangan yang mengancam sebuah sistem.Hasil dari penelitian ini antara Snort IPS dengan sistem Allertsnya yang responsif dalam menangkap pada gangguan pada sistem Allert yang tercatat didatabase sebanyak9453 yang terdiri pada Traffic Profile yaitu pada protokol TCP sebnyak 9%, UDP sebanyak <1% dan ICMP sebanyak 91% dan Honeypot Artillery yang dapat mendeteksi 1 alamat IP (192.168.10.8) dari mesin virtual box yang dibuat dan melakukan Block IP tersebut sebelum memiliki kesempatan lagi untuk menyerang keseluruhan sistem.Sebelum dipasang Honeypot Artillery dan Snort IPS pada server tidak ada laporan atau data mengenai jenis koneksi apa saja dan dari mana saja koneksi tersebut berasal tanpa adanya proteksi lebih yang membuat tidak amanya server, dengan ini Honeypot Artillery dan Snort IPS dirasa cukup untuk mengamankan dan menganalisis pola serangan attackers yang ingin melakukan intrusi ke sistem jaringan komputer dan dengan memperhatikan kekurangan yang ada dapat membuat penggabungan dua sistem keamanan ini menjadi lebih baik lagi. [13]

No	Judul	Tahun	Penulis	Isi Penelitian
1	Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware	2017	Agus, Nyoman Putra, Dewa	Menurut penelitian tersebut, sistem Snort mampu mengenali 250.519 data dengan 22 atribut layanan yang terbagi menjadi work dan leisure. Honeypot mampu memblokir 248.574 serangan data menggunakan 11 atribut yang masing-masing dapat mengidentifikasi IP penyerang dan tanggal serangan. Sistem Snort dan Honeypot dapat diimplementasikan pada back-end server tanpa memberatkan kinerja web server. Dengan menerapkan sistem Snort dan Honeypot, perlindungan berlapis dapat dijalankan secara otomatis selama 24 jam sehari dan dipantau secara berkala untuk jaringan yang lebih besar.
2.	Analisis Network Security Snort Menggunakan Metode Intruction Detection System (IDS) Untuk Optimasi Keamanan Jaringan Komputer	2018	Parniagon Panggabean, S.Kom., M.Kom [9]	Penelitian ini menguji tiga metode keamanan Snort yang difokuskan pada serangan Denial of Service (DoS) menggunakan Transmission Control Protocol (TCP), User Datagram Protocol (UDP), dan Hypertext Transfer Protocol (HTTP). Penelitian ini juga menguji metode serangan DoS menggunakan LOIC. Dengan metode sistem deteksi intrusi, tingkat keamanan jaringan komputer dapat dioptimalkan dengan mendeteksi serangan dan menginstruksikan administrator jaringan untuk melakukan

				tindakan pencegahan. Hasil pengujian Snort menunjukkan kemampuannya untuk mendeteksi serangan DoS menggunakan protokol TCP, UDP dan HTTP dengan menangkap alamat IP penyerang. Serangan ini meningkatkan beban pada CPU komputer yang diserang, mengakibatkan kelebihan beban sistem
3.	*Perancangan Analisis Keamanan Jaringan Nirkabel Dari DDoS (Distributed Denial Of Service) Berbasis Honeypot*	2017	Sutarti dan Khairunnisa [11]	Penelitian ini membahas tentang metode yang memungkinkan administrator jaringan untuk memantau lalu lintas berbahaya. Metode serangan yang dimasukkan dalam penelitian ini mencakup spam, malware, serangan DDoS, penipuan, dan virus. Hasil dari penggunaan sistem honeypot mempermudah pendeteksian, meningkatkan efisiensi, dan memudahkan analisis. Namun, kelemahan honeypots adalah bahwa sistem ini hanya dapat merekam aktivitas yang ditujukan kepada sistem produksi dan tidak mampu mendeteksi serangan terhadap sistem lainnya.
4.	*Sistem monitoring Serangan Jaringan Komputer Berbasis web Service Menggunakan Honeypot Sebagai*	2019	Indah Sari, Muh Yamin, LM. [12]	Penelitian ini juga melibatkan penggunaan Honeypot yang berperan dalam mendapatkan informasi tentang aktivitas penyerang dan metode yang mereka gunakan. Hasil penelitian ini menunjukkan bahwa pengembangan sistem pemantauan serangan jaringan menggunakan Honeypot sebagai IPS mencapai tingkat keberhasilan sebesar 33,96% untuk serangan masuk melalui port TCP dan 32,07% untuk serangan melalui protokol ICMP

	Intusion Prevention system			
5	*Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery*	2019	Alja Aminto, Wiwin Sulistyo [13]	Studi ini membandingkan Snort IPS dan sistem peringatan sebagai respons terhadap kegagalan sistem peringatan yang tercatat dalam database sebanyak 9453 kejadian. Profil lalu lintas terdiri dari protokol TCP sebesar 9%, UDP kurang dari 1%, dan ICMP. Honeypot berhasil mendeteksi 91% dari lalu lintas tersebut, termasuk satu alamat IP (192.168.10.8) yang mencoba menyerang sistem, sehingga berhasil diblokir sebelum memiliki kesempatan untuk merusak sistem secara keseluruhan. Tanpa perlindungan tambahan, koneksi tersebut berasal dari sumber yang tidak aman dan dapat mengancam keamanan server. Dengan menggunakan kombinasi Honeypot dan Snort IPS, keamanan sistem jaringan komputer dapat ditingkatkan dengan menganalisis pola serangan dari penyerang. Dengan mempertimbangkan kerentanan yang ada, kombinasi kedua sistem ini dapat meningkatkan keamanan secara signifikan.

Tabel 2. 1 Tabel Penelitian Sebelumnya

2.2 DASAR TEORI

2.2.1 JARINGAN INTERNET

Jaringan internet merupakan salah satu kebutuhan manusia saat ini, dan dapat membantu pengguna dalam banyak hal. Saat ini, kami menemukan bahwa jaringan Wi-Fi banyak digunakan di media akses jaringan internet. Keberadaan internet telah mengubah pola pikir masyarakat bahwa jaringan internet dapat menghubungkan ribuan hingga jutaan orang di belahan dunia manapun yang dapat terhubung melalui internet.[13]

2.2.2 FIREWALL

Firewall adalah mekanisme bertujuan untuk melindugi perangkat keras dan perangkat lunak. Proteksi bisa diberikan dengan menyaring, membatasi, atau menolak sebagian ataupun seluruh hubungan atau aktivitas segmental pada jaringan privat dengan jaringan eksternal yang tidak berada dalam cakupannya. Salah satu alat firewall yang paling umum digunakan pada sistem Linux adalah iptables. Iptables memungkinkan administrator jaringan untuk merancang dan mengkonfigurasi pengaturan firewall. Selain itu, administrator dapat mengkonfigurasi rantai atau yang biasa dikenal dengan rantai dan aturan pada sistem Linux. Firewall bekerja pada lapisan jaringan lapisan OSI. Fitur yang termasuk dalam firewall:

1. Memblokir lalu lintas data yang masuk baik dari sumber maupun tujuan.
2. Memblokir lalu lintas data yang keluar baik dari sumber maupun tujuan.
3. Memblokir lalu lintas data berdasarkan konten yang diakses.
4. Mengizinkan komunikasi data ke dalam jaringan internal.
5. Melaporkan lalu lintas data dan aktivitas firewall.

2.2.3 HONEYPOT

Honeypot adalah sistem atau komputer yang sengaja "menyerah" pada serangan hacker. Sistem ini menyediakan layanan palsu untuk serangan setiap peretas di server. Metode ini bertujuan untuk memberi tahu administrator server yang diserang tentang teknik intrusi peretas untuk melindungi server yang sebenarnya. Honeypot adalah sumber daya

komputer yang dibuat untuk menangkap, menyimpan, mengakses, dan menggunakan berbagai sumber daya yang tidak sah. Honeypot juga merupakan sumber daya keamanan yang dirancang untuk menyelidiki, menyerang, atau menghancurkan serangan. Honeypot dapat didefinisikan sebagai sumber daya sistem informasi yang dapat digunakan untuk mendeteksi masalah yang menggunakan sumber daya yang tidak sah atau melanggar hukum. [13]

Honeypots tidak memerlukan lingkungan khusus karena mereka tidak menyediakan layanan khusus apa pun kepada pengguna. Honeypot dapat ditempatkan di mana saja server dapat ditempatkan. Namun, beberapa lokasi lebih berharga daripada yang lain. Honeypots akan ditempatkan di lokasi berikut:

1. Front gateway (dekat jaringan internet publik)

   Keuntungan memiliki honeypot di lokasi ini adalah honeypot berada di jaringan publik dan mengkhususkan diri pada firewall, IDS, atau sumber daya keamanan lainnya karena tampilannya seperti ini: Tidak perlu dikonfigurasi di. Satu sistem eksternal ditangani. Selain itu, menempatkan honeypot di lokasi ini mengurangi risiko jaringan pribadi Anda jika honeypot berhasil disusupi atau dibajak. Honeypot dirancang untuk berisiko, sehingga mereka menarik dan menerima banyak lalu lintas berbahaya (tidak diinginkan), seperti pemindaian port dan pola serangan tertentu. Menempatkan honeypot di lokasi ini tidak mencatat lalu lintas atau menghasilkan peringatan di firewall atau IDS.

2. Zona Demiliterisasi (DMZ)

   Gateway biasanya memiliki sistem keamanan minimal berupa firewall. Keuntungan dari lokasi ini adalah bahwa honeypot berada di belakang firewall, sehingga setiap lalu lintas berbahaya yang biasanya dikirim ke honeypot akan secara otomatis melewati firewall dan masuk ke dalam firewall. Oleh

karena itu, informasi dikumpulkan. Namun, kelemahan dari lokasi ini adalah bahwa sistem lain di DMZ perlu dilindungi dari honeypots. Jika honeypot disusupi atau dibajak maka honeypot tersebut dapat digunakan untuk menyerang sistem lain di DMZ, bahkan honeypot dapat digunakan untuk menyerang firewall pada gateway.

3. Di belakang gateway (dekat jaringan intranet pribadi)

Ada beberapa alasan mengapa honeypots ditempatkan di sini. Salah satunya adalah mendeteksi penyerang dari dalam. Alasan lainnya adalah pendeteksian firewall yang tidak dikonfigurasi dengan benar yang menyebabkan lalu lintas yang tidak diinginkan. Ini mengalir ke jaringan pribadi. Menempatkan honeypots dengan cara ini hanya meningkatkan risiko jaringan pribadi Anda. Ini terjadi ketika honeypot berhasil disusupi atau dibajak. Firewall menganggap traffic diarahkan ke honeypot, sehingga traffic penyerang ke honeypot tidak terhalang oleh firewall yang ada. Penyerang kemudian mengakses jaringan pribadi melalui honeypot. Honeypot kemudian digunakan sebagai batu loncatan untuk menyerang jaringan pribadi.[14]

Ada dua kategori honeypots.

1. Production Honeypots

Production Honeypots berfungsi untuk mengurangi risiko serangan terhadap sistem keamanan jaringan informasi dalam suatu organisasi. Honeypot produksi ditempatkan pada jaringan produksi bersama dengan server produksi lainnya. Honeypots produksi adalah honeypots dengan sedikit interaksi dan mudah digunakan. Namun, ada lebih sedikit informasi tentang penyerang atau penyerang daripada honeypot penelitian.

2. Research Honeypots

Research Honeypots berfungsi agar mendapatkan informasi

sebanyak mungkin tentang penyerang sehingga administrator dapat mengetahuinya. Survei honeypot dilakukan untuk mengumpulkan informasi tentang motif dan taktik komunitas topi hitam di berbagai jaringan. Honeypot penelitian rumit untuk digunakan dan dipelihara, mengumpulkan berbagai informasi, dan terutama digunakan oleh penelitian, militer, atau organisasi.[15]

2.2.4 ZONA DEMILITERISASI (DMZ)

Firewall atau jaringan perimeter DMZ adalah jaringan perimeter keamanan yang berada di antara jaringan area lokal pribadi dan jaringan publik (Internet). DMZ didefinisikan sebagai komputer host atau jaringan kecil yang ditempatkan di zona netral antara jaringan pribadi dan publik suatu organisasi. DMZ mencegah pengguna eksternal mengakses langsung server yang berisi data perusahaan. NAT digunakan untuk meneruskan alamat asal ke alamat internal sementara PAT digunakan untuk meneruskan data yang masuk melalui satu atau lebih port dan protokol.

Lalu lintas ke DMZ dapat diizinkan atau ditolak, terlepas dari apakah itu berasal dari Internet atau jaringan internal. Manajemen lalu lintas dilakukan sepenuhnya melalui firewall DMZ. Secara umum, semua layanan yang disediakan untuk pengguna jaringan eksternal dapat ditempatkan di dalam DMZ. Layanan ini biasanya mencakup server web, server email, server FTP, dan server DNS. [7]

2.2.5 SNORT

Snort adalah perangkat lunak pendeteksi intrusi yang mampu menganalisis paket yang melewati jaringan secara real time dan menyimpannya di gudang data untuk mendeteksi berbagai serangan yang datang dari luar jaringan. Alat ini merupakan kombinasi dari analisis log dan sistem deteksi intrusi IDS, yang sangat berguna untuk merespons serangan server web. Fitur snort dapat membantu administrator sistem dan jaringan dengan memperingatkan mereka tentang upaya intrusi yang berpotensi berbahaya.

Snort adalah contoh program deteksi intrusi berbasis web. Program ini dirancang untuk mendeteksi upaya pembobolan sistem jaringan komputer. Karena Snort adalah sumber terbuka di bawah Lisensi Publik Umum GNU, Snort dapat digunakan pada sistem server yang aman secara gratis dan tanpa biaya lisensi.

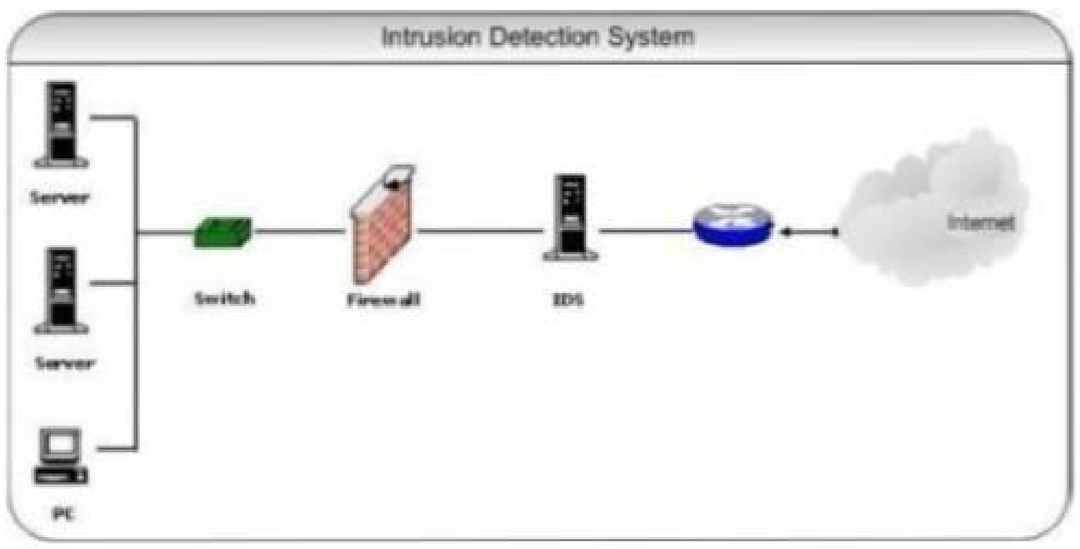
Karena Snort berada di inti switch bersama dengan server, pengguna yang mengakses server melewati core switch dan dipantau oleh server Snort IDS. Snort menerjemahkan paket tingkat aplikasi dan mendapatkan aturan untuk mengumpulkan lalu lintas spesifik yang berisi konten yang terkait dengan aplikasi yang mengeluarkan paket tersebut. Snort bekerja dengan beberapa departemen yang bertanggung jawab untuk menjalankan proses tertentu, mis. B. Blok penangkapan paket, blok decoder dan blok preprocessing. Pertama, aturan Snort dibuat. Jadi jika aturan menggunakan pelanggaran yang sama, peringatan akan ditampilkan dan pelanggaran akan dicatat di database. Log yang disimpan dalam database berfungsi sebagai bukti pesan.

2.2.6 INTRUSION DETECTION AND PREVENTION SYSTEMI (IDPS)

Sistem Deteksi dan Pencegahan Intrusi "IDPS" adalah sistem yang bertugas memantau host atau jaringan untuk mendeteksi aktivitas atau perilaku yang mencurigakan dan mengambil tindakan yang tepat terhadapnya. IDPS adalah gabungan dari Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). Sistem IDS dapat ditempatkan di berbagai titik dalam jaringan. IDS memiliki tugas untuk mendeteksi aktivitas yang mencurigakan dan memperingatkan administrator sistem. Oleh karena itu, administrator sistem harus memutuskan cara menangani peringatan ini. Di sisi lain, sistem IPS adalah sistem internal yang tidak hanya menghasilkan alarm, tetapi juga secara otomatis merespons aktivitas abnormal. IPS dapat memblokir sumber serangan atau memulihkan tautan yang rusak [17]. Di bawah ini adalah deskripsi dari sistem IDS dan IPS:

1. *Intrusion Detection System* (IDS)

IDS adalah perangkat lunak atau perangkat keras yang mendeteksi aktivitas mencurigakan pada sistem atau jaringan. IDS dapat menganalisis upaya penyusupan dan mengumpulkan bukti dengan memantau lalu lintas yang masuk dan keluar dari sistem atau jaringan. Biasanya, IDS bekerja dengan dua pendekatan berbeda, yaitu berbasis data dan berbasis perilaku. IDS menggunakan analisis paket untuk menentukan apakah paket tersebut merupakan serangan atau bukan [17]. Gambar 2.4 memberikan ikhtisar aplikasi IDS umum.



Gambar 2.1 Penerapan IDS [18]

Intrusi dapat diidentifikasi dengan menguping paket data, yang di bandingkan dengan aturan database IDS yang ada. Jika paket-paket tersebut memiliki persamaan, paket tersebut dianggap sebagai serangan. Metode ini disebut basis pengetahuan. Intrusi dideteksi dengan mengamati keadaan aplikasi dan menemukan anomali yang menyebabkan eksekusi aplikasi yang tidak wajar, seperti menyimpulkan bahwa anomali tersebut adalah serangan, tetapi metode kerja ini dapat digambarkan sebagai berbasis perilaku.

2.Intrusion Prevention System (IPS)

Sistem Perlindungan Intrusi "IPS" Dirancang untuk memantau lalu lintas jaringan, mendeteksi aktivitas mencurigakan, dan mencegah intrusi dan kejadian yang dapat mengganggu jaringan Anda. IPS dapat berupa perangkat lunak atau perangkat keras. IPS adalah pendekatan yang umum digunakan untuk membangun sistem keamanan informasi. IPS termasuk teknologi firewall dan sistem deteksi intrusi (IDS). Alat-alat ini sering digunakan untuk mencegah serangan memasuki jaringan lokal dengan memeriksa dan mencatat semua paket data dan mengidentifikasi paket ketika serangan terdeteksi. Oleh karena itu, IPS dapat bertindak sebagai firewall karena dapat membolehkan atau memblokir serangan yang masuk. Ada dua jenis sistem IPS: sistem pencegahan intrusi berbasis host (HIPS) dan sistem pencegahan intrusi berbasis jaringan (NIPS).

A. *Host Intrusion Prevention System* (HIPS)

Sistem pencegahan intrusi berbasis host yang sama "HIPS" sebagai sistem deteksi intrusi berbasis host "HIDS". Program Agen HIPS diinstal langsung pada sistem yang dilindungi dan memantau aktivitas sistem internal. HIPS berinteraksi dengan kernel dan layanan sistem operasi untuk memungkinkan HIPS memantau dan mencegat panggilan sistem yang mencurigakan untuk mencegah intrusi host. HIPS dapat digunakan dalam memantau aliran data dan aktivitas aplikasi tertentu.

B. *Network Intrusion Prevention System* (NIPS)

Sistem pencegahan intrusi berbasis jaringan (NIPS) tidak terbatas pada pemantauan oleh satu host saja, melainkan melakukan pemantauan dan perlindungan di seluruh

jaringan global. NIPS menggabungkan fungsionalitas IPS dengan firewall dan sering disebut sebagai IDS inline atau gateway sistem deteksi intrusi (IDS). Cara kerja umum dari IPS meliputi deteksi berbasis tanda tangan, deteksi berbasis anomali, dan pemantauan file pada sistem operasi host.

2.2.7 MAN IN THE MIDDLE (MiTM)

Serangan umum pada jaringan LAN dan WLAN disebut di bawah ini sebagai serangan man-in-the-middle.MITM. Jenis serangan ini secara aktif menguping koneksi jaringan pengguna yang ada sebelum lalu lintas pengguna mencapai tujuannya. Melalui jaringan penyerang, komunikasi pengguna dimaksudkan agar penyerang dapat membaca tanpa sepengetahuan pengguna. MITM adalah jenis serangan yang sulit dilacak oleh pengguna, bahkan secara online. Jaringan WiFi didukung oleh sistem autentikasi yang baik. Sebagian besar MITmer seseorang bergabung dengan jaringan yang sama dengan pengguna. Jika penyerang berhasil mendapatkan informasi penting dari pengguna, dampaknya akan sangat besar.[23]

2.2.8 DISTRIBUTED DENIAL OF SERVICE (DDoS)

Serangan *Distributed Denial Of Service (DDoS)* adalah aktivitas agar dapat menghentikan operasi normal komputer atau server. Serangan DDoS terjadi ketika seorang peretas terus menerus mengirimkan paket data yang sedang berjalan ke server target, membebani sistem dan membuatnya tidak dapat berfungsi dengan baik. Jenis*Distributed Denial Of Service (DDoS)* adalah:

1. ICMP Flood

   Penyerang mengirimkan beberapa ping berbahaya ke komputer dengan paket IP maksimum 65535 byte (paket ping normal adalah 84 byte). Hal ini dapat menyebabkan komputer Anda crash.

2. TCP Flood

   Setiap permintaan SYN untuk memulai koneksi TCP dengan

komputer harus dijawab oleh respons SYN-ACK dari komputer. Dalam skenario ini, pemohon salah mengirimkan beberapa permintaan SYN. Hal ini menyebabkan komputer menunggu setiap permintaan untuk diakui, menghabiskan sumber daya hingga sambungan baru tidak dapat dibuat, dan menyebabkan penolakan layanan pada komputer.

3 SYN Flooding

SYN *Flooding* adalah serangan yang dilakukan pada jaringan komputer dengan mengirimkan sejumlah besar permintaan SYN ke server target. SYN adalah tipe pertama dari tiga langkah dalam proses pembentukan koneksi TCP/IP. Dalam serangan SYN flooding, penyerang mengirimkan permintaan SYN palsu dengan alamat IP sumber yang salah atau tidak ada niat untuk menjalankan koneksi penuh.

4. UDP Flood

User Datagram Protocol (UDP) adalah protokol Internet yang mengirim pesan ke komputer lain melalui jaringan tanpa menunggu pengakuan dari komputer target. Dalam jenis serangan DDoS ini, target dibanjiri dengan paket UDP. Tujuan dari serangan itu adalah membanjiri port acak Pada komputer sasaran. Akibatnya, komputer berulang kali memeriksaport yang diminta, dan jika port tidak ditemukan, merespons dengan informasi bahwa port tidak ditemukan (paket ICMP). Proses ini menghabiskan banyak sumber daya (CPU dan memori) di komputer Anda dandapat membuat komputer Anda tidak dapat dijangkau.[19]

2.2.9 WIRESHARK

Wireshark adalah aplikasi yang dapat menganalisis jaringan yang digunakan untuk menangkap ataupun menganalisis paket data yang dikirim melalui jaringan komputer. Dengan menggunakan Wireshark, pengguna dapat memantau lalu lintas jaringan, menganalisis protokol, dan mendapatkan

wawasan tentang berbagai aspek komunikasi dalam jaringan.Wireshark dapat digunakan untuk menganalisis paket data pada berbagai protokol jaringan seperti TCP, UDP, IP, HTTP, DNS, dan banyak lagi. Perangkat lunak ini memungkinkan pengguna untuk melihat dan menganalisis isi paket, melacak aliran data, mengidentifikasi masalah jaringan, dan mendeteksi aktivitas berbahaya seperti serangan jaringan.[20]

2.2.10 QUALITY OF SERVICE (QOS)

Kualitas layanan (QoS) merupakan suatu kinerja layanan dari yang dapat menentukan kepuasan pengguna dengan layanan. Telekomunikasi dan Internet Protocol Harmonization Over Networks (TIPHON) mengklasifikasikan kualitas QoS menjadi empat kategori berdasarkan nilai parameter QoS.[21]

1. *Throughput*

   Throughput sebenarnya diukur pada saat tertentu saat mengirim file. Meskipun satuan bandwidth sama dalam bit per detik (bps), kinerja lebih baik menggambarkan bandwidth sebenarnya pada waktu tertentu dan dalam kondisi tertentu dan jaringan yang digunakan untuk mengunduh ukuran file tertentu. Throughput adalah jumlah total paket yang terdeteksi dalam interval tertentu dibagi dengan durasi interval tersebut. Dengan persamaan tersebut, nilai daya dapat dihitung :

   Persamaan perhitungan Throughput :

   $$Throughput = \frac{\text{Paket data diterima}}{\text{Lama Pengamatan}}$$

2. *Packet loss*

   Kehilangan paket disebabkan oleh degradasi sinyal jaringan, kegagalan perangkat keras jaringan, atau bahkan radiasi lingkungan. Packet loss adalah parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah paket yang hilang yang dapat disebabkan oleh tabrakan dan kemacetan jaringan. Untuk mencari nilai packet loss dapat dihitung persamaannya :

Persamaan perhitungan Packet Loss :

$$Packet\ loss = \frac{\text{(Paket data dikirim - Paket data diterima) x 100 \%}}{\text{Paket data yang dikirim}}$$

3. *Delay*

Delay adalah waktu yang diperlukan paket data untuk dikirim dari satu komputer ke komputer tujuan. Keterlambatan pengiriman paket di jaringan komputer disebabkan oleh antrian yang panjang atau pemilihan rute yang berbeda untuk menghindari kemacetan. Keterlambatan dapat disebabkan oleh jarak, penggerak fisik, kemacetan, atau waktu pemrosesan yang lama. Tentukan delay paket yang akan dikirim dengan membagi panjang paket (unit bit) dengan bandwidth link (unit bit/s). Untuk menghitung delay rata-rata, gunakan rumus seperti ini:

Persamaan perhitungan Delay (Latency) :

Rata Rata Delay=Total Delay / Total Paket Yang DiTerima

4. Jitter

Jitter adalah variasi delay (perbedaan slot waktu) antar paket di jaringan yang disebabkan oleh antrian panjang pemrosesan data di jaringan. Nilai jitter dipengaruhi oleh beban trafik dan banyaknya tabrakan antar paket (congestion) dalam jaringan. Semakin tinggi beban trafik pada jaringan. Untuk menghitung nilai jitter gunakan Persamaan

Persamaan perhitungan Jitter :

$$Jitter = \frac{\text{Total variasi } delay}{\text{Total paket yang diterima}}$$

$$\text{Total Variasi } Delay = Delay - (\text{rata-rata } delay)$$

5. Paket Delivery Ratio (DR)

Packet delivery ratio (PDR) adalah rasio antara banyaknya paket yang diterima oleh tujuan dengan banyaknya paket yang dikirim oleh sumber. Rumus menghitung packet delivery ratio yaitu:[22]

$$PDR = \frac{paket\ data\ rx}{paket\ data\ tx}\ x\ 100\%$$