SAINSTECH
INNOVATION JOURNAL

SIJ, Volume 3, Nomor 2, November 2020, Hal. 66-73

Studi Literatur: Cara Kerja Keamanan Internet dan Kerentanan dengan TCP/IP dan DNS

Literature Review: Internet Security Works and Some Basic Vulnerabilities with TCP/IP and DNS

Eliyah Acantha M Sampetoding[1)*], Monica Natalin[2)], Esther Sanda Manapa[3)], Valian Yoga P Ardhana[4)]

[1)] Teknik Informatika / STIK Rajawali Talaud
[2)] Sistem Informasi / STIK Rajawali Talaud
[3)] Transportasi / Universitas Hasanuddin
[4)] Teknologi Informasi / Universitas Qamarul Huda Badaruddin

**Corresponding Author: eacantha@gmail.com, Tel: +6281322483370*

Diterima pada *2 Sep 2020*, **Direvisi pertama pada** *15 Sep 2020*, **Direvisi kedua pada***28 Sep 2020*, **Disetujui pada***22 Okt 2020*, **Diterbitkan daring pada** *20 Nov 2020*

Abstract: *Internet security is a comprehensive term for a very broad issue that includes security for transactions conducted over the Internet. In general, Internet security includes browser security, security of data entered via Web forms, and authentication and overall protection of data sent over the Internet Protocol. On the internet infrastructure that guarantees security is TCP / IP, Interdomain Routing and DNS.*

Keywords: *Internet Security, TCP, IP, Routing, DNS*

Abstrak: *Keamanan Internet adalah istilah menyeluruh untuk masalah yang sangat luas yang meliputi keamanan untuk transaksi yang dilakukan melalui Internet. Secara umum, keamanan Internet meliputi keamanan browser, keamanan data yang dimasukkan melalui formulir Web, dan otentikasi dan perlindungan data secara keseluruhan yang dikirim melalui Protokol Internet. Pada infrastruktur internet yang menjamin keamanan adalah TCP/IP, Interdomain Routing dan DNS.*

Kata kunci: *Keamanan Internet, TCP, IP, Routing, DNS*

1. PENDAHULUAN

Internet untuk saat ini bukan hal yang asing bagi kehidupan sehari-hari dalam berbagai aktivitas seperti lingkungan rumah tangga, kegiatan perekonomian, didunia industri maupun pengelolaan pemerintahan. Namun, sebagai suatu jaringan yang terbuka, internet merupakan jaringan yang rentan akan berbagai ancaman. Berbagai ancaman dalam akses internet seperti identitas palsu pengguna, perubahan konten, dan penyadapan [1]. Seperti yang diketahui, dampak dari ancaman ini akan menimbulkan keengganan para pengguna internet untuk menggunakan internet sebagai media untuk melakukan kegiatan-kegiatan penting yang sebenarnya dapat dilakukan secara prakti [2] .

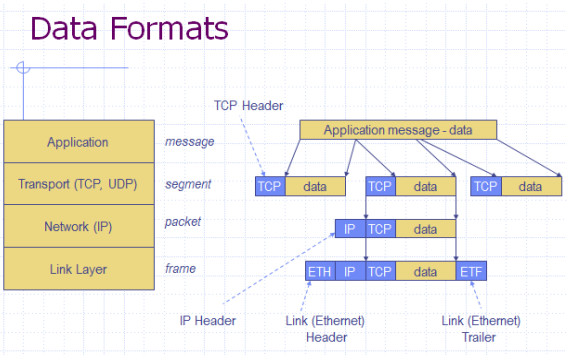
Terdapat banyak solusi dalam menghindari dan mengurangi ancaman-ancaman tersebut diatas, seperti mengembangkan suatu infrastruktur untuk menunjang pengamanan dalam melakukan aktivitas di internet. Infrastruktur ini diharapkan dapat menjamin para pengguna internet dalam mengakses datanya. Ada beberapa isu dalam keamanan internet yakni kerahasiaan (*confidentiality*), otentikasi (*authentication*), keutuhan pesan (*integrity*) dan keadaan tak tersangkal (*non repudiation)* [3].

Internet infrastruktur dibangun oleh perusahaan-perusahaan yang menjual jasa layanan koneksi ke internet. Perusahaan-perusahaan jasa layanan internet tersebut disebut dengan *Internet Service Provider* (ISP). Saluran utama jaringan ISP *dengan* internet disebut dengan *Backbone*. Backbone adalah saluran atau koneksi berkecapatan tinggi yang menjadi lintasan utama dalam sebuah jaringan. Jaringan *Backbone* menghubungkan beberapa jaringan dengan berkecepatan rendah melalui *gateway* [4]. Umumnya ISP menyewa *backbone* dari perusahaan lain, dan menggunakan bersama-sama dengan ISP lain sehingga menghemat biaya perusahaan, namun mengurangi kecepatan akses masing-masing internet. ISP biasanya menggunakan firewall untuk menjaman transaksi online yang dilakukan oleh pengguna.

Dalam internet infrastruktur juga terdapat lokal dan *interdomain routing* yakni TCP/IP untuk routing dan memberikan pesan serta BGP untuk *routing announcements*. Sedangkan untuk alamat nya menggunakan DNS (*Domain Name System*).

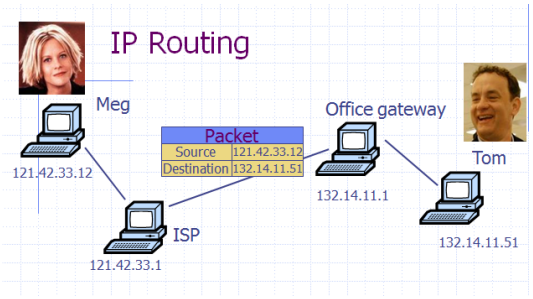
2. TINJAUAN PUSTAKA

TCP/IP (*Transmission Control Protocol / Internet Protocol*) merupakan sebuah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut dengan alamat IP6 (IP *address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP *Stack* [5].



Gambar 1. Layer TCP/IP [2]

TCP/IP mempunyai beberapa layer, yakni Application, Transport, Network (IP) dan Link (Data Link). Penjelasannya adalah sebagai berikut dimulai dari IP (internet protocol) yang berperan dalam pentransmisian paket data dari node ke node. IP mendahului setiap paket data berdasarkan 4 ke alamat tujuan. Internet authorities menciptakan range angka untuk organisasi yang berbeda. Organisasi menciptakan grup dengan nomornya untuk departemen. IP bekerja pada mesin gateaway yang memindahkan data dari departemen ke organisasi kemudian ke region dan kemudian ke seluruh dunia. Penjelasannya ada pada gambar 2.



Gambar 2. IP Routing [2]

Selanjutnya TCP (Transmission transfer protocol) berperan didalam memperbaiki pengiriman data yang benar dari suatu client ke server. Data dapat hilang di tengah-tengah jaringan oleh karena itu TCP dapat mendeteksi error atau data yang hilang dan kemudian melakukan transmisi ulang sampai data diterima dengan benar dan lengkap. Terakhir yakni Sockets yaitu merupakan nama yang diberikan kepada paket yang menyediakan akses ke TCP/IP pada kebanyakan sistem.

Protokol sendiri adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.

DNS (*Domain Name System*) atau biasa disebut sebagai DNS adalah suatu sistem yang memungkinkan nama suatu host pada jaringan komputer atau Internet ditranslasikan menjadi IP address atau sebaliknya, sehingga klien dapat terhubung ke web server atau ke mail server menggunakan domain bukan IP address. Keras [6].

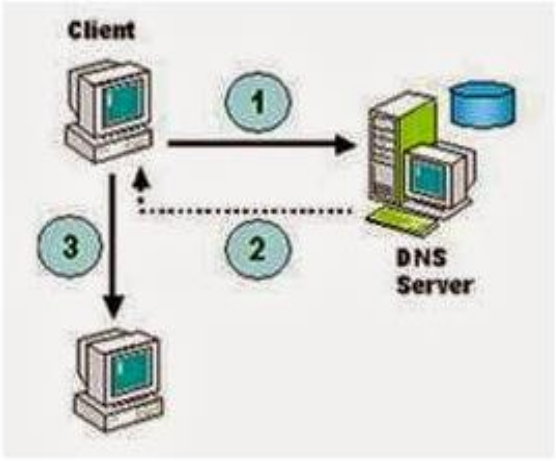
Komponen DNS dibagi ke dalam empat bagian, yakni pertama DNS Server yang merupakan sebuah komputer yang bertugas menjalankan program dari server DNS seperti service DNS server atau BIND dimana BIND menampung database DNS perihal informasi struktur pohon atau pengartian nama dari sebuah permintaan dari DNS *client*.

Kedua yaitu DNS Zone yang merupakan penampung bagian dari buah penamaan untuk server yang berhak atasnya. Contoh sebuah server DNS memiliki otoritas untuk ipb.ac.id atau ipb.edu dan setiap zone dapat disertakan dalam satu atau lebih domain.

Ketiga yaitu DNS *Resolver* yang merupakan sebuah services yang menggunakan protokol DNS untuk meminta informasi dari DNS server. Terakhir yaitu *Resource Record* merupakan arah masuknya database DNS yang digunakan untuk menjawab permintaan klient. Penjabaran dari sebuah

record tipe seperti alamat host (A), alias (CNAME), dan mail exchanger (MX).

Cara Kerja DNS menggunakan relasi client – server untuk resolusi nama. Pada saat klient mencari satu host, maka ia akan mengirimkan query ke server DNS. Query adalah satu permintaan untuk resolusi nama yang dikirimkan ke server DNS. Secara sederhana cara kerja DNS bisa dilihat pada gambar 3.



Gambar 3. Cara Kerja DNS [6]

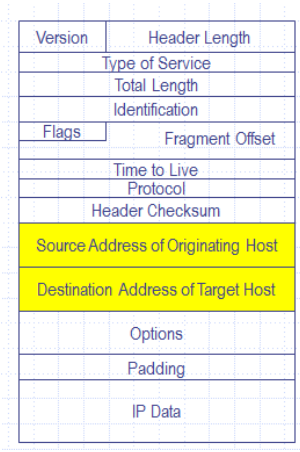
Pertama Pada komputer klient, sebuah program aplikasi misalnya http, meminta pemetaan IP Address (*forward lookup query*). Sebuah program aplikasi pada *host* yang mengakses domain system disebut sebagai *resolver*, *resolver* menghubungi DNS server, yang biasa disebut name server. Berikutnya yakni Name server mengecek ke local database, jika ditemukan, name server mengembalikan IP *Address* ke *resolver* jika tidak ditemukan akan meneruskan query tersebut ke name *server root server*. Terakhir barulah *client* dapat secara langsung menghubungi sebuah *website* / server yang diminta dengan menggunakan IP *Addressyang* diberikan oleh DNS server.

3. BASIC SECURITY

Pada infrastruktur internet, terdapat beberapa Security yang harusdiperhatikan.

3.1 *Internet Protocol* (IP Layer)

Pada IP layer, implementasi fitur keamanan (security) sangat kompleks karena banyak piranti yang terlibat. Security pada level ini menggunakan IP Security (IPSec). IPSec adalah sekumpulan protokol yang didesain oleh IETF (*Internet Engineering Task Force*) untuk menyediakan keamanan pada paket-paket data yang dikirim via Internet. IPSec tidak mendefinisikan metode enkripsi atau otentifikasi tertentu, melainkan menyedikan framework dan mekanisme security. Sedangkan user yang memilih metode enkripsi/otentifikasinya. Dapat dilihat pada gambar 4.



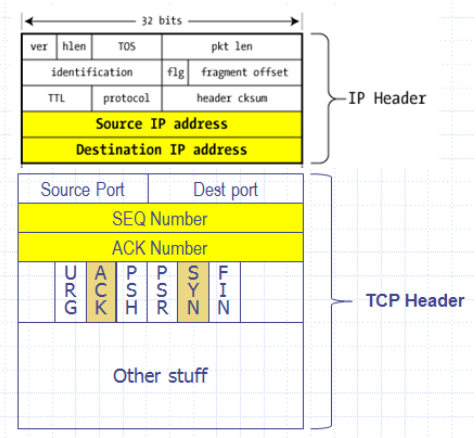
Gambar 4. Internet Protocol [1]

3.2 *Transmission Control Protocol* (TCP)

TCP/IP merupakan protokol yang paling banyak digunakan dan standar untuk komunikasi di Internet karena memiliki banyak kelebihan. Arsitektur TCP/IP bersifat terbuka sehingga siapapun dapat mengembangkannya. TCP/IP tidak tergantung kepada suatu sistem operasi maupun hardware. TCP/IP saat ini diterapkan di semua sistem operasi dan dapat berjalan di semua hardware jaringan.

TCP/IP merupakan protokol yang memiliki fasilitas routing sehingga dapat digunakan pada internetworking. TCP/IP juga merupakan protokol yang handal karena memiliki sistem pengontrol data agar data yang sampai di tempat tujuan benar-benar dalam keadaan baik. Karena kelebihannya tersebut, sangat banyak layanan dan aplikasi yang menggunakan TCP/IP, contohnya yang paling banyak digunakan adalah web. Saat ini terdapat dua versi TCP/IP, yaitu IPv4 (32 bit) dan IPv6 (128 bit). Sistem IPv4 menghasilkan 232 atau 42.949.67.296 namun sudah terpakai lebih dari 85% sehingga dalam waktu yang tidak lama lagi akan diganti dengan IPv6 yang dapat menciptakan lebih banyak alamat. Dapat dilihat pada Gambar 5.

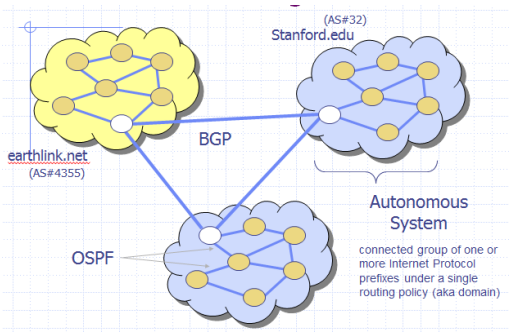
3.3 Routing Security



Gambar 4. Internet Protocol [1]

Routing pada prinsipnya adalah menemukan jalur terpendek ke tujuan. *Routing* berjalan pada lapisan internet atau berhubungan dengan IP. Suatu router akan mengecek apakah IP tujuan dari datagram yang diterima adalah IP-nya walaupun nomor *hardware* tujuan pada paket adalah nomor hardwarenya, jika bukan, router tersebut akan meneruskan (*forward*) ke *host* tujuan atau ke *router* lain. Ada dua kategori *routing*, yaitu *routing* statik dan *routing* dinamis. Pada kategori statik, informasi *routing* bersifat tetap sedangkan pada kategori dinamik, informasi didapatkan dari router lain dan dapat berubah-ubah sesuai kondisi jaringan. Pada *Routing Security* ada 3 *Interdomain Routing* yakni ARP, OSPF dan BGP.

Informasi pada routing dinamis saling disebarkan oleh setiap router ke router-router tetangganya [7]. Untuk menjalankan routing dinamis digunakan protokol routing yang terbagi atas dua jenis, yaitu interior dan eksterior. Yang digolongkan sebagai interior adalah protokol RIP (*Routing Information Protokol*) dan OSPF (*Open Shortest Path*), sedangkan BGP (*Border Gateway Protocol*) digolongkan sebagai tipe eksterior. Perbedaan antara tipe interior dan eksterior adalah tipe eksterior dirancang untuk bekerja antar autonomous system, sedangkan tipe interior untuk jaringan di dalam suatu autonomous system. Autonomous system adalah jaringan yang berada dalam satu administrasi.



Gambar 5. Interdomain Routing [1]

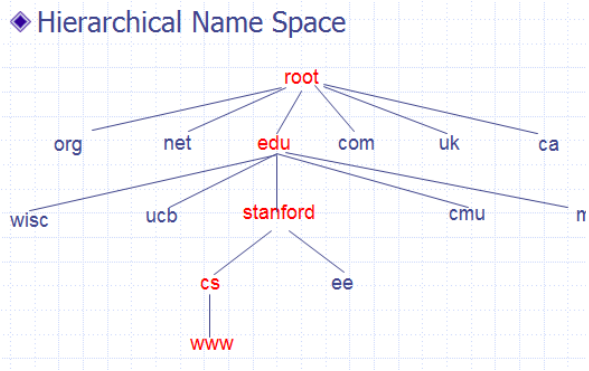
1) ARP (Address Resolution Protocol) adalah sebuah protocol dalam TCP/IP yang bertanggung jawab melakukan resolusi alamat ke dalam alamat *Media Access Control* (MAC *Address*). Isu keamanan disini adalah pada memaksimalkan trafik seperti penggunaan pada Wifi.

2) OSPF (Open Shortest Path First) Informasi pada router disebut dengan LSA (*Link State Advertisement*) yang memberikan data terhadap router kemudian menyusun diagram pohon yang menunjukkan hubungan antar router kemudian menentukan jalur terpendek untuk mencapai suatu host (*shortest path first*), dengan menggunakan LSA ini *routing loop* dapat dihindari. bisa menjalankan routing dengan sistem area dan backbone. Setiap area dibatasi oleh router backbone dan router-router backbone harus saling berhubungan. Router-router di dalam area hanya menjalankan routing untuk internal areanya dan tidak mengetahui struktur area yang lain. Sisemnya adalah jaringan internal suatu organisasi atau perusahaan.

3) *BGP* (*Border Gateway Protocol*) merupakan salah satu jenis routing protocol yang ada di dunia komunikasi data. Sebagai sebuah routing protocol, BGP memiliki kemampuan melakukan pengumpulan rute, pertukaran rute dan menentukan rute terbaik menuju ke sebuah lokasi dalam jaringan. Routing protocol juga pasti dilengkapi dengan algoritma yang pintar dalam mencari jalan terbaik. Isu keamanan disini adalah mengenai trafik palsu yang terdapat pada jaringan, karena jaringannya sangat luas. Akses jaringan juga tidak melakukan autenfikasi karena jenis dalam akses jaringannya adalah eksterior (diluar).

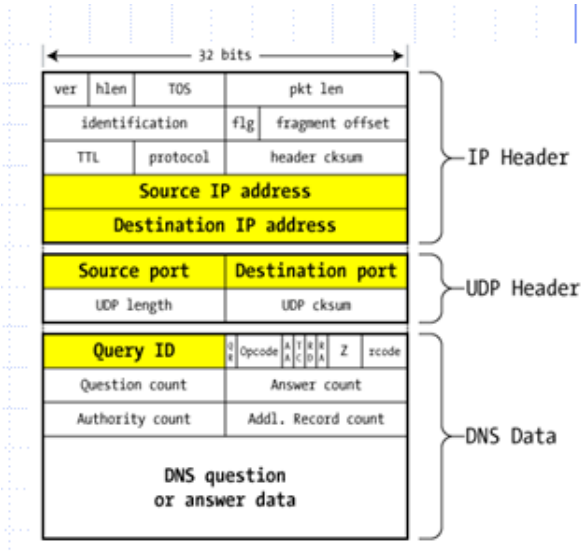
3.4 Domain Name System

DNS adalah cara untuk mempermudah akses terhadap suatu komputer di jaringan global [7]. Dengan berkembangnya World Wild Web, semakin banyak orang yang mengakses host-host di internet dan bertambah juga jumlah host di Internet. Dalam DNS dikenal adanya Top Level Domain (TLD). Contoh TLD adalah com (commercial), edu (pendidikan), dan mil (militer) sehingga terdapat domain, misalnya apple.com, ibm.com, dan mit.edu. TLD seperti di atas berdasarkan jenis organisasi.



Gambar 6. Hirarki pada DNS [1]

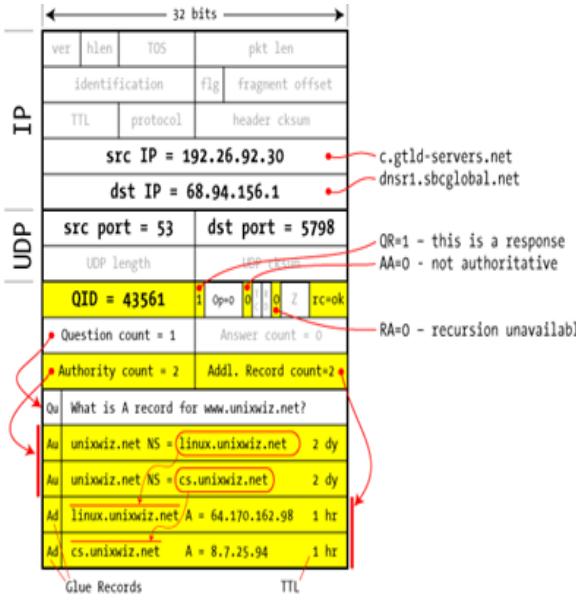
DNS server atau biasa disebut name server yang menyimpan kaitan antara suatu IP dengan nama-nama host. Selain berdasarkan kata-kata, ada juga sistem domain berdasarkan IP yang disebut reverse domain dan mempunyai top level domain "in-addr.arpa", misalnya IP 156.132.5.x tergabung di domain 5.132.156.in-addr.arpa. "itb.ac.id", "ee.itb.ac.id", "id", dan www.microsoft.com dapat menjadi nama host maupun domain atau biasa disebut zona. Setiap zona harus memiliki setidaknya satu DNS server.



Gambar 7. Data pada DNS [1]

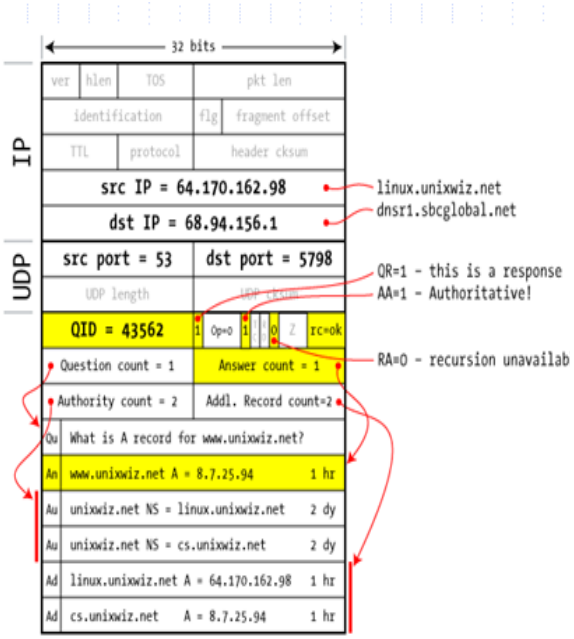
Terdapat dua kategori DNS server, yaitu primary server dan secondary server. Secondary server membentuk zona refresh dengan primary server dan hanya menyalin konfigurasi DNS dari primary server setiap selang waktu tertentu sebagai cadangan jika primary server mengalami gangguan.

Beberapa set konfigurasi yang diperlukan oleh sebuah name server adalah file boot script, file zona termasuk untuk reverse domain, dan file cache untuk server *cache-only*.



Gambar 8. Set Konfigurasi pada DNS [1]

F*ile cache* adalah rujukan menuju *root server global* yang menangani domain level atas dan digunakan untuk mengetahui host di luar domain lokal. *File cache* disediakan oleh Internic. Bagian terpenting pada konfigurasi DNS adalah konfigurasi file zona. Dalam file ini, dicatat kaitan antara alamat IP dengan nama-nama host serta kedudukan hot-host tersebut.seperti gambar (*Resolver* selanjutnya *Authoritative response to resolver*).



Gambar 8. *File cache* pada DNS [1]

Ada 4 jenis keamanan pada DNS yaitu (1) *Administrative security* : Bagian ini menggunakan file permission, konfigurasi server, BIND konfigurasi, dan DMZ. Semua itu adalah teknik yang relative simple dan bias di aplikasikan pada DNS server yang berdiri sendiri; (2) Zona transfer : Zona transfer bekerja menggunakan physical security, parameter pada BIND, atau eksternal *firewall*. Autentifikasi secara aman dari sumber dan tujuan dari zona transfer dapat atau tidak dapat di usahakan (3) Dynamic update : *Dynamic update*; (4) Zona integritas : Hal – hal yang diperlukan zona data yang digunakan oleh salah satu DNS yang lain.

Klasifikasi Keamanan merupakan sarana untuk memungkinkan pemilihan solusi yang tepat dan strategi untuk menghindari resiko berikut klasifikasinya yakni Ancaman Lokal, Server – Server, Server – Klien, dan Klien – Klien.

4. KESIMPULAN

TCP/IP adalah sekelompok protokol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu komputer ke komputer lainnya yang akan memastikan pengiriman data sampai ke alamat yang dituju. Sedangkan DNS adalah pencarian host name terhadap IP address di Internet. Pada DNS client (*resolver*) mengirimkan queries ke Name Server (DNS). Namer server ini akan menerima permintaan dan memetakan nama komputer ke IP address. DNS adalah pengelompokan secara hirarki yang terbagi atas *root-level domains*, *top-levels domains*, *second-level domains*, dan *host names*.

Kerentanan keamanan internet ada beberapa yakni kelemahan konfigurasi, akun pengguna tidak aman, akun sistem mudah menebak password, layanan internet yang salah dikonfigurasi, dan peralatan jaringan yang salah dikonfigurasi. Cara mengatasinya adalah mengeksploitasi celah, menambahkan otentikasi yang lebih, dan melakukan kontrol logikal akses pada setiap jaringan internet.

DAFTAR PUSTAKA

[1] B. Rahardjo, Keamanan Sistem Informasis Berbasis Internet, Bandung: PT INDOCISC, 2005.

[2] D. Boneh, "Internet Security: How the Internet works and some basic vulnerabilities," Spring, 2012.

[3] A. X. Liu, J. M. Kovacs, C.-T. Huang and M. G. Gouda, "A secure cookie protocol," in *14th International Conference on Computer Communications and Networks*, San Diego, 2005.

[4] M. Kende, "The Digital Handshake: Connecting Internet Backbones," CommLaw Conspectus. HEINONLINE, New York, 2003.

[5] W. Sugeng and T. D. Putri, Jaringan Komputer Dengan TCP/IP, Bandung: Modula, 2010.

[6] A. Sukmaaji, Rianto and T. A. Prabawati, Jaringan Komputer: Konsep dasar pengembangan jaringan dan keamanan jaringan, Andi: Yogyakarta, 2008.

[7] V. Y. P. Ardhana, E. S. Manapa, T. W. Sagala, Y. A. Siahaan and E. A. M. Sampetoding, "Evaluasi Kinerja Protokol Perutean AODV dan SDGR+R pada VANET dengan Studi Kasus Pelabuhan Lembar," *JTIM : Jurnal Teknologi Informasi Dan Multimedia,* vol. 2, no. 1, pp. 59-67, 2020.

[8] D. Ardiantoro, "Pengantar DNS (Domain Name System)," IlmuKomputer.com, 2003.