BAB II
TEORI PENUNJANG

1.1 Keamanan Jaringan

Suatu jaringan komputer memerlukan suatu keamanan untuk melindungi data-data yang ada dalam jaringan tersebut, keamanan jaringan atau *network security* merupakan segala aktifitas pengamanan suatu jaringan atsu *network*. Tujuan dari keamanan jaringan ini untuk menjaga *confidentiality*, *integrity* dan *availability* dari suatu serangan [1]. Berikut merupakan penjelasan *confidentiality*, *integrity* dan *availability.*

1. *Confidentiality*

   Confidentiality atau kerahasiaan adalah aspek yang menjamin kerahasiaan data atau informasi [9]. *Confidentiality* dengan definisi lain yaitu pencegahan bagi mereka yang tidak berkepentingan dapat mencapai informasi, berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut [10].

   Contoh dari *confidentiality* yaitu data-data yang bersifat pribadi (seperti nama, tempat tanggal lahir, *social security number*, agama, status perkawinan, penyakit yang pernah di derita, nomor kartu kredit, dan sebagainya) yang harus dapat di proteksi dalam penggunaan dan penyebarannya [10].

2. *Integrity*

   Integrity atau integritas adalah aspek yang menjamin informasi tidak boleh diubah tanpa seijin pemilik informasi, keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut [10].

   Contoh dari *integrity* yaitu pengamanan *e-mail* atau pesan agar tidak dapat diubah atau di *intercept* pada saat proses pengiriman [10].

3. *Availability*

   Availability atau ketersediaan merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan [9]. *Availability* dengan definisi lain yaitu upaya pencegahan ditahannya informasi atau sumber daya terkait oleh mereka yang tidak berhak, berhubungan dengan ketersediaan informasi ketika dibutuhkan [10].

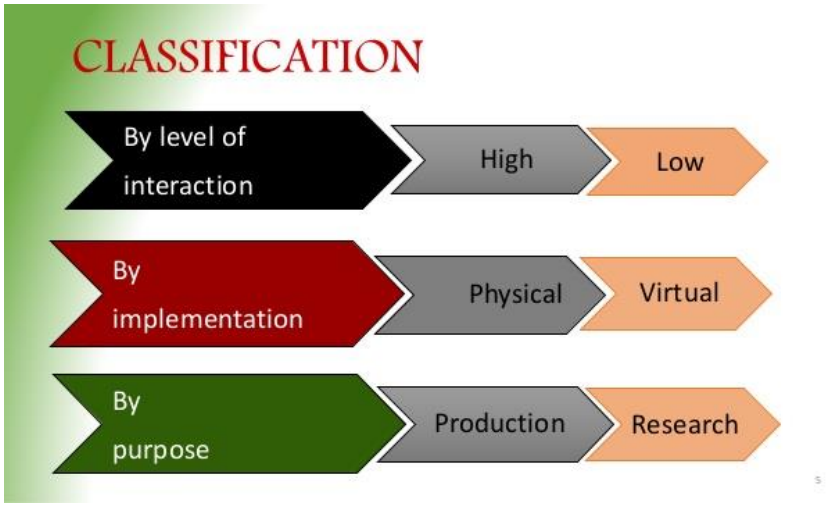
Contoh hambatan dari *availability* yaitu yang pertama adanya *dos attack*, dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down*, *hang* atau *crash*. Kedua, adanya *mailbomb*, dimana seseorang pengguna dikirimi ribuan *e-mail* dengan ukuran yang besar sehingga pengguna tidak dapat membuka *e-mail*nya atau kesulitan mengakses *e-mail*nya [10].

Keamanan jaringan yang utama sebagai perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan. Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan komputer yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan (Internet) [11].

1.2 *Honeypot*

Honeypot adalah *security resource* yang yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan. Pada umumnya *honeypot* berupa komputer, data, atau situs jaringan yang terlihat seperti bagian dari jaringan, tapi sebenarnya terisolasi dan dimonitor. Jika dilihat dari kacamata *attacker*, *honeypot* terlihat seperti layaknya sistem yang patut untuk diserang [12].

Pada dasarnya *honeypot* adalah suatu alat untuk mendapatkan informasi tentang penyerang. Selanjutnya administrator jaringan dapat mempelajari aktifitas-aktifitas yang dapat merugikan dan melihat kecenderungan dari aktifitas tersebut [13].



Gambar I.1 Klasifikasi Honeypot

Berdasarkan gambar 2.1, *honeypot* sendiri dibagi dalam beberapa klasifikasi, yaitu menurut implementasi, tujuan dan interaksinya.

1.2.1 Implementasi *Honeypot*

Honeypot diklasifikasikan menjadi 2, yaitu menurut implementasinya, berikut merupakan penjelasan dari klasifikasi *honeypot*:

1. *Physical*

   Berarti *honeypot* berjalan pada mesin fisik. Fisik sering menyiratkan interaksi yang tinggi, sehingga memungkinkan sistem untuk dikompromikan sepenuhnya. Mereka biasanya mahal untuk dipasang dan dirawat. Mempunyai *IP Address* tersendiri [13].

2. *Virtual*

   Dibandingkan dengan implementasi *physical*, implementasi *virtual* ini lebih ringan. Alih-alih menggunakan sistem komputer fisik yang bertindak sebagai *honeypot*. Implementasi ini dapat menggunakan satu komputer fisik yang menampung beberapa mesin virtual yang bertindak sebagai *honeypot*. Ini mengarah pada perawatan yang lebih mudah dan persyaratan fisik yang lebih rendah. Biasanya *VMware Workstation* digunakan untuk mengatur *honeypot virtual* tersebut. Simulator ini memungkinkan kita untuk menjalankan beberapa sistem operasi dan aplikasinya secara bersamaan pada satu mesin fisik, sehingga lebih mudah untuk mengumpulkan data [13].

1.2.2 Tujuan *Honeypot*

Menurut tujuannya *honeypot* dibagi menjadi 2, yaitu *production* dan *research honeypot,* berikut merupakan penjesalan dari tujuan *honeypot*:

1. *Production Honeypot*

   Digunakan untuk mengurangi resiko serangan pada sistem keamanan jaringan informasi dalam sebuah organisasi [13].

2. *Research Honeypot*

   Digunakan untuk mendapatkan informasi sebanyak mungkin tentang penyerang sehingga seorang administrator dapat mempelajari sebanyak mungkin informasi tersebut [13].

1.2.3 Jenis Interaksi *Honeypot*

Jenis interaksi *honeypot* dibagi berdasarkan *level of interaction. Level of interaction* mengukur derajat interaksi seorang penyerang dengan sistem informasi. Terdiri dari dua jenis yaitu:

1. *Low Interaction Honeypot*

Merupakan *honeypot* dengan tingkat interaksi *honeypot* yang didesain untuk menganalisa layanan seperti pada server yang asli sehingga penyerang hanya mampu memeriksa dan terkoneksi ke satu atau port tertentu. Layanan yang diberikan berupa emulasi yang bertujuan *attacker* tidak dapat berinteraksi secara langsung dengan layanan yang diberikan oleh sistem [14].

2. *High Interaction Honeypot*

Merupakan *honeypot* di mana *attacker* dapat berinteraksi secara langsung dan tidak ada batasan yang membatasi interaksi tersebut. Penyerang dapat berinteraksi didalam *web service*. Sistem tersebut terdiri dari berbagai jenis implementasi dan teknologi keamanan yang banyak digunakan untuk melindungi suatu sistem seperti firewall, IDS dan lain-lain [14].

1.3 Honeyd

Honeyd adalah *open source* program komputer yang dibuat oleh Niels Provos yang memungkinkan pengguna untuk membuat dan menjalankan beberapa virtual host pada jaringan komputer. *Host* virtual ini dapat dikonfigurasi untuk meniru beberapa jenis server yang memungkinkan pengguna untuk mensimulasikan jumlah tak terbatas konfigurasi jaringan komputer. *Honeyd* digunakan terutama dalam bidang keamanan komputer [12].

Honeyd digunakan terutama untuk dua tujuan. Menggunakan kemampuan perangkat lunak untuk meniru banyak *host* jaringan yang berbeda sekaligus (hingga 65536 host sekaligus), *honeyd* dapat bertindak sebagai gangguan potensi *attacker*. Jika jaringan hanya memiliki 3 server yang nyata, tetapi satu server menjalankan *Honeyd*, jaringan akan muncul menjalankan ratusan server untuk *attacker*. *Attacker* kemudian akan harus melakukan penelitian lebih lanjut (mungkin melalui rekayasa sosial) untuk menentukan server adalah nyata, atau *attacker* mungkin terjebak dalam *Honeypo*t [12].

1.4 *Attacker*

Attacker adalah individu atau kelompok yang berusaha mengeksploitasi kerentanan untuk keuntungan pribadi atau keuangan. *Attacker* tertarik pada segala hal, dari kartu kredit hingga desain produk dan apa pun yang berharga [5]. *Attacker* terbagi mejadi beberapa jenis, yaitu sebagai berikut:

1. *Amateurs*

Kadang disebut *script kiddie*. Mereka biasanya adalah *attacker* dengan sedikit keahlian atau tidak memiliki keahlian, sering menggunakan alat bantu yang ada atau petunjuk yang ditemukan di Internet untuk melancarkan serangan. Beberapa di antaranya hanya ingin tahu, sementara yang lainnya berusaha

untuk menunjukkan keahlian mereka dan menyebabkan kerugian. Mereka mungkin menggunakan alat bantu standar, namun hasilnya tetap dapat destruktif [5].

2. *Hackers*

Kelompok *attacker* ini membobol masuk ke komputer atau jaringan untuk mendapatkan akses. Tergantung pada tujuan pembobolan, penyerang ini digolongkan sebagai *White Hat Hackers*, *Grey Hat Hackers*, atau *Black Hat Hackers. White Hat Hackers* membobol masuk ke jaringan atau sistem komputer untuk menemukan kelemahan sehingga keamanan sistem dapat ditingkatkan. Pembobolan tersebut dilakukan dengan izin dan setiap hasil dilaporkan kembali ke pemilik. *Black Hat Hackers* memanfaatkan kerentanan apa pun untuk keuntungan pribadi, keuangan, atau politik yang ilegal. *Grey Hat Hackers* berada di antara *White Hat Hackers* dan *Black Hat Hackers*. *Grey Hat Hackers* mungkin menemukan kerentanan dalam suatu sistem. Penyerang topi abu-abu dapat melaporkan kerentanan kepada pemilik sistem jika tindakan itu sesuai dengan agenda mereka. Beberapa *Grey Hat Hackers* mempublikasikan fakta tentang kerentanan di *internet* sehingga dapat dimanfaatkan oleh *attacker* lain [5].

3. *Organized Hackers*

Hackers ini mencakup organisasi penjahat *cyber*, *hacktivis*t, teroris, dan *hackers* yang didukung negara. Pelaku kejahatan *cyber* biasanya adalah kelompok penjahat profesional yang berfokus untuk mendapatkan kontrol, kekuasaan, dan kekayaan. Penjahat ini sangat canggih dan teratur, dan mereka bahkan dapat memberikan kejahatan *cyber* sebagai layanan untuk penjahat lainnya. *Hacktivis*t membuat pernyataan politik untuk menciptakan kesadaran akan masalah yang penting bagi mereka. *Attacker* yang didukung negara mengumpulkan informasi atau melakukan sabotase atas nama pemerintah mereka. *Attacker* ini biasanya sangat terlatih dan didanai, dan serangan mereka fokus pada sasaran tertentu yang bermanfaat bagi pemerintah mereka [5].

1.5 *Threat*

Threat (ancaman) adalah setiap kegiatan yang dapat membahayakan informasi atau proses. Ancaman ini dianggap sebagai sesuatu yang negatif apabila mempengaruhi kerahasiaan (*Confidentiality*), integritas (*Integrity*), dan ketersediaan (*Availability*) dari sebuah sistem atau suatu layanan [5]. Terdapat 2 jenis *threat,* yaitu sebagai berikut:

1. *Internal Security Threat*

Ancaman internal berpotensi menimbulkan kerusakan yang lebih besar daripada ancaman eksternal karena pengguna internal memiliki akses langsung ke gedung dan perangkat infrastrukturnya. Karyawan juga memiliki pengetahuan tentang jaringan perusahaan, sumber dayanya, dan data rahasianya, serta berbagai tingkat pengguna atau hak istimewa administratif [5].

2. *External Security Threat*

Ancaman eksternal dari amatir atau penyerang terampil memanfaatkan kerentanan dalam jaringan atau perangkat komputer, atau menggunakan rekayasa sosial untuk mendapatkan akses [5].

1.6 *Attack*

Attack (serangan) merupakan aktivitas menghambat kerja sebuah layanan atau mematikannya, sehingga *user* yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut [5].

Berikut merupakan jenis-jenis dari *attack* yang dapat mengganggu lalu lintas dalam sebuah jaringan, yaitu sebagai berikut:

1. DoS *Attack*

DoS *attack* (*Denial of Service*) adalah jenis serangan jaringan. Serangan DoS menimbulkan beberapa macam gangguan layanan jaringan untuk pengguna, perangkat, atau aplikasi [5]. Ada dua jenis utama serangan DoS:

a. Volume Lalu Lintas yang Terlalu Besar

Bila jaringan, *host*, atau aplikasi menerima pengiriman data dalam jumlah sangat besar dengan kecepatan yang tidak dapat ditanganinya. Serangan ini menimbulkan kelambatan transmisi atau respons, atau kerusakan perangkat atau layanan [5].

b. Paket Dengan Format Berbahaya

Bila paket yang diformat secara berbahaya dikirim ke host atau aplikasi dan penerima tidak dapat menanganinya. Misalnya, penyerang meneruskan paket yang berisi kesalahan yang tidak dapat diidentifikasi oleh aplikasi, atau meneruskan paket yang tidak

diformat dengan semestinya. Hal ini menyebabkan perangkat penerima berjalan sangat lambat atau rusak [5].

DoS *attack* dianggap sebagai risiko besar karena dapat dengan mudah mengganggu komunikasi serta menyebabkan terbuangnya waktu dan uang dalam jumlah besar. Serangan ini cukup mudah untuk dilakukan, bahkan oleh penyerang yang tidak berpengalaman [5].

2. DDos *Attack*

DDoS *attack* (*Distributed Denial of Service*) mirip dengan serangan DoS namun berasal dari beberapa sumber yang terkoordinasi [5]. Sebagai contoh, sebuah serangan DDoS dapat berlangsung sebagai berikut:

Penyerang membangun jaringan *host* terinfeksi, yang disebut *botnet*. *Host* yang terinfeksi disebut *zombie*. *Zombie* ini dikendalikan oleh sistem pengendali [5].

Komputer *zombie* terus memindai dan menginfeksi lebih banyak *host*, sehingga menciptakan lebih banyak *zombie*. Bila sudah siap, peretas akan menginstruksikan sistem pengendali untuk membuat *botnet zombie* melaksanakan serangan DDoS [5].

3. SEO *Poisoning*

Mesin pencari seperti Google bekerja menurut peringkat halaman dan menampilkan hasil yang relevan berdasarkan permintaan pencarian pengguna. Tergantung pada relevansi kontennya, situs web dapat ditampilkan lebih tinggi atau lebih rendah dalam daftar hasil pencarian. SEO, singkatan dari *Search Engine Optimization* (Pengoptimalan Mesin Pencari), merupakan serangkaian teknik yang digunakan untuk menaikkan peringkat situs web oleh mesin pencari. Meskipun banyak perusahaan yang sah yang mengkhususkan diri dalam mengoptimalkan situs web agar berada di posisi lebih baik, pengguna berbahaya dapat menggunakan SEO untuk membuat situs web berbahaya ditampilkan di posisi lebih tinggi dalam hasil pencarian. Teknik ini disebut SEO *Poisoning* [5].

Tujuan paling umum SEO *Poisoning* adalah untuk meningkatkan lalu lintas ke situs berbahaya yang mungkin meng-*host malware* atau melakukan rekayasa sosial. Untuk memaksa situs berbahaya berperingkat lebih tinggi dalam hasil pencarian, penyerang memanfaatkan istilah pencarian yang popular [5].

4. Malware

Malware adalah singkatan untuk *Malicious Software* (Perangkat Lunak Berbahaya). Malware adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya

terhadap atau merusak sistem [5]. Di bawah ini adalah beberapa jenis malware yang umum:

a. *Spyware*

Malware ini dirancang untuk melacak dan memata-matai pengguna. *Spyware* sering berisi pelacak aktivitas, pengumpul penekanan tombol, dan pengambilan data. Dalam upaya untuk melewati prosedur keamanan, *spyware* sering memodifikasi pengaturan keamanan. *Spyware* sering melekatkan diri pada perangkat lunak yang sah atau dengan *Trojan horse* [5].

b. *Adware*

Perangkat lunak didukung iklan yang dirancang untuk secara otomatis menampilkan iklan. *Adware* sering terinstal bersama beberapa versi perangkat lunak. Beberapa *adware* dirancang hanya untuk menampilkan iklan namun lazim juga ditemukan *adware* yang disertai *spyware* [5].

c. *Bot*

Bot adalah malware yang dirancang untuk secara otomatis melakukan tindakan, biasanya secara *online*. Meskipun sebagian besar *bot* tidak berbahaya, yang meningkatkan penggunaan *bot* berbahaya adalah *botnet*. Beberapa komputer terinfeksi oleh *bot* yang diprogram untuk diam menunggu perintah yang diberikan oleh penyerang[5].

d. *Ransomware*

Malware ini dirancang untuk menahan sistem komputer atau data di dalamnya hingga tebusan dibayar. Biasanya *ransomware* bekerja dengan mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna. Beberapa versi lain *ransomware* dapat memanfaatkan kerentanan sistem tertentu untuk mengunci sistem. *Ransomware* tersebar melalui file yang diunduh atau beberapa kerentanan perangkat lunak [5].

e. *Scareware*

Ini adalah jenis malware yang dirancang untuk memaksa pengguna melakukan tindakan tertentu karena takut. *Scareware* memalsukan jendela *pop-up* yang menyerupai jendela dialog sistem operasi. Jendela ini menyampaikan pesan palsu yang menyatakan bahwa sistem berisiko atau perlu menjalankan program tertentu agar kembali beroperasi secara normal. Kenyataannya, tidak ada masalah

yang diperiksa atau dideteksi dan jika pengguna setuju dan menghapus program yang disebutkan untuk dijalankan, sistem miliknya akan terinfeksi malware [5].

f. *Rootkit*

Malware ini dirancang untuk mengubah sistem operasi untuk membuat *backdoor*. Penyerang kemudian menggunakan *backdoor* tersebut untuk mengakses komputer dari jarak jauh. Sebagian besar *rootkit* memanfaatkan kerentanan perangkat lunak meningkatkan hak istimewa dan memodifikasi *file* sistem. *Rootkit* juga lazim memodifikasi forensik sistem dan alat bantu pemantauan, membuat *rootkit* sangat sulit dideteksi. Sering, sistem operasi komputer yang terinfeksi *rootkit* harus dihapus dan diinstal ulang [5].

g. *Virus*

Virus adalah kode berbahaya yang dapat dijalankan yang terlampir pada *file* lain yang dapat dijalankan, sering kali merupakan program yang sah. Sebagian besar *virus* memerlukan pengaktifan oleh pengguna akhir dan dapat aktif pada waktu atau tanggal tertentu. *Virus* dapat tidak berbahaya dan hanya menampilkan gambar namun *virus* juga dapat bersifat merusak, misalnya *virus* yang mengubah atau menghapus data. *Virus* juga dapat diprogram untuk bermutasi untuk menghindari deteksi. Sebagian besar *virus* kini disebarkan melalui *drive* USB, disk optik, jaringan bersama, atau email [5].

h. *Trojan Horse*

Trojan horse adalah malware yang menjalankan operasi berbahaya dengan menyamar sebagai operasi yang diinginkan. Kode berbahaya ini mengeksploitasi hak istimewa pengguna yang menjalankannya. Sering kali, *Trojan horse* ditemukan di *file* gambar, *file* audio, atau permainan. *Trojan horse* berbeda dari *virus* karena melekatkan diri ke *file* yang tidak dapat dijalankan [5].

i. *Worms*

Worm adalah kode berbahaya yang menggandakan dirinya dengan secara mandiri mengeksploitasi kerentanan dalam jaringan. *Worm* biasanya memperlambat jaringan. *Virus* memerlukan *program host* agar dapat berjalan, namun *worm* dapat mengaktifkan diri sendiri. *Worm* hanya memerlukan partisipasi pengguna untuk infeksi awal. Setelah *host* terinfeksi, *worm* dapat menyebar dengan sangat cepat melalui jaringan. *Worm* memiliki pola yang serupa. Semua *worm*

dapat menimbulkan kerentanan, dapat menyebarkan diri, dan semua berisi muatan [5].

j. *Man In The Middle (*MitM*)*

MitM memungkinkan penyerang mengambil alih kontrol perangkat tanpa sepengetahuan pengguna. Dengan tingkat akses tersebut, penyerang dapat mencegat dan mengambil informasi pengguna sebelum mengirimkannya ke tujuan yang dimaksud. Serangan MitM secara luas digunakan untuk mencuri informasi keuangan. Banyak malware dan teknik ada untuk memberi penyerang kemampuan MitM [5].

k. *Man In The Mobile (*MitMo*)*

MitMo adalah jenis serangan yang digunakan untuk mengendalikan perangkat bergerak. Bila terinfeksi, perangkat bergerak dapat diinstruksikan agar mengungkapkan informasi sensitif pengguna dan mengirimkannya kepada penyerang. ZeuS, contoh eksploitasi dengan kemampuan MitMo, memungkinkan penyerang dengan diam-diam mengambil pesan SMS verifikasi 2 langkah yang dikirim kepada pengguna [5].

1.7 Zenmap

Zenmap adalah aplikasi *multi platform* sebagai *interface* sederhana untuk apikasi nmap. Nmap (*Network Mapper*) sendiri adalah sebuah aplikasi *open source* untuk explorasi *network* dan audit keamanannya. Nmap bekerja dengan melakukan scan terhadap komputer (*host*) *stand alone* ataupun host yang terhubung dalam sebuah jaringan, menentukan host-host yang aktif dalam suatu jaringan, menentukan informasi sistem operasi, port-port yang terbuka dan jenis firewall yang digunakan [15].

Zenmap bersifat *multi platform*, artinya bisa berjalan pada berbagai sistem operasi seperti Linux, Windows, Mac, FreeBSD, openBSD dan Sun OS. Nmap adalah aplikasi berbasis *command line* tetapi untuk kemudahan penggunaan dan analisis hasilnya disertakan aplikasi GUI yang dinamakan zenmap [15].

1.8 VMWare Workstation

VMWare Workstation adalah software yang memungkinkan *user* membuat sejumlah komputer semu dengan hanya menggunakan satu komputer *hardware* saja. Setiap komputer semu yang dibuat dengan *VMWare* dapat dipakai, seperti menggunakan komputer biasa [16].

VMWare menjadi sangat popular karena kemampuannya untuk membuat komputer semu yang sangat stabil dan mampu menggantikan tugas komputer biasa, terutama untuk pemakaian di lab pengujian atau lembaga pendidikan. Hal ini tentu luar biasa kegunaannya karena dapat membuat suatu sistem jaringan yang murah dan menghemat biaya dibandingkan jika setiap sistem operasi masing-masing harus memiliki komputernya sendiri [16].