BAB 2

TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Dalam penyusunan skripsi ini, penulis banyak terinspirasi dan mereferensi dari penelitian – penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada skripsi ini. Adapun penelitian yang berhubungan dengan skripsi ini antara lain yaitu :

Tabel 2. 1 Penelitian Terkait

Penelitian 1	
Penulis	(Stephani et al., 2020)
Judul	Implementasi dan Analisis Keamanan Jaringan IDS (*Instrusion Detection System*) Menggunakan Suricata pada *Web Server*
Metode	*Web Penetration Testing*
Hasil	Pengimplementasian IDS Suricata mampu memonitoring *traffic web server* dan menyimpan hasil deteksi, mencegah ancaman yang memasuki *web server* dan mengetahui apabila terdapat aktifitas mencurigakan masuk ke *log* Suricata. Pada Penelitian ini IDS Suricata dipadukan dengan *firewall* OPNsense yang mampu mencegah anomali pada *web server* dari ancaman.
Penelitian 2	
Penulis	(Syani, 2020)
Judul	Implementasi *Instrusion Detection System* (IDS) Menggunakan Suricata pada Linux Debian 9 Berbasis *Cloud Virtual Private Servers* (VPS)
Metode	*Network Development Life Cycle* (NDLC)
Hasil	Suricata mampu menampilkan *log-log* dari hasil aktivitas yang mencurigakan secara detail dengan waktu, tanggal

	dan alamat IP yang melakukan aktivitas tersebut. Suricata juga mampu mendeteksi aktivitas mencurigakan yang berhubungan dengan jaringan.
Penelitian 3	
Penulis	(Lukman et al., 2020)
Judul	Analisis Perbandingan Kinerja Snort dan Suricata sebagai *Instrusion Detection System* Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache.
Metode	Security Policy Development Life Cycle (SPDLC)
Hasil	1. Hasil pengujian dari penelitian menggunakan parameter efektifitas serangan dari *uncaptured* paket, IDS Suricata lebih unggul dibandingkan dengan IDS Snort yang melalui pengujian sebanyak 30 kali, data yang diperoleh IDS Suricata memiliki rasio 3,42% dan IDS Snort sebanyak 68,2%. 2. Hasil Pengujian menggunakan parameter *resource* dengan melalui pengujian sebanyak 30 kali, data yang diperoleh dari rata-rata rasio penggunaan CPU Snort sebanyak 78,31% dan Suricata sebanyak 80,08%. Namun IDS Suricata lebih unggul dalam penggunaan RAM yaitu hanya 11,36% dibandingkan dengan penggunaan Snort sebanyak 23,89%.
Penelitian 4	
Penulis	(dwi et al. 2021)
Judul	Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Instrusi Lalu Lintas di Jaringan.
Metode	*Benchmarking Methodology for Network Security Device Performance draft-ietf-bmwg-ngfw-performance-01*.
Hasil	Hasil pengujian dari penelitian ini menunjukkan nilai akurasi perbandingan antara IDS Snort (31%) dan IDS

	Suricata (61%) yang diuji melalui 3 skenario. Pada 2 skenario awal Suricata memiliki waktu yang sedikit lebih lama dibanding snort karena rules yang digunakan lebih banyak. Namun, pada skenario 3 ketika jumlah rules yang digunakan sama, maka Suricata memiliki waktu deteksi yang lebih cepat daripada Snort.
Penelitian 5	
Penulis	(Jehan et al., 2021)
Judul	*Evaluation of Data Center Network Security based on Next-Generation Firewall*.
Metode	*Comparison method.*
Hasil	Hasil pengujian dari penelitian ini menunjukkan penggunaan *firewall* pfSense dan Suricata dapat mencegah serangan jaringan dari pihak internal berdasarkan skenario pengujian yang dilakukan. Dengan menggunakan *firewall* pfSense dapat meningkatkan keamanan jaringan dibandingkan hanya menggunakan *firewall* tradisonal saja seperti mikrotik.

Pada penelitian yang akan dilakukan tidak hanya berfokus pada implementasi IDS Suricata saja. Namun, juga bagaimana IDS Suricata mampu mendeteksi ancaman serangan jaringan dan mencegah merusak jaringan. Cakupan ruang lingkup pada penelitian ini juga lebih luas karena tidak hanya berfokus untuk mendeteksi satu jenis serangan jaringan saja dan meliputi jenis serangan jaringan seperti *Denial of Service* (DoS), Slowloris, dan *Nmap Scan.*

2.2. Jaringan Komputer

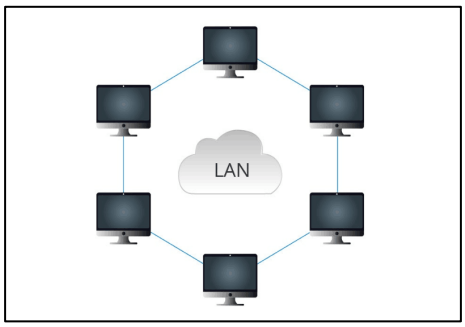
Jaringan komputer adalah kumpulan perangkat komputer yang saling terhubung untuk bertukar data dan sumber daya seperti penyimpanan data, atau koneksi internet (Ekklesia et al., 2021). Jaringan komputer dapat terdiri dari beberapa komputer yang terhubung secara langsung melalui kabel nirkabel, atau dapat terdiri dari ratusan hingga ribuan komputer yang terhubung melalui jaringan

yang lebih besar seperti internet. Jaringan komputer menungkinkan pengguna untuk berbagai informasi dan sumber daya, juga memungkinkan komunikasi dan kolaborasi antara pengguna di berbagai lokasi geografis yang berbeda. Jaringan komputer sangat penting dalam dunia digital saat ini, dan digunakan di berbagai lingkungan seperti perusahaan, institusi pendidikan, pemerintahan dan rumah tangga.

2.2.1 Jenis-jenis Jaringan Komputer

Ada beberapa Jenis jaringan komputer yang umum digunakan, diantaranya sebagai berikut (Buttu, 2023) :

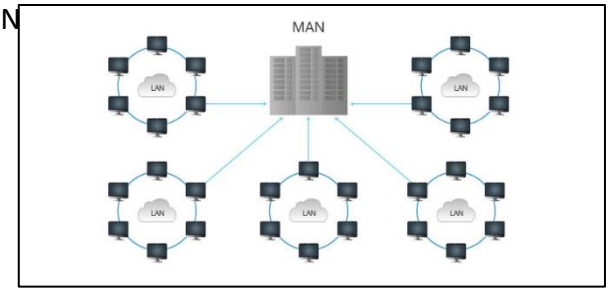
1. *Local Area Network* (LAN) : Jaringan area lokal adalah jaringan yang mencakup area terbatas seperti gedung atau kampus.



Gambar 2. 1 Local Area Network
(Sumber : community.fs.com)

Jaringan ini biasanya digunakan untuk menghubungkan perangkat dalam suatu organisasi atau perusahaan, dan memungkinkan berbagai sumber daya seperti *printer*, *scanner*, dan penyimpanan data.

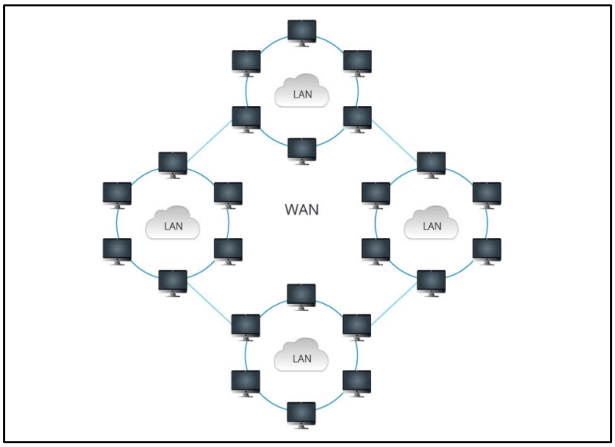
2. *Metropolitan Area Network* (MAN) : Jaringan area metropolitan adalah jaringan yang mencakup area yang lebih luas dari LAN, seperti kota atau wilayah. Jaringan ini biasanya digunakan untuk menghubungkan beberapa jaringan LAN



Gambar 2. 2 Metropolitan Area Network

(Sumber : community.fs.com)

3. *Wide Area Network* (WAN) : jaringan area luas adalah jaringan yang mencakup area yang sangat luas, bahkan melintasi negara atau benua.



Gambar 2. 3 Wide Area Network

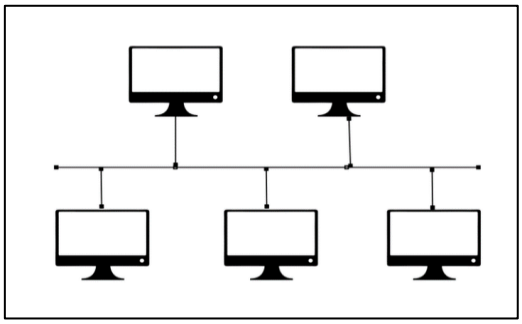
(Sumber : community.fs.com)

Jaringan ini biasanya digunakan untuk menghubungkan lokasi yang terpisah secara geografis dan memungkinkan akses ke sumber daya dan layanan dari berbagai lokasi yang berbeda.

2.2.2 Jenis-jenis Topologi Jaringan

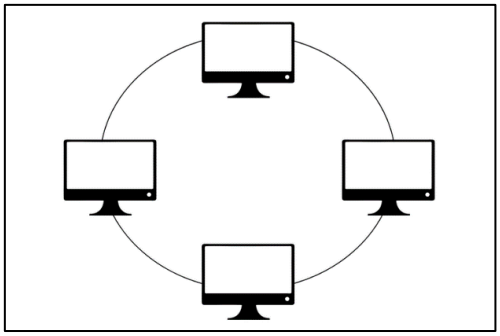
Topologi Jaringan adalah susunan atau tata letak fisik dari perangkat-perangkat jaringan komputer yang terhubung satu sama lain untuk memungkinkan komunikasi data. Topologi jaringan dapat diatur sedemikian rupa sehingga memberikan tingkat efisien dan kinerja yang optimal. Ada beberapa jenis topologi Jaringan yang umum digunakan, diantaranya sebagai berikut (Daegama et al., 2022) :

1. Topologi *Bus* : topologi jaringan yang menggunakan kabel tunggal sebagai jalur komunikasi, dan setiap perangkat terhubung ke kabel utama. Sinyal data dikirim melalui kabel utama dan diterima oleh semua perangkat yang terhubung ke jaringan.



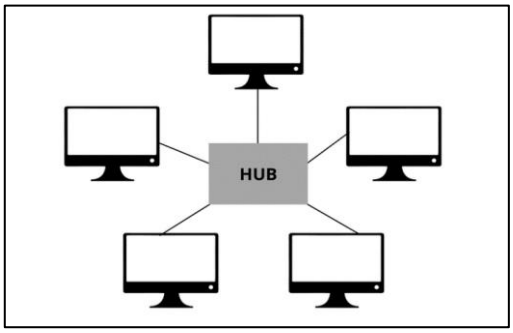
Gambar 2. 4 Topologi Bus
(Sumber : tekno.kompas.com)

2. Topologi *Ring* : pada topologi jaringan ini dihubungkan dalam sebuah bentuk lingkaran atau cincin. Data dikirim melalui jalur lingkaran, dan setiap perangkat berikutnya sampai data mencapai tujuan.



Gambar 2. 5 Topologi Ring
(Sumber : tekno.kompas.com)

3. Topologi *Star* : pada topologi jaringan ini, setiap perangkat dihubungkan ke pusat server menggunakan kabel sendiri. Data dikirim melalui server, yang kemudian mengirimkannya ke perangkat tujuan.



Gambar 2. 6 Topologi Star
(Sumber : tekno.kompas.com)

2.3 Protokol Jaringan

Protokol jaringan adalah aturan atau standar yang digunakan oleh komputer atau perangkat lain dalam jaringan komputer untuk berkomunikasi satu sama lain. Protokol jaringan mendefinisikan format data, pesan, dan tindakan yang diperlukan untuk mengirim dan menerima data melalui jaringan.

Protokol jaringan memungkinkan komputer dan perangkat lain dalam jaringan untuk berkomunikasi dan berinteraksi dengan satu sama lain dengan cara yang terorganisir dan terstruktur. Protokol jaringan juga membantu untuk memastikan keamanan dan privasi data yang dikirimkan melalui jaringan. Beberapa contoh protokol jaringan yang umum digunakan diantaranya adalah sebagai berikut (Pratama & Dharmesta, 2019).

2.3.1. TCP/IP (*Transmission Control Protocol/Internet Protocol)*

TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah kombinasi dari dua protokol yang paling penting dalam jaringan komputer, yaitu TCP (*Transmission Control Protocol*) dan IP (*Internet Protocol*). TCP adalah protokol yang bertanggung jawab untuk mengatur pengiriman data secara terurut, memastikan bahwa data yang dikirimkan diterima dengan baik dan memastikan koneksi yang stabil antara pengirim dan penerima data.

Sementara itu, IP adalah protokol yang digunakan untuk mengirimkan paket data dari satu komputer ke komputer lain melalui jaringan. IP bertanggung jawab untuk mengatur pengiriman data dalam bentuk paket-paket data yang dikirimkan dari satu alamat IP ke alamat IP lainnya. Dengan menggunakan kombinasi protokol TCP/IP, komputer dan perangkat lain dapat saling berkomunikasi dan bertukar data secara handal dan terstruktur melalui jaringan komputer. TCP/IP digunakan secara luas dalam berbagai aplikasi dan layanan jaringan, seperti web browsing, email, transfer file, dan masih banyak lagi.

2.3.2. UDP (*User Datagram Protocol*)

UDP (*User Datagram Protocol*) adalah salah satu protokol transport dalam jaringan komputer yang digunakan untuk mengirimkan data tanpa adanya koneksi antara pengirim dan penerima data. UDP bekerja pada layer transport dalam

model OSI (*Open Systems Interconnection)* dan tidak menjamin pengiriman data yang handal dan teratur seperti pada protokol TCP.

UDP adalah protokol yang lebih sederhana dan cepat dibandingkan dengan TCP, namun kurang handal karena tidak memiliki mekanisme *error checking* dan retransmission. Oleh karena itu, UDP sering digunakan untuk aplikasi yang membutuhkan pengiriman data yang cepat dan efisien, seperti video dan audio *streaming*, *game online*, dan aplikasi VoIP (*Voice over* IP).

Meskipun tidak menjamin pengiriman data yang handal, UDP memiliki keunggulan dalam hal kecepatan karena tidak memerlukan waktu untuk membuat koneksi dan tidak melakukan verifikasi ulang setiap paket data yang dikirimkan.

2.3.3. ICMP (*Internet Control Message Protocol*)

ICMP (*Internet Control Message Protocol*) adalah protokol yang digunakan untuk mengirimkan pesan error atau pesan kontrol lainnya antara perangkat dalam jaringan komputer. ICMP bekerja pada layer network dalam model OSI (*Open Systems Interconnection*) dan digunakan oleh perangkat-perangkat jaringan seperti router dan *firewall* untuk mengirimkan pesan error atau informasi kontrol lainnya ke perangkat lain dalam jaringan.

Contoh penggunaan ICMP antara lain adalah ketika ada paket data yang tidak dapat dihantar ke tujuan karena alamat IP tujuan tidak ditemukan atau tidak dapat dijangkau, maka perangkat jaringan akan mengirimkan pesan ICMP kepada pengirim untuk memberitahukan bahwa pengiriman data tidak berhasil.

Selain itu, ICMP juga digunakan untuk menguji konektivitas jaringan dan mendeteksi masalah jaringan. Sebagai contoh, perangkat jaringan dapat menggunakan protokol ICMP dengan mengirimkan paket ping ke perangkat lain dalam jaringan untuk menguji apakah perangkat tersebut dapat dijangkau atau tidak.

Meskipun ICMP tidak digunakan secara langsung oleh aplikasi jaringan seperti TCP dan UDP, namun ICMP merupakan protokol yang sangat penting dalam jaringan komputer karena membantu dalam mengidentifikasi dan menangani masalah jaringan.

2.4 Keamanan Jaringan

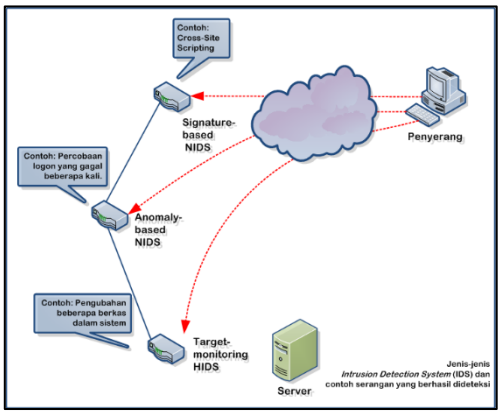
Keamanan jaringan merupakan perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer agar tidak dihancurkan, diubah agar sistem komputer mampu beroperasi dengan baik dan teratur. Keamanan jaringan komputer terdiri dari beberapa aspek penting yaitu perangkat lunak, perangkat keras jaringan, layanan *internet of things* (IoT) dan sumber daya. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer (Munawar et al., 2020) :

1. Kesalahan Informasi *Internet of Things* – biasanya terjadi ketika data yang dihasilkan oleh perangkat IoT tidak akurat, tidak lengkap, atau tidak dikelola dengan benar. Hal ini dapat terjadi karena beberapa faktor, seperti masalah pada perangkat keras, kesalahan pengukuran atau pengiriman data, atau masalah pada perangkat lunak yang mengelola data tersebut.
2. Serangan pada layanan latar belakang – serangan atau ancaman keamanan terhadap layanan yang berjalan secara otomatis di latar belakang pada sistem operasi. Layanan latar belakangan digunakan untuk melakukan tugas-tugas tertentu, seperti sinkronisasi data atau pembaruan otomatis, dan biasanya dijalankan tanpa interaksi pengguna.
3. Kehancuran integritas keamanan jaringan – ancaman keamanan jaringan terhadap integritas keamanan jaringan terjadi ketika keaslian atau otentikasi data dan sistem terganggu oleh akses yang tidak sah atau tindakan yang merusak. Conthnya, penjahat siber dapat mengubah data, merusak *file* sistem atau mengambil alih kontrol sistem, sehingga mengakibatkan kerugian yang signifikan dan bahkan dapat mengancam keseluruhan keberlangsungan bisnis atau organisasi.
4. Memberitahukan informasi komputer – saat informasi dalam jaringan komputer ditransmisikan secara langsung ke entitas yang tidak sah tanpa izin dari pengguna, maka sudah pasti informasi menjadi rentan.

2.5 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah teknologi yang digunakan untuk mengidentifikasi dan merespon aktivitas yang mencurigakan atau berpotensi berbahaya di dalam jaringan komputer atau sistem informasi. Tujuannya adalah untuk melindungi sistem dari ancaman keamanan seperti peretasan, serangan *malware*, dan kebocoran data. Ada dua tipe dasar yang terdapat dalam IDS (Alamsyah et al., 2020) :

1. *Host-based* IDS : Sistem deteksi instrusi yang diinstal pada sebuah host atau komputer individu untuk memonitor aktivitas di dalamnya, termasuk kegiatan pengguna dan aplikasi yang berjalan di *host* tersebut.
2. *Network-based* IDS : Sistem deteksi instrusi yang memantau lalu lintas jaringan dan mencari pola aktivitas yang mencurigakan atau berpotensi berbahaya, seperti serangan *Denial of Service* (DoS) atau pemindaian *port* yang mencurigakan.



Gambar 2. 7 Instrusion Detection System (IDS)
(Sumber : id.wikipedia.org)

2.5.1 Anomaly Based IDS

Anomaly Based IDS adalah jenis sistem deteksi intrusi yang mengidentifikasi serangan jaringan dengan mencari anomali atau perilaku yang tidak biasa pada lalu lintas jaringan. Sistem ini mencoba untuk memahami "normal" dan "tidak normal" dari pola lalu lintas jaringan dan mencari tanda-tanda aktivitas jaringan yang tidak sesuai dengan pola normal tersebut.

Dalam *Anomaly based* IDS, sebuah model atau profil digunakan untuk merepresentasikan perilaku normal dari jaringan atau *host* tertentu, dan IDS akan

membandingkan lalu lintas jaringan aktual dengan profil ini untuk mencari perilaku yang tidak biasa atau mencurigakan. IDS ini dapat mempelajari pola lalu lintas jaringan seiring waktu, dan secara otomatis mengubah profil atau model jika pola lalu lintas jaringan yang normal berubah.

Salah satu keuntungan dari *Anomali based* IDS adalah kemampuannya untuk mendeteksi serangan yang tidak diketahui sebelumnya atau serangan baru yang belum diketahui oleh sistem deteksi intrusi berbasis tanda tangan. Namun, demikian, ia juga dapat menghasilkan sejumlah besar *false positive* jika ada perubahan yang signifikan dalam pola lalu lintas jaringan yang dianggap sebagai ancaman oleh sistem. Oleh karena itu, perlu dilakukan analisis lebih lanjut untuk membedakan aktivitas jaringan yang sebenarnya mencurigakan dari kegiatan jaringan yang sah.

2.5.2 Signature Based IDS

Signature based IDS adalah jenis sistem deteksi intrusi yang mencari serangan jaringan dengan membandingkan pola lalu lintas jaringan yang ada dengan *database* tanda tangan atau *signature* serangan yang telah diketahui sebelumnya. Sistem ini mencoba untuk menemukan tanda-tanda yang sesuai dengan tanda-tangan serangan yang ada di dalam database untuk mengidentifikasi dan melaporkan serangan yang ada.

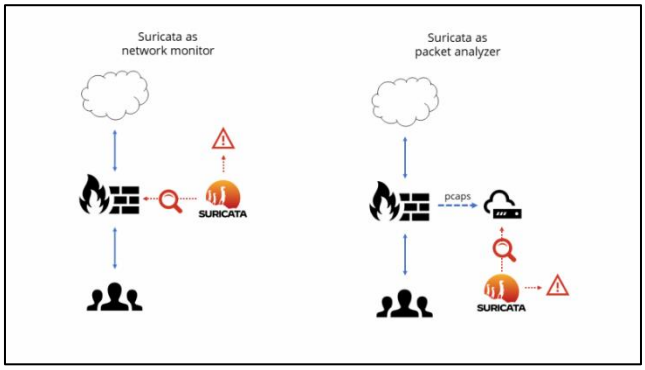
Signature based IDS sering menggunakan aturan atau *rule-based detection* yang mencocokkan pola lalu lintas jaringan yang ada dengan tanda-tangan serangan yang telah diketahui sebelumnya. Ketika ada pola lalu lintas jaringan yang cocok dengan tanda-tangan serangan dalam *database*, IDS akan mengidentifikasi aktivitas tersebut sebagai serangan dan memberikan peringatan kepada administrator jaringan atau melakukan tindakan lain sesuai dengan konfigurasi yang telah ditentukan.

Keuntungan dari *Signature based* IDS adalah dapat mengidentifikasi serangan yang telah diketahui dan terdokumentasi dengan baik, dan memberikan tindakan yang tepat untuk melindungi jaringan. Namun, kelemahannya adalah tidak dapat mendeteksi serangan baru atau tidak diketahui yang tidak cocok

dengan tanda-tangan serangan yang ada dalam *database.* Selain itu, seringkali *Signature based* IDS menghasilkan banyak *false positive* jika ada pola lalu lintas jaringan yang mirip dengan tanda-tangan serangan, tetapi sebenarnya merupakan aktivitas jaringan yang sah.

2.6. Suricata

Suricata adalah *Intrusion Detection System* (IDS) yang *bersifat open source*. Suricata melakukan analiasis lalu lintas jaringan dengan memeriksa paket data yang melewati jaringan, kemudian membandingkan informasi paket dengan aturan atau *rules* yang telah ditentukan sebelumnya.



Gambar 2. 8 Suricata
(Sumber : www.qacafe.com)

Jika paket data cocok dengan *rules* yang sudah ditentukan, suricata akan memicu pencegahan yang telah diprogram, seperti memberikan peringatan atau *alert* dan memblokir koneksi. Suricata dapat diintegritaskan dengan sistem manajeman keamanan jaringan untuk memungkinkan pencatatan dan analisis lebih lanjut atas laporan keamanan dan peringatan yang dikeluarkan. Suricata mampu melakukan deteksi otomatis pada layer 7 yaitu aplikasi seperti dns, *http*, *imap*, *ftp*, dan *smtp* (Syani, 2020).

2.7. Metode Serangan

Metode serangan berguna untuk menguji sistem dapat bekerja dengan baik sebagai berikut :

2.7.1. Denial of Service (DoS)

Denial of Service (DoS), atau sering disebut serangan penolakan layanan, adalah upaya yang dilakukan oleh penyerang untuk membuat sasaran (sistem

komputer, jaringan, atau layanan *online*) tidak dapat diakses oleh pengguna yang sah. Tujuan utama dari serangan DoS adalah untuk menyebabkan gangguan atau penurunan kinerja yang signifikan, bahkan hingga membuat sistem tersebut menjadi tidak responsif.

2.7.2 Slowloris

Slowloris adalah sebuah alat yang digunakan untuk melakukan serangan terhadap *server web* dengan cara memanfaatkan keterbatasan pemrosesan paralel pada server. Alat ini membuka ribuan koneksi *HTTP POST* dan secara perlahan mengirimkan *header HTTP* dengan sangat lambat, dengan tujuan memaksa *server web* target untuk terus mempertahankan koneksi terbuka. Koneksi-koneksi tersebut tidak pernah diselesaikan sehingga *server web* target kehabisan sumber daya untuk melayani permintaan dari klien yang sah atau klien yang ingin mengakses *server* tersebut.

Dampak dari serangan Slowloris adalah memblokir akses klien yang sah dan mengganggu kinerja *server web* target. Dengan menjaga koneksi terbuka secara terus-menerus, serangan ini menghabiskan sumber daya *server* dan menghambat kemampuan *server* untuk melayani permintaan klien yang valid. Dengan demikian, serangan Slowloris dapat menyebabkan penurunan kinerja atau bahkan keruntuhan layanan web.

Dalam konteks keamanan jaringan, serangan Slowloris merupakan salah satu bentuk serangan *Denial of Service* (DoS) yang bertujuan untuk melumpuhkan *server* dengan memanfaatkan keterbatasan sumber daya *server* tersebut. Oleh karena itu, langkah-langkah pencegahan yang tepat harus diambil untuk melindungi *server web* dari serangan Slowloris, seperti melakukan pembaruan perangkat lunak, menerapkan pembatasan koneksi, memantau lalu lintas jaringan, dan menggunakan solusi IDS/IPS yang dapat mendeteksi pola serangan Slowloris.

2.7.3 Nmap Scan

NMAP (*Network Mapper*) adalah sebuah perangkat lunak yang digunakan untuk pemetaan jaringan dan pemindaian keamanan. *Nmap scan* adalah proses

pemindaian yang dilakukan menggunakan perangkat lunak Nmap untuk mengidentifikasi dan memeriksa *host, port*, layanan, serta mengumpulkan informasi penting terkait dengan keamanan jaringan.

Pada dasarnya, *Nmap scan* memanfaatkan serangkaian teknik pemindaian yang dapat memberikan wawasan mendalam tentang jaringan yang sedang diuji. Dalam pemindaian ini, Nmap dapat melakukan berbagai jenis pemindaian, seperti pemindaian *port*, pemindaian versi layanan, pemindaian kerentanan, pemindaian OS, dan lain sebagainya.

Proses *Nmap scan* dimulai dengan memilih target jaringan yang akan dipindai, baik itu IP tunggal, kisaran IP, subnet, atau nama domain. Kemudian, Nmap akan mengirimkan serangkaian paket ke *hos*t-target menggunakan protokol TCP/IP atau UDP. Nmap akan menganalisis respons dari *host*-target untuk mengidentifikasi *host* yang aktif, *port* yang terbuka, layanan yang berjalan, serta versi perangkat lunak yang digunakan.

2.7.4 PingFlood

Pingflood adalah serangan jaringan yang bertujuan mengganggu ketersediaan (denial of service) atau menyebabkan penurunan kinerja pada jaringan atau sistem komputer dengan membanjiri target dengan paket ICMP echo request (ping). ICMP (Internet Control Message Protocol) adalah protokol yang digunakan untuk mengirim pesan kontrol dan kesalahan dalam jaringan IP.

Pada serangan pingflood, penyerang mengirimkan sejumlah besar permintaan ping ke alamat IP target secara berulang-ulang. Setiap permintaan ping meminta balasan dari target dengan mengirimkan paket echo request dan menunggu balasan echo reply. Dengan mengirimkan sejumlah besar permintaan ping dalam waktu singkat, penyerang membanjiri kapasitas jaringan target dan membuatnya tidak mampu menangani permintaan secara efisien.

2.8. Security Policy Development Life Cycle (SPDLC)

Security Policy Development Life Cycle (SPDLC) adalah serangkaian tahapan yang dirancang untuk membantu organisasi dalam mengembangkan kebijakan

keamanan jaringan yang lebih efektif (Santoso, 2019). Berikut adalah 5 tahapan yang ada pada metode SPDLC (Jufri & Heryanto, 2021) :

1. *Analysis* : Pada tahapan ini dilakukan perumusan masalah dan pengumpulan data berupa informasi IDS dalam peningkatan keamanan jaringan dan serangan yang terjadi. Hasil informasi yang di dapatkan dijadikan sebagai landasan dalam pemecehan masalah.
2. *Desain* : Pada tahapan ini dilakukan perancangan berupa topologi jaringan yang akan dibangun dan rancangan sistem operasi yang akan digunakan.
3. *Implementation* : Pada tahapan ini dilakukan implementasi dari rancangan topologi yang sudah dibangun pada tahapan sebelumnya yaitu dengan melakukan instalasi perangkat yang dibutuhkan dan melakukan konfigurasi *Software* yang diperlukan.
4. *Enforcement* : Pada tahapan ini akan dilakukan pengujian sistem dimana akan dilakukan pengamatan terhadap sistem yang sudah dibangun dan diterapkan apakah sistem sudah berjalan dengan baik dan benar.
5. *Enchancement* : Pada tahapan ini dilakukan perbaikan sistem yang telah dibangun meliputi peningkatan fungsional atas komponen dan spesifik dan melakukan pembaruan sistem.