

BAB II

TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Rujukan penelitian yang pertama yaitu dari jurnal Yao Tong, dan Shigeo Akashi dari *Department of Information Sciences Faculty of Science and Technology, Tokyo University of Science Noda City Chiba prefecture Japan* pada tahun 2019 dengan judul *A Feasible Method for Realizing Leakage of DHCP Transactions under the Implementation of DHCP Snooping*. Dalam penelitiannya mereka pengaruh dhcp snooping dalam transmisi data dalam sebuah jaringan.

Rujukan penelitian yang kedua yaitu dari jurnal Vladimir Brik, Jesse Stroik, dan Suman Banerjee dari *Department of Computer Sciences, University of Wisconsin-Madison, WI 53706, USA* pada tahun 2016 dengan judul . Dalam penelitiannya mereka membahas seberapa banyak bug yang terjadi di dalam kinerja DHCP dalam suatu jaringan.

2.2. Personal Komputer

Personal Komputer adalah sebuah mesin hitung elektronik yang secara cepat menerima informasi masukan digital dan mengolah informasi tersebut menurut seperangkat instruksi yang tersimpan dalam komputer tersebut dan menghasilkan keluaran informasi yang dihasilkan setelah diolah. (Ikhsan dan Kurniawan, 2015)



Gambar 2.1 Personal Komputer
(Sumber : www.malvinredtrebol.com)

2.3. Router

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh lapis *OSI*, *router* memiliki fasilitas *DHCP* (Dynamic Host Configuration Protocol), dengan mensetting *DHCP*, maka kita dapat membagi *IP address*, fasilitas lain dari *Router* adalah adanya NAT (Network Address Translator) yang dapat memungkinkan suatu *IP address* atau koneksi internet disharing ke *IP address* lain.

Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan internetwork, atau untuk membagi sebuah jaringan besar ke dalam beberapa *subnetwork* untuk meningkatkan kinerja dan juga mempermudah manajemennya. *Router* juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda (seperti halnya *router wireless* yang pada umumnya selain ia dapat menghubungkan komputer dengan menggunakan radio, ia juga mendukung penghubungan komputer dengan kabel *UTP*), atau berbeda arsitektur jaringan, seperti halnya dari *Ethernet* ke Token Ring. (Zaeni Miftah, 2018)



Gambar 2.2 Router
(Sumber : Zaeni Miftah, 2018)

2.4. Switch

Switch merupakan perangkat yang berfungsi untuk menghubungkan beberapa komputer ataupun perangkat jaringan agar dapat berbagi sumber daya. *Switch* juga merupakan perangkat keras yang memungkinkan terjadinya distribusi paket data antar komputer dalam jaringan dan mampu untuk mengenali topologi jaringan dibanyak *layer* sehingga data dapat langsung sampai ketujuan (Zaeni Miftah, 2018).



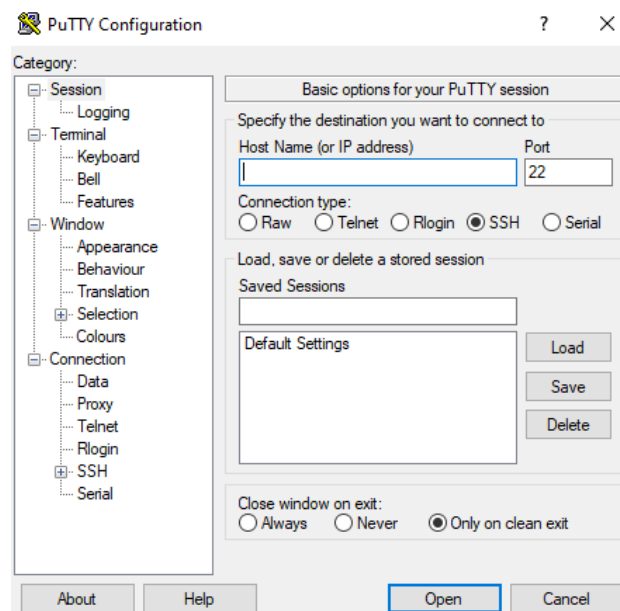
Gambar 2.3 Switch
(Sumber : Zaeni Miftah, 2018)

2.5. Kabel

Kabel mempunyai kemampuan dan spesifikasi yang berbeda. Jenis kabel yang menjadi standar dalam penggunaan untuk komunikasi data dalam jaringan komputer adalah kabel *Twisted Pair*. *Ethernet* juga dapat menggunakan jenis kabel *UTP (Unshielded Twisted Pair)*. Kabel *UTP* yang umum dipakai adalah kabel yang terdiri dari 4 pasang kabel terpilin. Terdapat tipe penyambung kabel jenis *UTP*, yaitu *straight trough cable*, *crossover cable* ditambah satu jenis pemasangan khusus untuk cisco *router*, yaitu *roll over cable*. Perbedaannya, *straight cable* dipakai untuk menghubungkan untuk beberapa unit komputer melalui perantara konsentrator (*hub/switch*) maupun *repeater*, sedangkan *crossover cable* digunakan untuk media komunikasi antar computer (tanpa *hub/switch*) atau dalam kasus tertentu berguna untuk menghubungkan *hub* ke *hub*. (Muzawi, 2018)

2.6. Putty

Putty adalah sebuah program open source yang dapat Anda gunakan untuk melakukan protokol jaringan *SSH*, *Telnet* dan *Rlogin*. Aplikasi ini merupakan aplikasi portable sehingga tidak perlu di install. Protokol ini dapat digunakan untuk menjalankan sesi remote pada sebuah komputer melalui sebuah jaringan, baik itu *LAN*, maupun internet. Program ini banyak digunakan oleh para pengguna komputer tingkat menengah ke atas, yang biasanya digunakan untuk menyambungkan, mensimulasi, atau mencoba berbagai hal yang terkait dengan jaringan. Program ini juga dapat Anda gunakan sebagai tunnel di suatu jaringan. (Dirgantara, 2019)

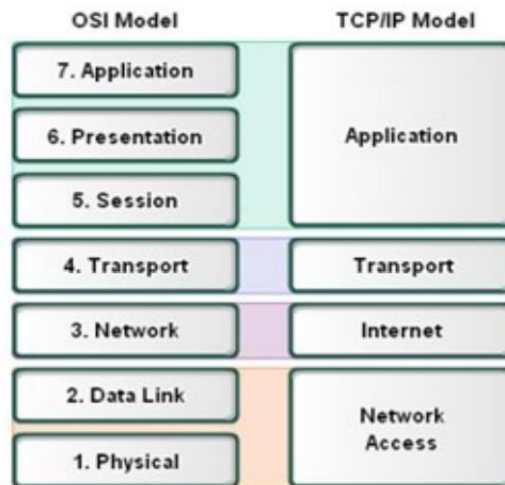


Gambar 2.4 Tampilan Putty
(Sumber : Dhimas Dirgantara, 2019)

2.7. TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukarmenukar data dari satu komputer ke komputer lain di dalam suatu jaringan. Prinsip pembagian lapisan pada *TCP/IP* menjadi protokol komunikasi data yang fleksibel dan dapat diterapkan dengan mudah di setiap jenis komputer dan antar-muka jaringan. Oleh karena sebagian besar isi kumpulan protokol ini tidak

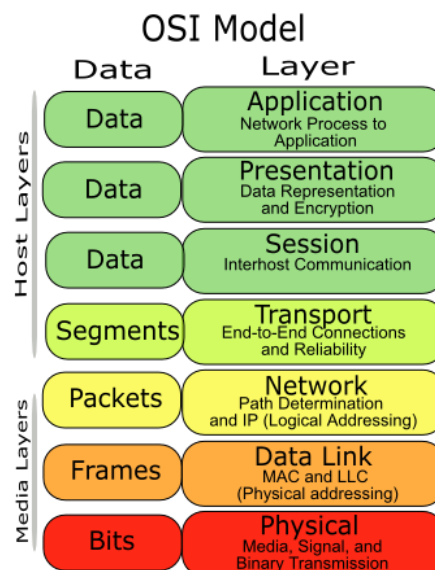
spesifik terhadap satu komputer atau peralatan jaringan tertentu. Gambar 2.4 menunjukkan perbandingan model OSI dan *TCP/IP*. (Siswo Wardoyo dkk, 2015)



Gambar 2.5 Perbandingan Model OSI dan *TCP/IP*
(Sumber: Siswo Wardoyo dkk, 2015)

2.8. OSI Layer

OSI *Layer* merupakan model referensi yang digunakan untuk memahami jaringan komputer secara umum. OSI *layer* telah dijadikan sebagai acuan saat mempelajari network yang dibangun menggunakan perangkat Cisco. OSI Reference Model atau model referensi OSI terdiri atas lapisan berjumlah 7 buah (*layer*), (Dwi Fitri Brianna dkk, 2016)



Gambar 2.6 OSI layer
(Sumber: Dwi Fitri Brianna dkk, 2016)

2.9. Data Link Layer

Data *Link Layer* merupakan lapisan kedua dari standard OSI. Tugas utama data link *layer* adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan ke *network layer*, data link *layer* melaksanakan tugas ini dengan memungkinkan pengirim memecah-mecah data input menjadi sejumlah data frame (biasanya berjumlah ratusan atau ribuan byte). Kemudian data link *layer* mentransmisikan frame tersebut secara berurutan dan memproses acknowledgement frame yang dikim kembali oleh penerima. Karena *physical layer* menerima dan mengirim aliran bit tanpa mengindahkan arti atau arsitektur frame, maka tergantung pada data link *layer*-lah untuk membuat dan mengenali batas-batas frame itu. (Vladimir Brik, 2016)

2.10. IP address (*Internet Protocol Address*)

IP address adalah metode pengalamatan pada jaringan komputer dengan memberikan sederet angka pada komputer (*host*), router atau peralatan jaringan lainnya. *IP address* sebenarnya bukan diberikan kepada komputer (*host*) atau router, melainkan pada interface jaringan dari *host* / router tersebut. IP (*Internet protocol*) sendiri di desain untuk interkoneksi sistem komunikasi komputer pada jaringan paket switched. Pada jaringan *TCP/IP*, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada *transfer* data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat *transfer* data, namun untuk komunikasi datanya, IP mengimplementasikan dua fungsi dasar yaitu addressing dan fragmentasi. (Siswo Wardoyo dkk, 2015)

2.10.1 IPv4

IPv4 adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan *TCP/IP* yang menggunakan protokol IP versi 4. Panjangnya adalah 32-bit, dan secara teoritis dapat mengalami hingga 4 miliar *host* komputer di seluruh dunia. Alamat IPv4 umumnya ditulis dalam notasi desimal bertitik (*dotted-desimal notation*), yang dibagi ke dalam empat buah oktet berukuran 8-bit. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255. Pengalamatan IPv4 menggunakan 32 bit yang setiap bit dipisahkan dengan notasi titik. Contoh notasi pengalamatan IPv4: FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF Nilai F dirubah menjadi nilai biner (1 dan 0) 11000000.10101000.00000010.00000001. Sehingga jika dirubah dalam desimal menjadi 192.168.2.1. (Siswo Wardoyo dkk, 2015)

2.11. Jenis Serangan

2.11.1 Sniffer

Sniffer adalah sebuah *device* penyadapan komunikasi jaringan komputer dengan memanfaatkan mode promiscuous pada *ethernet*. Karena jaringan komunikasi terdiri dari biner acak maka *sniffer* ini biasanya memiliki penganalisis protokol sehingga data biner acak dapat dipecahkan. Fungsi *sniffer* bagi pengelola bisa untuk pemeliharaan jaringan, bagi orang luar bisa untuk masuk ke dalam sistem. (Vladimir Brik, 2016)

2.11.2 Spoofing

Spoofing (penyamaran) biasanya dilakukan oleh pihak yang tidak bertanggung jawab untuk menggunakan fasilitas dan *resource* sistem. *Spoofing* adalah teknik melakukan penyamaran sehingga terdeteksi sebagai identitas yang bukan sebenarnya. (Vladimir Brik, 2016)

2.12 DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) merupakan salah satu protokol standar pada jaringan komputer yang berfungsi untuk membantu pengguna jaringan komputer memperoleh alamat (*IP address*) secara cepat dan otomatis. Dengan pengalamatan yang otomatis ini, maka pengguna jaringan komputer yang tidak memiliki seluk beluk pemahaman tentang pengalamatan jaringan (*IP address, subnetting, blok alamat IP, kelas IP address*) akan terbantu (Pratama, 2014:154). (Dwi Fitri Brianna dkk, 2016)

2.13 DHCP Snooping

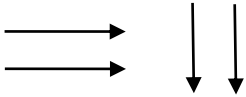
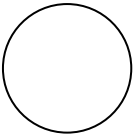
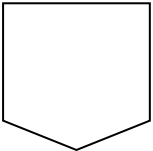

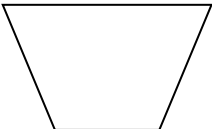
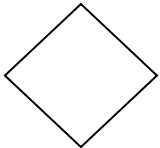
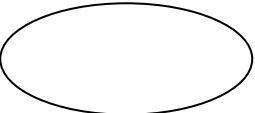
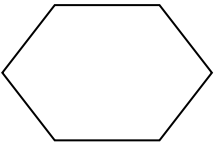
Dalam jaringan komputer, *DHCP snooping* adalah serangkaian teknik yang diterapkan untuk meningkatkan keamanan jaringan *DHCP*. Ketika server *DHCP* mengalokasikan alamat *IP* untuk klien di *LAN*, *DHCP snooping* dapat dikonfigurasi pada *switch LAN* untuk mengizinkan hanya klien dengan *IP* tertentu dan alamat *MAC* untuk memiliki akses ke jaringan. Dengan *DHCP snooping*, informasi tentang alamat *IP* dan sesuai alamat *MAC* disimpan dalam *database* pada *switch*. *DHCP snooping* dapat digunakan untuk fitur keamanan lain seperti penjaga sumber *IP* dan *ARP* dinamis, yang membuatnya menjadi komponen utama dari keamanan akses *LAN*. *DHCP snooping* juga dapat mencegah penyerang menambahkan server *DHCP* ke jaringan, menyebabkan kerusakan jaringan dan menambahkan komponen tidak sah. (Dwi Fitri Brianna dkk, 2016)


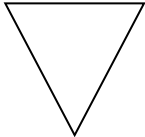
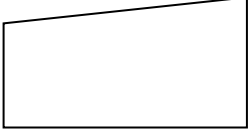

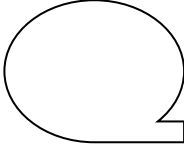
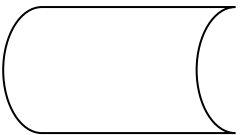


2.14 Definisi Flowchart atau Diagram Alir

Flowchart atau diagram alir merupakan representasi grafik dari langkah-langkah yang harus diikuti dalam menyelesaikan suatu permasalahan yang terdiri dari sekumpulan symbol, dimana masing-masing symbol mempresentasikan suatu kegiatan tertentu. *Flowchart* diawali dengan menerima *input*, pemrosesan *input*, dan diakhiri dengan menampilkan *oUTPut*.

Dalam penulisan *Flowchart* dikenal dua model, yaitu *system flowchart* dan *program flowchart*. *System Flowchart* adalah bagan yang memperlihatkan urutan prosedur dan proses dari beberapa *file* di dalam media tertentu, sedangkan *program flowchart* adalah bagan yang memperlihatkan urutan dan hubungan proses dalam suatu program (Sdarsono, 2017).

Tabel 2.1 Simbol-Simbol *Flowchart*

NO	SIMBOL	KETERANGAN
1		Simbol arus/ <i>flow</i> , berfungsi untuk menyatakan jalannya arus suatu proses
2		Simbol <i>connector</i> , berfungsi untuk menyatakan sambungan dari proses ke proses lainnya dalam halaman yang sama
3		Simbol <i>offline connector</i> , berfungsi untuk menyatakan sambungan dari proses ke proses lainnya dalam halaman yang berbeda
4		Simbol <i>process</i> , berfungsi untuk menyatakan suatu tindakan (proses) yang dilakukan oleh komputer
5		Simbol <i>manual</i> , berfungsi untuk menyatakan suatu tindakan (proses) yang tidak dilakukan oleh komputer
6		Simbol <i>decision</i> , berfungsi untuk menunjukkan suatu kondisi tertentu yang akan menghasilkan dua kemungkinan jawaban : ya/tidak
7		Simbol <i>terminal</i> , berfungsi untuk menyatakan permulaan atau akhir suatu program
8		Simbol <i>predefined process</i> , berfungsi untuk menyatakan penyediaan tempat penyimpanan suatu pengolahan untuk memberi harga awal

9		Simbol <i>keying operation</i> , berfungsi untuk menyatakan segala jenis operasi yang diproses dengan menggunakan suatu mesin yang mempunyai <i>keyboard</i>
10		Simbol <i>offline-storage</i> , berfungsi untuk menunjukkan bahwa data dalam simbol ini akan disimpan ke suatu media tertentu
11		Simbol manual input, berfungsi untuk memasukkan data secara manual dengan menggunakan online <i>keyboard</i>
12		Simbol <i>input/output</i> , berfungsi untuk menyatakan proses input atau <i>output</i> tanpa tergantung jenis peralatannya
13		Simbol <i>magnetic tape</i> , berfungsi untuk menyatakan input berasal dari pita magnetis atau <i>output</i> disimpan ke pita magnetis
14		Simbol <i>disk storage</i> , berfungsi untuk menyatakan <i>input</i> berasal dari <i>disk</i> atau <i>output</i> disimpan ke <i>disk</i>
15		Simbol <i>document</i> , berfungsi untuk mencetak keluaran dalam bentuk dokumen (melalui printer)
16		Simbol <i>punched card</i> , berfungsi untuk menyatakan <i>input</i> berasal dari kartu atau <i>output</i> ditulis ke kartu

(Sumber: Sdarsono, 2017)