BAB 2

LANDASAN TEORI

2.1. Penelitian Terkait

Dalam penyusunan skripsi ini, terdapat tinjauan pustaka dari penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada skripsi. Adapun penelitian yang dijadikan sebagai referensi penelitian saat ini, yaitu :

Tabel 2. 1 Penelitian Terkait

Penelitian 1	
Penulis (Tahun)	(Iqbal et al., 2020)
Judul	Analisa Dan Simulasi Keamanan Jaringan Ubuntu Server Dengan Port Knocking, Honeypot, Iptables, ICMP
Metode	NDLC (*Network Development Life Cycle*)
Hasil	Pada penelitian ini menggunakan *honeypot* sebagai *server* tiruan pada metode *port knocking*, dapat mengalihkan *port service* kepada *fake port* yang dibuat oleh *honeypot,* dan penggunaan *Iptables* dapat membloking *incoming packet* sehingga *port service* tidak akan terbuka.
Penelitian 2	
Penulis (Tahun)	(Sulaksono & Suharyanto, 2020)
Judul	Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server
Metode	VPN *(Virtual private Network)*
Hasil	Pada penelitian ini telah berhasil mengimplementasikan *cowrie* dan *honeypot* yang diterapkan sebagai mekanisme pertahanan atas penyerangan yang dilakukan oleh attacker.
Penelitian 3	
Penulis (Tahun)	(Siregar & Dermawati, 2020)

Judul	Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik Uniks Menggunakan Dionaea Sebagai Keamanan Jaringan
Metode	Honeypot Dionea
Hasil	Pada penelitian ini *Honeypot Dionea* dapat mendekteksi 63 dari 70 jenis antivirus yang bisa mendeteksi *malware* yang sejenis *worm*, yang akan memanfaatkan kerentanan dalam layanan *Microsoft Windows Server* untuk menginfeksi komputer dalam jaringan. *Honeypot dionaea* dapat mencatat banyak trafik yang terkoneksi dengan server kemudian menganalisis agar dapat membloking *malware.*
Penelitian 4	
Penulis (Tahun)	(Amal & Venkadesh, 2023)
Judul	H-DOCTOR: Honeypot based firewall tuning for attack prevention
Metode	Hybrid H -doctor
Hasil	Penelitian ini menggunakan tools Docker untuk menguji akurasi deteksi sistem yang menggunakan honeypot maupun tidak. Hasil dari penelitian ini menunjukkan akurasi yang mencapai Hylnt 73,25%, IDS 76,75% dan IDS berbasis honeypot 81,25%.
Penelitian 5	
Penulis (Tahun)	(Wilman et al., 2018)
Judul	Port Knocking Dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual
Metode	*Port Knocking* dan *Honeypot*
Hasil	Hasil dari penelitian ini, *Port Knocking* dan *Honeypot* mampu untuk mengamankan *server* dengan cara mengalihkan attacker kedalam sistem *honeypot* dan

	memonitoring aktifitas yang dilakukan attacker selama berada diserver bayangan.

Pada penelitian sebelumnya, salah satu teknologi yang digunakan dalam penelitian tersebut adalah firewall jenis *Iptables*. Firewall ini untuk memantau dan mengatur lalu lintas jaringan yang masuk dan keluar dari sistem, serta memastikan bahwa hanya lalu lintas yang diizinkan yang dapat melalui firewall tersebut.

Namun, pada penelitian yang akan dibahas kali ini, akan menggunakan firewall jenis *pfSense*. *PfSense* merupakan salah satu firewall *open source* yang digunakan untuk mengamankan jaringan serta fitur-fitur yang cukup lengkap untuk memantau dan mengatur lalu lintas jaringan, seperti *stateful packet filtering*, *intrusion detection/prevention system* (IDS/IPS), dan *virtual private network* (VPN).

2.2. Keamanan Jaringan

Keamanan jaringan komputer adalah suatu sistem keamanan yang bekerja untuk mendeteksi dan mencegah aktifitas dari pengguna yang tidak memiliki hak akses dalam suatu jaringan. Informasi yang terdapat pada komputer yang memiliki akses internet rentan terhadap serangan attacker sehingga dapat memungkinkan untuk mengakses data, merubah data, sampai dengan menghapus data dalam jaringan internet tersebut (Al Fikri & Djuniadi, 2021).

Gambar 2. 1 Keamanan Jaringan Komputer
Sumber : www.itgid.com

Terdapat dua elemen penting dalam pembentukan keamanan jaringan, yaitu :

1. Pembatas keamanan yang berfungsi sebagai perlindungan terhadap serangan, baik itu menurut fisik (nyata) atau virtual (software).
2. Rancangan keamanan yang berguna untuk membangun sistem pada perangkat guna untuk menjaga agar sistem tidak terdapat gangguan dari luar jaringan.

Faktor penting yang wajib diterapkan dalam membangun keamanan jaringan pada komputer, yaitu

1. *Confidentiality* (Kerahasiaan)

   Informasi yang ada pada sistem bersifat rahasia maka dari itu perangkat hanya boleh diakses oleh orang yang berhak.
2. *Authentication* (Autentifikasi)

   Pengguna wajib untuk membuktikan identitas jika ingin mengakses data pada sistem komputer untuk validasi pada perangkat guna menghindari pemalsuan pengguna.
3. *Integrity* (Integritas)

   Informasi pada sistem hanya pihak berwenang yang dapat mengubah atau menghapus data.
4. *Availability* (Ketersediaan Data)

   Informasi pada sistem harus tersedia bagi pihak yang berwenang.
5. *Access Control* (Pengaturan Akses)

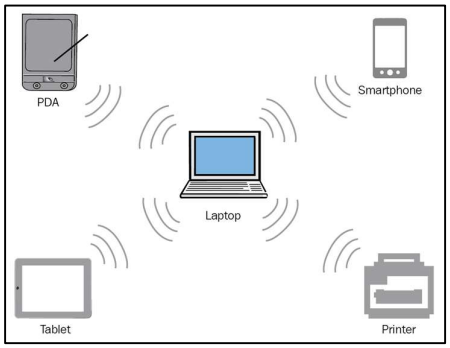
   Informasi (data) pada sistem hanya akan diberikan kepada pihak yang berwenang.

2.3. Klasifikasi Jaringan

Klasifikasi jaringan mengelompokkan atau pembagian jaringan berdasarkan berbagai kriteria tertentu. Klasifikasi jaringan digunakan untuk mempermudah pemahaman dan pengelolaan jaringan, serta membantu dalam pemilihan terknologi jaringan yang sesuai dengan kebutuhan. Klasifikasi jaringan juga berguna dalam memudahkan komunikasi dan berbagi sumber daya antara pengguna dan perangkat di dalam jaringan.

2.3.1. Personal Area Network (PAN)

Personal Area Network (PAN) adalah jaringan komputer yang mencakup area yang sangat kecil, biasanya terdiri dari perangkat-perangkat yang berada dalam jarak yang sangat dekat, seperti dalam jangkauan personal, seperti perangkat dalam satu ruangan atau perangkat yang dipakai oleh satu orang. PAN dirancang untuk memungkinkan pengguna menghubungkan perangkat-perangkat kecil, seperti smartphone, tablet, laptop, headset, dan perangkat lainnya, secara nirkabel melalui teknologi seperti Bluetooth, Infrared, Wi-Fi Direct, atau Near Field Communication (NFC). Dalam PAN, perangkat-perangkat dapat saling berkomunikasi dan bertukar data dengan cepat dan mudah, sehingga memudahkan pengguna untuk mengelola, memindahkan, dan membagikan data antar perangkat dengan mudah (Astrid Noviriandini et al., 2022).

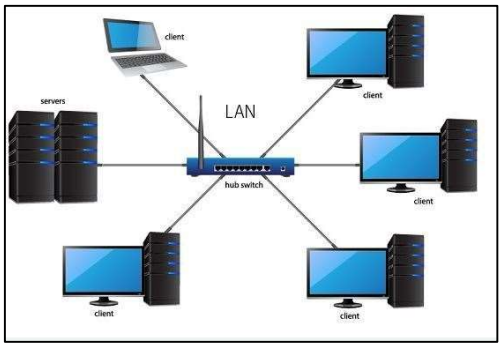


Gambar 2. 2 Personal Area Network (PAN)
Sumber : www.jagad.id.com

2.3.2. Local Area Network (LAN)

Local Area Network (LAN) adalah jaringan komputer yang terbatas pada area yang relatif kecil, seperti di dalam gedung, kampus, atau area perkantoran. LAN biasanya digunakan untuk menghubungkan beberapa perangkat komputer, seperti PC, printer, server, dan perangkat lainnya, sehingga pengguna dapat berbagi sumber daya, seperti file, data, aplikasi, dan perangkat keras (hardware) lainnya. LAN dapat menggunakan teknologi jaringan kabel atau nirkabel, seperti Ethernet, Wi-Fi, dan Bluetooth. LAN memiliki kecepatan transfer data yang tinggi

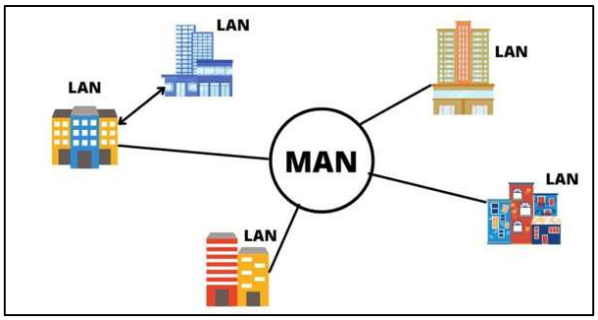
dan keamanan yang baik, karena jaringan hanya digunakan oleh pengguna yang memiliki akses terbatas ke jaringan (Desmira et al., 2022).



Gambar 2. 3 Local Area Network (LAN)
Sumber : www.dataglobal.co.id

2.3.3. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) adalah jaringan komputer yang mencakup area yang lebih luas daripada Local Area Network (LAN) tetapi lebih kecil daripada Wide Area Network (WAN). Area yang dicakup oleh MAN biasanya mencakup kota atau wilayah yang cukup besar, seperti kampus, kompleks perumahan, atau kawasan industri. MAN biasanya digunakan oleh organisasi atau perusahaan yang memiliki beberapa kantor atau lokasi di suatu kota atau wilayah tertentu dan membutuhkan jaringan yang efisien dan cepat untuk menghubungkan lokasi-lokasi tersebut (Astrid Noviriandini et al., 2022).

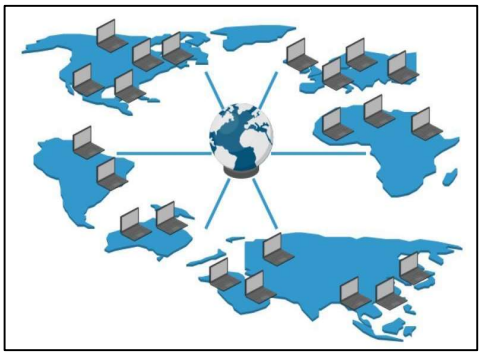


Gambar 2. 4 Metropolitan Area Network (WAN)

2.3.4. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jenis jaringan komputer yang mencakup area yang sangat luas, seperti negara, benua, atau bahkan seluruh dunia. WAN terdiri dari beberapa jaringan lokal (LAN) yang saling terhubung melalui perangkat

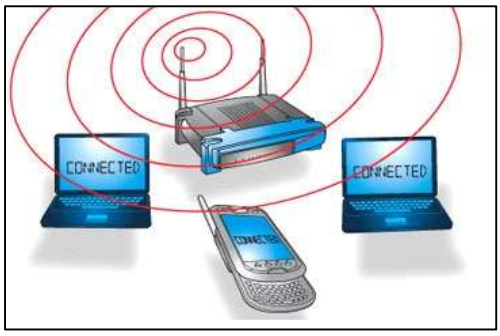
jaringan seperti router dan switch. WAN umumnya digunakan oleh organisasi besar atau perusahaan yang memiliki kantor cabang yang tersebar di beberapa lokasi yang jauh dan ingin terhubung ke jaringan pusat untuk mengakses sumber daya dan layanan yang sama. Contoh dari WAN termasuk Internet, jaringan seluler, dan jaringan satelit (Astrid Noviriandini et al., 2022).



Gambar 2. 5 Wide Area Network (WAN)
Sumber : www.diengcyber.com

2.3.5. Jaringan Tanpa Kabel

Jaringan tanpa kabel atau disebut juga dengan jaringan nirkabel (wireless network) adalah jenis jaringan komputer yang menggunakan teknologi transmisi data tanpa kabel atau kabel fisik. Jaringan nirkabel memungkinkan perangkat seperti laptop, smartphone, tablet, atau perangkat lain terhubung ke jaringan internet atau jaringan lokal tanpa harus menggunakan kabel (Astrid Noviriandini et al., 2022). Teknologi nirkabel menggunakan sinyal radio atau inframerah untuk mengirim dan menerima data antara perangkat-perangkat tersebut. Beberapa jenis jaringan nirkabel yang umum digunakan adalah WiFi, Bluetooth, dan 3G/4G/LTE. Keuntungan dari jaringan tanpa kabel adalah mobilitas dan fleksibilitas yang lebih tinggi karena perangkat-perangkat dapat bergerak bebas tanpa terbatas oleh kabel.



Gambar 2. 6 Jaringan Tanpa Kabel
Sumber : www.catatanshand.blogpsot.com

2.4. Perangkat Jaringan

Perangkat jaringan merujuk pada perangkat keras (hardware) yang digunakan untuk menghubungkan, mengelola, dan memfasilitasi komunikasi data antara perangkat lain dalam sebuah jaringan komputer. Perangkat jaringan dapat berupa perangkat fisik seperti switch, router, hub, access point, modem, gateway, firewall, dan server, serta perangkat virtual seperti virtual switch, virtual router, dan virtual firewall. Setiap perangkat jaringan memiliki fungsinya masing-masing untuk memastikan bahwa data dapat dikirim dan diterima dengan aman dan efisien dalam jaringan.

Gambar 2. 7 Perangkat Jaringan
Sumber : www.ilmugratis.blogspot.com

2.4.1. Ethernet Card

Ethernet Card atau kartu jaringan Ethernet adalah sebuah perangkat keras yang dipasang di dalam komputer atau perangkat jaringan lainnya, yang berfungsi untuk menghubungkan perangkat tersebut ke jaringan Ethernet. Ethernet Card mengubah sinyal digital yang dihasilkan oleh komputer atau perangkat jaringan lainnya menjadi sinyal analog yang dapat ditransmisikan melalui kabel jaringan

Ethernet. Ethernet Card juga bertanggung jawab untuk mengatur protokol dan pengiriman data antara perangkat yang terhubung ke jaringan.

2.4.2. Switch

Switch adalah salah satu perangkat jaringan komputer yang digunakan untuk menghubungkan beberapa perangkat jaringan dalam sebuah jaringan lokal atau LAN (Local Area Network). Fungsinya adalah untuk mempercepat dan mempermudah proses pengiriman data antara perangkat yang terhubung di dalam jaringan tersebut. Switch bekerja dengan cara meneruskan paket data ke perangkat tujuan yang tepat dengan menggunakan alamat MAC (Media Access Control) yang terkandung dalam paket data tersebut. Dalam sebuah jaringan LAN, switch menjadi perangkat yang sangat penting karena mampu meminimalkan konflik alamat dan mempercepat proses komunikasi antar perangkat di dalam jaringan tersebut (Yousif. & K.Al-Saffar., 2018).

2.4.3. Router

Router adalah perangkat jaringan yang digunakan untuk menghubungkan dua atau lebih jaringan komputer dan mengirimkan paket data antara mereka. Router dapat digunakan untuk menghubungkan jaringan komputer di rumah atau kantor, jaringan Internet, dan bahkan jaringan global seperti Internet. Fungsi utama router adalah untuk memproses dan meneruskan data paket antara jaringan, serta untuk memilih jalur terbaik untuk mengirim paket data dari sumber ke tujuan (Yousif. & K.Al-Saffar., 2018).

2.4.4. Modem

Modem yang sering digunakan berfungsi untuk mengubah sinyal digital menjadi sinyal analog, atau sebaliknya, untuk memungkinkan komunikasi data antara perangkat elektronik seperti komputer, laptop, atau router dengan jaringan telepon atau jaringan kabel.

2.5. NDLC (Network Development Life Cycle)

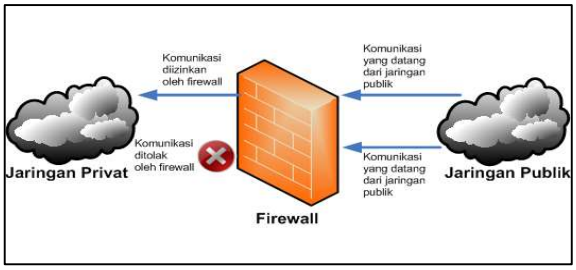
NDLC (Network Development Life Cycle) adalah sebuah metodologi yang digunakan dalam pengembangan jaringan komputer yang mancakup serangkaian tahap atau langkah-langkah yang harus dilakukan untuk membangun dan

mengembangkan jaringan yang aman dan efektif (Nurdadyansyah & Hasibuan, 2021). Metode NDLC terdiri dari empat tahapan utama, yaitu :

1. Analisa Kebutuhan : Tahapan perencanaan atau analisa kebutuhan untuk penentuan desain jaringan pemilihan teknologi yang tepat.
2. Desain : Setelah melakukan analisis kebutuhan, pada tahapan ini dilakukan perancangan jaringan, termasuk desain topologi, pemilihan perangkat keras (hardware) dan lunak (software).
3. Simulasi Prototype : Pada tahap ini akan membuat sistem jaringan dalam bantuk simulasi yang bertujuan untuk melihat kinerja sistem yang dibangun sesuai dengan kebutuhan.
4. Implementasi : Tahapan ini untuk membangun jaringan sesuai dengan desain yang telah dibuat pada tahap-tahap sebelumnya.

2.6. Firewall

Firewall adalah garis pertahanan pertama melawan ancaman eksternal ke jaringan internal. Firewall sebenarnya adalah penghalang yang mencegah attacker dari suatu sistem ke sistem yang lain. Untuk menjauhkan attacker dari jaringan komputer, harus memasang dan mengkonfigurasi firewall internet untuk memisahkan jaringan eksternal yang tidak dipercaya dari jaringan komputer internal terpecaya (Sulaman, 2011).



Gambar 2. 8 Firewall
Sumber : www.aptika.kominfo.go.id

2.6.1. Fungsi Dasar Firewall

Ketika traffic sampai di firewall, firewall akan memutuskan jaringan yang ijinkan maupun yang tidak bedasarkan pada aturan pada rules yang telah dibuat. Berikut fungsi dasar dari firewall, yaitu :

1. Mengatur dan mengontrol traffic jaringan
2. Melakukan autentifikasi terhadap akses
3. Melindungi sumber informasi dalam jaringan privat
4. Mencatat semua kejadian dan melaporkan kepada administrator

2.6.2. Klasifikasi Firewall

Fungsi dasar dari firewall untuk melindungi komputer dari internal maupun eksternal. Firewall merupakan sistem yang didesain khusus pada perangkat yang berada diantara dua jaringan guna untuk memisahkan jaringan internal dan eksternal.

Firewall diklasifikasikan dalam dua jenis umum, yaitu :

1. Desktop atau Personal Firewall

   Personal Firewall dibangun untuk melindungi satu komputer dari akses yang tidak sah maupun serangan eksternal, firewall ini hanya melindungi host dimana ia terinstal.

2. Network Firewall

   Network Firewall dibangun untuk melindungi seluruh jaringan dari akses yang tidak sah maupun serangan eksternal. Firewall ini memberikan perlindungan yang maksimal dan fleksibilitas.

Perbedaan dari kedua jenis adalah kapasitas jumlah host yang dapat dilindungi.

2.7. PfSense

PfSense adalah sebuah perangkat lunak *open source* yang berfungsi sebagai firewall dan router. PfSense didesain dengan tujuan untuk memberikan solusi yang aman dan efektif dalam mengelola jaringan. Perangkat lunak ini memiliki berbagai fitur seperti firewall, router, VPN, load balancing, captive portal, dan lain-lain. Dengan menggunakan pfSense, pengguna dapat mengontrol dan memonitor trafik jaringan dengan lebih mudah dan efisien (Arman & Rachmat, 2020).

PfSense memiliki antarmuka web yang mudah digunakan dan dapat dikonfigurasi melalui berbagai protokol seperti SSH, Telnet, dan console serial. Perangkat lunak ini juga mendukung banyak fitur keamanan seperti filter packet,

IDS/IPS, dan pengecekan malware. PfSense dapat diunduh secara gratis dan dapat digunakan tanpa biaya lisensi.

2.8. Honeypot

Honeypot merupakan perangkat lunak tipuan yang diatur untuk memikat dan menangkap penyerang dijaringan. Hal ini dilakukan dengan membuat server terlihat seolah-olah rentan terhadap serangan, sehingga dapat diamati dan dicatat aktifitas yang penyerang lakukan (Fitriana & Khasanah, 2018). Terdapat beberapa tahapan yang ada pada honeypot, antara lain :

1. Low Interaction Honeypot

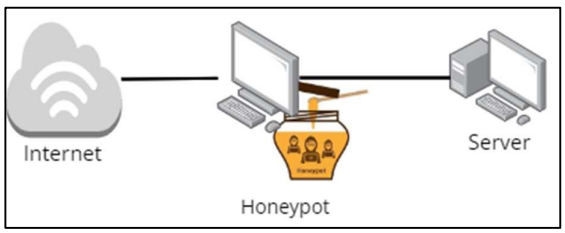
   Low interaction honeypot adalah sistem yang dibuat untuk meniru layanan jaringan atau sistem operasi tertentu. Terdiri dari sistem palsu sederhana dari port protokol tertentu. Honeypot jenis ini digunakan untuk memantau serangan yang tidak terlalu kompleks.

2. Medium Interaction Honeypot

   Medium interaction honeypot jenis ini menggunakan sistem operasi atau aplikasi yang sebenarnya. Honeypot ini pada umumnya lebih kompleks daripada low interaction honeypot karena memungkinankan attacker untuk berinteraksi dengan sistem operasi dan mendapatkan akses kesistem operasi sebenarnya.

3. High Interaction Honeypot

   High interation honeypot merupakan sistem operasi yang sebenarnya dan memungkinkan attacker untuk berinteraksi dengan sistem operasi dan perangkat lunak sebenarnya. Honeypot jenis ini sangat efektif dalam menangkap serangan yang kompleks.



Gambar 2. 9 Contoh Penempatan Honeypot Pada Server

2.9. Alamat IP

Alamat IP (*Internet Protocol)* merupakan alamat yang diberikan kepada jaringan komputer agar dapat dikenali oleh komputer lainnya (Sari & Kemala, 2020). Alamat IP adalah serangkaian angka unik dan diberikan untuk setiap perangkat yang terhubung ke internet. Alamat IP digunakan untuk mengidentifikasi dan membedakan setiap perangkat dalam jaringan.

Alamat IP terdiri dari empat angka, masing-masing terdiri dari 1 hingga 3 digit dan dipisahkan oleh titik. Setiap angka dapat berkisar dari 0 hingga 255. Contoh alamat IP 192.168.1.1.

Gambar 2. 10 Contoh Alamat IP

Pada Gambar 2.10 menunjukkan contoh alamat IP yang terdiri dari empat angka, yaitu 192.168.0.115 alamat IP ini dapat digunakan untuk mengidentifikasi dan membedakan perangkat dalam jaringan.

2.10. Protokol Jaringan

Protokol jaringan merupakan sebuah jaringan yang melakukan pertukaran data secara aman antara dua komputer atau lebih (Pratama & Dharmesta, 2019). Protokol jaringan menentukan data yang dikirim dan diterima oleh perangkat yang berbeda dalam jaringan.

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

TCP/IP (*Transmission Control Protocol/Internet Protocol*) merupakan sebuah protokol yang digunakan sebagai standar komunikasi dalam jaringan internet maupun jaringan komputer lainnya. TCP/IP dapat mengirimkan data kedalam perangkat jaringan dan memastikan data diterima dengan baik .

2.10.2. *User Datagram Protocol* (UDP)

UDP (*User Datagram Protocol*) merupakan protokol jaringan untuk mentransfer data antar perangkat dalam suatu jaringan. UDP memiliki kecepatan dalam mengirimkan data.

2.10.3. *Internet Control Message Protocol* (ICMP)

ICMP (*Internet Control Message Protocol*) adalah protokol yang digunakan untuk mengirim informasi tentang kesahan yang terjadi pada jaringan, seperti data yang tidak dapat dikirim atau diterima.

2.11. Metode Serangan

Metode Serangan bertujuan untuk menguji sistem agar dapat bekerja dengan baik, berikut contoh serangan yang akan diujikan yaitu :

2.11.1. Slowloris

Slowloris adalah serangan yang dilakukan dengan mengirmkan banyak koneksi HTTP atau permintaan yang tidak *valid* ke server yang ditargetkan. Serangan ini bertujuan mempertahankan koneksi server dengan memperpanjang permintaan sercara bertahap, tetapi tidak pernah menyelesaikan permintaan tersebut, sehingga tidak dapat memproses permintaan dari pengguna yang sah.

2.11.2. GoldenEye

GoldenEye adalah serangan yang dilakukan untuk memanfaatkan kelemahan keamanan yang ada dalam perangkat lunak dan protokol jaringan. Serangan ini dilakukan dengan membuat koneksi TCP penuh dan melakukan beberapa ratus permintaan secara berkelanjutan.

2.11.3. LOIC (Low Orbit Ion Cannon)

Loic merupakan perangkat lunak yang digunakan dalam serangan distribusi layanan (DDoS). LOIC dirancang untuk mengirimkan sejumlah besar permintaan ke server target untuk mengalirkan lalu lintas yang berlebihan dan membebani server tersebut hingga tidak dapat melayani permintaan pengguna yang sah.