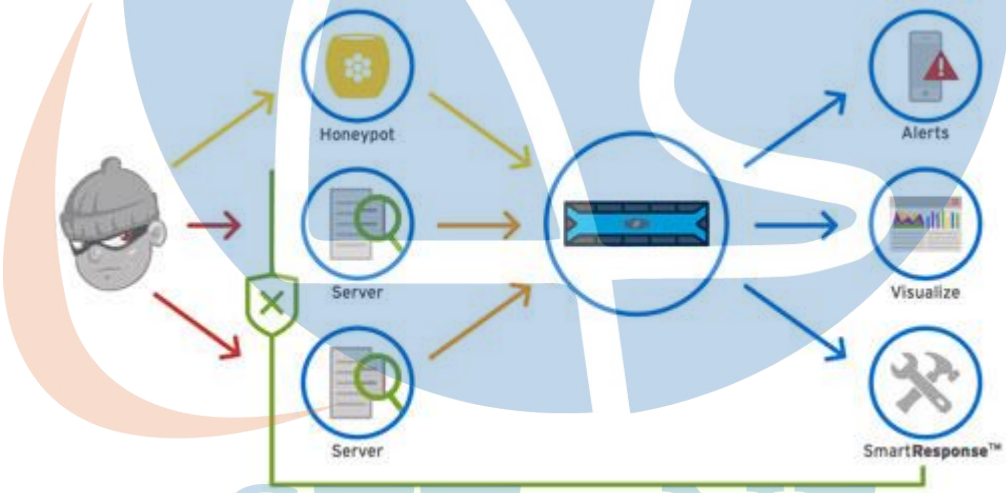
BAB II
LANDASAN TEORI

2.1 Honeypot

Honeypot merupakan sebuah sistem atau komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (attacker). Komputer tersebut melayani serangan yang dilakukan oleh attacker dalam melakukan penetrasi terhadap server tersebut. Honeypot akan memberikan data palsu apabila ada hal aneh yang yang akan masuk ke dalam sistem atau server. Secara teori Honeypot tidak akan mencatat trafik yang legal. [9]

Sehingga dapat dilihat bahwa yang berinteraksi dengan Honeypot adalah user yang menggunakan sumber daya sistem yang digunakan secara ilegal. Jadi Honeypot seolah-olah menjadi sistem yang berhasil disusupi oleh attacker, padahal penyerang tidak masuk ke sistem sebenarnya, tetapi masuk ke sistem yang palsu. [9]



Gambar 2.1 Alur kerja Honeypot

Pada dunia keamanan jaringan informasi banyak professional yang sangat tertarik pada Honeypot karena seorang pengamat serangan akan dapat melihat informasi secara nyata tentang suatu serangan. Kita sering mendengar perusakan sebuah situs web atau sebuah sistem keamanan jaringan pada bank yang di hack, tetapi kebanyakan dari kita tidak mengetahui bagaimana sipenyerang masuk dan apa yang sesungguhnya terjadi. Salah satu hal yang bisa

didapat dengan Honeypot adalah informasi bagaimana seorang penyerang dapat menerobos dan apa yang sudah dilakukannya. [9]

2.1.1 Klasifikasi Honeypot

Honeypot dapat diklasifikasikan berdasarkan pada tingkat interaksi yang dimilikinya, tingkatan ini berdasarkan pada aktivitas user di dalam sebuah sistem yang di izinkan oleh honeypot. Semakin tinggi aktivitas yang di izinkan maka akan semakin tinggi juga tingkat kerentanan sistem asli yang akan dikendalikan oleh peretas. [5]

a. Low Interanction Honeypot

Ini adalah tingkatan pertama atau yang paling rendah di dalam honeypot, sesuai dengan namanya honeypot tipe ini di desain dengan fitur yang sesederhana mungkin serta memiliki fungsionlitas yang dapat di katakan sangat dasar. Honeypot tipe ini hanya menduplikat beberapa layanyan service seperti http, telnet dan ftp. Penyerang dapat melakukan telnet kepada sistem serta mendapatkan informasi identitas sistem layaknya service telnet asli. [1]. Penyerang juga dapat melakukan aktivitas lain seperti brute force ataupun password cracking. Kelebihan menggunakan tingkatan ini ialah mudah untuk di konfigurasikan dan dapat mendeteksi serangan, khususnya pada proses scanning dan dsb. Namun di sisi lain ada beberapa kekurangan yang di dapat di lakukan secara manual oleh seseorang yang bukan menggunakan tools maka penyerang akan mudah mengetahui bahwa sistem ini adalah palsu. [1]

b. Medium Interaction Honeypot

Pada tipe ini memiliki interaksi yang lebih banyak di bandingkan dengan Low Interaction Honeypot. Honeypot tipe ini dapat meniru layaknya seperti Microsoft ISS web server termasuk fiturnya hampir mirip. Bahkan kita juga dapat memasukan sebuah script untuk membuat fungsionalitas yang berbeda. Seperti koneksi HTTP dibuat oleh honeypot ia akan merespon sebagai ISS web server dan memberikan informasi kepada penyerang sesuai dengan permintaan paket. Dengan kemampuan yang dimiliki ini kita dapat lebih leluasa dalam mengkonfigurasikan karena penyerang akan sulit untuk mengetahui bahwa server yang sedang iya serang adalah palsu. [1]

c. High Interaction Honeypot

Tipe ini adalah tipe tertinggi di dalam penggunaan honeypot, yang mana si penyerang dapat berinteraksi penuh dengan sistem tanpa adanya interaksi yang di batasi. Dikarenakan honeypot ini sudah tidak ada nya perbedaan dengan server aslinya. Namun hal tersebut justru beresiko besar untuk server asli jatuh ketangan peretas menjadi tinggi. Karena jika peretas sudah dapat akses root maka dia juga bisa membacdooring server asli. [12]. *Honeypot* tipe ini banyak sekali memiliki kelebihan yang sejajar dengan interaksinya yang sangat kompleks. Umumnya dibangun dengan topologi yang telah di persiapkan secara matang. Selain ini ada beberapa kekurangan di honeypot tipe ini yaitu implementasinya dan konfigurasi yang cukup rumit serta membutuhkan pengawawas yang lebih dan sifatnya berkala. Apalbila honeypot sudah jatuh ketangan peretas maka honeypot tipe ini menjadi ancaman bagi keamanan jaringan tersebut [12].

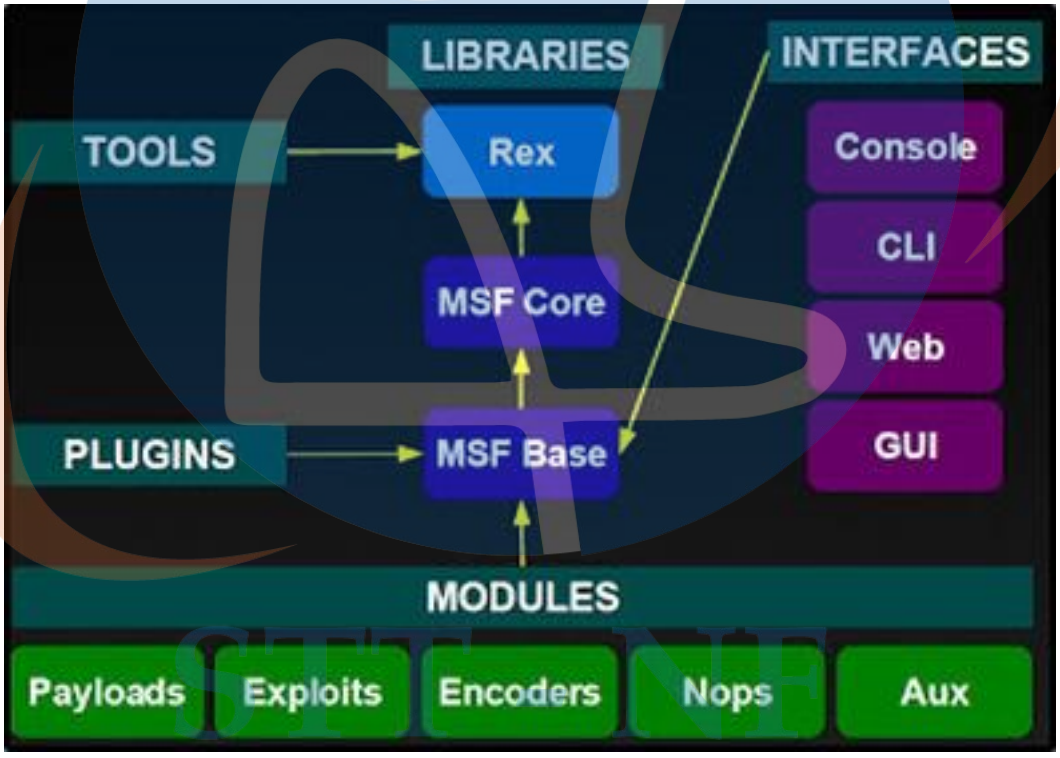
2.2 Dionaea

Dionaea adalah honeypot yang bersifat Low Interaction Honeypot yang diciptakan sebagai pengganti Nepenthes (Sentanoe, 2015). Dionaea menggunakan bahasa pemrograman python sebagai bahasa scripting, libemu untuk mendeteksi shellcode, mendukung Ipv6 dan TLS. Dionaea bertujuan untuk mendapatkan duplikasi data dari malware (Ion, 2015). Perangkat lunak (software) cenderung memiliki bug, yang seringkali dapat dieksploitasi oleh pihak lain untuk memperoleh informasi atau keuntungan.Dionaea memiliki kemampuan untuk mendeteksi dan mengevaluasi payload agar dapat memperoleh salinan malware.

Dalam mendeteksi payload, dionaea menggunakan libemu. Setelah dionaea memperoleh lokasi berkas yang diinginkan penyerang agar diunduh dari shellcode, dionaea akan mencoba untuk mengunduh berkas tersebut. Protokol untuk mengunduh berkas tersebut menggunakan tftp dan ftp yang diimplementasikan menggunakan bahasa pemrograman python (tftp.py dan ftp.py) sebagai bagian dari dionaea. Berkas diunduh melalui http yang dilakukan dalam modul curl yang memanfaatkan libcurl http. [11]

2.3 Metasploit

Metasploit Framework adalah sebuah *platform* pengembangan untuk menciptakan alat keamanan dan eksploitasi. Kerangka ini digunakan oleh profesional keamanan jaringan untuk melakukan tes penetrasi, *administrator* sistem untuk memverifikasi instalasi *patch*, vendor produk untuk melakukan pengujian regresi, dan peneliti keamanan di seluruh dunia. Kerangka ditulis dalam bahasa pemrograman Ruby dan termasuk komponen yang ditulis dalam C dan *assembler*. *Metasploit Framework* adalah sebuah platform pengembangan untuk menciptakan alat keamanan dan eksploitasi. Kerangka ini digunakan oleh profesional keamanan jaringan untuk melakukan tes penetrasi, *administrator* sistem untuk memverifikasi instalasi patch, vendor produk untuk melakukan pengujian regresi, dan peneliti keamanan di seluruh dunia. Kerangka ditulis dalam bahasa pemrograman *Ruby* dan termasuk komponen yang ditulis dalam C dan *assembler*.



Gambar 2.2 Arsitektur Metasploit

Berikut adalah syarat dasar dalam penggunaan *Metasploit*

a. *Exploit* : Hal ini mirip dengan kendaraan dalam kehidupan nyata yang membantu dalam memasuki atau menembus ke system karena setiap kerentanan atau cacat apapun dalam sistem

b. *Payload* : yang menetukan karya mengesploitasi

c. *Auxillary* : ini adalah beberapa aplikasi lain yang dikombinasikan dengan kerangka seperti *sniffer* , alat pencacahan

d. *Meterpreter* : ini adalah *payload* yang disuntikkan ke dalam proses system diesploitasi dimana ada proses tambahan dibuat dalam memori dan kemudian dapat bermigrasi ke setiap proses yang diinginkan dengan menggnakan *PID* (Process ID)

e. *Encoders* : Eksploitasi kadang – kadang terdeteksi oleh anti-virus sehinnga encoders ini dapat digunakan untuk membuat eksploitasi tidak terdeteksi dan memanipulasi kode.

f. *Nops* : dikenal sebagaii generator tidak ada operasi adalah membantu dalam membiarkan eksploitasi tetap tidak terdeteksi dari IDS.

g. *Plugins* : Memperluas fungsionalitas *console* tersebut.

2.4 Advanced Port Scanner

Advanced Port Scanner (APS) merupakan perangkat lunak yang dapat digunakan secara gratis untuk pemindaian port. Aplikasi APS memiliki keunggulan fitur pemindaian *port TCP* dan *UDP* secara lengkap pada alamat komputer tujuan. Kelebihan lain dari aplikasi APS adalah dapat mengetahui versi program yang menggunakan *port.* Penggunaan *APS* dapat dilakukan secara mudah, karena pengguna cukup menginputkan alamat komputer tujuan.

2.5 OWASP ZAP

OWASP ZAP (Zed Attack Proxy) merupakan sebuah aplikasi untuk melakukan penetration testing untuk menemukan *vulnerabilities*/ celah keamanan. Aplikasi *ZAP*

melakukan pengujian dengan menggunakan aplikasi *browser* untuk menjalankan instruksi serangan.

2.6 Metasploit Framework

Metasploit Framework merupakan aplikasi yang memiliki paket serangan *exploit. Metasploit* terdiri atas beberapa versi, yaitu *Framework, Community, Express, dan Pro*. Seluruh versi selain versi *Framework* memiliki interface berbasis web yang dapat dipakai dengan mudah. Dari seluruh versi yang ada, hanya versi *Framework* dan *Community* yang gratis. Selain itu, pengguna versi *Community* perlu melakukan registrasi terlebih dahulu. Modul pada Metasploit dikategorikan menjadi *encoder, nop generator, exploit, payload*, dan *auxiliary*. Modul *exploit* mewakili sebuah celah keamanan yang akan diujikan. Celah keamanan ini memungkinkan penyerang untuk mengakses sistem yang diserang.

2.7 Perangkat Jaringan Komputer

Dalam sebuah jaringan komputer, terdapat dua istilah untuk perangkat yang digunakan yaitu, *end device* dan *inttermediary device.*

1. *End Device*

   Merupakan perangkat pada pengguna jaringan komputer yang menjadi sumber atau tujuan dari pertukaran data. Perangkat ini memberi bentuk antarmuka (*interface)* antara pengguna dan jaringan komunikasi dasar. End device dapat memiliki berbagai istilah seperti node, host, station. Contoh beberapa end device yaitu PC, server, printer, laptop

2. Intermediary Device

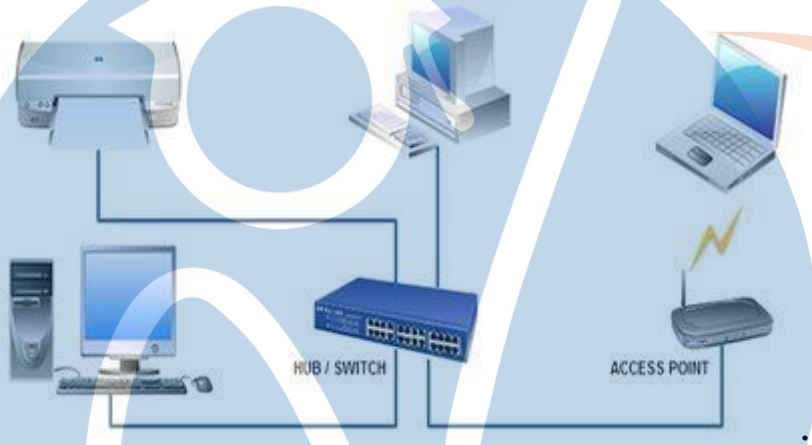
   Merupakan perangkat yang berfungsi sebagai penghubung antar perangkat yang ada di dalam jaringan komputer. Perangkat ini menyediakan dan bekerja untuk menjamin aliran data yang masuk melalui jaringan. Selain menghubungkan host secara individu ke jaringan. Perangkat intermediary juga dapat menghubungkan host secara individu ke jaringan, perangkat intermediary juga dapat

menghubungkan beberapa jaringan individu. Contoh beberapa *Intermediary Device* yaitu switch, hub,router,firewall [12]

Berdasarkan luas area cakupan, jaringan komputer di bagi menjadi :

a. LAN (Local Area Network)

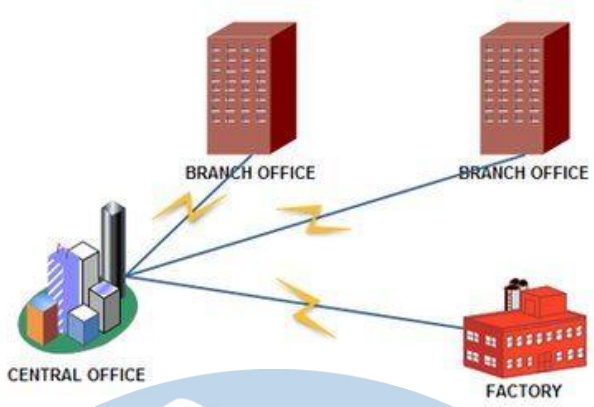
Salah satu jaringan komputer yang sangat populer. LAN (Local Area Network) adalah jaringan komputer yang mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah dan sekolah



Gambar 2.3 Contoh Struktur Local Area Network

b. MAN (Metropolitan Area Network)

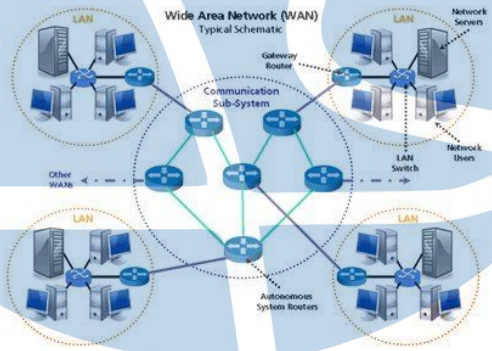
Metropolitan Area Network (MAN) adalah suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini berkisar antara 10 hingga 50 km.



Gambar 2.4 Contoh Struktur Metropolitan Area Network

c. WAN (Wide Area Network)

WAN (Wide Area Network) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. Internet merupakan contoh dari jaringan WAN ini.



Gambar 2.5 Contoh Struktur Wide Area Network

2.8 Penelitian Terkait

Penelitian ini mengacu pada beberapa penelitian terkait yang sudah pernah dilakukan sebelumnya. Berikut ini referensi dari penelitian sebelumnya yang digunakan pada penelitian ini.

Tabel 2.1 Penelitian Terkait

No.	Judul Penelitian	Tahun	Kesimpulan
1.	Analisis Dan Implementasi *Honeypot* Menggunakan *Dionaea* Sebagai Penunjang Keamanan Jaringan. Oleh : Triawan Adi Cahyanto	2016	Dari hasil pengujian dapat disimpulkan bahwa Dionaea dapat digunakan sebagai server palsu atau server tiruan sehingga dapat melindungi server asli ketika server tiruan tersebut mengalami serangan.
2.	Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (*Distributed Denial Of Service) Berbasis Honeypot)* Oleh : Sutarti	2017	Sistem honeypot yang digunakan penulis merupakan honeypots high interaction dengan rule sql injection dan denial of service (DoS),kedua rule tersebut bukanlah merupakan rule yang tergolong aman untuk sebuah sistem informasi yang besar, karena masih banyak tipe serangan yang bisa dilakukan oleh seorang attacker.
3.	Implementasi Virtual *Low-Interaction* Honeypot Dengan Dionaea Untuk Mendukung Keamanan Jaringan Oleh : Ahmad Fikri Nurrahman	2013	Low-Interaction Hoypot Dionaea telah berhasil membuat layanan palsu sebagai target serangna dan mencatat serangan atau aktivitas yang di anggap dapat membahayakan sistem jaringan

4	Penerapan Sistem Keamanan *Honeypot* Dan Ids Pada Jaringan Nirkabel (*Hotspot*) Oleh : Muh Masruri Mustofa	2017	Sistem honeypot telah berhasil meringankan tugas dari deteksi menjadi lebih sederhana, efektif dan murah. Konsepnya sendiri sangat mudah dipahami dan diimplementasikan. Honeypot sendiri ditujukan untuk mendeteksi serangan yang dilakukan oleh attacker dengan mengecohattacker tersebut dengan fasilitas mirror server.

Dari hasil penelitian pada ke empat penelitian yang di sebutkan dalam table yang diatas, posisi peneliti memiliki kedekatan dengan peneliti Ahmad Fikri Nurrahman yang berjudul IMPLEMENTASI VIRTUAL *LOW-INTERACTION* HONEYPOT DENGAN DIONAEA UNTUK MENDUKUNG KEAMANAN JARINGAN. Namun penelitian ini memiliki perbedaan ruang lingkup pengujian dan alat pengujian. Penelitian ini menerapkan pengujian *port scanning, exploit* dan *sql injection.* Aplikasi yang digunakan untuk pengujian *port scanning* adalah *Advanced Port Scanner (APS).* Sedangkan pengujian *exploit* menggunakan *Metasploit framework* dan pengujian *sql injection* menggunakan *OWASP ZAP*.