BAB III

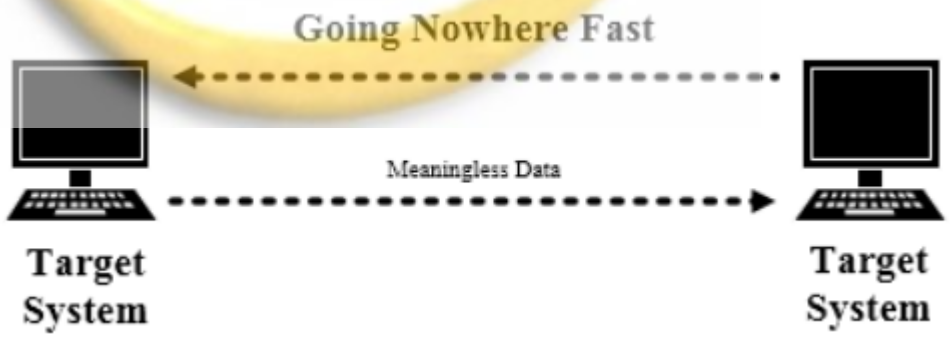
ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Serangan

Berikut ini adalah langkah analisis serangan pada tugas akhir ini. Percobaan serangan yang dilakukan adalah 2 jenis serangan. Serangan yang dilakukan adalah sebagai berikut:

a. DOS (*Denial-of-Service)* Attack

Pada tugas akhir ini serangan DOS dilakukan dengan menggunakan tools LOIC (Low Orbit Ion Canon). Cara kerja serangan DOS ini umumnya dilakukan dengan cara membanjiri lalu lintas jaringan dengan paket-paket tertentu sehingga mengakibatkan performa jaringan menurun ataupun membuat server tidak dapat diakses karena terlalu banyak permintaan service. Pada tugas akhir ini serangan DOS yang dilakukan adalah UDP Flooding. UDP Flooding merupakan teknik yang dilakukan dengan cara membanjiri lalu lintas jaringan dengan mengirimkan permintaan paket UDP kesalah satu mesin dalam jumlah besar sehingga mengakibatkan suatu mesin tersebut tidak dapat diakses serta jaringan yang diserang menjadi lambat. UDP flooding bersifat *connectionless.* Yaitu tidak memperhatikan apakah paket yang dikirimkan diterima atau tidak.



Gambar 15. DOS Attack

b. Sniffing Attack

Pada tugas akhir ini, penulis menggunakan sniffing attack untuk ujicoba serangan. Sniffing attack adalah salah satu jenis serangan yang dilakukan oleh penyerang yang ingin mengetahui kondisi dari jaringan yang akan diserang. Contohnya penyerang ingin mengetahui port apa saja yang terbuka dan penyerang maka akan mencari kelemahan dari port tersebut. Teknik sniffing ini merupaka suatu Teknik yang sangat susah untuk dicegah. Salah satu cara untuk dapat mendeteksinya adalah dengan IDS (Intrusion Detection System). Aktifitas sniffing terbagi menjadi 2 jenis yaitu passive sniffing dan active sniffing. Pada tugas akhir ini dilakukan jenis penyadapan passive sniffing. Passive sniffing dilakukan tanpa merubah data atau paket apapun pada jaringan. Tools yang digunakan untuk sniffing adalah Nmap. Nmap merupakan sebuah tools open source untuk eksplorasi dan audit keamanan jaringan. Nmap dirancang untung memeriksa jaringan secara cepat. Nmap menggunakan paket IP RAW untuk menentukan host mana saja yang tersedia pada jaringan, layanan apa yang ada pada jaringan, system operasi, firewall dan karakteristik lainnya.

3.2 Analisis Solusi

Dalam tugas akhir ini terdapat beberapa masalah yaitu infrastruktur jaringan yang rawan terhadap serangan dan tidak adanya pendeteksian adanya intrusi. Ada banyak sekali tools untuk mendeteksi adanya intrusi, Snort, Suricata, Bro-IDS, Expert-BSM, Fail2ban dan lainnya. Berikut beberapa penelitian terdahulu dan yang menginspirasi tugas akhir ini:

a. Snort

Snort adalah tools open source untuk IDS yang menyediakan analisis traffic secara realtime dan membuat log paket system. Snort merupakan tools analysis diantaranya sniffer, packet logger, forensic data analysis tools dan NIDS. Snort pun dikembangjan sebagai Intrusion Prevention System yang berjalan pada mode inline. Cara kerja snort ini adalah single thread. Jadi ketika adanya sebuah intrusi snort bekerja secara tunggal dalam satu waktu

b. Suricata

Sebuah mesin IDPS open source yang dibuat oleh perusahan non-profit Open Information Security Foundation. Mesin IDPS ini berbasis rules, sejumlah

aturan yang dibuat untuk mengawasi jaringan dan memberi peringatan kepada admin jika ada tindakan mencurigakan atau Serangan terhadap server. Suricata dirancang untuk dapat menyesuaikan dengan arsitektur dan perangkat jaringan terkini. Suricata bekerja secara multi thread.

c. Bro-IDS

Bro-IDS adalah salah satu framework monitoring jaringan yang mendeteksi intrusi secara real-time. Bro-IDS terdiri dari libpcap untuk menangkap paket, even engine untuk menghasilkan events berdasarkan analisis paket dan rule yang ditulis pada script. Script rule ini ditulis dalam Bahasa Bro.

d. Expert-BSM

Expert-BSM adalah sebuah HIDS (Host Intrusion Detection Sysytem) yang menggunakan knowledge base untuk mendeteksi intrusi dari dalam, pelanggaran kebijakan, oenyalahgunaan hak akses, dan lainnya. Expert-BSM menyediakan pengumpulan data, analisis intrusi dan antarmuka manajemen ids.

e. Fail2ban

Fail2ban memeriksa log dan mendeteksi patterns yang kemungkinan percobaan intrusi setelah itu melakukan aksi seperti menambahkan firewall dan memberitahu sys admin melalui email. Fail2ban bekerja secara multi thread dan listens pada unix socket.

3.3 Analisis Solusi Terbaik

a. Software

Dalam implementasi IDS dan IPS dalam IoT membutuhkan perangkat lunak. Dalam [2] dibahas perbandingan aplikasi untuk IDS dan IPS salah satunya *Suricata*. *Suricata* memiliki performa lebih baik daripada *snort*[2]. *Suricata* adalah *tool* gratis yang memiliki kemampuan untuk mendeteksi adanya intrusi juga penanganannya. *Suricata* terdapat juga di sistem operasi linux [2]. Berikut perbandingan beberapa tools IDS yang didapat dari sumber [2].

Tabel 6. Perbandingan *tools* IDS

Framework	Open Source	Linux Support	Network Based	IPS Function	Multi Thread	Scalability
Snort	✓	✓	✓	✓	✕	Medium
Suricata	✓	✓	✓	✓	✓	High
Bro-IDS	✓	✓	✓	✕	✕	Low
Expert-BSM	✕	✕	✓	✕	✕	High
Fail2ban	✓	✓	✓	✓	✓	High

Pada tabel tersebut terdapat solusi terbaik yaitu Suricata dan Fail2ban. Fail2ban memiliki arsitektur yang kompleks sehingga tidak disarankan untuk penggunaan cloud dengan banyak server dan sensor. Fail2ban tidak didukung oleh update signature yang tersedia di internet, sehingga harus mendefinisikan manual sedangkan Suricata signature tersebut bisa didownload dan langsung diterapkan. Pada tugas akhir ini ditentukan Suricata sebagai IDS/IPS software karena memiliki beberapa keunggulan yang telah disebutkan diatas.

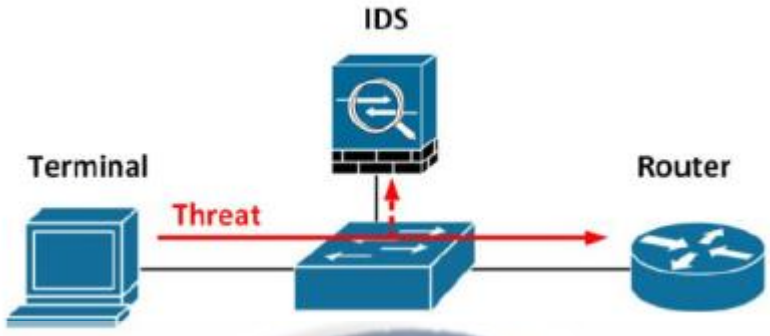
b. Hardware

Banyak sekali solusi yang ditawarkan sebagai hardware untuk mendeteksi Intrusi, seperti Palo Alto, Cisco, dan lainnya. Namun solusi tersebut terkendala biaya. Untuk membeli sebuah mesin IDS Palo Alto minimal memiliki dana sebesar $2000. Selain itu jika kita menggunakan hardware ini, tidak cocok untuk platform IoT dikarenakan perangkatnya yang besar sehingga tidak fleksibel pada penerapannya.

Untuk mengatasi masalah fleksibilitas yang ada pada IoT digunakanlah development boards. Banyak development boards yang tersedia dipasaran seperti Beaglebone, Banana Pi2, VoCore, Orange Pi, Raspberry Pi 2 dan 3. Raspberry Pi 3 dipilih karena sesuai dengan requirements dari Suricata seperti sistem operasi menggunakan linux, Ethernet Interface, USB port, RAM minimal 1 GB, multicore CPU.

3.4 Perancangan Sistem

Pengujian pada tugas akhir ini dilakukan didalam jaringan tersebut. Berikut topologi yang digunakan dalam pengujian system.



Gambar 16. Skenario pengujian IDS

Perancangan topologi seperti diatas menunjukan bahwa mesin IDS diletakkan didalam jaringan. Mesin IDS akan menangkap dan memeriksa segala jenis paket data lalu akan memeriksa jika terdapat serangan yang sesuai dengan database Suricata. Jika tidak terdapat keanehan maka akan memunculkan kedalam log yang nanti akan dibahas pada bab empat. Jenis mesin IDS yang dipakai pada penelitian ini adalah *Network Intrusion Detection System* (NIDS). NIDS bekerja menjadi IDS pada sebuah jaringan.

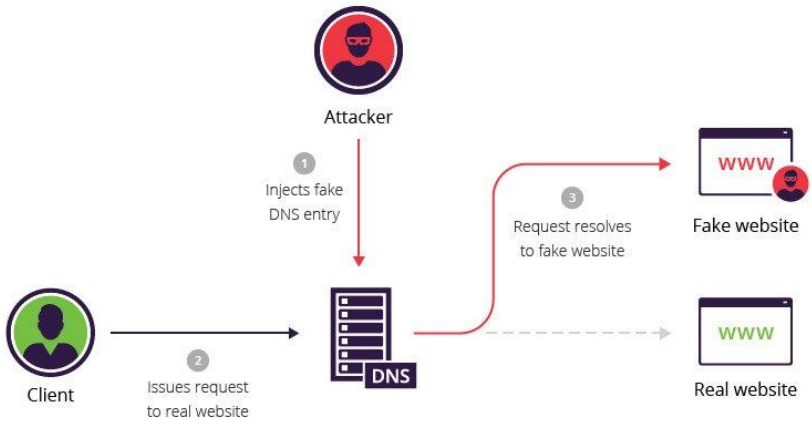
3.3.1 Perancangan Pengujian DOS Attack menggunakan LOIC

LOIC adalah sebuah tool yang dibuat untuk menghasilkan serangan DOS. LOIC berbasis GUI sehingga mudah untuk digunakan. Salah satu client mengirimkan serangan DOS menggunakan LOIC kesalah satu mesin misalkan Router atau device lain. Jenis serangan yang diterapkan pada system ini adalah UDP Flooding dengan 1234. Serangan UDP Flooding tidak mementingkan apakah paket tersebut diterima atau tidak.

3.3.2 Perancangan Pengujian Sniffing dengan Nmap

Pada tugas akhir ini pengujian sniffing dengan menggunakan Nmap. Pengujian dilakukan dengan cara memindai keseluruhan jaringan yang ada dan memeriksa port yang terbuka.

3.3.3 Perancangan Pengujian *MitM* menggunakan Ettercap



Gambar 17. DNS Spoofing

Pada tugas akhir ini pengujian *Man in the Middle Attack* menggunakan *tools* Ettercap. Jenis serangan *Man in the Middle Attack* yang digunakan pada penelitian ini adalah *DNS Spoofing*. Penyerang akan melakukan manipulasi terhadap alamat yang dituju.

3.5 Kebutuhan Perangkat

Kebutuhan perangkat ini merupakan kebutuhan untuk melakukan pendeteksian serangan, dimana kebutuhan perangkat ini yaitu kebutuhan software dan hardware.

a. Kebutuhan Software

Tabel 7. Kebutuhan software

No	Software	Fungsi
1	Suricata	Sebagai software yang digunakan untuk melakukan pendeteksian intrusi.
2	Unix Terminal	Sebagai software untuk melihat log adanya deteksi
3	LOIC	Sebagai software yang digunakan untuk melakukan serangan DOS
4	Nmap	Sebagai software yang digunakan untuk melakukan network scanning
5	Ettercap	Sebagai software untuk MiTM

b. Kebutuhan Hardware

Tabel 8. Kebutuhan hardware

No	Hardware	Spesifikasi
1	Raspberry Pi 3	SoC: Broadcom BCM2837, CPU: 4× ARM Cortex-A53, 1.2GHz, GPU: Broadcom VideoCore IV, RAM: 1GB LPDDR2 (900 MHz), Networking: 10/100 Ethernet, 2.4GHz 802.11n wireless, Bluetooth: Bluetooth 4.1 Classic, Bluetooth Low Energy, Storage: microSD, GPIO: 40-pin header, populated, Ports: HDMI, 3.5mm analogue audio-video jack, 4× USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Serial Interface (DSI)
2	Laptop 2 unit	Proc: Core i5 2,2 GHz, RAM: 8 GB, HDD 500 GB
3	Switch	Fastethernet 8 Port