SKRIPSI

KEAMANAN JARINGAN BERBASIS *INTRUSION DETECTION SYSTEM*

Disusun dan diajukan oleh:

NAZIHA AYN FAZHILA PINONTOAN
D041 19 1102

PROGRAM STUDI SARJANA TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA
2024

LEMBAR PENGESAHAN SKRIPSI

KEAMANAN JARINGAN BERBASIS *INTRUSION DETECTION SYSTEM*

Disusun dan diajukan oleh

Naziha Ayn Fazhila Pinontoan

D041191102

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Elektro Fakultas Teknik Universitas Hasanuddin
Pada Tanggal 6 Maret 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
Dr. Eng. Wardi, S.T., M. Eng.	Prof. Dr. H. Andani Achmad, M.T.
NIP 19720828 199903 1 003	NIP 19601231 198703 1 022

Ketua Program Studi,

Dr. Eng. Ir. Dewiani, M.T.
NIP 19691026 199412 2 001

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini :
Nama : Naziha Ayn Fazhila Pinontoan
NIM : D041191102
Program Studi : Teknik Elektro
Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

KEAMANAN JARINGAN BERBASIS *INTRUSION DETECTION SYSTEM*

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini, maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 6 Maret 2024

Yang Menyatakan

Naziha Ayn Fazhila Pinontoan

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh, Salam sejahtera bagi kita semua. Puji syukur senantiasa dipanjatkan ke hadirat Allah SWT yang dengan rahmat dan hidayah-Nya serta salam kepada Nabi Muhammad SAW sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul "**KEAMANAN JARINGAN BERBASIS INTRUSION DETECTION SYSTEM**". Skripsi ini disusun sebagai salah satu syarat untuk mendapatkan gelar Sarjana Teknik pada Departemen Teknik Elektro, Fakultas Teknik, Universitas Hasanuddin.

Pada penulisan skripsi ini, penulis banyak dihadapkan dengan berbagai hambatan, akan tetapi berkat adanya bimbingan, dukungan, dan bantuan dari berbagai pihak, akhirnya penulis dapat menyelesaikan tugas akhir ini dengan baik. Oleh karena itu, melalui kesempatan ini penulis juga mengucapkan penghargaan dan terima kasih kepada:

1. Allah SWT, yang senantiasa memberikan kesempatan berkat, akal budi, pengetahuan, dan segala yang tak terhitung jumlahnya untuk dapat menyelesaikan tugas akhir ini.
2. Kedua orang tua penulis, Ayahanda Teddy Yudianto dan Ibunda Diana Rahman atas segala doa, jasa, motivasi dan dukungan yang telah diberikan dan yang senantiasa mengingatkan penulis untuk menyelesaikan skripsi.
3. Kepada saudara-saudara penulis, Dwiki Putra Pinontoan yang senantiasa memberikan masukan positif selama penulisan tugas akhir ini, Najlah Billah Risqullah yang senantiasa menghibur penulis disaat penulis mulai merasa penat, Hugo Acatya yang senantiasa mengirimkan kasih sayangnya disaat penulis jauh dari rumah.
4. Bapak Dr. Eng. Wardi, S.T., M.Eng selaku pembimbing I dan Bapak Prof. Dr. Ir. H. Andani Achmad, M.T. selaku pembimbing II yang telah meluangkan waktu, tenaga, dan pikirannya dalam membimbing dan engarahkan penulis dalam pembuatan tugas akhir.
   u Dr. Eng. Ir. Dewiani, M.T. sebagai Ketua Departemen Elektro Fakultas eknik Universitas Hasanuddin.

6. Seluruh Dosen dan Staf Akademik Program Studi S1 yang senantiasa membagi ilmu selama ini.

Akhir kata, *Life can be heavy, especially if you try to carry it all at once. Part of growing up and moving into new chapters of your life is about catch and release. What I mean by that is, knowing what things to keep, and what things to release. I'm trying to tell you that losing things doesn't just mean losing. A lot of the time, when we lose things, we gains things too. Scary news is ; You're on your own now. Cool News is; You're on your own now.*

Makassar, 6 Maret 2024

Hormat saya

Penulis

ABSTRAK

NAZIHA AYN FAZHILA. Keamanan Jaringan Berbasis *Intrusion Detection System* (Dibimbing oleh Wardi dan Andani Achmad)

Wireless Local Area Network (WLAN) telah menjadi kebutuhan harian teknologi modern sehingga penggunaan terhadap WLAN juga ikut meningkat, seiringan dengan hal tersebut maka timbul kerentanan terhadap keamanannya. Oleh karena itu penelitian ini bertujuan untuk merancang sistem deteksi keamanan jaringan berbasis Intrusion Detection System (IDS) pada jaringan WLAN dan mengidentifikasi tingkat kerentanan jaringan terhadap serangan Denial-of-Service (DOS). Pada penelitian ini dirumuskan suatu masalah yakni bagaimana mendeteksi adanya serangan pada lalu lintas jaringan komputer dengan IDS pada jaringan WLAN dan mengidentifikasi tingkat kerentanan jaringan yang diuji. Metode penelitian melibatkan desain sistem keamanan jaringan dengan menggunakan Snort pada platform Windows, dengan dukungan dari Nmap untuk analisis lapisan keamanan. Hasil utama penelitian menunjukkan bahwa konfigurasi Snort pada mesin target mampu mendeteksi serangan DOS, termasuk ping of death, ping flood, dan port scanning serta diperoleh nilai kerentanan jaringan yang diuji pada angka 4,3 dari skala 10 pada CVSS yang dapat diartikan bahwa kerentanan jaringan yang diuji ada pada *level medium*.

Kata kunci : Keamanan jaringan, Intrusion Detection System, Snort, WLAN, Denial of Service.

ABSTRACT

NAZIHA AYN FAZHILA. Network Security Based on Intrusion Detection System (Supervised by Wardi and Andani Achmad)

Wireless Local Area Network (WLAN) has become a daily need of modern technology so that the use of WLAN also increases, along with this there is a vulnerability to its security. Therefore, this study aims to design an Intrusion Detection System (IDS)-based network security detection system on WLAN networks and identify the level of network vulnerability to Denial-of-Service (DOS) attacks. In this study, a problem was formulated, namely how to detect an attack on computer network traffic with IDS on a WLAN network and identify the level of vulnerability of the network being tested. The research method involves the design of a network security system using Snort on the Windows platform, with support from Nmap for security layer analysis. The main results showed that the Snort configuration on the target machine was able to detect DOS attacks, including ping of death, ping flood, and port scanning and obtained a network vulnerability score tested at 4.3 out of a scale of 10 on CVSS which can be interpreted that the tested network vulnerability is at the *medium level*.

Keywords : Network security, Intrusion Detection System, Snort, WLAN, Denial of Service.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini berada pada titik puncak dari pengimplementasian teknologi, hal ini tidak jauh dari semakin banyaknya pemanfaatan teknologi oleh manusia saat ini. Perkembangan teknologi meningkat secara eksponensial sejak ditemukannya internet, semakin banyak inovasi dan penelitian yang melibatkan teknologi paling *update*. Sehubungan dengan perkembangan teknologi yang sangat pesat maka semakin besar pula tingkat keamanan yang dibutuhkan suatu data atau informasi yang tersimpan pada *server* yang terhubung dengan publik.

Berdasarkan laporan dari *We Are Social*, terdapat sebanyak 204,7 juta pengguna internet di Indonesia per Januari 2022, jumlah itu meningkat 1,03% dari tahun sebelumnya. Berdasarkan data yang sama, jumlah kenaikan pengguna internet di Indonesia dalam kurun waktu 4 tahun terakhir ialah melonjak sebesar 54,25%. Di waktu lain, Badan Siber dan Sandi Negara menyatakan bahwa pada tahun 2022 terdapat lebih dari 700 juta serangan siber dengan trafik serangan paling tinggi terjadi pada Januari dengan jumlah serangan sebanyak 272.926.734 atau lebih dari sepertiga total serangan yang terjadi. Metode peretasan ini banyak menargetkan lembaga akademik dan juga lembaga pemerintahan daerah.

Perlu diingat kembali bahwa saat ini penggunaan jaringan semakin bertambah penting baik dalam pendidikan maupun dalam sebuah pekerjaan dan slaah satu hal penting dalam mengelola jaringan komputer yaitu keamanan dari jaringan itu sendiri, dengan banyaknya akses ke jaringan tersebut maka akan banya pula peluang kejahatan yang terjadi pada jaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut. Terdapat banyak Teknik yang dapat diupayakan dalam memperkecil tingkat kejahatan dalam jaringan ini. Salah satu upaya mendeteksi serangan jaringan adalah dengan metode *Intrusion Detection Systems* (NIDS), yang mana IDS ini dirancang pada titik yang direncanakan dalam untuk memeriksa lalu lintas dari semua perangkat dalam jaringan dengan n pengamatan lalu lintas yang melewati setiap subnet dan mencocokkan s yang diteruskan subnet dengan kumpulan serangan yang diketahui, erangan berhasil diidentifikasi, peringatan akan dikirim ke administrator.

Salah satu pengaplikasian IDS adalah memasangnya di subnet tempat firewall berada kemudian mengamati apakah terdapat serangan pada firewall tersebut.

Terdapat berbagai jenis IDS yang berkembang saat ini, antara lain: *Realsecure* dari *Internet Security Systems (ISS), Cisco Secure Intrusion Detection Systems* dari *Cisco Systems, eTrust Intrusion Detection* dari *Computer Associates,* dan *Symantec Client Security* dari *Symantec.* Namun terdapat pula IDS yang bersifat *Open Source* yakni, Snort. Snort adalah jenis NIDS yang memiliki prinsip kerja menganalisa paket yang melintasi jaringan yang di dalam snort ini terdapat data*base* yang memuat rules yang dikategorikan sebagai penyusupan. Snort menggunakan metode analisa *signatures* dan *anomaly detection*. Metode signatures ini bekerja dengan cara membandingkan antara *rules* sebuah *traffic* yang sedang dideteksi dengan *traffic* yang mengidentifikasikan terjadinya serangan terhadap jaringan. Sedangkan metode *anomaly* bekerja dengan membandingkan antara *rules* yang berisi *traffic* normal dengan *traffic* yang sedang dideteksi.

Salah satu jenis serangan yang dapat dideteksi pada sistem keamanan jaringan IDS ialah *Denial of Service* karena bentuk serangannya ialah dengan cara membanjiri lalu lintas jaringan dengan banyak paket data, dengan adanya IDS maka web *host* dapat mengenali anomali paket yang melintasi jaringan tersebut. Digunakannya snort sebagai *tools* pada penelitian kali ini dikarenakan snort dapat dijalankan pada Windows OS sejalan dengan pengujian serangan yang akan dilakukan pada Windows OS.

Setiap orang berhak merasakan rasa aman di mana pun dan kapan pun, dimulai dari ruang lingkup paling kecil hingga ruang lingkup yang luas. Seringkali keamanan jaringan difokuskan pada instansi instansi besar seperti universitas, perkantoran, instansi pemerintahan, dan sebagainya hingga luput bahwa rumah kita sendiri pun diperlukan rasa aman itu.

Oleh karena itu diperlukan penindakan yang tepat guna mencegah hal-hal yang tidak diinginkan tersebut pada jaringan lokal yang digunakan. Salah satu cara untuk mengatasi masalah tersebut ialah dengan menggunakan *anomaly-based detection* yang dapat mengetahui pola paket seperti apa yang akan pada sebuah sistem jaringan komputer, sehingga ketika ditemukan

anomali paket yang melalui suatu jaringan komputer akan dimunculkan peringatan agar sisi server dapat memeriksa paket tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah yang ada yaitu:

1. Bagaimana mendeteksi serangan pada lalu lintas jaringan komputer dengan *intrusion detection system* pada jaringan WLAN?
2. Bagaimana tingkat kerentanan jaringan setelah dilakukan pengujian *intrusion detection system*?

1.3 Tujuan

Tujuan dari penelitian ini adalah:

1. Merancang sistem deteksi keamanan jaringan dengan *intrusion detection system* pada jaringan WLAN.
2. Mengidentifikasi tingkat kerentanan jaringan WLAN terhadap serangan DOS saat dilakukan pengujian sistem deteksi keamanan berbasis *intrusion detection system.*

1.4 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan:

1. Memberikan sistem keamanan pada jaringan WLAN.
2. Memberikan wawasan dan pengetahuan bagi penulis dan para pembaca mengenai sistem keamanan jaringan pada jaringan lokal.
3. Dapat mengidentifikasi serangan pada WLAN demi menjaga keamanan jaringan.
4. Sebagai sumber referensi perkembangan teknologi keamanan sistem jaringan komputer.

1.5 Batasan Masalah

ı pembahasan masalah yang telah dibahas, penelitian ini pembahasannya ıtasi pada:

1. Penelitian ini hanya membahas sistem keamanan jaringan dengan metode *intrusion detection system*.
2. Penelitian hanya melakukan pengujian dengan menggunakan Snort.
3. Pengujian hanya mencakup tiga jenis serangan: *ping of death, ping flood,* dan *port scanning*.

1.6 Sistematika Penulisan

Adapun sistematika penulisan dari penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN, bab ini berisi uraian tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, pada bab ini menjelaskan teori-teori penunjang materi penelitian yang diambil dari berbagai sumber ilmiah yang digunakan dalam penulisan laporan tugas akhir.

BAB III METODE PENELITIAN, bab ini membahas tentang rancangan penelitian, waktu dan lokasi penelitian, bahan dan alat, teknik pengumpulan data, serta langkah-langkah penelitian yang digunakan dalam tugas akhir ini.

BAB IV HASIL DAN PEMBAHASAN, bab ini membahas tentang hasil pengujian yang telah dilakukan lengkap dengan analisis beserta oembahasan mengenai pengujian terkait.

BAB V PENUTUP, pada bab ini berisi tentang kesimpulan dari penelitian yang telah dilakukan dan juga berisi saran untuk pembaca yang menjadikan penelitian ini sebagai referensi di kemudian hari.

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

State of The Art merupakan jurnal yang digunakan sebagai referensi dalam penelitian ini. *State of The Art* juga memberikan penjabaran mengenai perbedaan antara penelitian terdahulu dan penelitian yang akan dilakukan. Berikut ini adalah *State of The Art* yang dijabarkan dalam bentuk tabel/matriks.

Tabel 1 *State of The Art*.

No.	Deskripsi Jurnal	Pembahasan
1.	**Simulasi Penggunaan *Intrusion Detection System* (IDS) Sebagai Kemanan Jringan dan Komputer** **Tahun:** 2020 **Peneliti:** Barany Fachri Fadli Hamdi Harahap	**Hasil Penelitian:** *Intrusion Detection System* bersifat pasif, yang hanya dapat mendeteksi jika ada serangan atau penyalahgunaan jaringan komputer. Pada saat menyerang *server* menggunakan DOS (*Denial of Service*) paket yang dibawa tidak menjadi batas serangan ke server tersebut. Sehingga, untuk membatasi serangan terhadap *server* tergantung waktu saat memberhentikan serangan pada *client* tersebut. **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut dapat memperkuat penelitian ini dengan memberikan referensi mengenai seberapa besar tingkat keberhasilan dalam mendeteksi adanya anomali paket yang melintasi jaringan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini membahas mengenai penggunaan Snort pada OS Linux Ubuntu saja, sedangkan penelitian yang akan dilakukan mengaplikasikan penggunaan Snort pada OS Windows.

2.	**Implementasi *Network Intrusion Detection System* (NIDS) Dalam Sitem Keamanna *Open Cloud Computing*** **Tahun:** 2019 **Peneliti:** Muqorobin Zul Hisyam Moch. Mashuri Hanafi Yudhi Setiyantara	**Hasil Penelitian:** Dengan menggunakan dua skenario serangan, yaitu penyerang berada di luar sistem dan penyerang di dalam sistem cloud, NIDS mampu menerima *traffic*, menganilisis dan merespon serangan dengan menampilkan *alert*. Dengan penempatan NIDS yang berada di luar sistem *cloud computing* membuat proses analisis *traffic* tidak mempengaruhi *server cloud computing.* **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut dapat memperkuat penelitian ini dengan memberikan referensi mengenai perbandingan hasil yang didaptkan ketika penyerangan terjadi di luar ataupun di dalam sistem jaringan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini membahas mengenai penggunaan Snort dalam mendeteksi dan mencegah ancaman pada sistem keamanan *open cloud computing* sedangkan penelitian yang akan dilakukan adalah penggunaan Snort dalam mendeteksi dan mencegah ancaman pada sistem keamanan jaringan WLAN.
3.	**Implementasi dan ılisa Keamanan ingan IDS**	**Hasil Penelitian:** IDS menggunakan Suricata dapat memonitoring *traffic* pada web server dan menyimpan hasil deteksi dan pencegah jika ada penyusup yang memasuki

	(*Intrusion Detection System*) **Tahun:** 2020 **Peneliti:** Elsa Stephani Fitria Nova Ervan Asri	web server. Serta dapat mengetahui apabila terdapat aktivitas mencurigakan masuk ke log Suricata. Implementasi Suricata dengan *firewall* OPNsense dapat mendeteksi dan mencegah anomali pada web server dari penyusup. Pengimplementasian IDS menggunakan Suricata pada web server dapat digunakna untuk membantu memberikan informasi terkait deteksi adanya serangan web scanning dengan memanfaatkan *tools dirbuster* dan *skipfish*, serta penggunaan s*Low*ris dari metode DDoS yang diterapkan pada IDS Suricata. **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan referensi mengenai rancangan *software* untuk merancang sistem keamanan jaringan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini membahas sistem keamanan jaringan menggunakan IDS Suricata sedangkan penelitian yang akan dilakukan menggunakan NIDS Snort.
4.	**Sistem Keamanan Jaringan Komputer Berbasis Teknik *Intrusion Detection System* (IDS) Untuk ndeteksi Serangan *ributed Denial of ice* (DDOS)**	**Hasil Penelitian:** Snort dapat diimplementasikan sebagai salah satu teknik keamanan jaringan pada sistem operasi ubuntu 20.04 LTS untuk mendeteksi serangan berupa *Ping Attack*, nmap (*port scanning*) dan DDOS. Serangan *ping*, *nmap*, dan DDOS yang dilakukan dimana serangan tersebut dapat dicegah dengan menerapkan *portsentry* sehingga serangan

	Tahun: 2023 **Peneliti:** Raihan Fauzi. Yusuf Muhyidin Dayan Singastia	seperti *ping attack*, *nmap* dan DDOS tidak bisa masuk ke dalam jaringan komputer. **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan referensi mengenai rancangan sistem keamanan jaringan terhadap serangan DDOS sesuai dengan rancangan penelitian yang akan dibuat. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini membahas sistem keamanan jaringan dengan metode IDS, sedangkan penelitian yang akan dilakukan menggunakan metode NIDS.
5.	**Intrusion Detection System for WiFi Network: A Deep Learning Approach** **Tahun:** 2020 **Peneliti:** Shaoqian Wang Bo Li Mao Yang Zhongjiang Yan	**Hasil Penelitian:** Secara teoritis berbagai jenis serangan yang ada dalam jaringan Wi-Fi dan mengusulkan pendekatan pembelajaran mendalam untuk masalah klasifikasi serangan. Kami memvalidasi pendekatan kami menggunakan kumpulan data AWID dan memilih 71 atribut setelah pemilihan fitur. Kami mengadopsi SAE dan DNN untuk tampil klasifikasi serangan. Hasil percobaan menunjukkan bahwa 7-hidden-layer model DNN mencapai akurasi tinggi untuk semua kategori. Akurasi klasifikasi normal, serangan injeksi, serangan peniruan dan serangan banjir adalah 98,4619%, 99,9940%, 98,3936% dan 73,1200%, masing-masing. **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan referensi mengenai pengaplikasian IDS pada jaringan WiFi. **Perbedaan dengan Penelitian yang Akan Dilakukan:**

		Penelitian dalam jurnal ini hanya menjelaskan prinsip kerja IDS dalam sebuah jaringan WiFi tanpa menjelaskan metode *defense* yang digunakan.
6.	**Anomaly *Base*d Intrusion Detection System in IoT Using Deep Learning: A Systemativ Literature Review** **Tahun:** 2021 **Peneliti:** Muaadh A.Alsoufi Shukor Razak Mahyezah Md Siraj Ibtehal Naefa	**Hasil Penelitian:** Studi ini meringkas dan mengatur literatur terkini yang terkait dengan deteksi intrusi berbasis anomali di IoT, menggunakan teknik pembelajaran mendalam sesuai dengan kata kunci dan RQ yang telah ditentukan sebelumnya. Sebanyak 26 studi dimasukkan, sesuai dengan kriteria eksklusi, inklusi, dan kualitas yang dinyatakan. Komprehensif taksonomi disajikan berdasarkan hasil studi yang dilakukan untuk intrusi anomaly deteksi di IoT menggunakan teknik pembelajaran mendalam. Studi ini memberikan wawasan tentang atribut dan pengetahuan deteksi intrusi anomali yang ada di lingkungan IoT, menggunakan teknik belajar mendalam. Selain itu, penelitian ini menyajikan perbandingan dalam hal kinerja, dataset yang digunakan, deteksi serangan, teknik, dan teknik evaluasi dalam setiap studi. Akhirnya, penelitian ini membahas tantangan yang dihadapi dalam deteksi intrusi anomali di IoT menggunakan pembelajaran mendalam. Makalah ini dapat memberikan peneliti rincian tentang suatu teknik dan metodologi terkini dalam deteksi intrusi anomali di IoT, menggunakan deep learning. Keterbatasan sistem deteksi intrusi berbasis anomali saat ini di penggunaan IoT teknik pembelajaran mendalam menunjukkan arah masa depan untuk perbaikan lebih lanjut dari IDS, mengingat karakteristik IoT.

		Alasan Menjadi Tinjauan Penelitian: Jurnal berikut memberikan referensi mengenai dasar teoritis mengenai *anomaly-based intrusion detection system*. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini mengaplikasikan IDS pada sistem IoT sedangkan penelitian yang akan dilakukan adalah pengaplikasian IDS pada WLAN.
7.	**Simulasi Snort Sebagai Alat Pendeteksi Intrusi Pada Web DAMN *Vulnerable Web Application*** **Tahun:** 2022 **Peneliti:** I Gede Walid Bangga Siti Madinah Ladjamuddin	**Hasil Penelitian:** Snort dapat mendeteksi serangan berupa Ping, SQL, Injection, dan XSS Script dengan baik. Sebuah deteksi serangan bergantung pada penerapan rules pada Snort. **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan referensi mengenai dasar teoritis mengenai konesp IDS sebagai pendeteksi ancaman pada paket yang melintasi jaringan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini hanya menguji kemampuan Snort sebagai alat pendeteksi ancaman, sedangkan penelitian yang akan dibuat adalah membuat *defense* terhadap ancaman.
8.	**Implementasi *Intrusion Detection System* Menggunakan Banyard dan *Base* Pada Sistem Operasi ux** **un:** 0	**Hasil Penelitian:** Dari hasil pengujian gangguan terhadap *server* Snort IDS. Snort IDS dapat mengenali jenis gangguan yang ditimbulkan dan dapat menampilkan secara cepat dan tepat kapan terjadinya gangguan dan dari mana asal gangguan tersebut. **Alasan Menjadi Tinjauan Penelitian:**

	Peneliti: Rizki Triandini Yeffry Handoko Putra	Jurnal berikut memberikan perbandingan penerapan IDS pada Banyard dan *Base* yang dijalankan pada Linux Ubuntu. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian dalam jurnal ini menerapkan IDS pada sistem operasi Linux ubuntu sedangkan penelitian yang akan dilakukan dijalankan pada Windows OS.
9.	**Implementasi Snort *Intrusion Detection System* Pada Sistem Jaringan Komputer** **Tahun:** 2018 **Peneliti:** Muhammad Halmi Dar	**Hasil Penelitian:** Snort-IDS bekerjadengan baik dalam mendeteksi serangan. Waktu tanggap Snort-IDS dalam menganalisis paket yang terdeteksi sebagai gangguan cukup cepat, yaitu tidak lebih dari 1 detik per paket gangguan. Dapat diartikan bahwa Snort-IDS sangat reaktif dalam menyikapi paket-paket yang terdeteksi sebagai gangguan. Snort-IDS juga mampu mendeteksi penyerangan-penyerangan yang digolongkan sebagai *Denial of Service*(DoS) seperti PingFlood, Syn Attack,TCP dan UDPAttack. Secara default, Snort memiliki keterbatasan dari segi aturan yang ada. Semakin lengkap aturan yang dimiliki, sistem akan semakin terlindungi dari gangguan penyusupan. Untuk menambahkan aturan, dibutuhkan pengetahuan yang mendalam tentang protokol dan *payload* serangan. Untuk pengembangan sistem keamanan jaringan yang lebih secure, tidak cukup hanya dengan menerapkan IDS. Sistem keamanan jaringan perlu dilengkapi dengan *Intrusion Prevention System*(IPS). **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan wawasan mengenai penerapan IDS pada sistem jaringan komputer lokal.

		Perbedaan dengan Penelitian yang Akan Dilakukan: Penelitian ini hanya fokus kepada bentuk serangan DDoS sedangkan penelitian yang akan dibuat akan mengaplikasikan *defense* terhadap beberapa serangan.
10.	**Keamanan Jaringan Nirkabel Menggunakan *Wireless Intrusion Detection System*** **Tahun:** 2019 **Peneliti:** Joko Dwi Santoso	**Hasil Penelitian:** Sistem IDS yang telah dibangun di dalamnya mendeteksi serangan yang terjadi adalah dengan melakukan pemindaian terhadap sejumlah sumber dan lalu lintas yang terjadi di dalam jaringan. Keseluruhan sistem mesin sensor IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer yang berbasis *open source*, dan didalam mendeteksi penyusup atau penyusup pada mesin sensor IDS akan dianalisis pada *BASE* (*Basic Analysis and Security Machine*). Mekanisme sistem kerja snort dan *BASE* yang telah berhasil diimplementasi dengan baik, dalam pengujian sistem snort dan *BASE* yaitu dengan menggunakan Ping Attack, *Port* Scanning(Nmap), dan DDOS. **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan wawasan mengenai penerapan IDS pada kemanan sistem jaringan *wireless.* **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini dilakukan pada jaringan internet yang tersedia sedangkan penelitian yang akan dibuat adalah menggunakan konfigurasi jaringan lokal buatan terbaru.

11.	**Implementasi Keamanan Jaringan Wireless LAN Menggunakan SNORT dan IPTABLES.** **Tahun:** 2020 **Peneliti:** Hari Agustian Toibah Umi Kalsum Hendri Alamsyah	**Hasil Penelitian:** Berhasil mengimplementasikan keamanan jaringan pada *Wireless* LAN dengan menggunakan SNORT dengan hasil konfigurasi yang mendeteksi adanya upaya penyusupan pada lalu lintas jaringan . **Alasan Menjadi Tinjauan Penelitian:** Jurnal berikut memberikan wawasan mengenai penerapan IDS menggunakan SNORT pada kemanan sistem jaringan *wireless.* **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini dilakukan dengan menggunakan OS dari Linux Ubuntu sedangkan penelitian yang akan dilakukan menggunakan OS dari Windows. Perbedaan berikutnya adalah jenis serangan yang dikonfigurasikan pada penelitian ini adalah DDoS.
12.	**Intrusion Detection Using Anomaly Detection Algorithm and SNORT** **Tahun:** 2022 **Peneliti:** Chika Yinka Banjo.	**Hasil Penelitian:** Penelitian ini menunjukkan bahwa penggunaan algoritma deteksi anomaly khususnya algoritma klasifikasi seperti Naive Bayes atau Decision Trees dapat meningkatkan kemampuan deteksi intrusi pada jaringan komputer. Dengan memantau pola lalu lintas jaringan dan perilaku pengguna, sistem dapat mengidentifikasi aktivitas yang tidak biasa atau mencurigakan yang mungkin merupakan tanda adanya serangan. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini mengintegrasikan algoritma deteksi anomali dengan Snort. **Perbedaan dengan Penelitian yang Akan Dilakukan:**

		Penelitian ini dilakukan dengan mengintegrasikan algoritma baru ke dalam Snort sebagai alat pendeteksi intrusi berbasis rules yang sudah matang.
13.	**Penerapan SNORT Sebagai Sistem Pendeteksi Keamanan Jaringan.** **Tahun:** 2022 **Peneliti:** Rahmat Novrianda Dasmen.	**Hasil Penelitian:** Berdasarkan hasil penerapan pendeteksi jaringan di snort menggunakan IDS (*Instruction Detection System*) dapat disimpulkan bahwa penggunaan sistem ini dapat mempermudah mendeteksi jaringan yang termasuk illegal (berbahaya untuk sebuah sistem operasi), mencegah kehilangan data dan informasi. Dengan adanya snort IDS dapat mengetahui jaringan apa saja yang masuk ke dalam system operasi. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini menggunakan Snort dalam penelitiannya yang juga digunakan pada penelitian yang akan dilakukan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini hanya melakukan pendeteksiannya saja tanpa menganalisis solusi apa yang bisa diberikan untuk mengantisipasi adanya serangan berikutnya.
14.	**Early Intrusion Destection System (IDS) Using Snort And Telegram Approach** **Tahun:** 2 **eliti:** Erlansari	**Hasil Penelitian:** Penelitian ini berhasil mengembangkan sebuah sistem deteksi intrusi yang memanfaatkan Snort, yang merupakan salah satu sistem deteksi intrusi berbasis *rules* yang didesain untuk mendeteksi serangan *port scanning* dan *brute force*. **Alasan Menjadi Tinjauan Penelitian:**

		Penelitian ini menggunakan Snort dalam penelitiannya yang juga digunakan pada penelitian yang akan dilakukan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini menggunakan pendekatan Telegram untuk memberikan peringatan dini pada administrator atau pengguna sistem tentang serangan yang terdeteksi dengan menggunakan fitus pesan pada Telegram.
15.	**Performance Analysis and Comparison of Snort on VariousPlatform** **Tahun:** 2020 **Peneliti:** Alka Gupta	**Hasil Penelitian:** Penelitian ini menyajikan analisis perbandingan kinerja Snort pada setiap platform sistem operasi. Hasilnya menunjukkan perbedaan kinerja yang meliputi perbedaan throughput, latensi, dan efesiensi penggunaan sumber daya. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini menggunakan Snort dalam penelitiannya yang juga digunakan pada penelitian yang akan dilakukan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini menggunakan perbandingan penggunaan Snort pada Linux, Mac OS, dan Windows OS.
16.	**Application of Snort and Wireshark in Network Traffic** **ılysis** **ıun:** 1	**Hasil Penelitian:** Penelitian ini melakukan analisis mendalam terhadap lalu lintas jaringan yang direkam dari lingkungan jaringan yang sesungguhnya. Analisis dilakukan pada berbagai aspek yakni lalu lintas jaringan, protokol yang digunakan, alamt sumber

	Peneliti: G. Jain	dan tujuan, dan juga pola komunikasi untuk mengidentifikasi pola yang mencurigakan. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini menggunakan Snort dalam penelitiannya yang digunakan pada penelitian yang akan dilakukan. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian menggunakan wireshark dalam proses pemantauan lalu lintas jaringan yang terjadi.
17.	**Network Packet Analysis in Real Time Traffic and Study of Snort IDS During the Variants of DoS Attack.** **Tahun:** 2020 **Peneliti**: Nilesh Kunhare	**Hasil Penelitian:** Penelitian ini melakukan analisis lalu lintas jaringan secara *real-time* dan mengkaji kinerja Snort IDS selama berbagai variasi serangan DoS. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini melakukan analisis jaringan yang terkonfigurasi oleh Snort. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini hanya melakukan analisis terhadap jaringan yang telah terkonfigurasi *rules* Snort.
18.	**Perancangan dan Analisis Sitem Keamanan Jaringan Komputer Menggunakan Snort** **Tahun:** 2021 **Peneliti:** ırou Wesley Purba	**Hasil Penelitian:** Penelitian ini dilakukan dengan menghubungkan beberapa komputer yang terdiri dari *server, client,* dan *attacker*. Komputer *server* telah diinstal *software* Snort yang berfungsi untuk menangkap paket yang menuju ke komputer *server* tersebut. Sedangkan komputer *attacker* telah diinstal *software* hping3 yang berfungsi untuk melakukan serangan DDOS. **Alasan Menjadi Tinjauan Penelitian:**

		Penelitian ini menggunakan Snort sebagai objek dalam penelitiannya. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini menggunakna serangan dengan menggunakan *software* hping3 dengan jenis serangan yang dilakukan adalah DDOS
19.	**Intrusion Detection and Prevention System Using Snort** **Tahun:** 2022 **Peneliti:** Shubham Sharma	**Hasil Penelitian:** Penelitian ini mengembangkan IDS dan IPS dengan menggunakna Snort sebagai *platform* utama yang mencakup instalasi, konfigurasi, dan penyesuaian Snort sesuai kebutuhan penelitian terkait. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini menggunkan Snort sebagai objek dalam penelitiannya. **Perbedaan dengan Penelitian yang Akan Dilakukan:** Penelitian ini melakukan konfigurasi sistem keamanan dengan mengembangkan IDS dan juga IPS secara bersamaan.
20.	**Analisis Kinerja Sistem Pencegahan Sitem Penyusupan Jaringan Menggunakan Honeypot Pada Windows.** **Tahun:** 2019 **eliti:** ma	**Hasil Penelitian:** Penelitian ini mencakup implementasi dan konfigurasi sistem Honeypot pada lingkup Windows yang digunakan untuk menarik serangan serta memantau dan mempelajari taktik serta teknik yang digunakan oleh penyerang. **Alasan Menjadi Tinjauan Penelitian:** Penelitian ini membantu peneliti dalam merancang sistem serangan yang digunakan pada penelitian yang akan dilakukan. **Perbedaan dengan Penelitian yang Akan Dilakukan:**

		Penelitian ini melakukan konfigurasi sistem keamanan dengan menggunakan Honeypot.

2.2 Jaringan Komputer

2.2.1 Sejarah Jaringan Komputer

Sebelum kehadiran dari jaringan komputer yang memungkinkan untuk komunikasi langsung antar komputer, komunikasi serta perhitungan yang melibatkan komputer pada zaman dahulu, biasanya dilakukan dengan cara manual yang mana manusia sebagai alat komunikasinya.

Konsep jaringan komputer pertama kali muncul pada tahun 1940-an di Amerika Serikat pada salah satu poyek yang cukup besar saat itu yakni pengembangan komputer MODEL I yang dikerjakan di Laboratorium Bell dan grup riset Harvard University. Pada awal pengerjaannya, proyek ini hanya ingin memanfaatkan sebuah perangkat komputer yang harus digunakan bersama.

Memasuki tahun 1950-an saat jenis komputer mulai membesar hingga teciptanya super komputer, yang mana komputer diharuskan untuk melayani beberapa terminal. Kemudian ditemukan konsep distribusi proses berdasarkan waktu yang kemudian dikenal dengan nama TSS (*Time Sharing System*), maka bentuk pertama dari jaringan diaplikasikan. Pada sistem ini beberapa terminal dihubung seri pada sebuah host komputer. Pada prosess TSS mulai Nampak perpaduan antara teknologi komputer dan teknologi telekomunikasi yang pada permulaannya berkembang sendiri-sendiri.

Pada tahun 1970, ketika beban pekerjaan bertambah banyak dan harga dari perangkat komputer besar terasa mahal, diterapkanlah pemrosesan distribusi (*Distributed Processing*) yang mana pada proses ini beberapa *host* komputer mengerjakan suatu pekerjaan besar yang dilakukan secara paralel untuk melayani terminal-terminal yang dihubung seri pada setiap *host* komputer. Dalam proses distribusi ini, sudah mutlak diperlukan paduan antara teknologi komputer dan telekomunikasi sebab semua *host* komputer wajib melayani terminal-terminal

u perintah dari komputer pusat.

anjak ketika harga komputer kecil mulai menurun dengan konsep

yang sudah matang, penggunaan dari komputer beserta jaringannya sudah

mulai beragam dimulai dari menangani proses bersama maupun komunikasi antar komputer (*Peer to Peer System*) saja tanpa melalui komputer pusat maka dari itu mulailah dikembangkan teknologi jaringan lokal yang kemudian dikenal dengan sebutan LAN.

2.2.2 Pengertian Jaringan Komputer

Jaringan komputer adalah interkoneksi (saling berhubungan) antara sekelompok komputer dan kelompok lainnya. Dengan jaringan komputer, komputer menjadi satu kesatuan yang menyebabkan data dapat diakses dan dipertukarkan tanpa harus memindahkan dan membawa media penyimpanan data ke komputer lain. Selain itu, jaringan komputer juga dapat terkoneksi dengan internet.

Jaringan komputer ini sendiri merupakan jaringan telekomunikasi yang memungkinkan antar komputer untuk bisa berkomunikasi dengan saling bertukar data, jaringan data dibangun dengan kombinasi antara perangkat keras dan perangkat lunak. Ketika terdapat dua atau lebih komputer saling berkomunikasi atau bertukar data, sebenarnya ada bagian-bagian dari jaringan yang berperan sebagai pihak yang menerima dan ada yang berperan sebagai pihak yang memberi. Pihak yang menerima layanan disebut sebagai *client* dan pihak yang memberi layanan disebut sebagai *server*.

Terdapat beberapa jenis jaringan komputer yang umum dijumpai dan diklasifikasikan menurut cakupan areanya, yaitu:

- LAN (*Local Area Network*)

  Local Area Network ialah konsep yang menghubungkan perangkat jaringan dalam cakupan wilayah yang relatif kecil. Umumnya digunakan pada gedung sekolah, kantor, universitas, dan sebagainya. Konsep dari jaringan ini cenderung pada menggunakan konektivitas, misalnya Ethernet. Namun, terdapat juga LAN dengan teknologi nirkabel atau *wireless* yang kemudian dikenal sebagai *Wireless Local Area Network* (WLAN).

- MAN (Metropolitan Area Network)

  Metropolitan Area Network ialah konsep yang menghubungkan perangkat
  an dalam cakupan wilayah yang cukup luas karena menghubungkan
  gkat jaringan antar kota. Jika penggunaan dari *Local Area Network*
  gap tidak memungkinkan untuk membangun jaringan maka jaringan

Metropolitan Area Network menggunakan akan digunakan karena cakupan wilayahnya lebih besar daripada *Local Area Network*.

- WAN (*Wide Area Network*)

  Metropolitan Area Network ialah konsep yang menghubungkan perangkat jaringan dalam cakupan wilayah sangat luas dan menggunakan peralatan yang sangat canggih jika dibandingkan dengan MAN dan LAN. Konsep ini biasanya digunakan untuk menghubungkan atau membangun koneksi jaringan antar negara atau bahkan antar benua, salah satu penggunaan peralatan canggih yang digunakan adalah *fiber optic* yang instalasinya ditanam di dalam tanah maupun di bawah laut.

2.3 Sistem Keamanan Jaringan

Adanya keamanan dalam jaringan komputer sangat penting dilakukan untuk dapat memonitor akses jaringan dan juga mencegah terjadinya penyalahgunaan sumber daya jaringan yang tidak sah. Tugas dari sistem keamanan jaringan dikontrol oleh administrator jaringan. Segi keamanan didefinisikan dalam lima poin yakni *confidentiality* yang mensyaratkan bahwa informasi (data) hanya dapat diakses oleh pihak berwenang, Integrity yang mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang berwenang, Availability yang mensyaratkan bahwa informasi tersedia kepada pihak yang berwenang ketika dibutuhkan, *authentication* yang mensyaratkan bahwa pengirim dari suatu informasi dapat diidentifikasi dengan benar dan dapat dijamin bahwa identitasnya tidak palsu, dan yang terakhir ialah *nonrepudiation* yang mensyaratkan bahwa pengirim maupun penerima informasi tidak dapat menyangkal pengiriman ataupun penerimaan pesan.

Keamanan jaringan sendiri bisa didefinisikan sebagai perangkat komputer yang terhubung ke jaringan memiliki ancaman keamanan yang jauh lebih besar jika dibandingkan dengan komputer yang tidak terhubung dengan apapun. Dengan diadakannya pengendalian yang lebih teliti, maka resiko tersebut dapat dikurangi. Selama bertahun-tahun , telah dikembangkan berbagai jenis *tool* yang bertujuan nguji keamanan jaringan serta mengeksploitasi *vulnerbiality* jaringan.

2.4 Network Security Attack

Serangan terhadap jaringan komputer bisa kita kaitkan dengan *computer abuse* (penyalahgunaan komputer), *computer crime* (kejahatan komputer), dan *computer related crime* (kejahatan yang berhubungan dengan komputer). *Computer abuse* dapat kita definisikan sebagai Tindakan yang sengaja melibatkan komputer yang pelaku kejahatannya memperoleh keuntungan dari korbannya. *Computer crime* dapat didefinisikan sebagai tindakan melanggar hukum yang mana pengetahuannya tentang komputer sangat luas, umumnya dikenal sebagai "peretas" yang secara ilegal menjelajahi ataupun mencuri informasi pribadi suatu perusahaan maupun individu. *Computer related crime* adalah dapat didefinisikan sebagai kejahatan yang berkaitan dengan komputer tidak terbatas pada jenis kejahatan apapun. Kejahatan tersebut mencakup kejahatan yang menghancurkan komputer itu sendiri maupun komputer tersebut beserta isinya.

Berdasarkan buku Ec-Council, serangan keamanan dapat diklasifikasikan menjadi:

1. Serangan pasif yang melibatkan penyadapan dan pemantauan lalu lintas jaringan dan aliran data pada jaringan target dan tidak merusak data. Serangan ini sangat sulit dideteksi karena penyerang tidak memiliki interaksi aktif dengan sistem atau jaringan target.
2. Serangan aktif yang merusak data dalam transit atau mengganggu komunikasi atau layanan antar sistem untuk melakukan *bypass* atau membobol sistem yang aman. Penyerang meluncurkan serangan pada sistem atau jaringan target dengan mengirimkan *traffic* secara aktif yang dapat dideteksi.
3. Serangan *close-in* yang dilakukan saat penyerang berada di dekat proximity fisik dengan sistem atau jaringan target untuk mengumpulkan, modifikasi informasi atau mengganggu aksesnya.
4. Serangan distribusi terjadi ketika penyerang mengutak-atik *hardware* atau *software* sebelum instalasi.

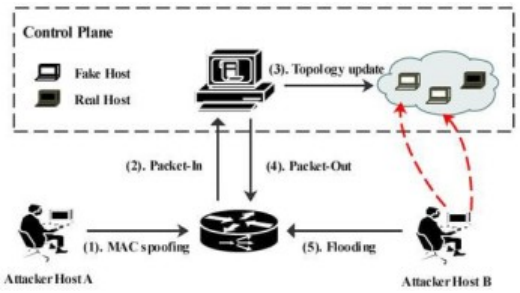
2.5 Attacks for Wireless Network

pada jaringan Wi-Fi umumnya terbagi atas dua kategori, yakni serangan perlindungan kerahasiaan data, kontrol terhadap akses jaringan, dan data; yang kedua adalah serangan berdasarkan pendekatan unik terhadap

penerapan jaringan nirkabel, desain, dan pemeliharaan. Selain itu, serangan pada jaringan Wi-Fi dapat terbagi atas tujuh kategori:

a. *Injection*

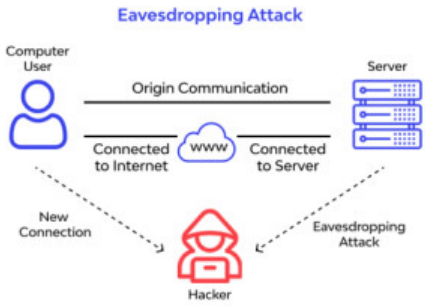
Pada jaringan Wi-Fi, seoarang penyerang dapat menerapkan injeksi pesan dengan menginstal *software* terkait. Penyerang dapat mengimplementasikan paket data palsu, memodifikasi header atau akhir dari paket data, serta mengutak-atik bagian apapun pada paket data. Setelah paket diinjeksikan ke transmisi data yang relevan maka penyerang dapat mengontrol seluruh proses pengiriman pesan.



Gambar 1. *Injection*

b. *Eavesdropping Adversary and Network Traffic Analysis*

Karena karakteristiknya, media transmisi jaringan Wi-Fi bersifat terbuka sehingga penyerang dapat menguping informasi jaringan pada jaringan Wi-Fi melalui perangkat terkait. Meskipun pesan telah dienkripsi, tetap ada kerentanan dalam proses transmisi data. Penyerang dapat melakukan analisis dan juga perhitungan pada paket informasi untuk mendapatkan sebagian atau keseluruhan dari pesan tertentu.



Gambar 2. *Eavesdropping Adversary and Network Traffic Analysis*

c. *Unauthorized Access*

Pada jaringan Wi-Fi, sinyal ditransmisikan oleh gelombang elektromagnetik. Dalam area layanan yang dibentuk oleh AP (*access point*), setiap terminal nirkabel dapat mengakses AP. Akses tidak sah mengartikan bahwa pengguna mengakses terminal nirkabel perangkat melalui AP, namun akses ini tidak diizinkan oleh AP. Jaringan Wi-Fi menerapkan mekanisme autentikasi searah, terminal kabel mengirimkan permintaan autentikasi ke AP, dan AP tidak mengautentikasi terminal nirkabel. Autentikasi searah akan memberikan kesempatan kepada penyusup untuk memasuki jaringan melalui AP. Sejumlah besar permintaan autentikasi dapat menyebabkan AP tidak berfungsi dengan baik dan kemudian penyerang dapat mencuri data atau informasi jaringan.

d. *Session Hijacking*

Serangan ini umumnya terdiri atas dua bagian. Pertama, penyerang menggunakan beberapa metode untuk memaksa *station* (STA) untuk memutuskan hubungan dari AP. Setelah itu, penyerang akan membuat koneksi dengan AP sebagai STA palsu, mencusi sesi pesan, dan mengontrol sesi pengiriman dan penerimaan. Serangan ini umumnya juga terbagi atas dua bentuk yaitu pembajakan aktif dan pembajakan pasif. Pembajakan aktif dilakukan dengan mengganti *host* dalam sesi dengan penyerang lalu mengmbil alih proses transmisi data. Pembajakan pasif dilakukan dengan memantau aliran data antara dua pihak untuk mendapatkan data sensitif atau data yang bersifat rahasia.

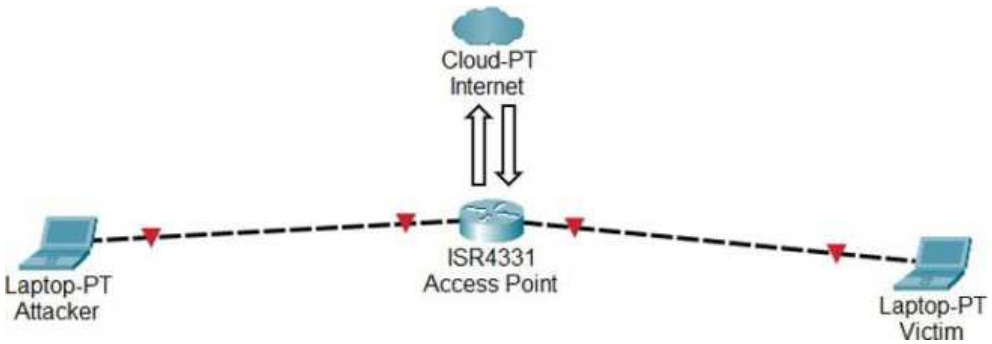
e. *Forged AP*

Alamat MAC AP disertakan pada *header* paket di jaringan Wi-Fi. *Header* paket data tersebut ditampilkan sebagai *clear text* selama proses transmisi data. Penyerang bisa memperoleh alamat MAC dari AP dan mengubah alamat MAC-nya ke alamat AP yang valid.

in-the-Middle Attack

Serangan *man-in-the-middle* adalah salah satu bentuk serangan tidak langsung. Mode serangan ini adalah untuk menempatkan komputer yang dikendalikan penyusup antara dua komputer yang saling berkomunikasi yang terhubung ke jaringan melalui berbagai cara teknis. Komputer ini dapat mencegat serta mengutak-atik data komunikasi tanpa pihak komputer *host* dan komputer *client* menyadarinya. Ketika *host* A dan *host* B berkomunikasi, infomasi akan dteruskan oleh *host* C yang berperan sebagai perantara. Dengan cara ini, host C dapat menguping dan mengutak-atik informasi dari proses komunikasi tersebut dan mencapai tujuannya dengan mengirimkan informasi palsu ke salah satu *host*.

g. DoS



Gambar 3. *Denial of Service*

Serangan DoS (Denial of Service) adalah jenis serangan yang sangat serius dan yang paling umum dijumpai pada jaringan kabel maupun jaringan nirkabel. Tujuan dari serangan ini adalah untuk membuat jaringan tidak dapat melayani pengguna yang sah. Penyerang dapat memulai berbagai bentuk penolakan serangan layanan. Penyerang dapat menyiarkan sejumlah besar sinyal interferensi. Saluran jaringan nirkabel selalu sibuk, sehingga pengguna yang sah tidak dapat menggunakan saluran untuk mengirim permintaan normal. Seorang penyerang juga dapat mengirim sejumlah besar pesan yang tidak valid ke AP. a, sumber daya AP habis dan mengalami *crash*. Serangan DoS sendiri beberapa bentuk jenis serangan diantaranya ialah:

1. *Ping of Death*

   Serangan ini dilakukan dengan cara mengirimkan paket IP lebih dari batas minimum *fragbites* dalam satu kali pengiriman paket yang diijinkan oleh protokol IP. Ini adalah salah satu fitur protokol TCP/IP dengan memecah-belah paket yang masuk menjadi sub-paket. Jenis serangan ini menggunakan *utility ping* yang ada pada sistem operasi computer. Ping ini digunakan untuk mengecek waktu yang akan diperlukan untuk mengirim data tertentu dari satu komputer ke komputer lainnya.

2. *Ping Flood*

   Ping flood terjadi Ketika target menerima *request* ICMP secara cepattanpa menunggu respon. Jenis serangan seperti ini akan menyebabkan semua *bandwidth* yang masuk ataupun keluar terkena dampaknya yang akhirnya menyebabkan server menjadi lambat.

3. *Port Scanning*

   Port scanning adalah tahapan awal untuk mendeteksi *port-port* yang terbuka dan mendapatkan informasi dari *port* yang terbuka pada target, servis apa yang dijalankan, versi dari server, dan sebagainya. Dengan sistem ini memungkinkan menjadi awal mula terjadinya serangan terhadap sumber daya yang terdapat pada jaringan, karena dengan informasi tersebt mata penyerang dapat secara langsung memanfaatkannya untuk melakukan eksploitasi dari protokol/*port* tersebut.

2.6 Intrusion Detection System

Intrusion Detection System (IDS) merupakan aset berharga dalam sistem keamanan jaringan. IDS berusaha untuk memantau atau bahkan mencegah upaya yang mengganggu atau membahayakan *user* dari sumber daya sistem dan jaringan. Secara umum IDS terbagi atas 3 jenis yakni *Network Intrusion Detection System* (NIDS) yang merupakan IDS yang memantau lalu lintas jaringan berbahaya, *Host Intrusion Detection System* (HIDS) yang memantau aktivitas pada suatu host, dan *Distributed Intrusion Detection System* yang mengkorelasikan peristiwa dari HIDS atau NIDS yang berbeda.

Intrusi juga dapat didefinisikan sebagai segala jenis aktivitas tidak sah yang menyebabkan kerusakan pada sistem informasi. Hal ini dapat diartikan bahwa setiap serangan yang dapat menimbulkan kemungkinan ancaman terhadap kerahasiaan, integritas, atau ketersediaan informasi akan dianggap sebagai gangguan. Misalnya aktivitas yang membuat layanan komputer tidak responsif terhadap pengguna yang sah dianggap sebagai gangguan. IDS ini sendiri dapat berupa perangkat lunak atau perangkat keras yang digunakan untuk mendeteksi akses tidak sah dari sistem komputer atau jaringan. Sistem ini akan memantau lalu lintas pada jaringan lalu mencari dan mencatat ancaman dan memperingatkan untuk merespon. Tujuan dari IDS adalah untuk mengidentifikasi berbagai jenis lalu lintas jaringan berbahaya dan penggunaan komputer yang tidak dapat diidentifikasi oleh *firewall*. Ini sangat penting untuk mencapai perlindungan yang tinggi terhadap tindakan yang mengganggu ketersediaan, integritas, bahkan kerahasiaan sistem komputer. Sistem IDS dapat dikategorikan secara luas menjadi dua kelompok yakni *Signature Intrusion Detection System* (SIDS) dan *Anomaly Based Intrusion Detection System* (AIDS).

IDS dapat memantau status jaringan yang sedang berjalan dan sistem secara *real time* dan mendeteksi berbagai jenis serangan. Telah banyak penelitian terkait penggunaan teknologi IDS dalam skala besar jaringan area lokal nirkabel seperti kampus dan jaringan perusahaan.

2.7 Snort

Snort adalah tool atau aplikasi yang bersifat *open source* dari IDS. *Snort* dirancang agar dapat beroperasi pada *command line* dan diintegrasikan ke beberapa aplikasi pihak ketiga serta mendukung *cross platform*. *Snort* akan menganalisis seluruh lalu lintas pada jaringan untuk melakukan *sniffing* dan mencari beberapa jenis penyusupan ataupun serangan yang terjadi dalam sebuah jaringan. *Snort* dapat dioperasikan dalam 3 mode yakni:

1. *Sniffer mode*, yang dioperasikan untuk melihat paket yang lewat di dalam jaringan.
2. *Packet Logger Mode*, yang dioperasikan untuk mencatat semua paket yang lewat di jaringan untuk dianalisa nantinya.
3. *Intrusion Detection Mode*, yang dioperasikan untuk mendeteksi serangan yang dilakukan pada jaringan komputer. Penggunaan mode ini, perlu dilakukan setup dari beberapa *rules* yang akan membedakan paket normal dan paket yang terindikasi sebagai serangan.