ANALISIS KEAMANAN JARINGAN *WIRELESS* DARI SERANGAN DNS *SPOOFING* PADA PENGGUNA *FREE WIFI* DI KOTA BATAM

SKRIPSI

Oleh:
Rudi Darwis
130210194

PROGRAM STUDI SISTEM INFORMATIKA
UNIVERSITAS PUTERA BATAM
2017

ANALISIS KEAMANAN JARINGAN *WIRELESS* DARI SERANGAN DNS *SPOOFING* PADA PENGGUNA *FREE WIFI* DI KOTA BATAM

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Rudi Darwis
130210194

PROGRAM STUDI SISTEM INFORMATIKA
UNIVERSITAS PUTERA BATAM

2017

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik Universitas Putera Batam maupun di perguruan tinggi lainnya.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 17 Februari 2017

Yang membuat pernyataan

Rudi Darwis

130210194

ANALISIS KEAMANAN JARINGAN *WIRELESS* DARI SERANGAN DNS *SPOOFING* PADA PENGGUNA *FREE WIFI* DI KOTA BATAM

Oleh
Rudi Darwis
130210194

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini

Batam, 17 Februari 2017

Hotma Pangaribuan, S.Kom., M.SI.
Pembimbing

ABSTRAK

Perkembangan teknologi informasi yang sangat pesat saat ini yaitu menggunakan udara sebagai medium jaringan *wireless*, penyerang dengan mudah menembus jaringan dan dapat memperkenalkan masalah keamanan jaringan, ancaman, risiko dan jenis lain dari serangan dan diikuti oleh perkembangan *cyber crime* yang semakin berkembang pesat. Salah satu kejahatan *cyber crime* yang selalu berkembang adalah DNS *spoofing*. Jaringan *wireless* LAN banyak digunakan dalam *free wifi* di taman, fasum, dam *public area, café* dan mall. Namun pada umumnya dibutuhkan keamanan jaringan salah satunya yaitu DNS *spoofing* untuk dapat mencegah terjadinya serangan DNS *spoofing*. Penyerangan DNS *spoofing* menggunakan *tools ettercap* dan *wireshark* untuk menganalisis *packet* data jaringan. Tugas DNS adalah untuk mengkonversi alamat yang dapat dibaca manusia dimasukkan pada *address* bar *browser* ke mesin alamat IP dibaca. *Spoofing* berarti meniru orang atau komputer lain, biasanya dengan memberikan informasi palsu. *Spoofing* dapat mengambil banyak bentuk di dunia komputer, yang semuanya melibatkan beberapa jenis representasi palsu informasi. Ada berbagai metode dan jenis yaitu serangan *spoofing* IP, ARP, *E-Mail*, *Web*, dan DNS *spoofing.* Dari hasil penelitian *wireless* didapatkan *free wifi* yang kemananan jaringannya tentang DNS *spoofing* masih lemah dan didapatkan juga *free wifi* yang dikategorikan kuat dalam keamanan jaringan.

Kata kunci : Teknologi Informasi, *Wireless*, Serangan, Keamanan Jaringan, ancaman, *Cyber Crime, Free Wifi, Ettercap, Wireshark, Packet, DNS Spoofing.*

ABSTRACT

Information technology development is very rapid at this time is to use air as the medium of a wireless network, the attacker to easily penetrate tissue and may introduce network security issues, threats, risks and other types of attacks, followed by the development of cyber crime is growing rapidly. One crime that is always evolving cyber crime is DNS spoofing. LAN wireless network is widely used in the free wifi in parks, public facilities, public dam area, café and a mall. But in general it takes network security one of them is to be able to prevent DNS spoofing DNS spoofing attacks. DNS spoofing attack using ettercap tools and wireshark to analyze network data packet. DNS task is to convert human readable address entered in the browser address bar into machine readable IP address. Spoofing means impersonating someone or another computer, usually by providing false information. Spoofing can take many forms in the computer world, all of which involve some kind of false representation of information. There are various methods and types of IP spoofing attacks, ARP, E-Mail, Web, and DNS spoofing. From the results obtained free wifi wireless network security of DNS spoofing is still weak and is also free wifi available, categorized strong in network security.

Keywords : *Information Technology, Wireless, Attack, Network Security, threats, Cyber Crime, Free Wifi, Ettercap, Wireshark, Packet, DNS spoofing.*

KATA PENGANTAR

Puji dan Syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam
2. Ketua Program Studi Teknik Informatika Putera Batam
3. Bapak Hotma Pangaribuan, S.Kom., M.SI. selaku pembimbing skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Kedua Orang Tua, Kakak Adik dan semua keluarga saya yang telah mendukung, mendoakan dan membimbing saya serta memberi semangat dalam pembuatan skipsi ini.

6. Rekan-rekan mahasiswa Program Studi Teknik Informatika Universitas Putera Batam yang selalu memberi dukungan dan semangat kepada saya dalam mengerjakan dan menyelesaikan skripsi ini.

Saya menyadari bahwa dalam penulisan tugas akhir ini masih terdapat kekurangan dan masih jauh dari kesempurnaan. Saya sangat mengharapkan kritik dan saran yang bersifat membangun demi kesempurnaan tugas akhir ini. Semoga hasil yang telah dicapai dalam tugas akhir ini dapat bermanfaat bagi kita semua.

Semoga Tuhan Yang Maha Esa membalas semua kebaikan dan selalu mencurahkan rahmat-Nya kepada kita semua. Amin.

Batam, 17 Februari 2017

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi semakin berkembang hal tersebut terjadi untuk memenuhi kebutuhan manusia agar dalam menjalankan aktivitasnya dimudahkan. Salah satu dari perkembangan teknologi adalah jaringan komputer. Jaringan komputer merupakan sebuah sistem yang terdiri dari komputer, *sofware*, dan perangkat-perangkat lainnya yang bekerja sama agar bisa berkomunikasi dengan membagi sumber daya serta pengaksesan informasi. Namun, dibalik dari kemudahan yang disediakan oleh jaringan komputer terdapat banyak ancaman kejahatan atau resiko pada bidang ini atau yang biasa disebut dengan *cyber crime.* Ancaman dapat berupa fisik maupun logik yang secara langsung maupun tidak langsung mengganggu kegiatan yang sedang berlangsung pada jaringan.

Cyber crame adalah bentuk kejahatan yang terjadi di internet atau dunia maya yang menjadi alat sasaran atau tempat terjadinya kejahatan yaitu mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer. Salah satu jenis *cyber crime* yang bisa terjadi yaitu dengan teknik DNS *spoofing* dimana ancaman tersebut yang dijadikan fokus pada penelitian ini. *Spoofing* adalah menjelma atau menyamar untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dimana penyerang berhubungan dengan pengguna yang berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya.

Hasil penelitian Singh dan Maini (2011:5) *domain system name* (DNS) adalah sebuah sistem penamaan hirarkis yang dibangun di atas basis data terditribusi untuk komputer, jasa, atau sumber daya lain yang terhubung ke internet atau jaringan pribadi. Itu bermakna menerjemahkan nama *domain* ke manusia ke dalam numerik pengidentifikasi yang terkait dengan peralatan jaringan untuk tujuan menemukan dan menangani perangkat ini di seluruh dunia. Pekerjaan DNS adalah untuk mengubah alamat dapat dibaca manusia yang dimasukkan pada alamat *browser* ke alamat IP yang dapat dibaca mesin. DNS *spoofing* adalah istilah yang mengacu pada tindakan menjawab permintaan DNS yang dimaksudkan untuk lain *server* (DNS *server*). Pengaturan ini dapat dalam pertukaran *server-server* (DNS *server* meminta lain untuk pemetaan) atau di sebuah dialog *client-server* (ketika seorang c*lient* meminta DNS *server* untuk pemetaan).

Wifi adalah salah satu teknologi *wireless* yang memungkinkan pengguna dapat mengakses internet tanpa harus menghubungkan kabel ke *switch* terlebih dahulu. Pengamanan jaringan *wifi* lebih ditekan pada bagian *access point* karena AP adalah titik akses pertama agar *user* bisa terhubung dengan jaringan *wifi.* (Oktavian, 2015:61) mengamankan AP meliputi dua aspek utama, *user authentication* dan *data encryption. user authenticati* mengatur bagaimana cara *client* berasosiasi dengan AP, sedangkan data *encryption* mengatur algoritma pengenkripsian data pada lalu lintas jaringan. Pengamanan ini bertujuan untuk mencegah *client-client* yang tidak memiliki hak/wewenang terkoneksi kedalam jariangan.

Wifi memiliki *protokol* tersendiri untuk mengatur pengamanan sistem yaitu *wireless security protokol.* Terdiri dari WEP (*Wired Equivalent Privacy*), WPA (*Wifi Protected Access*), dan WPA2 (*Wifi Protected Access version* 2). *Protokol-protokol* tersebut akan mengenkripsi data yang ditransmisikan oleh AP sehingga *client* yang ingin berasosiasi dengannya harus memiliki *key* terlebih dahulu. Masing-masing memiliki kelebihan dengan kekurangan masing-masing dari segi algoritma pengenkripsian atau mekanisme kerja *protokolnya*.

Menurut Oktavian (2015:46) *Hospot* adalah area dimana orang atau *user* dengan menggunakan PC, smartphone, atau perangkat-perangkat lain yang memiliki *wireless* adapter dapat terkoneksi dengan internet tanpa harus menggunakan media kabel. Jadi kalau *wifi* adalah teknologinya, maka *hospot* adalah daerah/tempat yang menggunakan dan mengimplementasikan teknologi tersebut.

Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki banyak kelebihan dibandingkan teknologi kabel, diantaranya kemudahan akses komunikasi data dan akses internet di posisi mana selama masih berada dalam jangkauan *wireless*. Selain menawarkan berbagai kemudahan, dalam jaringan WLAN (*Wireless Local Area Network*), terdapat resiko keamanan yang lebih kritis dibandingkan dengan jaringan kabel karena medium udara dalam jaringan *wireless* tidak bisa dikontrol secara fisik. Hal ini membuat parapenyerang/penyusup (*hacker*) dan kejahatan dunia maya (*Cyber crame*) menjadi tertarik untuk melakukan berbagai aktifitas yang biasanya ilegal terhadap jaringan *wireless.*

Penyerangan yang dilakukan oleh *hacker* dan *cyber crame* sangat bervariasi, mulai dari *Sniffing packet, packet injection, illegal authentication*, sampai *cracking* WEP (*Wired Equivalent Privacy*), dan *Cracking* WPA (*Wifi Protected Acces*)/WPA2. Maka dilakukannya kajian terhadap konsep keamanan jaringan WLAN (*Wireless Local Area Network*), dalam hal menggunakan DNS *Spoofing*, untuk mengetahui yang dilakukan oleh para *hacker* dan *Cyber crame* dalam melakukan penyerangan,dengan melakukan pembuktian terhadap ancaman dan serangan dalam jaringan *wireless*. Hal ini diharapkan dapat mencari solusi bagi para pengguna (*user*) ataupun administrator untuk meningkatkan keamanan jaringan *wireless* terutama DNS *spoofing.*

Dari uraian diatas maka penulis tertarik membuat suatu penelitian dengan judul **ANALISIS KEAMANAN JARINGAN *WIRELESS* DARI SERANGAN DNS *SPOOFING* PADA PENGGUNA *FREE WIFI* DI KOTA BATAM**.

1.2. Identifikasi Masalah

Berdasarkan permasalahan diatas, maka permasalahan-permasalahan yang dapat didefinisikan adalah sebagai berikut:

1. Masih banyak pengguna *internet* yang tidak mengetahui dan tidak perduli dengan kejahatan DNS *spoofing.*
2. Sulitnya bagi pengguna *internet* untuk memeriksa keamanan DNS *spoofing.*
3. Kurangnya informasi pengetahuan tentang keamanan DNS *spoofing* yang memungkinkan untuk menghindari kejahatan di *internet.*

1.3. Pembatasan Masalah

Maka perlu dibuat batasan masalah. Adapun batasan masalah pada penelitian ini adalah:

1. Fokus penelitian ini tentang analisis keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam
2. Penelitian ini dilakukan di *free wifi* di taman, *fasum,* dam *public area, café,* dan mall.
3. Penelitian pada sistem keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam menggunakan aplikasi *wireshark* dan aplikasi *ettercap.*

1.4. Perumusan Masalah

Berdasarkan masalah yang ada, maka rumusan masalah yang dapat disimpulkan penulis adalah:

1. Bagaimana cara pengujian keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam?
2. Bagaimana melakukan analisa jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam?
3. Bagaimana melakukan tindakan pencegahan serangan jaringan *wireless* dari serangan DNS *Spoofing* pada pengguna *free wifi* di Kota Batam?

1.5. Tujuan Penelitian

Adapun tujuan penelitian adalah sebagai berikut:

1. Mengetahui hasil pengujian keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam
2. Mengetahui hasil analisa jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam
3. Mengetahui hasil tindakan pencegahan serangan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam?

1.6. Manfaat Penelitian

Penulis mengharapkan dapat memberikan manfaat kepada pembaca secara toeritis (keilmuan) maupun praktis (guna laksana), manfaat tersebut antara lain:

1.6.1 Secara Teoritis

1. Menambah ilmu pengetahuan tentang keamanan DNS *spoofing.*
2. Dapat membantu mahasiswa untuk menjadikan sebagai referensi jika membutuhkan informasi tentang DNS *spoofing.*
3. Berharap penelitian ini berguna bagi pembaca
4. Salah satu syarat mendapatkan gelar sarjana teknik informatika

1.6.2 Secara Praktis

1. Memberikan pemahaman kepengguna *wireless* tentang DNS *spoofing*
2. Dapat mencegah perkembangan kejahatan DNS *spoofing*

BAB II
LANDASAN TEORI

2.1. Teori Dasar

2.1.1. Pengenalan Jaringan Komputer

Menurut Waloeya (2012:1) jaringan komputer dapat diartikan sebagai sebuah rangkaian yang terdiri dari dua atau lebih komputer. Komputer-komputer ini akan dihubungkan satu sama lain dengan sebuah sistem komunikasi. Dengan jaringan komputer ini, setiap pengguna komputer yang terjaring di dalamnya akan saling tukar menukar data, program, dan sumber daya komputer lainnya seperti media penyimpanan, printer, dan lain-lain.

Jaringan komputer yang berhubungan komputer-komputer pada lokasi berbeda dapat dimanfaatkan untuk mengirim surat elektronik (*e-mail*), mengirim *file* data (*upload*), dan mengambil *file* data dari tempat lain (*download*), serta berbagai kegiatan akses informasi pada lokasi yang terpisah agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer akan meminta dan memberikan layanan (*service*). Pihak yang meminta memberikan atau mengirim layanan disebut pelayanan (*server*). Arsitektur ini disebut dengan sistem *client server* dan digunakan pada hampir seluruh aplikasi jaringan komputer.

2.1.1.1 Berdasarkan Ruang Lingkup

Menurut Bahrul, dkk (2012:2) ruang lingkup yang dimaksud di sini adalah seberapa banyak dan seberapa besar jaringan komputer tersebut akan dibangun. Berdasarkan ruang lingkupnya, sebuah jaringan komputer dapat dibedakan menjadi 3, yaitu:

1. ***Local Area Network* (LAN)**

Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometre. LAN sering kali digunakan untuk menghubungkan komputer pribadi dan *work station* dalam suatu perusahaan (kantor) atau pabrik-pabrik untuk memakai bersama sumber daya (*resource*, misalnya printer) dan saling bertukar informasi.

2. ***Metropolitan Area Network* (MAN)**

Metropolitan Area Network (MAN) merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.

3. ***Wide Area Network* (WAN)**

Wide Area Network (WAN) merupakan jaringan *area* luas, berupa jaringan komputer yang mencakup *area* besar seperti antar negara atau bahkan benua atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik. WAN dimanfaatkan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain sehingga pengguna komputer di lokasi yang satu dapat berkomunikasi dengan pengguna komputer yang berbeda

pada lokasi yang lain, dan juga dimanfaatkan untuk menghubungkan LAN antar lokasi.

2.1.1.2 Berdasarkan Konfigurasi

Menurut Arifin (2009:68) berdasarkan konfigurasi, sebuah jaringan komputer terbagi atas 2, yaitu:

1. Jaringan *Client Server*

Banyak digunakan pada jaringan dengan jumlah komputer yang banyak, dimana terdapat satu atau lebih komputer yang dijadikan sebagai pusat (*server*). *Server* dapat dibedakan berdasarkan tugas dan fungsinya misalnya data *server, email server, proxy server, web server*, dan lain-lain. *Server* juga bertugas melakukan manajemen *client.*

2. Jaringan *Peer-to-Peer*

Sistem ini banyak digunakan pada jaringan dengan jumlah komputer yang sedikit, dimana komputer masing-masing memiliki status kedudukan yang sama dan tidak memerlukan sistem terpusat (*server*). Pertukaran data dilakukan dengan *system file sharing*. Tiap komputer dalam jaringan dapat menggunakan printer bersama dengan *system* printer *sharing*.

2.1.1.3 Berdasarkan Media Penghantar Jaringan

Menurut Utomo (2012:12) berdasarkan media penghantarnya, jaringan komputer dapat dibedakan menjadi 2, yaitu:

1. Menggunakan Media Kabel

Jaringan komputer ini menggunakan kabel sebagai media penghantarnya. Data akan mengalir melalui kabel. Kabel yang digunakan bisa berbahan tembaga

atau serat optik (*fiber* optik). Bahan tembaga biasanya digunakan untuk jaringan LAN, sedangkan untuk jaringan MAN atau WAN biasanya menggunakan gabungan antara kabel tembaga dan serat optik.

2. Menggunakan Media Udara

Jaringan komputer ini tidak menggunakan kabel. Media penghantar antara komputernya menggunakan gelombang radio. Frekuensi yang digunakan untuk jaringan komputernya tinggi, yaitu 2,4 GHz dan 5 GHz.

2.1.1.4 Kabel Versus *Nirkabel*

Secara umum, perbandingan antara jaringan komputer yang berbasis kabel dengan jaringan yang *nirkabel* terlihat pada tabel berikut: (Utomo, 2012:13).

Tabel 2.1 Kabel Versus *Nirkabel*

Sumber: Utomo (2016)

Kategori	Jaringan Kabel	Jaringan *Nirkabel*
Instalasi	a. Menggunakan *ethernet card* dan *network adapter, central device* seperti pengalih. b. Kabel jaringan terhubung antara satu komputer ke komputer lainnya dengan berbagai *topologi* jaringan.	a. Menggunakan *adapter* WLAN dan *central device,* yaitu *access point.* b. Menggunakan konfigurasi *ad hoc* dan *infrastruktur.*
Harga	Harga kabel serta	Investasi awal cukup mahal di

	hub/pengalih cukup murah.	mana harganya bisa berkali lipat dari harga jaringan yang berbasis kabel
Reliabilitas	Teknologi kabel *ethernet, hub,* atau pengalih cukup andal, hanya konektor yang kadang menjadi kendala.	WLAN kurang andal, terutama pada teknologi IEEE 802.11b dan g, yang mudah terkena gangguan dari alat lain, seperti *oven mikro* gelombang atau telepon *nirkabel*.
Kinerja	Teknologi yang menggunakan *ethernet* mempunyai tingkat kecepatan yang tinggi, sampai 100 Mbps.	Teknologi IEEE 802.11b mendukung kecepatan sampai 11 Mbps (1/10 dari kecepatan *fast ethernet* yang ada pada jaringan kabel). Selain itu, kinerja jaringan *nirkabel* juga terganggu pada jarak/lokasi. Semakin jauh letak pengguna, semakin rendah kecepatannya.
Mobilitas	Jaringan kabel hanya tebatas pada ruangan/daerah yang mempunyai koneksi kabel saja. Jika diinginkan	Tidak terikat pada lokasi tertentu saja sehingga pengguna masih dapat terkoneksi ke jaringan di mana

	ketempat lainnya, pengguna harus menarik kabel ke lokasi lain yang dimaksud.	pun mereka berada.
Keamanan	a. Keamanan bisa dilakukan pada *router.* b. Bisa juga dilakukan pada komputer *client* dengan menggunakan *firewall* yang ada pada masing-masing komputer *client* sehingga keamanan terjamin.	Karena transmisinya melalui medium udara, jaringan ini mudah disusupi oleh pihak lain. Singkatnya, sisi keamanannya belum begitu terjamin.

2.1.2 Dasar Jaringan Wireless

Wireless seperti yang anda sering dengar adalah jaringan tanpa kabel yang menggunakan udara sebagai media transmisinya untuk menghantarkan gelombang elektromagnetik (Oktavian, 2015:46). *Wireless* sebenarnya sudah lama sejak lama, dimulai dari penemuan radio dan dilanjutkan oleh penemuan radar. Telepon seluler atau *smartphone* yang anda gunakan pun menggunakan teknologi *wireless*, tidak ada kabel menancap pada *handphone* anda yang terhubung kekantor pusat penyedia kartu *seluler*.

Kemudian muncul istilah *wifi*, yaitu singkatan dari *wireless fidelity* adalah sebuah teknologi jaringan tanpa kabel (*nirkabel*) yang menggunakan frekuensi tinggi. Frekuensi yang digunakan oleh teknologi *wifi* berada pada *spektrum* 2,4GHz–5GHz. Kalau *wireless* adalah teknologinya, maka *wifi* adalah bagian/anggota dari teknologi *wireless*. Gelombang *wifi* dikhususkan untuk penggunaan transfer data di dalam jaringan komputer. Oleh karena itu teknologi sangat berhubungan dengan dunia internet. Agar komputer anda bisa menggunakan teknologi ini, maka anda harus memiliki *wireless* adapter yaitu *hardware* yang dapat menangkap serta berkomunikasi melalui frekuensi gelombang yang sama dengan yang digunakan oleh *wifi* yaitu dalam rentang 2,4GHz–5GHz.

2.1.2.1 Revolusi *Nirkabel*

Menurut Utomo (2012:18) sejarah jaringan *nirkabel* tidak lepas dari masalah komunikasi data yang menggunakan jaringan radio karena jaringan *nirkabel* menggunakan gelombang radio dalam proses transmisinya. Penggunaan jaringan radio dimulai sejak perang dunia II oleh para tentara Amerika. Mereka telah mengembangkan teknologi transmisi data dengan medium radio. Hal ini mendorong para peneliti dari Universitas *Hawai* untuk mengembangkan hal yang sama dengan menciptakan jaringan pertama menggunakan teknologi radio yang bakal menjadi jaringan *nirkabel* nantinya yang disebut *ALOHNET* pada tahun 1971. Jaringan WLAN (*wireless* LAN) pertama ini terdiri atas tujuh komputer yang saling berkomunikasi dalam *topologi* jaringan bintang secara *dupleks.* Kemudian, IBM juga melakukan percobaan pada akhir tahun 1970 untuk

merancang sebuah WLAN dengan menggunakan teknologi *inframerah* (IR) untuk mencari alternatif penggunaan *ethernet* IEEE 802. Kegiatan tersebut juga dilakukan oleh perusahaan *Hewlett-Packard* (HP) dengan menguji LAN *nirkabel* menggunakan RF (frekuensi radio). Hasil kedua perusahaan tersebut hanya mencapai rekor laju data 100 Kbps sehingga produk tersebut tidak dikomersialkan karena tidak memenuhi standar IEEE 802 untuk LAN, yaitu 1 Mbps.

Pada tahun 1985 *Federal Communication Commission* (FCC) menetapkan pita frekuensi untuk keperluan industri, *industrial, scentific,* dan *medical* (ISM *band*), yaitu sebesar 902-928 MHz, 2400-2483,5 MHz, dan 5725-5850 MHz yang sifatnya tidak berlisensi (*unlicensed)* sehingga pengembangan WLAN secara komersial mulai memasuki tahap yang serius.

Pada tahun 1990 WLAN dapat dipasarkan dengan produk yang menggunakan teknik *spread spectrum* (SS) pada pita ISM, dengan frekuensi terlisensi 18-19 GHz dan teknologi IR berlaju data > 1 Mbps.

Pada tahun 1997 sebuah lembaga independen bersama IEEE membuat spesifikasi atau standar *nirkabel* pertama yang diberi kode 802.11. Peralatan yang sesuai dengan standar 802.11 dapat bekerja pada *frekuensi* 2,4 GHz dan kecepatan transfer data teoretis maksimal sebesar 2 Mbps.

Pada bulan Juli 1999 IEEE kembali mengeluarkan spesifikasi baru yang bernama 802.11b. kecepatan transfer data teoretis maksimal yang dapat dicapai adalah 11 Mbps. Kecepatan transfer data sebesar ini sebanding dengan *ethernet* tradisional (IEEE 802.3 10Mbps atau 10Base-T). Peralatan yang menggunakan standar 802.11b juga dapat bekerja pada frekuensi 2,4 GHz. Namun, salah satu

kekurangan peralatan *nirkabel* yang bekerja pada frekuensi ini adalah terjadinya gangguan dari telepon *nirkabel*, *oven mikro* gelombang, atau peralatan lain yang menggunakan gelombang radio pada frekuensi yang sama.

Kemudian, IEEE juga membuat spesifikasi 802.11a yang menggunakan teknik berbeda. Frekuensi yang digunakan adalah 5 GHz dan mendukung kecepatan transfer data teoretis maksimal sampai 54 Mbps. Gelombang radio yang dipancarkan oleh peralatan 802.11a relatif susah menembus dinding atau penghalang lainnya. Jarak jangkau gelombang radio relatif lebih pendek dibanding 802.11b. Secara teknis, 802.11b tidak kompatibel dengan 802.11a. Namun, saat ini masih cukup banyak pabrik peralatan keras yang membuat peralatan yang mendukung kedua standar tersebut.

Pada tahun 2002 IEEE membuat spesifikasi baru lagi yang dapat menggabungkan kelebihan 802.11b dan 802.11a. Spesifikasi yang diberi kode 802.11g ini bekerja pada *frekuensi* 2,4 Ghz dengan kecepatan transfer data teoretis maksimal 54 Mbps. Peralatan 802.11g kompatibel dengan 802.11b sehingga dapat dipertukarkan. Misalnya, sebuah komputer yang menggunakan kartu jaringan 802.11g dapat memanfaatkan AP 802.11b dan sebaliknya.

Tahun 2006, 802.11n dikembangkan dengan menggabungkan teknologi 802.11b dan 802.11g teknologi yang diusung dikenal dengan istilah *Multi Input Multiple Output* (MIMO) yang merupakan teknologi *wifi* terbaru. MIMO ini menawarkan peningkatan transfer data, keunggulan reliabilitas, serta peningkatan jumlah *client* yang dapat terkoneksi. Daya tembus MIMO terhadap beberapa penghalang cukup baik dan jangkauannya lebih luas sehingga dapat

menempatkan laptop sesuai keinginan. AP MIMO juga dapat mengenali gelombang radio yang dipancarkan oleh *adapter wifi* 802.11a/b/g dan dapat menghasilkan kecepatan transfer data sebesar 108 Mbps.

2.1.2.2 Keunggulan Jaringan Wireless LAN

Menurut Hantoro (2009:5) berikut ini adalah beberapa keuntungan ketika menggunakan jaringan *wireless* LAN.

1. Tingkat Mobilitasnya Tinggi

Wireless LAN memungkinkan *client* untuk mengakses informasi secara *real time* dimanapun dalam jangkauan WLAN sehingga meningkatkan kualiatas layanan dan produktifitas yang tidak mungkin dapat diberikan oleh jaringan LAN biasa. Pengguna dimanapun berada baik di *area* kantor bahkan di area publik (*hospot*) akan selalu dapat tersambung ke internet. Dengan demikian akan mendukung komunikasi suara, data dan informasi yang lebih cepat.

2. Kemudahan dan Kecepatan Instalasi

Instalasi WLAN sangat mudah dan cepat tanpa harus menarik dan memasang kabel melalui dinding atau atap. Kabel digunakan hanya untuk menghubungkan AP (*access point*) ke jaringan (HUB/*switch*/*router*). Sedangkan koneksi dari *station* (komputer) pelangga terhubung ke jaringan *via* radio. Lain halnya bila menggunakan *wired* LAN maka tiap *station* (komputer) yang akan tersambung ke jaringan LAN diperlukan penarikan kabel satu per satu HUB/*switch.*

.

3. Fleksibel

Dengan teknologi WLAN, memungkinkan untuk membagun jaringan pada area yang tidak mungkin atau sulit untuk dijangkau oleh kabel seperti di kota-kota besar, di tempat-tempat yang tidak tersedia infrastruktur kabel.

4. Menurunkan Biaya Kepemilikan

Meskipun biaya investasi awal untuk perangkat keras WLAN lebih mahal dari pada LAN konvensional, tapi biaya instalasi dan perawatan jaringan WLAN lebih murah, sehingga secara total dapat menurunkan besar biaya kepemilikan. Di samping itu sangat cocok untuk lingkungan dinamis di mana sering terjadi perpindahan, penambahan atau perubahan posisi kerja.

5. *Scalable*

WLAN dapat digunakan dengan berbagai topologi jaringan sesuai dengan kebutuhan instalasi atau spesifikasi, mulai dari jaringan independen yang hanya terdiri dari beberapa klien saja, sampai jaringan infrastruktur yang terdiri dari ribuan klien. Proses implementasi WLAN dapat dilakukan secara bertahap sesuai dengan kebutuhan. Misalkan untuk tahap awal hanya memasang 1 AP kemudian berkembang menjadi beberapa AP sesuai dengan kebutuhan.

6. Produktifitas

Kapabilitas dalam hal komputasi merupakan syarat mutlak suatu korporasi agar produktifitas karyawannya dapat diandalkan. Dengan dukungan teknologi WLAN maka karyawan (*workers*) dapat selalu tersambung ke internet dalam keadaan *mobile*. Dengan dukungan perangkat *mobile* maka karyawan dapat cepat merespon kebutuhan atau komplen pelanggan. Hasil akhir tingkat penjualan dan

loyalitas pelanggan juga semakin meningkat. Dalam keadaan tertentu maka proses pengambilan keputusan dapat segera dilakukan.

2.1.2.3 Kerugian Jaringan *Nirkabel*

Menurut Utomo (2012:23) selain beberapa keuntungan, pengguna jaringan *nirkabel* juga mempunyai beberapa kelemahan jika ditinjau dari beberapa faktor, yaitu:

1. Faktor Keamanan

Karena jaringan *nirkabel* bekerja dengan medium udara, sebenarnya transmisi data dapat ditangkap dan disadap oleh siapa saja sehingga banyak sekali tipe serangan yang terjadi pada jaringan *nirkabel*. Namun, ada beberapa teknik dan tip optimalisasi jaringan *nirkabel* untuk pencegahan preventif.

2. Faktor Kecepatan

Jaringan *nirkabel* dapat menyediakan transmisi data hingga 54 Mbps dan 11 Mbps. Namun, hal itu juga dipengaruhi oleh lingkungan sehingga laju data yang didapat menjadi 24 Mbps dan 11 Mbps. Faktor cuaca sangat berpengaruh terhadap kualitas sinyal, mengingat bahwa sistem transmisi yang digunakan adalah medium gelombang radio di udara, sehingga bisa memberikan penundaan kepada pengguna.

3. Faktor Biaya (*Cost*)

Harga komponen untuk membuat sebuah jaringan *nirkabel* saat ini masih tergolong mahal sehingga implementasinya membutuhkan perencanaan yang tepat. Walaupun biaya awalnya sangat tinggi, biaya perawatannya masih lebih murah dibandingkan dengan berkabel. Selain itu, jaringan nirkabel ini sangat

cocok untuk lingkungan yang dinamis, maksudnya sering mengalami perpindahan atau rotasi lingkungan kerja.

Terlepas dari keuntungan dan kerugiaan jaringan *nirkabel*, saat ini pemanfaatan teknologi *nirkabel* telah banyak digunakan baik didalam perusahaan (*privat*) maupun di lokasi publik (*hospot*). Semakin maraknya pengguna jaringan *nirkabel* menunjukkan bahwa keuntungan *nirkabel* lebih besar dibandingkan dengan kerugiannya.

2.1.2.4 *Topologi Wifi*

Menurut Prabawati (2010:5) *topologi* sebuah jaringan *wifi* dapat dibedakan menjadi 2, yaitu:

1. *Topologi Ad Hoc*

Topologi ad hoc adalah *topologi* jaringan *wifi* di mana komputer maupun *mobile station* terhubung secara langsung tanpa menggunakan AP. Jadi, komunikasi langsung dilakukan melalului masing-masing perangkat *wireless* yang terdapat pada komputer atau perangkat komunikasi lainnya. Prinsip kerja *ad hoc* sama dengan prinsip kerja jaringan komputer secara *peer to peer.*

2. Topologi Infrastruktur

Topologi infrastruktur adalah *topologi* pada jaringan *wifi* dimana komputer-komputer maupun *mobile stations* dalam suatu jaringan terhubung melalui AP. Jadi, setiap komputer maupun *mobile station* yang hendak berhubungan harus melewati AP terlebih dahulu, baru kemudian dapat menggunakan sumber daya yang ada pada jaringan.

2.1.2.5 Komponen Utama Jaringan *Wifi*

Menurut Maslan dan Wangdra (2012:107) terdapat empat komponen yang berfungsi menerima dan mengirimkan data dari WLAN:

1. *Access point*

Access point berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan keperangkat *wireless* LAN yang lain dan dikonversikan ulang menjadi sinyal frekuensi radio.

2. *Wireless* LAN *interface*

Wireless LAN *interface* merupakan *device* yang dipasang di *access point* atau di *mobile/desktop* PC, *device* yang dikembangkan secara massal adalah dalam bentuk PCMCIA (Personal *Computer Memory Card International Association*) *card.*

3. *Wired* LAN

Wireless LAN merupakan jaringan kabel yang sudah ada, jika *wired* LAN tidak ada maka hanya sesama *wireless* LAN saling terkoneksi.

4. *Mobile/desktop PC*

Mobile/desktop PC merupakan perangkat akses untuk *client*, *mobile* PC pada umumnya sudah terpasang *port* PCMCIA sedangkan *desktop* PC harus ditambahkan PC *card* PCMCIA dalam bentuk ISA *(Industry Standard Architecture*) atau PCI (*Peripheral Component Interconnect) card*.

2.1.2.6 *Hotspot*

Menurut Maslan dan Wangdra (2012:109) *wireless* LAN bukanlah *mobile*, tetapi dikembangkan untuk mendukung pengguna *stasioner* didalam sebuah *area* yang kecil (*small reach*), yaitu hanya beberapa radius meter jaraknya dari *centric access point* (AP), ini merupakan unsur inti pada setiap *wireless* LAN. Akan tetapi *wireless* LAN dapat juga mendukung para pemakai *mobile*, dengan menggunakan suatu publik *wireless* LAN, yang sering direferensikan sebagai *hotspot*. Internet mengakses *via hotspot* yang *provisioned* oleh suatu WISP (*wireless* internet *servis provider*), walaupun *hotspot* masih ditemukan hanya pada tempat yang konsentrasi pemakaian tinggi, seperti aula konferensi, ruang bersantai pelabuhan udara, hotel, atau *cafe*, maka pemakai *mobile* yang tidak di dalam jangkauan jaringan (*wired* maupun *wireless* internet), boleh menghubungkan ke internet *via* publik *wireless* LAN dan boleh memanfaatkan *rate* data tinggi. Bagaimanapun, komunikasi *wireless* umum muncul suatu permasalahan antara lain faktor keamanan. Demikian pula *wireless* LAN tidak terkecuali, oleh karena itu permasalahan benar-benar harus dipelajari dan dikembangkan dalam mengatasinya. *Hotspot services* dirancang untuk kemudahan yang maksimum bagi pengguna *wireless* LAN, sehingga biasanya tidak menawarkan WEP atau WPA *encryption,* jika berhubungan dengan suatu *hotspot* yang dianggap semua data yang dikirim mungkin *unencrypted.* Karena *wireless* LAN mengijinkan *peer to peer* koneksi, maka semua pengguna jaringan dapat saling melihat apa isi data pada masing-masing komputer bahkan *file-fil*e rahasia dapat diamati bila tidak dilindungi seperti informasi, angka-angka kartu kredit, IP *address* koneksi, isi *e-*

mail, pesan tertentu yang akan dikirim dan *file* rahasia lainnya. Seseorang dengan mudah dapat melakukan pengrusakan misalnya dengan dimasukan *virus* yang dapat menghentikan kegiatan komputer yang ada.

2.1.2.7 Penyerangan pada *Hotspot*

Menurut Maslan dan Wangdra (2012:110) penggunaan *wireless* LAN mempunyai faktor keunggulan yaitu selalu menyediakan sambungan jaringan tanpa harus memakai kabel. 50% dari 1000 perusahaan di Amerika menggunakan teknologi ini yang didasari oleh perkembangan teknologi dari standard 802.11x. Akan tetapi system jaringan ini hampir kurang memadai dan kurang perhatian terhadap keamanan informasi. Kemanan dari *system* jaringan ini sangat menentukan suksesnya suatu kinerja bisnis dan memerlukan faktor penting dalam mencapai tujuan perusahaan. Peralatan dari standard 802.11b mempunyai biaya yang rendah hal ini membuat teknologi tersebut begitu atraktive dan membuat para penyerang (*attacker)* mudah untuk melakukan serangan. Tetapi dengan manajemen yang baik dan *setting* yang bagus serta didukung oleh peralatan dan perlengkapan yang mendukung yang dimiliki hal tersebut dapat diatasi.

Resiko serangan yang munkin akan terjadi pada *standard* 802.11b dapat dikategorikan sebagai berikut:

1. ***Insertion Attack***

Insertion attack didasari oleh adanya *device-device* yang bekerja tidak sesuai dengan prosedur baku (*unauthorizded device*) atau menciptakan jaringan *wireless* baru tanpa melalui proses pengamanan. Pada jenis serangan ini, seorang penyerang mencoba melakukan koneksi kedalam jaringan *wireless* seorang *client*

menggunakan laptop dan melakukan *access point* dapat dirubah untuk meminta sebuah *password,* orang tersebut (penyerang) berusaha masuk dan dapat melakukan koneksi kedalam jaringan internal dengan mudah. Meskipun beberapa *access point* menggunakan *password* yang sama untuk semua *access client,* sebaiknya semua pengguna memakai *password* baru setiap kali melakukan *access point*. Suatu perusahaan munkin tidak selalu berhati-hati bahwa ada saja pegawai internal yang ada didalam perusahaan secara tidak sadar telah menyebarkan kapabilitas dari *wireless* ke dalam jaringan, dalam hal ini perusahaan memerlukan suatu kebijaksanaan untuk memastikan konfigurasi pengamanan *access point*.

2. *Interception* dan *Monitoring Traffic Wireless*

Sebagai jaringan tanpa kabel, ada kemungkinan terjadi pemotongan jalur *wireless*, penyerang harus berada dalam suatu jangkauan jarak akses sekitar 300 kaki untuk *type* 802.11b supaya serangan bisa berjalan, penyerangan bisa berada dimana saja, dimana terdapat kemungkinan koneksi jaringan bisa masuk. Keuntungan pemotongan jalur *wireless* ini adalah serangan tersebut hanya memerlukan penempatan dari suatu agen yang berfungsi memantau *system* yang mencurigakan. Semua ini memerlukan akses ke dalam aliran data di dalam jaringan. Ada dua pertimbangan penting untuk tetap bekerja pada radius atau jarak pada *type* 802.11b. Pertama, posisi antena *didesign* secara langsung, yang dapat meneruskan signal transmisi atau jarak penangkalan signal dari *device* 802.11b. Oleh karena itu jangkauan maksimum 300 kaki adalah suatu *design* instalasi normal untuk *type* ini.

Kedua, *design* pola lingkaran, pada pola ini signal dari 802.11b hampir selalu menembus signal dibelakang batas *area* hal ini dimaksudkan untuk meng-*cover* signal tersebut. *Wireless packet analysis*, seorang penyerang melakukan *capture* terhadap jalur *wireless* menggunakan teknik yang sama dengan seorang *user* yang tidak diundang atau pekerja yang ceroboh di dalam jaringan kabel. Banyak cara untuk melakukan *capture,* bagian pertama, dimana data yang secara *typical* akan menyertakan *user name* dan *password* seorang yang memaksa masuk dan melakukan penyamaran sebagai seorang *user* legal, dengan menggunakan informasi dari hasil *capture* ini digunakan untuk melakukan pembajakan *user session command* yang tidak sesuai dengan prosedur resmi yang ada.

3. *Jamming*

Denial of Service Attack/DoS *Attack* mudah untuk diterapkan ke dalam jaringan *wireless*. Dimana jalur tidak dapat menjangkau *client* atau *access point* sebab jalur yang tidak resmi membanjiri frekuensi akses tersebut. Seorang penyerang dengan peralatan dan perlengkapan yang memadai dapat dengan mudah membanjiri dengan frekuensi 2,4 GHz. Membuat signal menjadi rusak sampai jaringan *wireless* berhenti berfungsi. Dalam hal lain kawat telepon, monitor mini dan *device* lain yang beroperasi dengan frekuensi 2,4 GHz dapat merusak jaringan *wireless* tersebut dengan menggunakan frekuensi ini. DoS *attack* ini dapat berasal dari luar *area* kerja *wireless*.

4. *Client To Client Attack*

Client wireless dapat saling berkomunikasi satu sama lain dengan melakukan *access point* terlebih dahulu. Oleh karena itu *user* perlu untuk perlu

melakukan perbandingan terhadap *client* tidak hanya sekedar melawan suatu ancaman eksternal tetapi juga melawan satu sama lain.

5. *File Sharing* dan Serangan Melalui Layanan TCP/IP

Layanan *wireless client* yang berjalan menggunakan pelayanan yang diberikan oleh TCP/IP seperti *web server*, atau *file shering* terbuka untuk pemakaian yang sama dari kesalahan konfigurasi setiap *user* didalam suatu jaringan yang menggunakan kabel.

6. DoS (*Denial of Service*)

Suatu *device wireless* yang membanjiri *clienti wireless* lain, dengan menggunakan paket palsu, menciptakan suatu DoS *attack,* IP atau MAC palsu, segaja atau tidak dapat menyebabkan kerusakan pada jaringan.

7. Serangan *Brute Force Attack* Terhadap *Password* Seorang *User*

Sebagai besar *access point* menggunakan suatu kunci tunggal atau *password* yang dimiliki oleh *client* pada jaringan *wireless*. Serangan *brute force* ini mencoba melakukan uji coba terhadap kunci akses tersebut dengan memalsukan beberapa kemungkinan.

8. Serangan Terhadap *Enkripsi*

Standard 802.11b menggunakan sebuah *system enkripsi* yaitu WEP (*Wireless Equivalent Privacy*). Tidak banyak peralatan siap tersedia untuk mengangkat masalah ini, tetapi perlu diingat bahwa para penyerang selalu dapat merancang alat yang dapat mengimbangi *system* keamanan yang baru.

2.2. Teori Khusus

2.2.1 DNS (*Domain Name System*)

Menurut penelitian Modi, *et al*. DNS adalah sistem penamaan hirarkis untuk komputer dan menyediakan layanan di internet. *Domain Name Services* menerjemahkan nama *domain* yang dapat dibaca manusia ke dalam beberapa alamat IP yang sesuai. Ketika tipe *user* nama *domain* ke dalam *browser*, komputer mengirim permintaan ke *name server* (NS) yang dikelola oleh Internet *Service Provider* (ISP). Jika nama *server* ditemukan URL yang diminta pada terblok, maka alamat dikembalikan ke *browser*. Jika URL yang diminta tidak dalam *cache* maka nama *server* akan mengirimkan permintaan hirarki DNS lanjut dari *name server*. Tetapi penyerang menggunakan beberapa trik dalam menambahkan atau memodifikasi data DNS diambil untuk mengirim pengguna *browser*. Seorang pengguna dapat mengunjungi situs yang situs penipuan dan pengguna mengirimkan data *credential* akun mereka. Serangan ini juga disebut serangan *pharming* dan juga disebut DNS pembajakan.

Menurut Oktavian (2015:204) DNS (*Domain Name System*) adalah sebuah *system* yang dibangun dan bertujuan untuk menyimpan informasi tentang nama *host* dan nama *domain* dalam bentuk *database* tersebar didalam internet. DNS menyediakan IP *address* untuk setiap nama *host* yang diakses di dalam internet. Keberadaan DNS sangat penting, karena *protokol-protokol* jaringan tidak mengerti dengan tipe data *string*. Oleh karena itu komputer tidak tahu dengan yang namanya *www.google.com*, *www.facebook.com*, dll karena didalam jaringan, ia hanya dapat mencari *host* lain menggunakan IP *address*.

Tapi *browser* mengerti *Uniform Resource Locator* (URL) yang anda tuliskan, padahal yang anda tuliskan sebagai ID sebuah *host* berbentuk *string*. Di sinilah fungsi penting sebuah DNS, ketika anda mengetikkan *www.google.com*, *browser* akan menghubungi DNS *server* lalu bertanya "berapakah IP *address* dari *www.google.com*?". DNS *server* kemudian mencari informasi IP *address* dari *www.google.com* di dalam *database* yang tersebar di internet. Setelah menemukan informasi yang dicari, DNS *server* kemudian mengirimkannya kembali ke *browser*. Dengan informasi IP *address* yang diperoleh, *browser* dapat melakukan koneksi ke *web server* dari *google*. DNS tidak hanya diperuntukkan terhadap jaringan internet, namun dapat juga diimplementasikan di dalam jaringan internet yang berskala sedang maupun kecil seperti WAN atau LAN. DNS dapat diibaratkan seperti sebuah buku telepon, anda dapat mencari alamat dari seseorang.

Menurut Sukmaaji dan Rianto (2008:158) fungsi DNS adalah menerjemahkan nama komputer ke dalam IP *address. Client* DNS tersebut *resolvers* dan DNS *server* disebut *name server. Resolvers* atau *client* mengirimkan permintaan ke *name server* berupa *queries. Name server* akan memproses dengan cara melakukan cek ke lokal *database* DNS, menghubungi *name server* lainnya atau akan mengirimkan *message failute* jika tetnyata permintaan dari *client* tidak ditemukan. Proses tersebut disebut dengan *foward lookup query* yaitu permintaan *client* dengan cara pemetaan nama komputer (*host*) ke dalam IP *address.* Dalam proses kerjanya *resolvers* akan mengirim *queries* ke *name server*, kemudian *name server* melakukan cek ke lokal *database*, atau menghubungi *name server* lainnya.

Jika ditemukan akan diberitahukan ke *resolvers* dan jika tidak akan mengirimkan *failure message*. Selanjutnya, *resolvers* menghubungi *host* yang dituju dengan menggunakan IP yang diberikan oleh *name server*.

Domain name space dalam DNS merupakan sebuah hierarki pengelompokan *domain* berdasarkan nama, yang terjadi dalam beberapa bagian diantaranya *root-level domain. Top-level domain, second-level domain,* dan *host names*. *Root-level domain* merupakan tingkatan (*level*) paling tinggi yang diekspresikan dengan titik (“.”). Setelah *root level domain*, terdapat *top level domain. Top level domain* terbagi dalam tiga kelompok, yaitu *generic domain, country domain*, dan *inverse domain. Genetic domain* merupakan *domain* yang umum digunakan dalam jaringan internet, misalnya *com* (organisasi komersial), *edu* (intitusi pendidikan), *gov* (intitusi pemerintahan), *int* (organisasi internasional), *mil* (group militer), *net* (*support center* jaringan), dan *org* (organisasi *nonprofit*). *Country domain* adalah *domain* yang memiliki arti suatu negara dan umumnya menggunakan dua karakter (misalnya *id* untuk Indonesia), pada *level*-1 (di bawahnya) umumnya pada *country domain* menunjukkan nama dari suatu instansi. *Inverse domain* adalah *domain* yang digunakan untuk *mapping* dari alamat ke nama. DNS dibentuk oleh dua *server* yakni *primary server* (*master*) dan *secondary server* (*slave*).

Primary server, sesuai dengan namanya, *primary* atau *master* adalah pemegang daftar lengkap dari sebuah domain yang dikelolahnya. *Server* ini memegang otoritas penuh atas *domainnya*. *Server ns1.stikom.edu* memegang otoritas penuh atas *domain* **.stikom.edu*. otoritas penuh berarti *server* yang

bertanggung jawab untuk mengelola nama-nama *host berdomain stikom.edu* dan sub-sub *domain* di bawahnya. Selain itu, hanya *server* ini yang dapat membuat sub *domain* di bawah *stikom.edu*. *Secondary server*, merupakan *backup* dari *primary server*. Sama seperti *primary, secondary* juga memuat daftar lengkap sebuah *domain*. Hubungan antara *primary* dan *secondary* ini seperti *mirror*. Bila ada perubahan di *primary server*, *secondary server* akan mengikuti secara periodik. *Secondary* memerlukan izin dari *primary* untuk melakukan singkronisasi. Singkronisasi disebut dengan *zona transfer. Secondary* diperlukan sebagai *backup* bila *primary crash* atau sibuk dan untuk mempermudah pendelegasian.

DNS dibuat dengan arsitektur aplikasi *client/server*. Proses yang dilakukan DNS untuk melakukan *mapping* suatu nama *host* ke dalam alamat *host* atau dari alamat *host* ke nama *host* disebut *name-address resolution*. Sebuah *host* yang melakukan *mapping* suatu alamat ke dalam nama atau dari nama ke alamat dengan memanggil DNS *client* disebut dengan istilah *resolver*. Sebuah *resolver* mengakses DNS *server* tersebut ditemukan informasi dari suatu nama *domain* yang diakses, secara langsung informasi tersebut dapat diketahui. Akan tetapi jika seandainya dalam *server* tersebut tidak ditemukan, maka DNS *server* akan menghubungi *server* lain guna mendapatkan informasi yang dibutuhkan.

2.2.2 *Spoofing*

Menurut penelitian Joshi, *et al*. *Spoofing* adalah satu kesatuan yang menyamar sebagai lain. Serangan berbasis *spoofing* yang terkenal di internet setidaknya untuk dua dekade terakhir. Meskipun mereka terkenal dan baik dan

bagaimana mereka mengatasi tantangan-tantangan.

Serangan berdasarkan *spoofing* tidak hanya terus, mereka tersebar luas. *Spoofing* pernah populer di TCP SYN jenis banjir serangan. Seiring waktu, *spoofing* semakin digunakan dalam berbagai jenis serangan. *Spoofing* sering merupakan bagian integral dari berbagai DoS (*Denial of Service*) serangan. Di masa lalu, *spoofing* banyak digunakan di DDoS (*Distributed Denial of Service*) dan DRDoS (*Distributed Refleksi Denial of Service*) serangan.

Meskipun IP *spoofing* berdasarkan (di mana sumber alamat IP dalam paket IP palsu) adalah jenis yang paling populer dari *spoofing*, jenis lain *spoofing* juga muncul di internet:

a. MAC *spoofing*: MAC *spoofing* dilakukan dengan menetapkan sumber alamat MAC dari *frame ethernet* ke alamat MAC milik mesin yang berbeda.
b. ARP *spoofing*: Ini melibatkan mengirimkan ARP paket dengan *ethernet* MAC yang tidak sesuai dengan alamat IP yang diminta dalam paket permintaan ARP.
c. DNS *spoofing*: DNS *spoofing* terjadi ketika komputer lain bukan *server* DNS yang *valid* balasan untuk permintaan DNS seolah-olah datang dari *server* DNS yang *valid*.
d. *E-mail spoofing*: Ini melibatkan mengirimkan *email* oleh pengguna tetapi mengubah alamat *email* sumber seperti yang tampaknya.

Spoofing A dengan B dilakukan untuk berbagai tujuan. Kadang-kadang *spoofing* adalah serangan itu sendiri. Lebih umum, *spoofing* adalah bagian dari

serangan yang lebih besar. Berikut adalah beberapa alasan umum untuk *spoofing*:

a. B mencari hak istimewa dari A: Hal ini terjadi, misalnya, ketika otentikasi berdasarkan alamat IP.
b. B bermaksud untuk menyembunyikan jalurnya: ini sering digunakan sebagai metode untuk menyembunyikan identitas B ketika B terlibat dalam serangan misalnya, serangan DoS.
c. Sebagai serangan terhadap A: paket Misalnya, UDP serangan banjir menggunakan ditempa untuk mencoba dan menghubungkan layanan *chargen* UDP ke layanan UDP gema di situs lain. Sebagai contoh lain, pertimbangkan serangan DRDoS mana alamat IP sumber yang palsu adalah korban.

Tergantung pada jenis serangan di mana *spoofing* digunakan, ada berbagai konsekuensi dari serangan:

a. Layanan tidak sah: *Spoofing* digunakan untuk mencuri hak dari *user* lain.
b. Kehilangan *Service* pada Target: *Spoofing* digunakan untuk menyebabkan penolakan layanan. Sering *spoofing* digunakan untuk menyerang target.
c. Sulit untuk melacak penyerang: Karena *spoofing*, itu adalah kertas ini awalnya dipresentasikan pada sulit untuk melacak lokasi penyerang nyata dalam peristiwa serangan.
d. Sekunder korban: hal ini karena jaminan kerusakan dari serangan *spoofing*. Dalam beberapa kasus, *spoofing* dapat mengakibatkan sekunder korban. Hal ini terjadi, misalnya, mana alamat IP sumber palsu yang digunakan sebagai mekanisme untuk menyembunyikan jejak penyerang.

Korban utama dapat mengirimkan tanggapan ke alamat palsu sumber (sekunder korban) dan dalam proses dapat menguasai mereka.

e. paket yang tidak perlu menyumbat *net*: Ini juga karena kerusakan jaminan dari serangan *spoofing*. Semua paket palsu adalah paket yang seharusnya tidak masuk jaringan di tempat pertama. Akibatnya, mereka menimbulkan beban tambahan pada sistem jaringan yang paket tersebut menyeberang. Hal ini terutama relevan dalam beberapa serangan DDoS baru-baru ini di mana *spoofing* digunakan. Metode utama dari serangan ini berbasis *bandwidth*banjir sejumlah besar paket kepada korban atau ke jaringan korban jenuh *bandwidth*.

Metode utama untuk mengatasi *spoofing* adalah penyaringan paket palsu. melakukan penelitian untuk menguji seberapa baik filter internet palsu paket. Mereka memperkirakan bahwa sekitar seperempat dari Internet masih rentan terhadap *spoofing*.

Dari pembahasan di atas, maka diambil kesimpulan sebagai berikut:

a. *Spoofing* tersebar luas.
b. Konsekuensi dari *spoofing* yang parah.
c. Internet sekarang tidak cukup siap untuk menangani *spoofing. Spoofing* merupakan masalah penting dan mendesak yang dihadapi internet.

2.2.3 Kejahatan Komputer

Kejahatan komputer dapat digolongkan dari yang sangat berbahaya sampai mengesalkan. Banyak cara yang dilakukan oleh penjahat komputer untuk

memenuhi keinginannya. (Sukmaaji dan Rianto 2008:158) untuk mengantisipasi kondisi tersebut perlu ditingkatkan sistem pengamanan. Dalam teknologi komputer keamanan dapat diklasifikasikan menjadi 4, yaitu:

1. Keamanan yang bersifat fisik (*physical security*)

Keamanan yang bersifat fisik termasuk akses orang ke gudang, peralatan, dan media yang digunakan. Beberapa berkas penjahat komputer (*crackers*) mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan. Misalnya pernah diketemukan coretan *password* atau manual yang dibuang tanpa dihancurkan. *Wiretapping* atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakkan juga dapat dimasukkan ke dalam kelas ini. *Denial of service*, yaitu akibat yang ditimbulkan sehingga *servis* tidak dapat diterima oleh pemakai juga dapat dimasukkan ke dalam kelas ini. *Denial of service* dapat dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan). Beberapa waktu yang lalu ada lubang keamanan dari implementasi *protocol* TCP/IP yang dikenal dengan istilah *syn flood attack*, dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*).

2. Keamanan yang berhubungan dengan orang

Keamanan yang berhubungan dengan orang termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Seringkali kelemahan keamanan sistem informasi tergantung kepada manusia (pemakai atau pengelola).

Ada sebuah teknik yang dikenal dengan istilah sosial engineering yang sering digunakan oleh kriminal ini berpura-pura sebagai orang yang berhak mengakses informasi. Misalnya kriminal ini berpura-pura sebagai pemakai yang lupa *passwordnya* dan minta agar diganti menjadi kata lain.

3. Keamanan dari data dan media serta teknik komunikasi (*cummunications*)

Keamanan dari data dan media serta teknik komunikasi yang termasuk dalam kelas ini adalah kelemahan dalam *sofware* yang digunakan untuk mengelolah data. Seorang kriminal dapat memasang *virus* atau *Trojan horse* sehingga dapat mengumpulkan informasi (seperti *password*) yang semestinya tidak berhak diakses.

4. Keamanan dalam operasi

Keamanan dalam operasi termasuk prosedur yang digunakan untuk mengatur dan mengelolah sistem keamanan, dan juga termasuk prosedur setelah serangan (*pos attack recovery*)

2.2.4 Aspek-Aspek Keamanan Komputer

Keamanan komputer meliputi beberapa aspek diantaranya:

1. *Authentication*:

Agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki (Ariyus, 2006:2)

Sukmaaji dan Rianto (2008:161) *Authentication* berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang

mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang kita hubungi adalah betul-betul *server* yang asli. Masalah pertama, membuktikan keaslian dokumen. Dapat dilakukan dengan teknologi *watermarking* dan digital *signature*. *Watermarking* juga dapat digunakan untuk menjaga intelektual *property*, yaitu dengan menandai dokumen atau hasil karya dengan tanda tangan pembuat. Masalah kedua biasanya berhubungan dengan *access control*, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan *password*, keamanan *biometric* (ciri-ciri khas orang), dan sejenisnya.

2. *Integrity*

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 (Ariyus, 2006:2)

Sukmaaji dan Rianto (2008:160) Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin informasi. Adanya *virus, trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi. Sebuah *e-mail* dapat saja ditangkap (*intercept*) di tengah jalan, diubah isinya (*altered, tampered, modified*), kemudian diteruskan ke alamat yang dituju. Penggunaan *engkripsi* dan digital *signature* misalnya, dapat mengatasi masalah ini. Salah satu contoh kasus *trojan horse* adalah distribusi paket program TCP *wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak

bertanggung jawab. Jika anda memasang program yang berisi *troja horse* tersebut, maka ketika anda merakit (*compile*) program tersebut, dia akan mengirimkan *e-mail* kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem. Contoh serangan ini adalah yang disebut *man in the middle attack* di mana seseorang menempatkan di tengah pembicaraan dan menyamar sebagai orang lain.

3. *Nonrepudiation*

Merupakan hal yang bersangkutan dengan si perngirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut. (Ariyus, 2006:3)

Sukmaaji dan Rianto (2008:163) Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan *e-mail* untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan *e-mail* tersebut. Aspek ini sangat penting dalam hal *electronic commerce*. Penggunaan digital *signature, certifiates*, dan teknologi *kriptografi* secara umum dapat menjaga aspek ini. Akan tetapi, hal ini masih harus didukung oleh hukum sehingga status dari digital *signature* itu jelas legal.

4. *Authority*

Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.

5. *Confidentiality*

Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.

6. *Privacy*

merupakan lebih kearah data-data yang sifatnya *privat* (pribadi).

7. *Availability*

aspek *avialibility* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

8. *Access control*

aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal itu biasanya berhubungan dengan masalah *authentication* dan juga *privacy. Access contro*l sering kali digunakan menggunakan kombinasi *user id* dan *password* atau dengan menggunakan mekanisme lainnya.

2.2.5 Aspek-Aspek Ancaman Keamanan

Menurut Ariyus (2006:3) terdapat 4 aspek-aspek ancaman keamanan antara lain:

1. *Interruption*

Interruption merupakan suatu ancaman terhadap *avaibability*, informasi atau ada yang ada dalam sistem komputer dirusak, dihapus, sehingga jika dibutuhkan maka sudah tidak ada lagi.

2. *Interception*

Interception merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi yang ada di dalam sistem disadap oleh orang yang tida berhak mendapatkan akses ke komputer di mana informasi tersebut disimpan.

3. *Modification*

Modification merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan orang tersebut.

4. *Fabrication*

Febrication merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan suatu informasi sehingga orang yang menerima informasi tersebut menyangka informasi tersebut bersal dari orang yang dikehendaki oleh si penerima informasi tersebut.

2.2.6 *Wireless Security Protocols*

Menurut Oktavian (2015:62) Terdapat beberapa *mode user authentication* yang terimplementasi pada AP saat ini antara lain:

1. WEP *Open System Authentication*

Tipe *autentikasi* ini tidak memiliki mekanisme pengamanan untuk *user* yang ingin berasosiasi dengan AP sehingga siapapun *client*-nya bebas untuk berarsosiasi dengan AP dan terkoneksi ke dalam jaringan. Ibarat rumah, maka pintunya terbuka lebar dan tidak terkunci. Tapi walaupun anda sudah bisa masuk ke dalam area rumah melalui pintu masuk, namun belum tentu diizinkan atau dapat berbicara serta berkomunikasi di dalam rumah karena bahasa yang digunakan untuk berkomunikasi di dalam rumah tersebut berbeda dengan bahasa yang anda gunakan. Ini lah yang disebut data *encryption* dalam kaitannya dengan asosiasi yang dilakukan *client* dengan AP. Di dalam *protokol* WEP terdapat WEP

key yaitu sebuah kata kunci yang ada dipihak *client* walaupun AP bila *protokol* WEP diaktifkan maka AP terlebih dahulu mengecek data yang dikirimkan oleh *client*, apakah data telah *dienkripsi* dengan WEP *key* yang sama dengan WEP *key* yang ada pada AP atau tidak, jika sama maka data akan diteruskan ke tujuan, jika tidak maka data akan dibuang. Jaringan wifi dengan *open system* termasuk jaringan yang tidak aman karena tidak ada pengengkripsian pada data. Peneliti sangat menyarankan untuk berhati-hati dalam melakukan *browsing* atau apapun itu di dalam jaringan ini karena data-data yang dikirim melalui jaringan bersifat *plain text,* artinya orang lain dapat dengan mudah membaca data.

2. WPA (*Wifi Protected Access*)

Keamanan jaringan WEP sudah tidak dapat dijamin lagi, beberapa dekade yang lalu *hacker* telah menemukan cara untuk meng-*crack* WEP *key* bahkan hanya dalam waktu kurang lebih 10 menit. Hal ini membuat *aliansi wifi* (para pengembang *wifi*/802.11 *standard*) mencari *protokol* baru yang dapat menutup celah dari WEP. Dikembangkanlah *protokol* keamanan baru yaitu WPA (*Wifi Protected Access*). Pada awal ditemukannya kelemahan pada WEP oleh para *hecker,* pihak pengembang menjadi gusar sehingga agak terburu-buru dalam mencari pengganti WEP. WPA yang dikembangkan bisa disebut sebagian perbaikan dari WEP dan bukan merupakan sesuatu yang baru. Jadi masih terdapat banyak kekurangan pada WPA karena teknik pengengkripsiannya saja yang berbeda dari WEP. Secara umum *mekanisme authentication*-nya masih sama seperti yang dimiliki WEP. WPA awalnya menggunakan algoritma TKIP (*Temporal Key Intergrity Protokol*) untuk mengengkripsi datanya sebagai

pengganti *algoritma* RC4 yang digunakan oleh WEP. Kemudian dikembangkan lagi sehingga tersedia *algoritma* baru yang dapat digunakan yaitu AES (*Advanced Encryption Standard*), *algoritma* yang lebih baik dibanding dengan TKIP.

3. WPA2 (*Wifi Protected Access Version* 2)

Wifi protected access version 2 (WPA2) adalah pengembangan yang benar-benar baru dari *protokol* keamanan *wifi*, diselesaikan pada tahun 2004 oleh aliansi *wifi*. Menawarkan keamanan yang paling tinggi dengan tetap menggunakan *algoritma* TKIP dan AES sebagai *algoritma* pengenkrepsian datanya. Dikembangkan pula *algoritma* baru untuk mengengkripsi data yaitu CCMP. Tapi sebaik apapun pengembangannya, tidak ada sistem yang benar-benar aman. Selalu ada jalan bagi *hacker* agar dapat masuk ke dalam suatu *system*. WPA/WPA2 pun tidak luput dari target para *hacker*.

2.2.7 Macam-Macam Serangan

Menurut Ariyus (2006:45) terdapat beberapa macam-macam serangan antara lain:

1. *Intrussion*

Pada penyerangan jenis ini, seorang penyerang akan dapat meggunakan sistem komputer yang kita miliki. Sebagian penyerang jenis ini menginginkan akses sebagaimana pengguna yang memiliki hak untuk mengakses sistem.

2. *Intelligence*

Intelligence merupakan para *hacker* atau *Cracker* yang melakukan suatu kegiatan untuk mengumpulkan segala informasi yang berkaitan dengan *system* target. Berbagai cara dapat ditempuh untuk mendapatkan informasi tersebut, baik

melalui internet, mencari buku-buku atau jurnal. berdiskusi di *mailing list* atau IRC, dan lain-lain. Termasuk juga mendapatkan informasi dari mantan karyawan yang pernah bekerja ditempat tersebut. Contoh data yang dibuang di *harddisk* mereka bisa membangkitkan kembali dan memperhatikan data tersebut ini biasanya dilakukan oleh seorang mantan karyawan yang berkerja di suatu perusahaan atau kita pernah mendaftar di suatu perusaan *online* maupun *offline*, karena *email* utama dan *password* utama kita jangan sampai diketahui oleh siapapun, gunakan *email* saat *log in* di suatu perusahaan *host*, berbeda dengan saat kita *log in* di data yang kita kelola yang benar-benar *privasi.*

3. *Land Attack*

Land attack merupakan salah satu macam serangan terhadap suatu *server*/komputer yang terhubung dalam suatu jaringan yang bertujuan untuk menghentikan layanan yang diberikan oleh *server* tersebut sehingga terjadi gangguan terhadap layanan atau jaringan komputer tersebut. Tipe serangan semacam ini disebut sebagai *Denial of Service* (DOS) *attack*. LAND *attack* dikategorikan sebagai serangan SYN (SYN *attack*) karena menggunakan packet SYN (*synchronization*) pada waktu melakukan 3-*way handshake* untuk membentuk suatu hubungan berbasis TCP/IP. Dalam 3-*way handshake* untuk membentuk hubungan TCP/IP antara *client* dengan *server*, yang terjadi adalah sebagai berikut:

a. Pertama, *client* mengirimkan sebuah paket SYN ke *server/host* untuk membentuk hubungan TCP/IP antara *client* dan *host*.

b. Kedua, *host* menjawab dengan mengirimkan sebuah paket SYN/ACK (*Synchronization/Acknowledgement*) kembali ke *client*.
c. Akhirnya, *client* menjawab dengan mengirimkan sebuah paket ACK (*Acknowledgement*) kembali ke *host*. Dengan demikian, hubungan TCP/IP antara *client* dan *host* terbentuk dan transfer data bisa dimulai.

Dalam sebuah LAND *attack*, komputer penyerang yang bertindak sebagai *client* mengirim sebuah paket SYN yang telah direkayasa atau *dispoof* ke suatu *server* yang hendak diserang. Paket SYN yang telah direkayasa atau *dispoof* ini berisikan alamat asal (*source address*) dan nomor *port* asal (*source port number*) yang sama persis dengan alamat tujuan (*destination address*) dan nomor *port* tujuan (*destination port number*). Dengan demikian, pada waktu *host* mengirimkan paket SYN/ACK kembali ke *client*, maka terjadi suatu *infinite loop* karena *host* sebetulnya mengirimkan paket SYN/ACK tersebut ke dirinya sendiri. *Host/server* yang belum terproteksi biasanya akan *crash* atau *hang* oleh LAND *attack* ini. Namun sekarang ini, LAND attack sudah tidak efektif lagi karena hampir semua sistem sudah terproteksi dari tipe serangan ini melalui paket *filtering* atau *firewall*.

4. *Logic Bomb*

Logic Bomb Merupakan Program yang dimasukan ke dalam sebuah komputer yang bekerja untuk memeriksa kumpulan kondisi di system, jika kondisi-kondisi yang dimaksud ditemukan oleh program tersebut, maka program akan mengeksekusi perintah-perintah yang ada di dalamnya. *Logic bomb* bisa bisa berjalan jika ada pemicunya. Biasanya pemicu terjadi jika *user* menjalankan

program tertentu yang ada di dalam komputer atau dengan salah satu tombol *keyboard* dan pemicu lainnya yang mungkin di buat. Program tersebut banyak di gunakan oleh *hacker* atau *cracker* untuk mengambil keuntungan dari sebuah komputer.

5. *Operation System Fingerprinting*

Merupakan suatu istilah yang umum yang digunakan oleh seseorang *cracker* untuk menganalisis sistem operasi pada sebuah sistem yang akan diserang. Hal tersebut dapat dilakukan dengan berbagai cara. Cara yang paling umum adalah dengan melakukan *telnet* ke *server* yang akan dianalisis. Jika *server* yang dituju memiliki fasilitas *telnet*, sering kali ada barner yang menunjukkan nama sistem operasi beserta versi dari OS tersebut. Apabila server tersebut tidak memiliki servis *telnet*, tetapi memiliki servis lainnya seperti FTP. Servis FTP tersedia pada port 21. Jika hal tersebut sudah diketahui, maka lakukan *telnet* ke port 21 dengan memberikan perintah sehingga diberikan informasi tentang operasi sistem tersebut.

6. *Smurf Attack*

Smurf Attack merupakan serangan yang dilakukan dengan mengubah alamat IP dari datangnya *request* (IP *Spoofing*). Penggunaan IP *Spoofing* ini memungkinkan respon dari *ping* tadi dialamatkan ke komputer yang alamatnya dipalsukan. Akibatnya, komputer akan dibanjiri paket data. Hal ini akan mengakibatkan pemborosan *bandwith* jaringan. Komputer bisa juga menjadi *hang* karena terus dibanjiri paket data. Untuk menjaga agar jaringan tidak menjadi perantara bagi serangan ini, *broadcast adressing* harus dimatikan di *router*,

kecuali jika sangat dibutuhkan untuk keperluan *multicast*. Alternatif lain dengan *memfilter* permohonan ICMP *echo* pada *firewall*. Ada baiknya juga kita memiliki *upstream firewall* yang diset untuk *memfilter* ICMP *echo* atau membatasi *traffic echo* agar presentasinya lebih kecil dibandingkan *traffic* jaringan seluruhnya.

7. *Sniffer*

Merupakan suatu program yang sifatnya melakukan pencurian atau penyadapan data. Meskipun data yang dicuri tidak hilang secara fisik, *sniffer* merupakan program yang sangat berbahaya karena dapat menyadap *password* atau data penting lain. Contoh program *sniffer* antara lain: *capture*, *sniffit*, *tcpdump* dan *webxray* pencegahan terhadap serangan ini adalah dengan mengenkripsi data akan ditransfer ke dalam jaringan.

8. *Scanning*

Scanning adalah kegiatan para *hacker* atau *cracker* untuk mengidentifikasi sistem yang menjadi target serangan dan mencari celah keamanan yang akan digunakan untuk menembus suatu sistem. Kegiatan *scanning* dari sisi jaringan sangat berisik dan mudah dikenali, kecuali jika menggunkan *stealth scanning*. *Scanning tool* yang paling terkenal adalah *nmap*. Selain itu ada juga *SuperScan* dan *UltraScan* yang banyak digunakan pada sistem *Windows*.Untuk pencegahan, program *scanner* pada umumnya menggunakan paket SYN dan ACK untuk mendeteksi celah keamanan pada sustu sistem. Juga dengan memasang *firewall,* seperti *Zone Alarm*.

9. *Social Engineering*

Identifikasi dan profil resiko dari orang yang memiliki akses. Sering kali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai dan pengelola) dan sering digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi. Misalnya, kriminal tersebut berpura-pura sebagai pemakai yang lupa *passwordnya* dan minta agar diganti mejadi kata lain.

10. *Syn Attack*

Serangan yang dilakukan apabila ditemukan kelemahan dari spesifikasi TCP/IP. Paket SYN dikirimkan pada saat memulainya *handshake* (terkoneksi) antara aplikasi sebelum pengirim data dilakukan

11. *Backdoor*

Seperti namanya, *Backdoor* merupakan suatu akses pintu belakang yang diciptakan *hacker* setelah berhasil menjebol suatu sistem. Hal ini dimaksudkan agar *hacker* mudah mendapat akses kembali ke dalam sistem yang sudah diserangnya.

12. *Cross Scripting Attack*

Seorang *cracker* bisa mengeksploitasi pertukaran *cookies* antara *browser* dan *web server*. Fasilitas tersebut dapat mengaktifkan *script* yang dapat mengubah tampilan *web*. Bahayanya, ternyata *script* tersebut bisa menjalankan *malware*, dan membaca informasi penting seperti *password* dan nomor kartu kredit. Pada dasarnya *cracker* akan *mengeksploitasi* kelemahan dari suatu aplikasi, seperti CGI *script* yang tidak bisa memeriksa input atau kerawanan pada ISS RDS pada *showcode.asp* yang mengizinkan dijalankannya perintah secara *remote*.

13. *Denial of Service Attack*

Merupakan suatu istilah yang digunakan untuk menyebut serangan yang dilakukan dengan mengulangi *request* ke *server* dari beberapa sumber secara simultan. Serangan ini bertujuan membuat *server* kewalahan untuk melayani permintaan yang dikirim dan berakhir dengan berhentinya aktivitas *server* tersebut (*hang*). Berhasil atau tidaknya serangan ini sangat dipengaruhi oleh *bandwith server*. Jika *bandwith* semakin besar, maka semakin sulit *server* tersebut disesaki data sampah yang dikirim *hacker*. Dengan kata lain, semakin sulit *hacker* melumpuhkan *server* tersebut. Tetapi *hacker* biasanya punya jalan lain, mereka tidak hanya menggunakna satu komputer, tetapi menggunakan puluhan komputer yang dibajak untuk melakukan *denial of service attack*. Untuk meluncurkan serangan, seorang *hacker* hanya mengirimkan sebuah perintah, yang diteruskan kepada banyak komputer lain yang kemudian melakukan *denial of service attack* sehingga *server web* dapat dilumpuhkan dengan sangat cepat.

14. *Cyber Espionage*

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (komputer *network system*) pihak sasaran. Kejahatan tersebut biasanya ditunjukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang komputerisasi.

15. *Carding*

Carding merupakan suatu kejahatan dengan cara mencuri dan menipu suatu *website e-comersial* untuk mendapatkan produk yang ditawarkan. Berbagai cara

dilakukan *carder* untuk mendapatkan kartu kredit milik orang lain, salah satunya dengan membuat *website* palsu sehingga pemilik kartu kredit memasukkan nomor kartu kreditnya. Data yang sudah dikumpulkan dimanfaatkan untuk kepentingannya sendiri.

16. *Eavesdropping*

Memantau seseorang atau sekelompok individu yang melakukan komunikasi data dan mencatat identitasnya untuk disalah gunakan dikemudian hari. Seseorang menyadap *user ID* dan *password* yang tidak diacak yang dikirim melalui jaringan. Penyadap ilegal yang lebih canggih dapat mencuri semua isi pesan seperti *e-mail*, transaksi *web*, atau *file* yang di *download*.

2.2.8 *Hacker* dan *Cracker*

Menurut Sukmaaji dan Rianto (2008:166) dua istilah ini paling sering disebutkan ketika kita berbicara mengenai keamanan data. *Hacker* dan *cracker* dianggap sebagai orang yang bertanggu jawab atas berbagai kasus kejahatan komputer (*cyber crime*) yang semakin marak. Padahal jika dilihat siapa dan apa yang dilakukan oleh *hacker* dan *cracker*, maka anggapan tersebut bisa dikatakan tidak 100% benar.

Hacker adalah sebutan untuk mereka yang menggunakan keahliannya dalam hal komputer untuk melihat, menemukan, dan memperbaiki kelemahan sistem keamanan dan sebuah sistem komputer ataupun dalam sebuah *sofware*. Hasil pekerjaan biasanya mengenai dipublikasikan secara luas dengan harapan sistem atau *sofware* yang didapati memiliki kelemahan dalam hal keamanan dapat disempurnakan di masa yang akan datang. Sedangkan *cracker* memanfaatkan

kelemahan-kelemahan pada sebuah sistem atau *sofware* untuk melakukan tindakan kejahatan.

Dalam masyarakat *hacker*, dikenal hierarki atau tindakan. *Hacker* menduduki tempat ke 2 dalam tindakan tersebut dan *cracker* dalam tingkatan ke 3. Selain itu, masih ada beberapa tingkatan lain seperti *lamer* (*wanna be*). Berbeda dengan *hacker* dan *cracker* yang mencari dan menentukan sendiri kelemahan sebuah sistem, seorang *lamer* menggunakan hasil temuan untuk melakukan tindak kejahatan. Seorang *lamer* biasanya hanya memiliki pengetahuan yang sedikit mengenai komputer terutama mengenai sistem keamanan dan pemrograman. Dalam komunikasi *hacker*, *lamer* murupakan sebutan yang bisa dibilang memalukan. Seorang *hacker* memiliki tujuan untuk menyempurnakan sebuah sistem, sedangkan seorang *cracker* lebih bersifat destruktif. Umumnya *cracker* melakukan *cracking* untuk menggunakan sumber daya disebuah sistem untuk kepentingan sendiri.

Istilah *hacker* sendiri masih belum baku karena bagi sebagian orang *hacker* mempunyai konotasi positif, sedangkan bagi sebagian lain memiliki konotasi negatif. Bagi kelompok yang pertama (*old school*), untuk pelaku yang jahat biasanya disebut *cracker*. Batas antara *hacker* dan *cracker* sangat tipis. Batasan ini ditentukan oleh etika, moral dan integritas dari pelaku sendiri. Salah satu yang membedakan antara *cracker* dan *hecker*, atau antara computer *underground* dan *computer security industry* adalah masalah etika. Keduanya memiliki basis etika yang berbeda dan munkin memiliki interpretasi yang berbeda terhadap suatu topik yang berhubungan dengan masalah komputasi.

Dalam teknologi *web*, aktivitas *hacker* umumnya dikenal dengan istilah *web hacking* dengan melakukan *deface situs*, *SQL injection*, dan pemanfaatan kelemahan *script web programming* (*cross site scripting*). *Deface* adalah suatu aktifitas mengubah halaman atau isi suatu situs *web* sehingga tampilan atau isinya berubah. SQL *injection attack* merupakan salah satu teknik dalam melakukan *web hacking* untuk menggapai akses pada sistem *database*. Teknik ini memanfaatkan kelemahan dalam bahasa pemrograman *scripting* pada SQL dalam mengolah suatu sistem *database* yang memungkinkan seseorang tanpa *account* dapat masuk dan lolos verifikasi dari SQL *server*.

2.2.9 Standar Jaringan Komputer

2.2.9.1 (IEEE) 802.11

Standard Institute of Electrical and Electronics Engineers (IEEE) 802.11 adalah spesifikasi kendali akses medium dan lapisan fisik untuk mengimplementasikan komunikasi komputer *wireless local area network* (WLAN) di frekuensi 2.4, 3.6, 5, dan 60 GHz diciptakan dan dioperasikan oleh IEEE. Versi dasar dirilis tahun 1997 dan telah melalui serangkaian pembaruan dan menyediakan dasar bagi produk jaringan *nirkabel wifi* (situs *wikipedia*)

2.2.9.1.1 Spesifikasi IEEE 802.11

Menurut Sofana (2008:346) spesifikasi yang dibuat oleh IEEE(*Standard Institute of Electrical and Electronics Engineers*)ternyata tidak hanya sebatas 802.11a/b/g saja. Masih ada beberapa lagi yang dapat dikategorikan dalam keluarga besar 802.11. Banyaknya spesifikasi yang dikeluarkan oleh IEEE

kadangkala membuat pengguna komputer bingung. Berikut ini perbedaan masing-masing spesifikasinya:

Tabel 2.2 Spesifikasi 802.11
Sumber: Sofana (2016)

Spesifikasi	Keterangan
802.11	Spesifikasi WLAN yang pertama, dibuat pada tahun 1997. Kecepatan transfer data maksimal yang dapat dicapai sebesar 2 Mbps.
802.11a	Dibuat pada tahun 1999. Menggunakan frekuensi 5 Ghz dan kecepatan transfer data maksimal 54 Mbps.
802.11b	Dibuat pada tahun 1999. Menggunakan frekuensi 2,4 Ghz dan kecepatan transfer data maksimal 54 Mbps.
802.11c	Merupakan spesifikasi yang dipakai untuk keperluan koneksi *bridge*. Sekarang 802.11c telah diubah menjadi 801.1.
802.11d	Dibuat pada tahun 2001. Spesifikasi ini dipakai untuk pengaturan spektrum sinyal.
802.11e	Dukungan QoS (*Quality of Service*) pada *protokol* WLAN.
802.11f	Dibuat pada tahun 2003. Merupakan standar bagi *protokol* komunikasi antar *access point*
802.11g	Dibuat pada tahun 2003. Menggunakan frekuensi 2,4 Ghz dan kecepatan transfar data maksimal 54 Mbps.

802.11h	Dibuat pada tahun 2003. Merupakan pengembangan 802.11a dan dibuat untuk mengantisipasi persoalan regulasi yang diterapkan negara-negara dibenua eropa dan asia pasifik.
802.11i	Dibuat pada tahun 2004. Pengembangan 802.11 dengan dukungan *security*.
802.11j	Dibuat pada tahun 2004. Pengembangan sinyal 5 Ghz dan mendukung regulasi yang diterapkan oleh Negara Jepang.
802.11k	Masih dalam tahap pengembangan. Merupakan spesifikasi yang digunakan untuk sistem manajemen WLAN.
802.11l	Dukungan kemampuan *security* pada WLAN. Spesifikasi ini akhirnya dibatalkan oleh IEEE, karena dapat menimbulkan kebingungan (sudah didefinikan pada 802.11i).
802.11m	Untuk keperluan pemeliharaan dokumentasi seluruh keluarga 802.11.
802.11n	Ditunjukan untuk WLAN dengan kecepatan transfer data 108 Mbps. Di pasar dapat dijumpai dengan merk dagang MIMO atau Pre-802.11n.

2.2.9.1.2 Perbandingan Perangkat 802.11 a/b/g

Menurut Sofana (2008:348) Ada sebagian orang yang berpendapat bahwa istilah *wifi* hanyalah untuk peralatan standar IEEE 802.11b. kebetulan istilah *wifi*

digunakan ketika spesifikasi 802.11b dibuat. Memang fakta menunjukkan cukup banyak produk yang dibuat mengikuti standar 802.11b.

Tabel 2.3 Perbandingan Perangkat 802.11 a/b/g
Sumber: Sofana (2016)

	802.11a	**802.11b**	**802.11g**
Kompatibilitas	IEEE 802.11a *Wifi certified*	IEEE 802.11b *Wifi certified*	IEEE 802.11g *Wifi certified*
Jumlah *channel*	4 atau 8 *non overlapping*	3 *non overlapping*	3 *non overlapping*
Jangkauan dalam ruang tertutup (*indoor range*)	40 ft (12m) @ 54 Mbps 300 ft (91m) @ 6 Mbps	100 ft (30m) @ 11 Mbps 300 ft (91m) @ 1 Mbps	100 ft (30m) @ 54 Mbps 300 ft (91m) @ 1 Mbps
Jangkauan di area terbuka (*outdoor range*-arah sinar/garis lurus)	100 ft (30m) @ 54 Mbps 1000 ft (305m) @ 6 Mbps	400 ft (120m) @ 11 Mbps 1500 ft (460m) @ 1 Mbps	400 ft (120m) @ 54 Mbps 1500 ft (460m) @ 1 Mbps
Kecepatan transfer	54, 48, 36, 24, 18,	11, 5.5, 2 dan 1	54, 48, 36, 24, 18, 12, 9,

data	12, 8, dan 6 Mbps	Mbps	dan 6 Mbps
Teknik modulasi	*Orthogonal frequency division multiplexing* (OFDM), 5 GHz	*Diirect sequence Spread* (DSSS) menggunakan *complementary code keying* (CCK), 2.4 GHz	*Orthogonal frequency division multiplexing* (OFDM), 2.4 GHz

Saat ini dapat dijumpai beberapa jenis spesifikasi *wifi*, yaitu 802.11a, 802.11b, 802.11g. peralatan 802.11g kompatibel dengan 802.11b, sehingga dapat dipertukarkan. Sebuah komputer yang menggunakan *wifi* adapter 802.11g dapat memanfaatkan *access point* 802.11b dan begitu pula sebaliknya (Sofana 2008:372).

1. Pilihan perangkat 802.11a jika:

a. Memerlukan kecepatan transfer data (teoritis) hingga 54 Mbps
b. WLAN akan digunakan untuk aplikasi multimedia, transfer *file* berukuran besar seperti: gambar/video/audio
c. Menghindari atau meminimalkan interferensi dengan peralatan *wireless* lain.
d. Sebuah *access point* hendak diakses oleh (relatif) banyak *user*
e. Berencana suatu saat nanti akan memperbesar kapasitas *host* pada WLAN.

2. **Pilihan perangkat 802.11b jika:**
    a. Memerlukan kecepatan transfer data (teoritis) sebesar 11 Mbps
    b. Ingin memperluas WLAN 802.11b yang sudah ada.
    c. Menginginkan perangkat WLAN yang dapat menjangkau seluruh bagian ruangan (*indoor*)
    d. Menginginkan perangkat WLAN yang dapat melakukan penetrasi tembok penghalang secara optimal.
    e. Memerlukan akses WLAN menggunakan paket PC, PDA, dan peralatan genggam lainnya.
    f. Sebuah *access point* hanya akan diakses oleh (relatif) sedikit user.
3. **Pilihan perangkat 802.11g jika:**
    a. Memerlukan kecepatan transfer data (teoritis) hingga 54 Mbps
    b. Ingin memperluas WLAN 802.11b atau g yang sudah ada.
    c. WLAN akan digunakan untuk aplikasi multimedia, transfer *file* berukuran besar seperti: gambar/video/audio.
    d. Menginginkan perangkat WLAN yang dapat menjangkau seluruh bagian ruangan (*indoor*)
    e. Menginginkan WLAN yang dapat menjangkau/melakukan penetrasi tembok penghalang dengan baik.
    f. Sebuah *access point* hanya akan diakses oleh (relatif) sedikit *user*.

2.2.9.2 Standar ISO 27002

Menurut peneitian Yuyun (2014) ISO/IEC 27002 adalah suatu standar keamanan informasi yang diterbitkan oleh *International Organization for*

Standardization (ISO) dan *International Electrotechnical Commission* (IEC), yang berjudul teknologi informasi, teknik keamanan dan kode praktek untuk manajemen keamanan informasi .

ISO/IEC 27002:2005 telah berkembang dari BS7799, yang diterbitkan pada pertengahan 1990-an. *The British Standard* diadopsi oleh ISO/IEC sebagai ISO/IEC 17799:2000, direvisi pada tahun 2005 dan dinomori ulang (tetapi sebaliknya tidak berubah) pada tahun 2007 untuk menyelaraskan dengan ISO/IEC 27000 standar seri lainnya.

ISO/IEC 27002 memberikan rekomendasi praktik terbaik untuk manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab untuk memulai, menerapkan atau mempertahankan sistem manajemen keamanan informasi (ISMS). Keamanan informasi didefinisikan dalam standar dalam konteks pelestarian kerahasiaan (memastikan bahwa informasi dapat diakses hanya untuk mereka yang berwenang untuk memiliki akses), integritas (menjaga akurasi dan kelengkapan informasi dan pengolahan metode) dan ketersediaan (memastikan bahwa pengguna yang berwenang memiliki akses ke informasi dan aset terkait bila diperlukan). Standar ISO27002 berisi bagian utama sebagai berikut:

1. Penilaian risiko
2. Kebijakan keamanan arah manajemen
3. Organisasi keamanan informasi tata kelola keamanan informasi
4. Manajemen aset persediaan dan klasifikasi aset informasi

5. Aspek keamanan untuk karyawan yang bergabung, bergerak dan meninggalkan sebuah organisasi keamanan sumber daya manusia
6. Fisik dan lingkungan keamanan perlindungan fasilitas komputer
7. Komunikasi dan manajemen operasi manajemen kontrol keamanan teknis dalam sistem dan jaringan
8. Akses kontrol pembatasan hak akses ke jaringan, sistem, aplikasi, fungsi dan data
9. Akuisisi sistem informasi, pengembangan dan pemeliharaan membangun keamanan ke dalam aplikasi
10. Manajemen insiden keamanan informasi mengantisipasi dan merespon dengan tepat terhadap pelanggaran keamanan informasi
11. Manajemen kontinuitas bisnis melindungi, memelihara dan memulihkan proses dan sistem bisnis penting
12. Kepatuhan memastikan kesesuaian dengan kebijakan keamanan informasi, standar, hukum dan peraturan

2.3. *Tools*

2.3.1 Aplikasi *Wireshark*

Menurut Kurniawan (2012:15) *wireshark* adalah *tool* yang ditujukan untuk penganalisian paket data jaringan. *Wireshark* melakukan pengawasan paket secara waktu nyata (*real time*) dan kemudian menangkap data dan menampilkannya selengkapnya mungkin. *Wireshark* bisa digunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi *wireshark* dapat berjalan di banyak *platform*, seperti *linux, windows,* dan *mac*.

Ada banyak hal yang dapat kita lakukan dengan *wireshark*. Berikut adalah beberapa contoh skenario yang mungkin menggambarkan kapan kita perlu menggunakan *wireshark*.

1. Melakukan *troubleshoot* permasalahan jaringan
2. Melakukan pengujian masalah keamanan
3. Melakukan *debungging* implementasi *protokol*
4. Belajar *protokol* jaringan

Wireshark ini diibaratkan sebagai media *tool* sehingga pemakaiannya diserahkan kepada penggunanya, apakah untuk kebaikan atau kejahatan. Hal ini karena *wireshark* dapat digunakan untuk mencuri informasi sensitif yang berkeliaran pada jaringan. Contohnya kata sandi, *cookie*, dan sebagainya.

Wireshark dapat dikatakan sebagai *tool* analisis paket data jaringan yang paling sering digunakan. Berikut adalah sebagian fitur pada *wireshark*:

1. Tersedia untuk *flatform* UNIX, *linux, windows,* dan *mac*
2. Dapat melakukan *capture* paket data jaringan secara *real time*
3. Dapat menampilkan informasi *protokol* secara lengkap
4. Paket data dapat disimpan menjadi *file* dan nantinya dapat dibuka kembali
5. Pemfilteran paket data jaringan
6. Pencarian paket data dengan kriteria spesifik
7. Pewarnaan penampilan paket data sehingga mempermudah menganalisisan paket data
8. Menampilkan data statistik

2.3.2 Aplikasi *Ettercap*

Ettercap merupakan salah satu *tools* yang dapat digunakan untuk melakukan *spoofing*. *Ettercap* dapat diinstall pada *operating system windows* maupun *linux*. Pada *linux back track* khususnya *ettercap* sudah terinstall sejak *operating system* terinstall. Disini saya mengunakan *operating system kali linux*. Untuk mendapatkan *password* dan *username* saat melakukan *spoofing*, kita harus memastikan agar paket data yang berupa *username* dan *password* dari target dapat masuk ke komputer, sehingga kita harus melakukan *spoofing* sebelum target memasukan *password* dan *username akunnya*. sehingga ketika sang target sudah masuk kedalam suatu situs yang ingin peneliti *spoofing akunnya* kita harus memutus koneksinya, agar dia melakukan *login* ulang sehingga akunnya kita dapat dalam proses spoofing yang peneliti lakukan. Untuk memutuskan koneksi ini kita dapat melakukannya dengan aplikasi atau *tools* seperti *netcut* pada *windows*, akan tetapi pada *linux* ada yang namanya *tuxcut*. *tuxcut* ini fungsinya seperti *netcut*, dan *tuxcut* mempunyai kelebihan untuk memproteksi dirinya dari *netcut* lainnya.

2.4. Penelitian Terdahulu

Adapun penelitian terdahulu antara lain:

1. Nama Jurnal : Jurnal Internasional dari Penelitian Ilmiah dan Publikasi

Judul Jurnal : Berbagai Solusi Untuk Serangan *Spoofing* Alamat Resolusi *Protokol*

Penulis Jurnal : S. Venkatramulu dan Dr.C.V Guru Rao

Volume Jurnal : 3

Nomor Jurnal : 7

Tahun Jurnal : July 2013

ISSN Jurnal : 2250-3153

Pembahasan :

Komputer yang terhubung ke IP/*Ethernet* LAN memiliki dua alamat, satu adalah MAC (*media access control*) alamat, kedua adalah alamat IP. ARP *spoofing* memungkinkan penyerang untuk mencegat data frame pada LAN, memodifikasi lalu lintas, atau menghentikan lalu lintas sama sekali. Seringkali serangan itu digunakan sebagai pembuka untuk serangan lain, seperti penolakan layanan atau serangan pembajakan. Serangan hanya dapat digunakan pada jaringan yang menggunakan *Address Resolution Protocol* (ARP), dan terbatas pada segmen jaringan lokal. Kartu jaringan, disebut alamat MAC.

ARP beroperasi dengan mengirimkan permintaan ARP paket. Permintaan ARP mengajukan pertanyaan alamat IP *client*, kemudia kirim MAC kembali ke pengirim. Paket ini disiarkan ke semua komputer di LAN, bahkan pada jaringan diaktifkan.

The Address Resolution Protocol (ARP adalah protokol banyak digunakan untuk menyelesaikan alamat lapisan jaringan ke alamat *link* layer. Ketika sebuah *Internet Protocol* (IP) datagram dikirim dari satu *host* ke yang lain pada jaringan *area* lokal, alamat IP tujuan harus diubah menjadi alamat MAC untuk transmisi melalui lapisan data *link*. Ketika alamat IP *host* diketahui, dan alamat MAC yang dibutuhkan, paket *broadcast* yang dikirim pada jaringan lokal. Jaringan *host*

secara otomatis akan *cache* setiap ARP balasan yang mereka terima, bahkan entri ARP yang belum berakhir akan ditimpa ketika ARP baru membalas paket diterima. Tidak ada metode dalam protokol ARP dengan yang *host* dapat mengotentikasi rekan dari mana paket berasal. Perilaku ini adalah kerentanan yang memungkinkan ARP *spoofing* terjadi.

Prinsip dasar di balik ARP *spoofing* adalah untuk mengeksploitasi kerentanan tersebut di atas dalam protokol ARP dengan mengirimkan palsu pesan ARP ke LAN. Serangan *spoofing* ARP dapat dijalankan dari *host* dikompromikan di LAN, atau dari mesin penyerang yang terhubung langsung ke target LAN. Umumnya, tujuan dari serangan ini adalah untuk mengasosiasikan alamat MAC penyerang dengan alamat IP dari *host* target, sehingga lalu lintas dimaksudkan untuk *host* target akan dikirim ke penyerang MAC sebaliknya.

2. Nama Jurnal : Jurnal Internasional Penelitian Inovatif dalam Komputer dan Komunikasi Rekayasa

Judul Jurnal : Deteksi dan Lokalisasi Beberapa Penyerang *Spoofing* Menggunakan Analisis *Cluster* di Jaringan *Wireless*

Penulis Jurnal : Deepak Bilolikar dan Shital Y Gaikwad

Volume Jurnal : 3

Nomor Jurnal : 4

Tahun Jurnal : April 2015

ISSN Jurnal : 2320-9801

Pembahasan :

Sebagai komputasi dan jaringan seni pertunjukan ukuran persegi bergeser dari infrastruktur kabel ke jaringan komunikasi *nirkabel*, *mobile* dan terbuka, untuk meningkatkan kecepatan komputasi jaringan. Namun seperti ukuran persegi hanya rentan untuk beberapa dan gaya serangan *opposer* seperti serangan *spoofing*. Dasarnya identitas berdasarkan sebagian besar *spoofing* serangan atau menyamar serangan persegi mengukur sederhana untuk memulai dan tambahan itu akan menyebabkan cedera penting untuk kinerja jaringan. serangan *spoofing* tambahan memfasilitasi berbagai macam serangan *traffic injection*, seperti serangan pada daftar manajemen akses (ACL), tujuan akses pelayan tanpa (AP) serangan, dan akhirnya *Denial of-Service* (DoS) serangan. Teknik-teknik *cryptographical* yang biasa untuk mengatasi gaya seperti pelanggaran keamanan. Oleh karena itu, perlu untuk

a. Mendeteksi kehadiran *spoofing* serangan
b. Menentukan jumlah penyerang
c. Melokalisasi beberapa lawan pendekatan

Kebanyakan yang ada menggunakan skema kriptografi untuk mengatasi serangan *spoofing* potensial. Namun, penerapan skema kriptografi membutuhkan mekanisme distribusi, manajemen, dan pemeliharaan kunci yang dapat diandalkan. Hal ini tidak selalu diinginkan untuk menerapkan metode kriptografi karena infrastruktur, komputasi, dan *overhead* manajemen. Selanjutnya, metode kriptografi rentan terhadap simpul kompromi, yang merupakan masalah serius karena kebanyakan node *nirkabel* yang mudah diakses, sehingga memori mereka untuk dapat dengan mudah dipindai. Peneltian ini mengusulkan untuk

menggunakan korelasi spasial berbasis RSS, properti fisik yang terkait dengan setiap node *nirkabel* yang sulit untuk memalsukan dan tidak bergantung pada kriptografi sebagai dasar untuk mendeteksi serangan *spoofing*. Sejak perhatian adalah pada penyerang yang memiliki lokasi yang berbeda dari node *nirkabel* yang sah, memanfaatkan informasi spasial untuk mengatasi serangan *spoofing* memiliki kekuatan yang unik untuk tidak hanya mengidentifikasi adanya serangan ini, tetapi juga melokalisasi lawan. Keuntungan tambahan dari menggunakan korelasi spasial untuk mendeteksi serangan *spoofing* adalah bahwa hal itu tidak akan memerlukan biaya tambahan atau modifikasi pada perangkat *nirkabel* sendiri.

3. Nama Jurnal : Jurnal Internasional Dari Elektronika, Listrik dan Teknologi Komputer

Judul Jurnal : Deteksi *Spoofing* Serangan di Jaringan *Nirkabel* Menggunakan *Fuzzy Logic*

Penulis Jurnal : Seyedeh Zahra Rajabi, Seyed Javad Mirabedini Shirazani, dan Ali Haronabadi

Volume Jurnal : 4

Nomor Jurnal : 12

Tahun Jurnal : Juli 2014

ISSN Jurnal : 2305-0543

Pembahasan :

Deteksi serangan *spoofing* identitas adalah salah satu isu yang paling penting dalam keamanan dan *intrusion detection* dalam jaringan *nirkabel*. Di

antara yang paling serangan *spoofing* penting dalam jaringan *nirkabel* interior, seperti 802.11, dapat menunjuk ke MAC *spoofing* alamat dimana penyerang mencoba untuk mengirim paket dan menyerang jaringan melalui MAC alamat *spoofing* bukannya node diperbolehkan dalam jaringan. Ada teknik utama, termasuk *enkripsi* WPA dan WPA2, metode SSDI dan penyaringan alamat MAC mencegah intrusi. Namun, penyerang hanya bisa melewati hambatan keamanan.

Menggunakan berbagai metode *enkripsi*, seperti serangan *spoofing* adalah antara yang paling umum dan metode tradisional untuk pencegahan serangan dalam jaringan *nirkabel*. Tapi mengenkripsi teknik selalu rumit perhitungan dengan *overhead* data dan karenanya menggunakan teknik tidak tepat di semua jaringan. Selain itu, teknik *enkripsi* melindungi *frame* data dan penyerang bisa *spoof frame* administrasi dan kontrol dan menembus jaringan. Menerima kekuatan sinyal (RSS) untuk mendeteksi serangan *spoofing*. RSS adalah salah satu ciri fisik node dan stasiun *nirkabel* yang unik untuk setiap perangkat dan dapat dianggap nilai energi *asreceived* sinyal dari diterima *frame* yang diukur dengan antena diterima. RSS adalah nilai pengukuran yang hampir tidak dapat palsu dan memiliki korelasi dengan lokasi pengirim pesan, karena *nirkabel* perangkat tidak dapat biasanya mengubah kekuatan, perubahan yang kuat dan parah mengirim RSS pengukuran dari alamat MAC mengirimkan *frame* mungkin mengindikasikan serangan *spoofing*.

Teknik dijelaskan dan dirancang sistem *fuzzy* disajikan. Teknik ini menganggap dua kondisi:

a. Jika node RSS adalah tetap dan perbedaan tingkat rendah dengan tidak

banyak perubahan, node adalah tetap dan statis dan kemudian lokasi simpul diperkirakan menggunakan aturan *fuzzy*. Dan serangan terdeteksi, jika kondisi dihitung adalah di luar jangkauan yang diinginkan.

b. Jika tingkat energi yang diterima dari node adalah variabel, node ini dapat dianggap sebagai mencurigakan satu atau energi perubahan adalah karena perubahan lokasi dan mobilitas node. Dengan demikian, kondisi simpul diperkirakan sebagai metode.

c. Jika penyerang dimaksudkan untuk menipu kondisinya, teknik yang disarankan dapat mendeteksi serangan karena dalam setiap interval waktu, lokalisasi dan analisis level sinyal yang diterima terjadi di beberapa titik akses. Jalur akses lain dapat mendeteksi *spoofing* lokasi ini. Sehingga setelah lokalisasi dan status dari setiap node, jalur akses mengirimkan informasi untuk jalur akses yang dipilih sebagai server untuk perbandingan lain terjadi sesuai dengan kondisi dan tingkat sinyal dalam interval waktu semua jalur akses dan tingkat sehingga deteksi meningkat dan tingkat kesalahan berkurang.

4. Nama Jurnal : Jurnal Internasional Dari Ilmu Petahuan dan Teknologi

Judul Jurnal : Simulasi DNS *Spoofing* Serangan untuk Evaluasi Keamanan Model Berbasis

Penulis Jurnal : Golriz Khazan dan Mohammad Abdollahi Azgomi

Pembahasan :

Metode evaluasi ketergantungan evaluasi Ordinal yang mengidentifikasi mengklasifikasikan dan peringkat mode kegagalan atau peristiwa kegagalan komponen kombinasi atau kondisi lingkungan yang akan menyebabkan kegagalan sistem, seperti mode kegagalan, efek dan analisis kritis (FMECA) , kehandalan blok diagram (RBD) dan pohon kesalahan. evaluasi probabilistik yang mengevaluasi dalam hal probabilitas sejauh mana beberapa atribut (tindakan) puas, seperti rantai *Markov*, jaring *Petri stokastik* (dengan solusi analitis atau simulasi). Upaya evaluasi keamanan kuantitatif (QSE) dari sistem biasanya didasarkan pada rantai *Markov*, metode formal dan merah-tim, tapi memperkenalkan dan menggunakan kerangka kerja terpadu untuk pemodelan, simulasi dan QSE merupakan masalah terbuka. *SimEvents* meluas *Simulink* dengan kejadian diskrit model simulasi perhitungan. Dengan *SimEvents*, model berdasarkan aktivitas dari sistem yang dikembangkan untuk mengevaluasi parameter sistem, seperti kemacetan, pertentangan sumber daya dan keterlambatan pemrosesan. Hal ini dimungkinkan untuk mengkonfigurasi entitas dengan atribut yang ditetapkan pengguna dan kemudian entitas agregat dan atribut untuk model hirarki data dan transportasi dalam aplikasi seperti jaringan berbasis paket, perencanaan misi, kontrol pengawasan, sistem operasi *real time* dan arsitektur komputer. Dalam tulisan ini, simulasi *sistem name domain* (DNS) untuk QSE berdasarkan kejadian diskrit simulasi (DES) menggunakan *SimEvents* disajikan. Pertama, sistem dalam keadaan normal dan kemudian kedatangan penyerang adalah simulasi dan ketersediaan sistem, sebagai tindakan keamanan yang penting, di setiap saat waktu simulasi dievaluasi. Akhirnya, sebuah studi

kasus DNS simulasi serangan *spoofing* dilakukan dan ukuran ketersediaan sistem dievaluasi.

5. Nama Jurnal : Jurnal Internasional Dari Ilmu: Dasar dan Riset Terapan(IJSBAR)

Judul Jurnal : Pencegahan Sesi Pembajakan dan IP Spoofing dengan Sensor Nodes dan Kriptografi Pendekatan

Penulis Jurnal : Abhishek Kumar Bharti dan Manoj Chaudhary

Volume Jurnal : 6

Nomor Jurnal : 1

Tahun Jurnal : 2012

ISSN Jurnal : 2307-4531

Pembahasan :

Sesi Pembajakan adalah salah satu serangan yang populer di *man-in-middle* serangan yang memberikan suatu mekanisme untuk mencegah sesi serangan pembajakan. Seorang pengguna yang mencoba untuk *login* atau sudah *login* ke *server*, penyerang mengambil kontrol atas sesi, pada dasarnya membajak sesi dari pengguna dan terus koneksi ke *server* berpura-pura menjadi pengguna. Pembajakan sesi memiliki keuntungan besar untuk para penyerang mereka tidak perlu membuang jam dan jam untuk memecahkan sandi, karena pengguna sudah dikonfirmasi dan dalam sesi aktif itu membuat yang jauh lebih mudah untuk hanya mendengarkan lalu lintas di jaringan tanpa sepengetahuan pengguna. Ada tiga jenis serangan pembajakan sesi:

a. Aktif Sesi Pembajakan

Penyerang akan membungkam salah satu mesin, biasanya komputer klien, dan mengambil alih posisi klien dalam pertukaran komunikasi antara *workstation* dan *server*. Dan drop koneksi antara pengguna dan *server*. Ada berbagai metode untuk menjatuhkan koneksi ke *server*, salah satu yang paling umum adalah untuk mengirim sejumlah besar lalu lintas, dan jenis serangan yang dikenal sebagai *Denial of Service*. Dengan melakukan penyerang ini memiliki kontrol penuh atas sesi dan berkomunikasi dengan server berpura-pura bahwa itu adalah pengguna dikonfirmasi menunjukkan bagaimana pembajakan sesi khas dilakukan antara klien dan *server* oleh penyerang.

b. Pasif Sesi Pembajakan

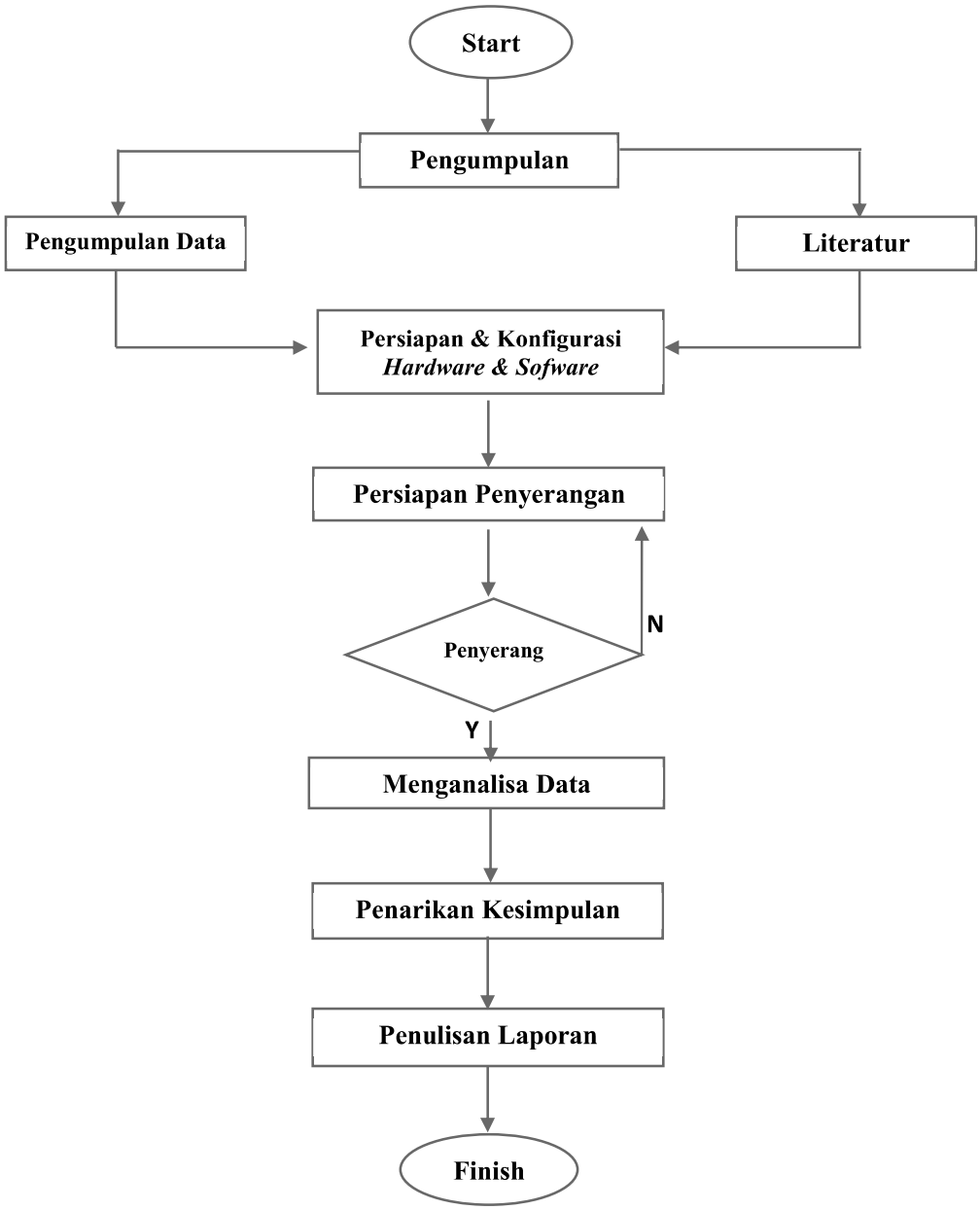
Serangan sesi pembajakan Pasif mirip dengan serangan aktif, tapi daripada menghapus pengguna dari sesi komunikasi, penyerang memonitor lalu lintas antara *workstation* dan *server*. Dalam sesi pasif penyerang mendengarkan semua data dan menangkap mereka untuk serangan di masa depan, dalam kebanyakan kasus untuk melakukan jenis serangan pembajakan adalah penting bahwa penyerang dimulai dengan modus pasif.

c. *Hybrid* Sesi Pembajakan

Serangan ini adalah kombinasi dari serangan aktif dan pasif, yang memungkinkan penyerang untuk mendengarkan lalu lintas jaringan sampai sesuatu yang menarik ditemukan. Penyerang kemudian dapat memodifikasi serangan dengan menghapus komputer *workstation* dari sesi, dan dengan asumsi identitas mereka.

2.5. Kerangka Pemikiran

Kerangka berfikir merupakan kerangka pikir mengenai hubungan antar variabel yang terlibat dalam penelitian atau hubungan antar konsep dengan konsep lainnya dari masalah yang diteliti sesuai apa yang telah diuraikan pada deskripsi teoritis. Konsep dalam hal ini merupakan suatu abstraksi atau gambaran yang dibangun dengan menggeneralisasikan suatu pengertian. Oleh karena itu, konsep tidak dapat diamati dan diukur secara langsung, agar konsep ini dapat diamati dan diukur, maka konsep tersebut harus dijabarkan terlebih dahulu menjadi variabel-variabel (Noor, 2011:251)



Gambar 2.1 Kerangka Berpikir
Sumber: Olahan Peneliti (2016)

Sesuai dengan diagram alir penelitian diatas penelitian ini dilakukan dalam beberapa tahapan:

a. Menyiapkan *literatur*, buku-buku, jurnal, *ebook* dan artikel untuk menunjang penelitian.

b. Mencari informasi data-data yang ada dari lokasi penelitian
c. Menyiapkan *hardware* dan *software* yang dibutuhkkan untuk menunjang pelaksanaan penelitian.
d. Melangkah untuk melakukan sebuah percobaan penyerangan pada *wireless free* di tempat penelitian untuk mendapatkan informasi tentang keamanannya.
e. Menganalisa data-data yang didapatkan dari hasil percobaan penyerangan.
f. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan serangan DNS *spoofing* melihat dari sisi pengguna.
g. Penulisan loporan yaitu tahap akhir dari suatu penelitian dan merupakan hasil akhir yang diwujudkan dalam bentuk karya tulis ilmiah.

2.6. *Hipotesis*

Hipotesis adalah jawaban sementara terhadap rumusan masalah atau sub masalah yang diajukan oleh peneliti, yang dijabarkan dari landasan teori atau kajian teori dan masih harus diuji kebenarannya. Karena sifatnya masih sementara, maka perlu dibuktikan kebenarannya melalui data empirik yang terkumpul atau penelitian ilmiah (Alma, 2008:37). Berdasarkan kerangka berpikir di atas, maka dapat ditarik rumusan atau dugaan sementara yang diambil sebagai hipotesis sebagai berikut:

1. Keamanan jaringan *wireless* dari serangan DNS *Spoofing* pada

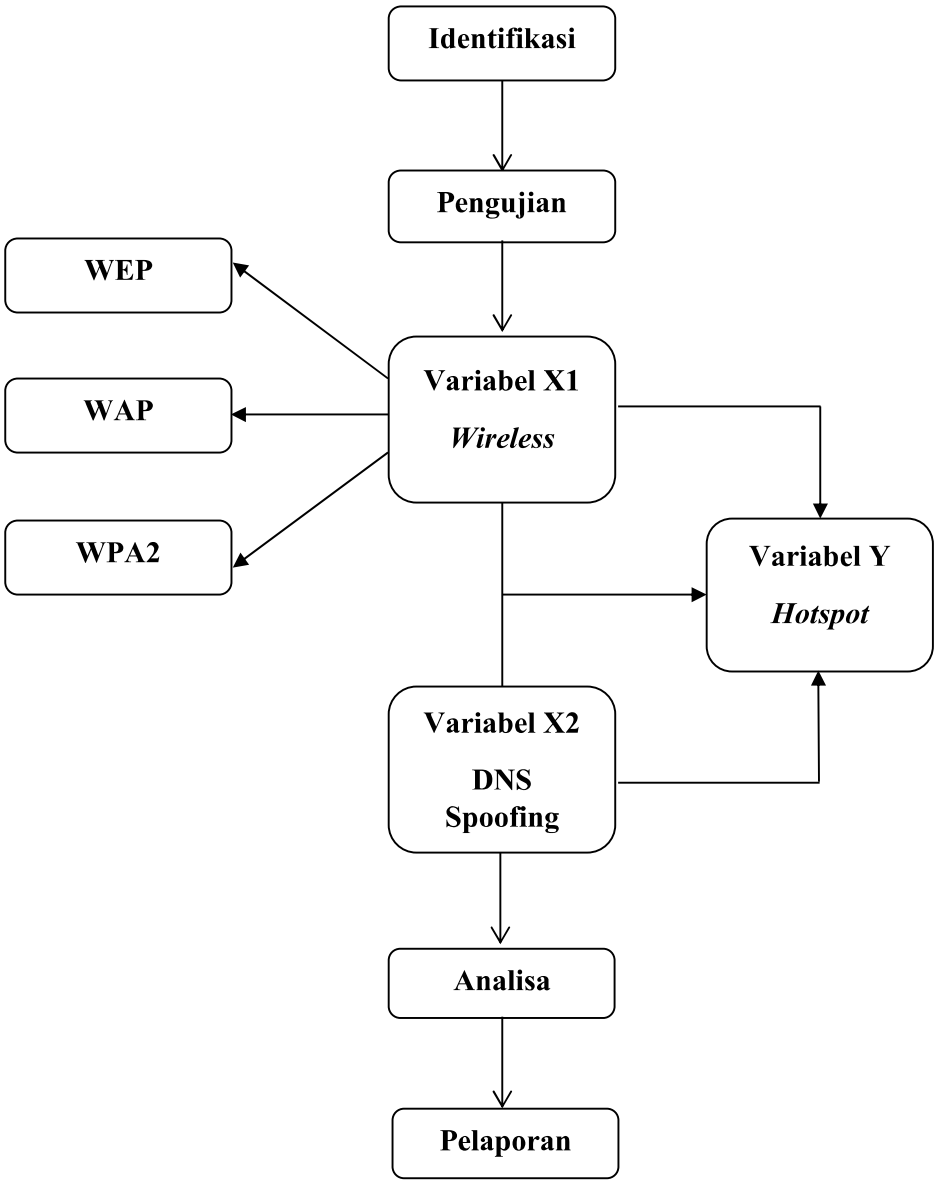
pengguna *free wifi* di Kota Batam dipersepsikan baik.

2. Analisa jaringan *wireless* dari serangan DNS *Spoofing* pada pengguna *free wifi* di Kota Batam dipersepsikan baik.
3. Tindakan pencegahan serangan jaringan *wireless* dari serangan DNS *Spoofing* pada pengguna *free wifi* di Kota Batam dipersepsikan baik.

BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Menurut Noor (2011:108) desain penelitian adalah semua proses yang diperlukan dalam perencanaan dan pelaksanaan penelitian. Dalam hal ini, komponen desain dapat mencakup semua struktur penelitian diawali saat menemukan ide, menentukan tujuan, kemudian merencanakan penelitian (permasalahan, merumuskan, menentukan tujuan penelitian, sumber informasi dan melakukan kajian dari berbagai pustaka, menentukan metode yang digunakan, analisis data dan menguji hipotesis untuk mendapatkan hasil penelitian).



Gambar 3.1 Desain Penelitian
Sumber: Olahan Peneliti (2016)

Tahapan-tahapan yang digunakan dalam proses forensik antara lain:

1. Identifikasi

Identifikasi dilakukan terhadap kebutuhan-kebutuhan, baik kebutuhan fungsional sistem maupun identifikasi kondisi jaringan *wireless*. Pada tahapan

identifikasi ini peneliti berhasil mengidentifikasi kebutuhan alat dan bahan, identifikasi veriabel yang diteliti, jangka waktu penelitian dan tempat penelitian.

2. Pengujian

Mulai dilakukan pengujian terhadap keamanan *wireless*. Peneliti serangan disini hanya dilakukan untuk melihat apakah penyerangan dengan metode DNS *spoofing* dapat lebih aman tanpa melakukan manipulasi terhadap *wireless*, sehingga tidak akan mengganggu kondisi pengguna yang sedang mengakses.

3. Variabel X1 *Wireless*

Pengujian dilakukan terhadap variabel *wireless*. Apakah *wireless* tersebut menggunakan *autintikasi* yaitu WEP, WAP dan WPA2 di dalam jaringan yang diteliti?

4. Variabel X2 DNS *Spoofing*

Pengujian dilakukan terhadap DNS *Spoofing*. Apakah pada jaringan wireless terdapat serangan DNS *Spoofing* atau tidak ada serangan DNS *Spoofing*?

5. Variabel Y *Hotspot*

Lokasi atau tempat untuk mengetes dan menganalisa *wireless* terhadap serangan DNS *Spoofing*.

6. Analisa

Analisa dilakukan dari hasil serangan keamanan DNS *Spoofing*, hal ini berguna untuk menemukan kelemahan-kelemahan *wireless*. Berdasarkan hasil analisa, juga diharapkan dapat diperoleh solusi untuk pengembagan keamanan *wireless*.

7. Pelaporan

Pada tahap pelaporan, mulai dilakukan dokumentasi terhadap hasil penelitian beserta analisisnya.

3.2 Operasional Variabel

Menurut Sugiyono (2014:2) dalam penelitian kuantitatif, biasanya peneliti melakukan pengukuran terhadap keberadaan suatu variabel dengan menggunakan instrumen penelitian. Setelah itu mungkin peneliti melanjutkan analisis untuk mencari hubungan satu variabel dengan variabel lainnya

Variabel merupakan gejala yang menjadi fokus penelitian untuk diamati. Variabel itu sebagai atribut dari sekelompok orang atau obyek yang mempunyai variansi antara satu dengan yang lainnya dalam kelompok itu. Tinggi, berat badan, sikap, motivasi, kepemimpinan, disiplin kerja, warna rambut merupakan atribut dari seseorang. Selanjutnya berat, ukuran, bentuk, dan warna merupakan atribut dari obyek. Atribut ini akan bervariasi bila terjadi pada sekelompok orang atau obyek yang diambil secara random. Bila tinggi badan, motivasi kerja, kemampuan, gaya kepemimpinan dari 30 orang sama, maka semua itu bukanlah variabel. Jadi dikatakan variabel karena ada variansinya.

3.3. Metode Pengumpulan Data

Menurut Sugiyono (2014:224) teknik pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data. Tanpak mengetahui teknik pengumpulan data, maka peneliti tidak akan mendapatkan data yang memenuhi standar data yang ditetapkan.

3.3.1 *Library Research*

Pengumpulan data dilakukan dengan mempelajari bahan-bahan tertulis berupa buku, jurnal, prosiding, surat kabar, browsing melalui internet terhadap masalah yang berkaitan.

3.3.2 Observasi

Menurut Alma (2008:76) observasi yaitu melakukan pengamatan secara langsung ke objek penelitian untuk melihat dari dekat kegiatan yang dilakukan. Apabila objek penelitian bersifat perilaku dan tindakan manusia, fenomena alam (kejadian-kejadian yang ada di alam sekitar), proses kerja dan penggunaan responden kecil.

3.3.3 Penelitian Ekperimen

Menurut Noor (2011:42) Penelitian eksperimen dapat didefinisikan sebagai metode sistematis guna membangun hubungan yang mengandung fenomena sebab akibat. Penelitian eksperimen merupakan metode inti dari model penelitian yang menggunakan pendekatan kuantitatif. Dalam metode eksperimen, meneliti harus melakukan 3 persyaratan yaitu kegiatan mengontrol, memanipulasi, dan observasi. Dalam penelitian eksperimen, peneliti membagi objek atau subjek yang diteliti menjadi 2 kelompok yaitu kelompok *treatment* yang mendapatkan perlakuan dan kelompok kontrol yang tidak mendapatkan perlakuan. Karakteristik penelitian eksperimen yaitu:

1. Memanipulasi/mengubah secara sistematis keadaan tertentu.

2. Mengontrol variabel, yaitu mengendalikan kondisi penelitian ketika berlangsungnya manipulasi
3. Melakukan observasi, yaitu mengukur dan mengamati hasil manipulasi

3.3.4 Tindakan (*Action Research*)

Menurut Alma (2008:52) penelitian tindakan adalah suatu proses yang dilalui oleh seseorang atau perkelompok yang menghendaki perubahan dalam situasi tertentu untuk menguji prosedur yang diperkirakan akan menghasilkan perubahan tersebut dan kemudian, setelah sampai pada tahap kesimpulan yang dapat dipertanggung jawabkan, melaksanakan prosedur tersebut. Tujuan utama penelitian tindakan adalah untuk mengubah situasi, perilaku, organisasi dan termasuk struktur mekanisme kinerja, iklim kerja, sarana & prasarana, dan lingkungan sekitarnya.

Penelitian tindakan merupakan penelitian yang bertujuan untuk mengembangkan metode kerja yang paling efisien, sehingga biaya produksi dapat ditekan pada produktivitas lembaga dapat meningkat. Penelitian melibatkan penelitian dan pengawai untuk mengkaji bersama-sama tentang kelemahan dan dukungan prosedur kerja, metode kerja, dan alat-alat kerja yang digunakan dan selanjutnya mendapatkan metode kerja baru yang dipandang paling efisien lalu diuji cobakan, dievaluasi secara terus menerus dalam pelaksanaannya sehingga sampai ditemukan metode yang paling efisien untuk dilaksanakan.

Ada 5 tahapan dalam melakukan penelitan tindakan (*Action research)*, yaitu:

1. Melakukan diagnosa (*diagnosing*)

Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan, untuk menganalisis DNS *spoofing* pada tahap ini peneliti mengidentifikasi secara langsung *wireless* apakah terjadi DNS *spoofing* atau tidak.

2. Membuat rencana tindakan (*action planning*)

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada, pada tahap ini peneliti membuat sketsa awal dan menentukan isi yang akan ditampilkan nantinya.

3. Melakukan tindakan (*action taking*)

Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Selanjutnya setelah dianalisis sesuai dengan rencana tindakan maka peneliti dapat mengambil suatu hasil penelitian.

4. Melakukan evaluasi (*evaluating*)

Setelah masa implementasi (*action taking*) dianggap cukup kemudian peneliti melaksanakan evaluasi hasil dari implementasi, dalam tahap ini dilihat bagaimana serangan DNS *spoofing* pada *wireless*.

5. Pembelajaran (*learning*)

Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan *review* tahap-pertahap yang telah berakhir kemudian penelitian ini dapat berakhir. Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi organisasi dievaluasi oleh peneliti dan dikomunikasikan.

3.3.5 Dokumentasi

Menurut Alma (2008:77) dokumentasi adalah ditunjukkan untuk memperoleh data langsung dari tempat penelitian, meliputi buku-buku yang relevan, peraturan-peraturan, laporan kegiatan, foto-foto, film dokumenter, data yang relevan penelitian.

3.4 Lokasi dan Jadwal Penelitian

3.4.1 Lokasi Penelitian

Penelitian ini dilakukan di *area* jaringan *wireless* pada *free wifi* di Kota Batam. Lokasi penelitian dilakukan di *free wifi* di taman, fasum, dam *public area, café,* dan mall. Berikut ini tempat penelitiannya:

1. HOC Coffee & Clothing Marina
2. Grand Kopi Botania
3. Coffee Town Mall BCS
4. Taman Internet Sekupang
5. Taman Internet Lubuk Baja
6. Taman Internet Telkom Batu Aji

3.4.2 Jadwal Penelitian

Setiap rancangan penelitian perlu dilengkapi dengan jadwal kegiatan yang akan dilaksanakan. Dalam jadwal berisi kegiatan apa saja yang akan dilakukan, dan berapa lama yang akan dilakukan. Berikut ini adalah jadwal penelitian:

Tabel 3.1 Jadwal Penelitian
Sumber: Olahan Peneliti (2016)

No	Kegiatan	Waktu Penelitian																			
		Oktober 2016				November 2016				Desember 2016				Januari 2017				Februari 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan judul																				
2	Konsultasi dengan dosen pembimbing																				
3	Revisi Judul																				
5	Pengajuan Bab I Pendahuluan																				
6	Pengajuan Bab II Kajian Pustaka																				
7	Pengajuan Bab III Metode Penilitian																				
8	Pengajuan Bab IV Hasil Penelitian dan Pembahasan																				
9	Pengajuan bab V simpulan dan saran																				
10	Penyempurnaan Keseluruhan penelitian																				
11	Pengumpulan soft cover																				