BAB II
DASAR TEORI

2.1 TINJAUAN PUSTAKA

Elsa Stephani, Fitri Nova, dan Ervan Asri melakukan penelitian pada tahun 2020 berjudul "Impelementasi dan Analisa Keamanan jaringan IDS (*Intrusion Detection System*) Menggunakan Suricata Pada Webserver" secara garis besar memaparkan tentang penerapan Suricata sebagai IDS yang dibangun menggunakan *firewall* OPNsense dapat digunakan untuk mendeteksi maupun mencegah anomali pada *webserver* dari serangan DDoS dan web *scanning*, serta Suricata tidak memiliki *shared object rules* [4].

Penelitian yang berjudul "Perbandingan *Intrusion Prevention System* (IPS) pada Linux ubuntu dan Linux CentOS" tahun 2020 oleh Suryayusra dan Dedi Irawan secara garis besar membahas tentang pengujian kinerja kedua linux dengan menggunakan IPTables dan fail2ban sebagai IPS untuk serangan *brute force* melalui SSH, FTP, dan TELNET. Hasil dari penelitian tersebut menunjukan bahwa dalam pembuatan rules ubuntu lebih mudah karena lebih banyak perintah yang bisa dipakai, namun Linux CentOS lebih aman dibandingan dengan Ubuntu karena Ubuntu sering melakukan pembaruan sehingga dapat mempengaruhi rules yang telah dibuat [5].

Penelitian pada tahun 2019 yang dilakukan oleh Rudy Suwanto, Ikhwan Ruslianto, dan Muhammad Diponegoro berjudul "Implementasi *Intrusion Prevention System* (IPS) menggunakan SNORT dan *IPTables* pada Monitoring Jaringan Lokal Berbasis *Website*". Penelitian ini mendeskripsikan tentang penerapan SNORT sebagai IPS dalam jaringan area lokal dan *IPTables* sebagai sistem manajemen serangan berdasarkan alamat IP penyerang dengan *website* sebagai sarana pemantauan kinerja server dan serangan yang terjadi. Pada penelitian tersebut serangan difokuskan pada serangan *ping-of-death* dan pemindaian *port* yang menargetkan *port icmp, tcp,* dan *udp*. Hasil dari penelitian menunjukkan bahwa tingkat keberhasilan sistem adalah 90% dalam mendeteksi serangan *ping-of-death* dan 85% dalam serangan pemindaian *port*. Waktu aksi rata-

rata *IPTables* adalah 2,27/detik untuk menerima (*accept*), 1,42/detik untuk menolak (*reject*), dan 5,0/detik untuk membuang (*drop*) [6].

Ririn Agustin, Iskandar Fitri, dan Novi Dian Natasia melakukan yang berjudul "Implementasi Metode *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) berbasis SNORT Server untuk Keamanan Jaringan LAN". Penelitian yang dilakukan pada tahun 2018 tersebut memaparkan tentang penerapan IDS menggunakan SNORT sebagai *rule base* dan IPS diimplementasikan bersama firewall atau IPTables untuk menghadapi serangan TCP flood, UDP flood, dan ICMP flood. Hasil dari penelitian ini yaitu saat diuji dengan 1 client atau lebih melakukan serangan, IDS mampu mendeteksi serangan dengan baik dan menghasilkan nilai akurasi rata-rata 99,8% sedangkan untuk IPS mampu memblok *Internet Protocol* (IP) dengan mem-*filtered* IP penyerang [6].

Penlitian oleh Rua Mohamed Thiyab, DR. Musab A. M. Ali, dan Farooq Basil Abdulqader pada tahun 2017 dengan judul "*The Impact of SQL Injection Attacks on The Security of Databases*". Penelitian ini bertujuan untuk menyelidiki pengaruh validasi input yang buruk dari *query* SQL, untuk membedakan parameter yang digunakan untuk SQL berbahaya pada keamanan *database server* dan untuk meningkatkan tingkat penyaringan masukkan antara *user* asli dan yang berbahaya pada aplikasi web dinamis dalam *e-commerce*. Teknik yang digunakan yaitu *CombinedDetect* berdasarkan metode pengkodean JavaScript dan PHP untuk mendeteksi *query* SQL berbahaya dan mengisolasinya sebelum dikirim ke server. Hasil dari penelitian ini diperoleh *query* parameter yang terdiri dari tiga tahapan (registrasi, *login*, dan pencarian) merupakan teknik yang aman terhadap injeksi SQL [7].

Penelitian yang dilakukan tidak lepas dari hasil penelitian yang telah disebutkan pada subbab 2.1 tinjauan Pustaka, kemudian disajikan pada tabel 2.1 dibawah ini.

Tabel 2.1 Tinjauan Pustaka Penelitian Terdahulu

No.	Jurnal	Tahun	Keterangan
1	Elsa Stephani, Fitri Nova, Ervan Asri, "Implementasi dan Analisa Keamanan	2020	Suricata digunakan sebagai IDS yang dibangun menggunakan *firewall* OPNsense digunakan

	Jaringan IDS *(Intrusion Detection System*) Menggunakan Suricata Pada *Webserver*"		untuk mendeteksi maupun mencegah anomali pada *webserver* dari serangan DDoS dan *web scanning*, serta Suricata tidak memiliki shared *object rules*
2	Suryayusra dan Dedi Irawan, "Perbandingan *Intrusion Prevention System* (IPS) pada Linux ubuntu dan Linux CentOS"	2020	Penerapan fail2ban dan IPTables pada linux Ubuntu dan CentOS sebagai IPS berhasil untuk menangani serangan Brute force melalui SSH, FTP, dan TELNET.
3	Rudy Suwanto, Ikhwan Ruslianto, dan Muhammad Diponegoro, "Implementasi *Intrusion Prevention System* (IPS) Menggunakan SNORT dan *IPTables* pada Monitoring Jaringan Lokal Berbasis Website"	2019	SNORT sebagai IPS untuk mendeteksi serangan *ping of death* dan pemindaian *port* dengan *IPTables* sebagai sistem penangannya dan *webserver* sebagai media pemantauan kinerja server.
4	Ririn Agustin, Iskandar Fitri, Novi Dian Natasia, "Implementasi Metode *Intrusion Detection System* (IDS) *dan Intrusion Prevention System* (IPS) Berbasis Snort Server untuk Keamanan Jaringan LAN"	2018	Penerapan IDS Snort sebagai rule base dan IPS menggunakan *firewall* atau *IPTables* untuk menangani jenis serangan TCP flood, UDP flood, dan ICMP flood dengan melihat akurasi dari IDS dan kemampuan IPS dalam menangani serangan.
5	Rua Mohamed Thiyab, DR. Musab A. M. Ali, Farooq Basil, dan Abdulqader, "*The Impact of SQL Injection Attacks on The Security of Databases*".	2017	Memaparkan tentang pengaruh injeksi SQL pada *database* server dan meningkatkan tingkat penyaringan dengan menggunakan *CombinedDetect* berdasarkan metode pengkodean JavaScript dan PHP.

2.2 DASAR TEORI

2.2.1 Jaringan Komputer

Kumpulan dari beberapa komputer yang dihubungkan oleh suatu sistem komunikasi yang memungkinkan setiap komputer untuk saling bertukar data dan sumber daya lainnya disebut jaringan komputer. Jenis jaringan komputer berdasarkan luas lingkupnya antara lain [8]:

1. *Local Area Network (LAN)*

Jaringan komputer ini yang paling sederhana dan kecil cakupannya. Jaringan LAN biasa digunakan dalam satu ruangan, satu rumah, dan lain sebagainya. Transmisi yang digunakan menggunakan kabel namun sekarang sudah ada yang menggunakan nirkabel. Topologi yang digunakan juga juga topologi sederhana seperti bus dan ring. Kecepatan transfer pada jaringan ini yaitu sekitar 10 – 1000 MBps

2. *Metropolitan Arean Network (MAN)*

Kumpulan dari beberapa LAN yang berada dalam suatu kota disebut sebagai MAN. Cakupan MAN kurang lebih 50 – 100 km.

3. *Wide Area Network (WAN)*

Jenis jaringan komputer yang memiliki cakupan daerah lebih dari 100 – 1000 km adalah WAN. WAN merupakan kumpulan dari jaringan kecil seperti LAN dan MAN.

Setiap perangkat yang terhubung dengan jaringan komputer memiliki risiko ancaman serangan yang dilakukan oleh *hacker* dan *cracker* atau bahkan oleh lingkungan sekitar. Tidak melihat seberapa luas jangkauan jaringan tersebut para penyerang akan tetap melakukan ancaman serangan sehingga diperlukannya sebuah sistem keamanan jaringan komputer. Jenis – jenis keamanan jaringan pada dasarnya dibagi menjadi 5 (lima) yaitu [9] :

a. Keamanan Fisik

Jenis keamanan ini lebih difokuskan pada perlindungan dari sisi *hardware* (perangkat keras). Tujuannya yaitu agar menjaga *hardware* tetap prima dan bisa beroperasi dengan lancar tanpa adanya kerusakan.

b. Proteksi Virus

Serangan yang dilakukan oleh virus dapat menyebabkan kerusakan pada sistem komputer sehingga diperlukan pengamanan dengan menggunakan *software* antivirus.

c. Keamanan jaringan

Keamanan jaringan ini dilakukan dengan menggunakan *software* atau perintah tertentu seperti menggunakan proxy ataupun *Firewall* tujuannya yaitu untuk memfilter pengguna yang berada dalam suatu jaringan.

d. Otorisasi akses

Otorisasi akses yaitu jenis keamanan jaringan yang memberlakukan kata sandi atau *password* saat akan mengakses sesuatu. Tujuannya yaitu agar administrator dapat memastikan dan memfilter *user* tertentu saja yang dapat mengakses sebuah jaringan.

e. Penanganan bencana

Pencegahan berbagai kerusakan dan kehilangan berbagai data – data penting yang berada disebuah jaringan komputer yang disebabkan oleh bencana alam yang tidak dapat dipresiksikan kapan datangnya sangat diperlukan. Sehingga dapat meminimalisir kerusakan sistem jaringan komputer.

2.2.2 Keamanan Jaringan

Keamanan suatu komputer merupakan berhubungan dengan pencegahan dini dan deteksi terhadap tindakan yang mengganggu yang tidak dikenali dalam sistem komputer. Keamanan *cyber* merupakan salah satu aspek penting dari sebuah sistem informasi. Keamanan informasi meliputi perlindungan terhadap beberapa aspek termasuk *Confidentiality*, *Integrity*, dan *Availability* seperti yang ditunjukkan pada gambar 2.1 [10].

Gambar 2.1 Aspek Keamanan Komputer [10]

1. *Confidentiality* (kerahasiaan) yaitu menjamin kerahasiaan data dengan memastikan hanya pihak berwenang yang dapat mengakses data, termasuk data data yang dikirim, diterima, atau disimpan.
2. *Integrity* (integritas) yaitu memastikan bahwa data tidak berubah tanpa izin dari pihak yang berwenang (*authorized*) dengan tetap menjaga keakuratan, keutuhan informasi dan metode prosesnya.
3. *Availability* (ketersediaan/aksesibilitas) yaitu memastikan bahwa data selalu tersedia saat dibutuhkan dan memastikan pihak yang memiliki wewenang dapat menggunakan data tersebut.

Ada banyak metode yang dapat digunakan untuk mengamankan jaringan. Semua metode itu dimasukkan dalam *Security Information Management* (SIM). SIM adalah metode keamanan jaringan yang umum, berarti terdapat metode keamanan jaringan lain yang lebih spesifik untuk suatu permasalahan atau teknik yang digunakan. Beberapa metode yang dapat diterapkan untuk mengamankan jaringan komputer ialah seperti berikut:

1. *Port scanning*

Port scanning atau pemindai *port* digunakan untuk mengidentifikasi kelemahan jaringan melalui *port* yang sedang digunakan. *Port scanner* memiliki cara kerja dengan memanfaatkan paket pengiriman *broadcast* untuk setiap *port*. *Port scanner* akan menerima jawaban dari *port* dan aplikasi yang digunakan untuk menerima

koneksi tersebut, dengan demikian akan memungkinkan untuk masuk ke sebuah *port* untuk melihat kendala yang dialami.

2. *Intrusion Detection System / Intrusion Prevention System*

IDS dan IPS adalah sistem yang digunakan untuk mendeteksi dan melindungi sistem jaringan dari ancaman serangan di luar atau di jaringan. IDS hanya dapat memantau jaringan dengan cara kerja menerima *copy packet* yang ditujukan ke *host* untuk dilakukan pengecekan. Ketika terdapat paket yang mencurigakan, maka akan diberlakukan sistem *alert* namun paket akan tetap sampai ke *host* tujuan. Sedangkan IPS lebih aktif bekerjasama dengan *Firewall* dan dapat bekerja dalam jaringan (*inline*). IPS dapat memberikan keputusan dapat diterima atau tidaknya sebuah paket.

3. *De-Militarized Zone (DMZ)*

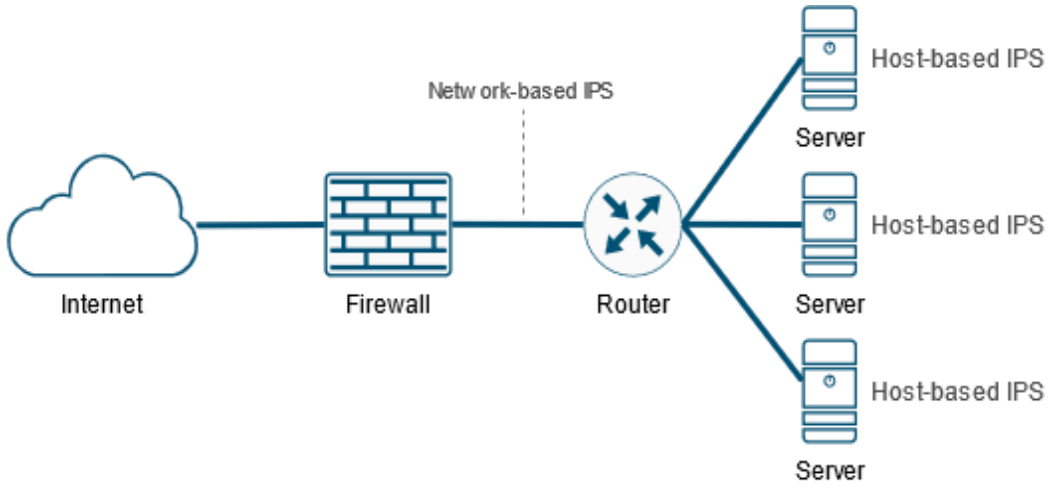
Metode DMZ merupakan mekanisme untuk melindungi sistem internal dari ancaman serangan pihak lain yang mencoba masuk tanpa adanya hak akses. DMZ melakukan perpindahan semua layanan dari satu jaringan ke jaringan lain.

2.2.3 *Intrusion Detection System* (IDS)

IDS ialah sebuah perangkat atau aplikasi yang mampu mendeteksi adanya malfungsi sistem. Awalnya IDS adalah pengembangan dari firewall, yaitu sistem yang memisahkan antara jaringan internal dan eksternal. Firewall dianggap tidak cukup karena hanya bertindak sebagai pemisah dan tidak memeriksa paket data sehingga memungkinkan lolosnya paket berbahaya. Sistem pendeteksi serangan ini digunakan untuk memantau sistem komputer secara *real-time* untuk melihat aktivitas mencurigakan seperti mendeteksi pengguna yang tidak berwenang yang mencoba masuk. Ketika aktivitas mencurigakan terkait dengan *traffic* jaringan terdeteksi, IDS akan memperingatkan kepada sistem atau administrator jaringan. IDS terbagi menjadi *Host-based Intrusion Detection System* (HIDS) dan *Network-based Intrusion Detection System* (NIDS). HIDS bekerja hanya untuk memantau semua aktivitas dalam satu *host* saja, sedangkan NIDS bekerja memantau semua lalu lintas jaringan, tidak terfokus pada sebuah *host* [11].

2.2.4 *Intrusion Prevention System* (IPS)

Intrusion Prevention System (IPS) adalah salah satu metode yang digunakan untuk mencegah ancaman serangan yang menembus masuk jaringan lokal. IPS menggabungkan *Firewall* dan sistem deteksi intrusi (IDS). IPS akan memverifikasi dan mencatat semua paket data serta mengenali paket sensor. Ketika serangan terdeteksi, IPS akan memblokir akses semua paket data yang teridentifikasi tersebut dan mencatatnya (log). IPS bertindak sebagai *Firewall* yang mengizinkan (*allow*) dan memblokir (*block*), dengan IDS yang dapat melakukan deteksi paket secara mendetail [3].



Gambar 2.2 Topologi NIPS dan HIPS

Berdasarkan pada gambar 2.2, IPS terbagi menjadi 2 jenis yaitu :

1. *Host – based Intrusion Prevention System* (HIPS)

HIPS merupakan sebuah sistem pencegahan berlapis-lapis yang menggunakan *packet filtering*, dan metode pencegahan *real-time* untuk menjaga *host* berada dalam keadaan efisien performansi yang layak. HIPS bekerja dengan mencegah kode – kode berbahaya yang memasuki *host* agar tidak dieksekusi tanpa perlu mengecek *thread signature*.

2. *Network – based Intrusion Prevention System (NIPS)*

NIPS merupakan sistem pencegahan yang memantau dan melindungi *host* di jaringan global daripada secara khusus memantau satu *host*. Jenis IPS ini dapat mencegat semua lalu lintas jaringan dan memeriksa aktivitas dan kode yang

mencurigakan. NIPS adalah kombinasi dari IPS dan *firewall*, umumnya dikenal sebagai mode *inline* atau *Gateway Intrusion Detection System* (GIDS).

Sistem kerja yang dimiliki oleh IPS yaitu pendeteksian berbasis *signature*, anomali, dan monitoring file. Berikut ini adalah penjelasan mengenai metode pendeteksian dalam IPS:

a. Signature – based detection

Pendeteksian berbasis *signature* yaitu dengan cara mencocokkan lalu lintas jaringan dengan *signature* database IPS yang berisi *attacking rule* atau aturan serangan dan penyusupan yang sering dilakukan oleh penyerang. Metode ini akan melindungi sistem dari jenis – jenis serangan yang telah diketahui sebelumnya. Oleh karena itu, agar sistem keamanan tetap terjaga maka data *rules* harus terus tetap *update*.

b. Anomaly – based detection

Pendeteksian berbasis anomali memperhitungkan pola lalu lintas jaringan yang terjadi. Biasanya dilakukan dengan menggunakan teknik statistik. Namun, kelemahannya adalah kemungkinan munculnya *false positive*, yaitu terdapat pesan atau log yang dilaporkan padahal tidak ada serangan yang terjadi. Sehingga tugas *network administrator* menjadi lebih rumit karena harus memilih mana yang merupakan serangan sebenarnya.

2.2.5 Firewall

Firewall adalah pertahanan terhadap serangan dari dalam maupun luar jaringan dengan suatu konfigurasi yang tepat sehingga memungkinkan untuk mengamankan data menjadi jauh lebih aman. *Firewall* merupakan sistem yang memungkinkan lalu lintas jaringan yang dianggap aman untuk dilewati dan memblokir lalu lintas jaringan yang tidak aman. *Firewall* biasanya digunakan untuk mengontrol akses kepada siapa saja yang dapat mengakses jaringan pribadi dari luar. Tugas – tugas *Firewall* diantaranya yaitu memfilter jaringan yang tidak diinginkan, dan merekam atau mencatat serta memberitahu administrator terhadap segala menembus kebijakan security [12].

2.2.6 *IPTables*

IPTables adalah program aplikasi berbasis linux yang memungkinkan administrator untuk mengkonfigurasi tabel ip yang disediakan oleh *Firewall* kernel Linux. *IPTables* berlaku untuk IPv4, IPv6, arptables ARP, dan tables ke frame Ethernet. *IPTables* merupakan *firewall* yang sering digunakan karena memiliki berbagai fungsi untuk melakukan pengaturan terhadap keluar masuknya paket data. *IPTables* memiliki 3 tabel yaitu NAT, MANGLE, dan FILTER. Penggunaanya disesuaikan dengan fungsinya masing – masing. NAT digunakan untuk melakukan *Network Address Translation* atau mengganti *field* alamat asal ataupun alamat tujuan dari sebuah paket. MANGLE digunakan untuk melakukan penghalusan paket seperti TTL, TOS, dan *MARK*. *FILTER* digunakan untuk melakukan *filtering* paket, apakah paket akan di *DROP, LOG, ACCEPT*, dan *REJECT* [13].

2.2.7 Suricata

Gambar 2.3 adalah logo dari suricata. Suricata merupakan sebuah *software* keamanan jaringan berbasis *opensource* yang dikembangkan serta dimiliki oleh *Open Information Security Foundation* (OISF) dan vendornya. Suricata adalah *network* IDS, IPS dan sebuah mesin monitor keamanan jaringan dengan performa tinggi yang memiliki kemampuan *Multi-threaded* [14]. Suricata mampu mendeteksi gangguan secara *real-time*, pencegahan intrusi *inline* (IPS), pemantauan keamanan jaringan (NSM), dan pemrosesan PCAP *offline*.

Gambar 2.3 Logo Suricata

Suricata memeriksa *traffic* jaringan menggunakan *rules* dan *signature* yang kuat dan Lua scripting untuk mendukung pendeteksian serangan yang kompleks. Keuntungan menggunakan Suricata yaitu [15]:

1. IDS dan IPS Suricata mengimplementasikan *signature language* yang lengkap untuk mencocokkan dengan ancaman yang dikenal, 25 *policy violation,* dan perilaku berbahaya. Suricata juga mendeteksi banyak anomaly pada lalu lintas yang diinspeksi. Suricata mampu menggunakan *ruleset* dari *Emerging Threats* Suricatadan VRT *ruleset*.
2. *Highly Performance* Suricata mampu melakukan inspeksi lalulintas multi-gigabit. *Engine* pada Suricata dibangun secara *Multi-threading* memungkinkan perangkat keras mencapai kecepatan 10 Gb dalam lalu lintas nyata tanpa mempegaruhi aturan. Suricata dapat menjalankan satu instansi dan akan menyeimbangkan beban pemrosesan pada setiap prosesor melalui sensor Suricata yang dikonfigurasi.
3. Identifikasi protokol dapat secara otomatis terdeteksi oleh Suricata selama komunikasi, yang memungkinkan penulis *rules* untuk menulis aturan untuk protokol alih-alih *port* yang diharapkan. Hal ini membuat *Suricata Malware Command* dan *control channel* menjadi unik. Saluran off HTTP CnC, yang biasanya lolos di sebagaian besar sistem IDS tetapi tidak di Suricata. Pada Suricata dapat mencocokkan *field* protokol mulai dari url http sampai SSL *certificate identifier* dengan menggunakan kata kunci khusus.
4. Suricata dapat mengidentifikasi ribuan jenis file yang melintasi suatu jaringan. Tidak hanya mengidentifikasi tetapi juga dapat menandai untuk diekstraksi dan file akan di tulis ke disk dengan file data meta yang menggambarkan penangkapan dan aliran. MD5 *checksum* file dihitung dengan cepat, sehingga daftar MD5 hash dapat disimpan dalam jaringan.

Suricata sebagai IDS akan mengambil paket data yang ada pada jaringan komputer akan dilakukan deteksi dengan Suricata *rules based*, jika terdeteksi serangan maka akan memberi peringatan dengan menyimpan data pada log. Suricata sebagai IPS yaitu untuk melakukan pengamanan yang dapat mendeteksi adanya aktivitas mencurigakan dan mencegah aktivitas tersebut. Dengan mengambil paket data yang ada pada jaringan komputer kemudian akan dilakukan

deteksi dengan Suricata *rules based*, jika terdeteksi sebagai aktivitas mencurigakan maka Suricata akan mengeluarkan peringatan dan IPS akan melakukan *blocking* paket dengan cara memeberikan *rule* pada IPTables atau *Firewall.*

2.2.8 Serangan Jaringan

Serangan terhadap keamanan jaringan dibagi menjadi serangan fisik dan serangan *logic*. Serangan fisik merupakan serangan yang terjadi pada *hardware*-nya yang menyebabkan kerusakan seperti terjadi gangguan pada kabel, kerusakan *harddisk*, dan korsleting. Serangan *logic* merupakan serangan terhadap perangkat lunak jaringan. Jenis serangan ini yang paling rawan terjadi. Beberapa bentuk serangan *logic* diantaranya yaitu :

1. *Denial of Service (DoS)*

DoS adalah tindakan yang dapat mengganggu sebuah layanan (*service*) sehingga pengguna yang berhak atau pengguna yang berkepentingan tidak dapat menggunakan layanan tersebut. DoS merupakan jenis serangan terhadap sebuah komputer atau server yang menghabiskan sumber daya yang dimiliki sehingga tidak dapat menjalankan fungsinya dengan benar.

2. *Distributed Denial of Service (DDoS)*

Jenis serangan ini memiliki mekanisme yang sama dengan DoS namun memiliki dampak yang lebih besar. Serangan DDoS menggunakan banyak *host* untuk menyerang satu buah *host* target dalam jaringan.

3. *SQL Injection*

Jenis serangan ini merupakan teknik menyerang yang memanfaatkan celah keamanan pada database dan aplikasinya.

4. *DNS Poisoning*

Serangan yang mengeksploitasi kerentanan dalam DNS untuk mengalihkan lalu lintas internet dari server yang sah dan menuju ke yang palsu.

5. *Man in the Middle*

Jenis serangan ini menempatkan *hacker* atau penyerang di tengah-tengah komunikasi antara 2 orang. Penyerang akan mencuri berbagai informasi penting yang berada dalam komunikasi tersebut. Selain itu penyerang juga dapat menyisipkan *malware*.

2.2.9 SQL Injection

Injeksi SQL merupakan teknik yang memungkinkan penyerang untuk memasukan perintah (*query*) SQL yang berbahaya sehingga dapat memanipulasi logika perintah SQL untuk mendapatkan akses ke database dan informasi penting lainnya. Penyerang dapat mempengaruhi *syntax* SQL, kekuatan, fleksibilitas dari database, dan mempengaruhi sistem operasi untuk database. Ada beberapa jenis dari serangan SQL *Injection* diantaranya yaitu [16]:

1. *Union-Based SQL Injection*

Jenis serangan yang menggunakan operator UNION, kombinasi dari dua statement untuk mengambil data dari database.

2. *Error-Based SQL Injection*

Jenis serangan ini hanya dapat berjalan pada Microsoft SQL Server. Metode serangan ini akan membuat aplikasi menunjukkan error ketika mengakses database kemudian penyerang akan mempelajari informasi sistem seperti database, versi database, sistem operasi, dan lain sebagainya.

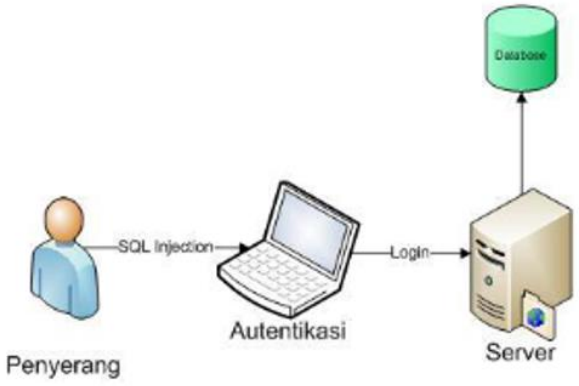
3. *Blind SQL Injection*

Serangan ini tidak ada pesan *error* yang diterima dari database. Terdapat 2 jenis serangan Blind SQL *Injection* yaitu *content-based* blind SQL *Injection* dan time-based blind SQL *Injection*.

Berikut beberapa ancaman dari SQL *Injection* [17]:

a. Mendapatkan akses (*bypass authentication*), penyerang melakukan serangan untuk mendapatkan akses penuh tanpa perlu menggunakan *username* dan *password*.
b. Pencurian informasi, pengambilan semua informasi yang ada terutama informasi yang bersifat *sensitive* seperti *username* dan *password*.
c. Mengubah dan menghapus data asli, penyerang dapat melakukan modifikasi baik itu mengubah maupun menghapus informasi yang terdapat didalam database.
d. *Denial of service*, ancaman ini mengirimkan permintaan palsu ke server yang tidak dapat ditangani oleh server sehingga pengguna tidak dapat mengakses administratif sistem.

e. *Identify Spoofing*, serangan yang bertujuan untuk meyakinkan pengguna percaya bahwa web yang bersangkutan adalah web asli padahal bukan.
f. Pada dasarnya injeksi SQL adalah contoh dari kategori kerentanan yang lebih umum dan dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip ditambahkan ke bahasa yang lain.



Gambar 2.4 SQL *Injection* melalui autentikasi [18]

Gambar 2.4 menjelaskan tentang penyerang memanfaatkan autentikasi atau halaman login untuk membentuk logika tertentu agar dapat masuk ke dalam database. SQL Injeksi dapat dilakukan manual dengan memasukan *query* SQL *Injection* ke dalam sebuah form, namun sekarang terdapat banyak *tool* yang digunakan untuk melakukan SQL *Injection*. Ada beberapa contoh *tool* yang dapat digunakan yaitu :

1. SQLMap

SQLMap adalah *tool* berbasis *open-source* yang dijalankan menggunakan *command* dan *support* untuk database *MySQL, Oracle, PostgreSQL, MicrosoftSQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase* dan SAP MaxDB.

2. BSQL *Hacker*

Tool ini dirancang untuk mengeksplorasi hampir seluruh database. BSQL Hacker dikembangkan oleh Portcullis Labs.

3. The Mole

Mole dapat melewati beberapa sistem IDS/IPS dengan menggunakan filter *generic* dan dapat mengeksplorasi hanya dengan menggunakan URL yang rentang dan string valid.

4. Pangolin

Merupakan *tool* untuk melakukan injeksi SQL secara menyeluruh pada web. Pangolin memiliki tampilan *user-friendly* dan juga *support* hampir seluruh database.

5. Harvij

Kelebihan dari *tool* ini yaitu menggunakan GUI yang sederhana dan dapat melakukan injeksi dengan kemungkinan berhasil tinggi.

2.2.10 SQLMap

SQLMap adalah *software* berbasis *opensource* yang digunakan untuk mendeteksi dan mengeksploitasi kelemahan pada sebuah web serta dapat mengambil alih database server. Tampilan awal SQLMap dapat dilihat seperti pada gambar 2.5. Penyerang yang menggunakan SQLMap selain dapat menyerang database SQL juga dapat mengambil detail struktur database, melakukan modifikasi (melihat atau menghapus) data dan mengakses sistem file dari server. Fitur – fitur yang terdapat dalam SQLMap diantaranya yaitu :

1. Mendukung untuk beberapa database seperti *MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache, Derby, Amazon Redshift, Vertica,* dan *McCoy*.
2. Mendukung 6 jenis metode injeksi yaitu *Boolean – based blind, Time – based blind, Error – based, UNION – based,* Inteferential, dan *Out – of – band. Boolean – based blind* adalah teknik injeksi yang bergantung pada pengiriman perintah SQL ke database agar aplikasi mengembalikan hasil yang berbeda. *Time – based blind* adalah teknik injeksi yang bergantung pada pengiriman perintah SQL yang memaksa database untuk menunggu waktu yang telah ditentukan sebelum merespons dengan tujuan untuk menunjukkan kepada *attacker* benar atau salahnya hasil dari perintah yang dikirimkan. *Error – based* adalah teknik injeksi berdasarkan pada *error message* yang dikirim oleh database untuk mendapatkan informasi tentang struktur database. *UNION – based* merupakan teknik yang berdasarkan pada pemanfaatan operator SQL UNION untuk menggabungkan hasil dari dua atau lebih pernyataan yang

kemudian dikembalikan sebagai bagian dari respons. Interferensi adalah teknik injeksi untuk mengeksploitasi database tetapi membutuhkan waktu yang cukup lama karena penyerang dapat memodifikasi struktur data dalam database. *Out – of – band*, teknik ini dapat terjadi jika penyerang tidak dapat menggunakan saluran yang sama untuk meluncurkan serangan.

3. SQLMap dapat langsung terhubung ke database menggunakan DBMS, IP address, *port*, dan nama database tanpa melakukan SQL *Injection.*
4. Secara otomatis mengenali format *password hash* dan mendukung pemecahannya dengan menggunakan serangan berbasis kamus.
5. Dapat mengunduh dan meng-unggah file apapun dari server database MySQL, PostgreSQL atau *Microsoft SQL Server* [17].

Gambar 2.5 Tampilan SQLMap pada *Command Prompt*

2.2.11 Response time

Response time atau waktu tanggap adalah waktu tanggap yang diberikan oleh *interface* ketika pengguna mengirimkan *request* ke server. *Response time testing* merupakan pengujian *response time* yang mengacu pada waktu yang dibutuhkan sebuah server dalam sistem untuk merespons permintaan dari *user* lain. Waktu yang dibutuhkan ketika sistem atau CPU mengambil langkah terhadap suatu *input* tertentu sampai proses selesai. *Response testing* memiliki dua karakteristik yaitu waktu tanggapan rata-rata dan waktu tanggapan maksimum.

Pengujian waktu respon adalah pengukuran jumlah waktu yang berlalu antara permintaan pengguna dengan respons dari server, aplikasi, situs web, dan

lain sebagainya. Waktu respon rata-rata atau (ART) adalah pengukuran jumlah waktu yang dibutuhkan sebuah server atau aplikasi untuk merespons semua input dan permintaan datanya. Waktu respons yang rendah berarti memiliki kinerja yang lebih baik, karena server atau aplikasi mambutuhkan lebih sedikit waktu untuk menanggapi permintaan baru. Waktu respons maksimum merupakan bagian dari ART. Pengukuran waktu respons maksimum membantu administrator untuk menentukan nilai maksimum apa yang memperlambat waktu respons [18].