

# Analisis Keamanan Jaringan LAN berdasarkan Log Data CCR (*Cloud Core Router*) pada Laboratorium SMK Telkom Jakarta

Nur Hafifah<sup>1</sup>, Ade Nurhayati<sup>2</sup>

<sup>1,2</sup>Akademi Teknik Telekomunikasi Sandhy Putra Jakarta

<sup>1,2</sup>Jalan Daan Mogot KM 11, RT. 1/RW.4,Cengkareng, Daerah Khusus Ibukota Jakarta 11710, Indonesia

adenurhayati@akademitelkom.ac.id

---

**Abstrak** – D Semakin besar suatu jaringan maka manajemen jaringan menjadi lebih kompleks dan rumit. Oleh karena itu perlu adanya manajemen jaringan yang tepat. Melihat perkembangan Jaringan LAN (Local Area Network) sebagai salah satu teknologi jaringan komputer, maka sudah seharusnya SMK Telkom Jakarta menerapkan keamanan jaringan untuk memperlancar proses pengiriman data secara aman dan tepat sasaran dengan memanfaatkan sumber daya yang telah tersedia sehingga dapat bekerja sama semaksimal mungkin. Untuk dapat mengetahui kelemahan dan kelebihan dari penerapan keamanan jaringan komputer yang ada dan bisa ditingkatkan kemampuannya untuk keperluan yang lebih luas lagi, serta dapat meminimalkan masalah yang akan terjadi di kemudian hari sehingga dapat segera diperbaiki. Serta untuk membantu meningkatkan performansi keamanan jaringan Local Area Network (LAN) di SMK Telkom Jakarta. Pada penelitian proyek akhir di Laboratorium SMK Telkom Jakarta dengan melakukan Analisis Keamanan Jaringan Local Area Network (LAN) dengan cara menghubungi admin jaringan tersebut lalu kita membaca log data mikrotik CCR (Cloud Core Router) yang mencakup sistem lalu di berikan data log yang nantinya akan dianalisa selama periode 1-4 September 2020. Pada hasil analisa jaringan di laboratorium SMK Telkom Jakarta sudah terbilang cukup aman dikarenakan versi mikrotiknya selalu dicek jika ada update terbaru enkripsi, security atau bugfix nya diperbaharui. Dan kejadian yang sering terjadi adalah PPTP Error dengan persentase 17,91% melalui pesan user authentication failed dimana maksud dari pesan ini adalah warning sebagai admin, ada yang berusaha masuk ke mikrotik tetapi tidak berhasil.

**Kata kunci** – Keamanan Jaringan, Jaringan LAN (Local Area Network)

**Abstract :**

*Abstract— The bigger a network, the network management becomes more complex and complicated. Therefore it is necessary to have proper network management. Seeing the development of LAN (Local Area Network) networks as one of the computer network technologies, SMK Telkom Jakarta should implement network security to streamline the process of sending data safely and on target by utilizing available resources so that they can work together as much as possible. To be able to find out the weaknesses and strengths of the application of existing computer network security and its capabilities can be improved for a wider purpose, and can minimize problems that will occur in the future so that they can be repaired immediately. And to help improve the security performance of the Local Area Network (LAN) network at SMK Telkom Jakarta. In the final project research at the SMK Telkom Jakarta Laboratory by conducting a Network Security Analysis of the Local Area Network (LAN) by contacting the network admin then we read the CCR (Cloud Core Router) mikrotik log data which includes the system and then provide log data which will be analyzed later. during the period 1-4 September 2020. In the results of network analysis at the SMK Telkom Jakarta laboratory, it is quite safe because the proxy version is always checked if there is a new encryption, security or bugfix update. And the incident that often happens is PPTP Error with a percentage of 17.91% through the message user authentication failed where the meaning of this message is a warning as admin, some try to enter the proxy but it doesn't work.*

**Keywords** – Network Security, LAN (Local Area Network)

## I. PENDAHULUAN

### A. Latar Belakang

Perkembangan teknologi jaringan komputer dewasa ini semakin pesat seiring dengan kebutuhan masyarakat akan layanan yang memanfaatkan jaringan komputer. Mulai dari sekedar mengerjakan tugas sampai dengan kebutuhan bersosialisasi melalui situs jejaring sosial. Komputer yang dulu tidak terhubung dengan komputer lainnya atau hanya berdiri sendiri, sekarang menjadi sebuah keharusan untuk terhubung dengan komputer lainnya. Baik itu melalui jaringan lokal, jaringan LAN (*Local Area Network*) telah menjadi suatu teknologi

yang sangat banyak digunakan baik di perusahaan, kantor, kampus, sekolah ataupun di perumahan.

Semakin besar suatu jaringan maka manajemen jaringan menjadi lebih kompleks dan rumit. Oleh karena itu perlu adanya manajemen jaringan yang tepat. Selama ini keamanan pada jaringan lokal yang sedang berjalan kurang diperhatikan dari ancaman yang mungkin saja ada untuk merusak, maupun mencuri data yang ada di lingkungan SMK Telkom Jakarta. Maka dalam penelitian ini mencoba untuk menganalisa permasalahan dan persoalan yang timbul dalam

keamanan jaringan, yang melingkupi area jaringan lokal di sekitar instansi tersebut.

## B. Tujuan Penelitian

1. Mengetahui peralatan hardware dan sistem dalam membangun keamanan jaringan *Local Area Network* (LAN) di Laboratorium SMK Telkom Jakarta.
2. Menganalisa jaringan pada laboratorium SMK Telkom Jakarta.
3. Menganalisa tingkat keamanan jaringan *Local Area Network* (LAN), sehingga dapat mengetahui kekurangan dan kelebihan keamanan jaringan yang diterapkan pada Laboratorium SMK Telkom Jakarta.

## C. Rumusan Masalah

1. Apa saja hardware, software dan sistem operasinya dalam pengembangan keamanan jaringan *Local Area Network* (LAN) di Laboratorium SMK Telkom Jakarta?
2. Bagaimana tingkat Keamanan Jaringan *Local Area Network* (LAN) Laboratorium SMK Telkom Jakarta?
3. Apa saja kelebihan dan kekurangan sistem keamanan jaringan LAN berdasarkan topologi dan media transmisi di Laboratorium SMK Telkom Jakarta?

## D. Batasan Masalah

1. Analisa *Hardware* dan i yang digunakan dalam keamanan jaringan LAN.
2. Jaringan yang dianalisa adalah jaringan pada Laboratorium SMK Telkom Jakarta.
3. Parameter yang digunakan dilihat dari tingkat kegagalan akses jaringan dan pencurian data.

## II. DASAR TEORI

### A. *Local Area Network* (LAN)

LAN adalah singkatan dari *Local Area Network*. LAN terdiri dari beberapa komputer yang terhubung dalam suatu jaringan. Pada jaringan ini, setiap komputer dapat mengakses data dari komputer lain. Selain itu, komputer dapat mengakses data dari komputer lain. Jumlah komputer yang terhubung pada LAN relatif kecil, misal komputer-komputer di rumah, warnet, tempat kos, dan beberapa tempat lain yang komputernya termasuk di dalam LAN, yang berada dalam satu bangunan. Setiap komputer yang terhubung pada LAN mempunyai IP Address yang berbeda.[1]

### B. Topologi Jaringan Star

Topologi ini merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut ke semua simpul atau *client* yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau *client server*. Setelah hubungan jaringan dimulai oleh server maka setiap *client server* sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server.[2]

a. Keuntungan:

- 1). Sangat handal diantara topologi yang lain.
- 2). Mudah dikembangkan.
- 3). Keamanan data tinggi.
- 4). Kemudahan akses ke jaringan LAN lain.

b. Kerugian:

- 1). Lalu lintas data yang padat menyebabkan jaringan lambat.
- 2). Jaringan tergantung pada terminal pusat.

### C. Perangkat Keras (*Hardware*)

#### 1. *Personal Computer* (PC)

*Personal Computer* (PC) merupakan media utama dalam sebuah jaringan, oleh karenanya PC mempunyai peran yang sangat penting. Rangkaian PC yakni berupa *motherboard*, *processor*, *monitor*, *keyboard*, *harddisk*, dan komponen lainnya. Karena seperti yang telah diketahui, itu semua adalah faktor-faktor pendukung bahkan merupakan pondasi dari PC.[3]

#### 2. *Media Transmisi*

Dalam membangun suatu jaringan di butuhkan media transmisi untuk komunikasi yang saling terhubung antara satu dengan lainnya dalam bentuk gelombang listrik atau elektromagnetik sebagai media pengirimnya maupun menerima data.[4] Media transmisi terbagi menjadi dua yaitu jaringan kabel dan *wireless*, yang dalam penggunaannya diterapkan dari faktor harga *performance* jaringan yang diinginkan, ada atau tidaknya medium tersebut.

#### 3. *LAN Card* (Kartu Jaringan)

*LAN Card* merupakan sebuah alat yang sangat penting dalam membangun sebuah jaringan, baik dalam skala kecil maupun besar. Kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang dipasang pada slot ekspansi di dalam komputer. Kartu Jaringan umumnya telah menyediakan *port* koneksi untuk kabel koaksial ataupun kabel *twisted pair*. [5]

#### 4. *Bridge*

*Bridge* merupakan perangkat yang membagi satu buah jaringan kedalam dua buah jaringan. Ini digunakan untuk mendapatkan jaringan yang efisien, karena pertumbuhan jaringan yang sangat cepat sehingga diperlukan suatu jembatan. Diibaratkan bahwa *Bridge* ini

seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk. Dia mengatur agar informasi di antara kedua sisi jaringan tetap berjalan dengan baik dan teratur. *Bridge* juga dapat digunakan untuk mengkoneksi diantara jaringan yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.[2]

#### 5. HUB

HUB adalah kotak persegi panjang kecil, biasanya terbuat dari plastik, yang menerima daya dari stop kontak pada dinding biasa. HUB menyatukan kabel-kabel *network* dari tiap-tiap *workstation*, server atau perangkat lain. HUB bekerja dengan metode *broadcast*, sehingga semua *port* yang ada akan dikirim sinyalnya.[6]

#### 6. Switch

*Switch* merupakan sebuah konsentrator sama dengan HUB. Perbedaannya adalah pada cara pengiriman/penyaluran data pada jaringan. Bekerja dengan metode mengakses tabel MAC *Address*, jadi kalau sinyal berasal dari port satu ke port lainnya, tidak akan di *broadcast* ke port yang tidak dituju. Fungsinya sama dengan *bridge* (menghubungkan dua buah LAN). *Switch* terdiri dari beberapa port sehingga *switch* disebut *multiport bridge*. Dengan kemampuannya tersebut, jika salah satu *port* pada *switch* sibuk maka *port-port* lain akan masih tetap berfungsi. Namun, *bridge* dan *switch* tidak dapat meneruskan paket IP yang ditujukan komputer lain yang secara logika berbeda jaringan.[5]

#### 7. Router

*Router* dapat mengetahui keseluruhan jaringan, melihat sisi mana dalam jaringan komputer yang paling sibuk dan bisa menarik data dari sisi yang sibuk tersebut sampai sisi tersebut bersih. Jika LAN terkoneksi ke Internet maka *router* akan menterjemahkan informasi antara LAN dan Internet. Jadi dapat dirangkum bahwa *router* mempunyai fungsi mengatur jalur sinyal secara efisien, mengatur pesan diantara dua buah protokol, mengatur pesan diantara topologi jaringan linear Bus dan Bintang (*star*), dan mengatur pesan yang melewati Kabel *fiber optic*, kabel koaksial atau kabel *twisted pair*. [4]

#### 8. Modem (Modulator Demodulation)

1. Modem internal, merupakan modem yang terpasang di dalam PC. Modem internal berbentuk *card* yang terpasang pada slot yang ada pada *motherboard*.

2. Modem eksternal, merupakan modem yang terpasang di luar PC. Untuk menghubungkan dengan PC melalui port komunikasi seperti COM1 atau dengan port USB.[4]

#### 9. Access Point

*Access Point* (AP) merupakan komponen yang berfungsi untuk mengirim atau menerima data yang berasal dari adapter *wireless*. *Access point* (AP) pada WLAN berfungsi seperti HUB/*Switch*, tanpa menggunakan *access point*, perangkat *wireless* (PC/Laptop yang mempunyai *wireless adapter*) hanya dapat berkomunikasi menggunakan *point to point* (2 komputer). Tipe *point to point* ini seperti sistem jaringan kabel tanpa HUB, sering disebut *cross link*. *Access point* mengeluarkan sinyal SSID (*Service Set Identification*) yang merupakan nama sinyal radio yang diberikan pada jaringan tanpa kabel (*wireless network*). Agar dapat terhubung dengan *access point*, semua komputer yang akan dihubungkan harus diisikan SSID yang dikeluarkan oleh *access point*. Penamaan standar SSID menggunakan nama default, tetapi dapat juga diganti dengan nama lain.[6]

#### 10. Mikrotik Routerboard

Mikrotik *Routerboard* merupakan salah satu jenis mikrotik yang sistem pemakaiannya terdapat *hardware* agar dapat menjalankan fungsi *router* mikrotik. Unikinya, di dalam *routerboard* sudah terdapat sistem operasi yang dapat digunakan layaknya sebuah komputer. Cara menggunakan *routerboard* ini juga sama halnya ketika kita menggunakan CPU. Ada prosesor, Memori ROM, memori RAM, dan juga sistem operasi. Untuk sistem operasi yang digunakan pada *routerboard* memiliki sistem operasi khusus. Nama sistem operasi yang digunakan adalah *RouterOS*. [3]

### D. Perangkat Lunak (Software)

#### 1. Sistem Operasi

Sistem Operasi adalah perangkat lunak yang bertanggung jawab memberikan kita kemudahan mengendalikan komputer. Menyediakan pilihan perintah untuk dieksekusi dan selanjutnya menyediakan informasi atau aksi yang kita perlukan.[7]

Secara umum, sistem operasi bertugas untuk mengatur dan mengendalikan perangkat keras serta aplikasi agar dapat bekerja dengan baik, fleksibel dan seimbang dengan cara yang dapat diprediksi. Pada komputer desktop yang kita gunakan, sistem operasi mengendalikan prosesor, memori, perangkat penyimpanan dan lainnya.[8]

#### 2. Antivirus

*Antivirus software* atau sering dikenal dengan *Antivirus* (disingkat dengan AV) merupakan perangkat lunak yang digunakan/didesain untuk mencegah, mendeteksi, dan mengambil tindakan untuk menglucuti atau menghilangkan program jahat/*malware*

(*computer virus, keyloggers, backdoors, trojan horses, adware, spyware*, dan lain sebagainya). Supaya dapat melindungi dengan efektif *Antivirus* harus bekerja secara tersembunyi setiap saat dan harus selalu diperbaharui sehingga dapat mendeteksi versi terbaru dari *malware*.

Program *antivirus* merupakan bagian paling dasar dari *multi-layer* strategi keamanan-bahkan untuk pengguna komputer yang sangat mahir. serangan yang terus menerus terjadi pada *browser, plug-in*, bahkan sistem operasi hal ini menjadikan proteksi dari *antivirus* sangat penting.[8]

## E. Protokol TCP/IP

TCP/IP (*Transport Control Protocol / Internet protocol*) merupakan salah satu protokol atau standar aturan jaringan yang sering digunakan pada jaringan berskala besar dan luas. TCP/IP dipakai karena bersifat fleksibel dan mudah digunakan. TCP/IP terdiri dari beberapa lapisan protokol. Dalam penerapannya, TCP/IP menggunakan protokol sampai dengan 4 level fungsi *layer* dalam arsitektur protokol.[4]

Lapisan *layer* TCP :

- a. *Network Access Layer*
- b. *Internet Layer*
- c. *Transport Layer*
- d. *Application Layer*

## F. IP Address

IP (*Internet protocol*) *Address* merupakan alamat yang diberikan kepada komputer-komputer yang terhubung dalam suatu jaringan. IP *Address* terdiri dari dua bagian, yaitu: *Network ID* dan *Host ID*. *Network ID* menentukan alamat dalam jaringan (*network address*) sedangkan *host ID* menentukan alamat dari peralatan jaringan yang sifatnya unik untuk membedakan antara satu mesin dengan mesin yang lain. Ibarat sebuah alamat rumah, *Network ID* seperti alamat rumah dan *Host ID* seperti nomor rumah.

IP *Address* berdasarkan perkembangannya dibagi menjadi dua jenis :

1. Ipv4 (*Internet protocol* versi 4) merupakan IP *Address* yang terdiri dari 32 bit yang dibagi menjadi 4 segmen berukuran 8 bit.
2. Ipv6 (*Internet protocol* versi 6) merupakan IP *Address* yang terdiri dari 128 bit yang digunakan untuk mengatasi permintaan IP *Address* yang semakin meningkat.

IP *Address* terdiri dari 32 bit angka biner yang dituliskan dalam bentuk empat kelompok dan masing-masing kelompok terdiri dari delapan (oktat) bit yang dipisahkan oleh tanda titik. IP *Address* dapat juga ditulis dalam bentuk angka desimal dalam empat kelompok, dari angka 0-255.[5]

## G. Keamanan Jaringan Komputer

### 1. Klasifikasi Serangan Komputer

- a. Keamanan Fisik (*Physical Security*)
- b. Keamanan Data dan Media
- c. Keamanan dari Pihak Luar
- d. Keamanan dalam Operasi

### 2. Serangan Keamanan Jaringan

#### a. *Social Engineering*

Biasanya orang yang melakukan *social engineering* akan menyamar sebagai orang yang memakai sistem dan lupa *password*, sehingga akan meminta kepada orang yang memiliki akses pada sistem untuk mengubah atau mengganti *password* yang akan digunakan untuk memasuki sistem tersebut.[5]

#### b. Dos/DDoS

Dos (*Denial of service*) adalah suatu teknik serangan yang digunakan untuk memakan atau menghabiskan resource yang dimiliki oleh komputer target atau sasaran, baik berupa *processor*, memori, ataupun *bandwidth*. Namun pada umumnya yang paling sering diserang adalah *bandwidth*.

DDoS (*Distribution Denial of service*) adalah suatu teknik serangan yang dilakukan secara bersamaan baik dari suatu wilayah ataupun dari berbagai wilayah di dunia yang terhubung dengan suatu jaringan.[5]

#### c. *Password Cracker*

Jenis dari *password cracker* adalah sebagai berikut :

1. *Brute Force* adalah Suatu cara yang digunakan dengan mengombinasikan kemungkinan huruf dari a-z, A-Z, dan angka 0-9.
2. *Dictionary* adalah Suatu cara dalam memecahkan suatu password dengan membandingkan kemungkinan dengan kata-kata yang telah terdaftar.[3]

#### d. *Sniffing dan Spoofing*

*Sniffing* merupakan suatu teknik yang digunakan untuk mengambil atau mencuri atau menyadap data yang berada pada lalu-lintas suatu jaringan.

*Spoofing* merupakan suatu teknik yang digunakan untuk memanipulasi atau meracuni suatu lalu-lintas jaringan dengan cara mengubah atau memanipulasi suatu data identitas agar terlihat sebagai pengguna.[3]

#### e. *Scanning*

*Scanning* merupakan tindakan yang pertama-tama dilakukan untuk mengetahui bagian-bagian *service* mana

saja dari sistem yang sedang dijalankan atau terbuka.[3]

f. **Backdoor dan Trojan**

*Backdoor* merupakan suatu pintu rahasia yang dapat digunakan untuk keluar masuk dari sistem yang telah berhasil ditembus tanpa menaruh kecurigaan admin yang mengelola komputer tersebut.

*Trojan* merupakan suatu program yang sifatnya merusak. Cara kerjanya adalah dengan memanipulasi data menjadi suatu program yang legal, sehingga tidak mengundang kecurigaan.

3. **Firewall**

*Firewall* kita gunakan untuk membatasi akses antara dua jaringan yang saling terhubung, yaitu antara jaringan internal dengan jaringan yang lebih global (internet). *Firewall* diletakkan di antara kedua jaringan tersebut, sehingga semua informasi yang keluar maupun yang masuk harus melewati *firewall*. [1]

Tujuan utama firewall adalah menjaga agar akses internal maupun eksternal dari orang yang tidak berwenang atau tidak mempunyai akses tidak dapat dilakukan. *Firewall* merupakan suatu cara yang efektif untuk melindungi jaringan dari ancaman gangguan lewat internet. Selain itu, *firewall* dalam jaringan komputer membatasi dan menjaga kerusakan pada satu bagian jaringan agar tidak menyebar ke bagian lain pada jaringan.

4. **Penggunaan Jaringan Firewall**

a. **Packet Filtering**

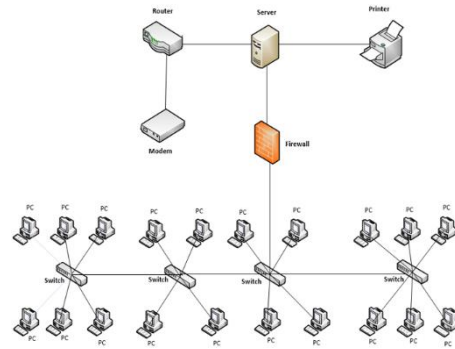
*Packet filtering* sering disebut juga *screening router*, yaitu suatu *router* yang melakukan routing paket antara jaringan internal dan jaringan eksternal sesuai dengan kebijakan keamanan yang digunakan pada suatu jaringan. [1]

b. **Sistem Proxy**

*Proxy* merupakan suatu program server atau aplikasi spesifik yang dijalankan pada mesin *firewall*. Setiap komunikasi yang terjadi antara dua buah jaringan dilakukan melalui suatu operator (*Proxy Server*). Sebuah *firewall* biasanya akan menggunakan kombinasi antara *packet filtering* dan sistem *proxy*. [9]

III. **SISTEM KEAMANAN JARINGAN LAB SMK TELKOM JAKARTA**

A. **Arsitektur Jaringan di Lab SMK Telkom Jakarta**



Gambar 1.1 Topologi Jaringan Lab SMK Telkom

B. **Perangkat Keras (Hardware)**

Dibawah ini spesifikasi Komputer client. Tabel 1.1 merupakan spesifikasi perangkat keras pada komputer client di SMK Telkom Jakarta.

Tabel 1.1 Spesifikasi Perangkat Keras

Nama Perangkat Keras	Keterangan
Motherboard	ECS H61H2-M2
Processor	InteR Core i3 210 2nd G
Chip	Intel ® GMA 3100
Memori	DDR 3 4GB PC 10600
Manufacturrer	Intel Corporation
Monitor	LCD LG!!WSB 17"
Disk Drive	LG Optical Drive DVD±RW
Keyboard	Simbada 922
Mouse	Simbada 922
VGA	Intel® HD Graphics 384Mb
Power Supply	Azzura 3000 450 W

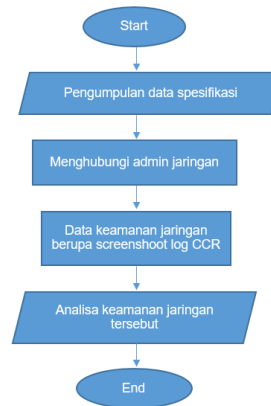
Dalam mengatur lalu lintas data dan alokasi *bandwidth* dibutuhkan sebuah perangkat dalam jaringan yang terhubung langsung. Table 1.2 adalah spesifikasi media penghubung pada jaringan LAN SMK Telkom Jakarta.

Tabel 1.2 Spesifikasi Media Penghubung

Media Penghubung	Tipe	Spesifikasi
Modem	ZTE ZXHN F609	<ul style="list-style-type: none"> <li>➤ ITU-T G.984.x GPON standards</li> <li>➤ 1.244Gbps burst mode upstream, 2.488Gbps downstream</li> <li>➤ IEEE 802.11b/g/n</li> </ul>

		➤ NAT/ SNTP
Switch	Switch HP V1410-16 (J9662A)	<ul style="list-style-type: none"> <li>➤ 16 Fast Ethernet 10/100Mbps Ports</li> <li>➤ Latency : 100 Mb Latency: &lt; 10.6 <math>\mu</math>s (LIFO 64-byte packets) Throughput : up to 2.3 million pps (64-byte packets) Switching capacity : 3.2 Gbps</li> <li>➤ Power consumption : 3.6 W (maximum). tegangan : 100-240 VAC. Input operating. current : 0.3 A. Input frequency : 50/60 Hz</li> </ul>
Mikrotik Router	CCR1009-7G-1C-1S+v6 47 (stable)	<ul style="list-style-type: none"> <li>➤ CPU : TLR4-00980CH-10CE-A3 1 GHz 9 Cores</li> <li>➤ RAM : 2GB Onboard</li> <li>➤ Power Jack : 110/220V</li> <li>➤ Serial Port : DB9/RS232</li> </ul>

### C. Flowchart



**Gambar 1.2 Flowchart Penelitian**

Tahapan pengambilan data keamanan jaringan di Lab SMK telkom adalah sebagai berikut :

- a. Pengumpulan data spesifikasi komputer melalui KAUR Lab di SMK Telkom Jakarta berupa Data Excel
- b. Selanjutnya untuk mendapatkan data keamanan jaringan saya harus menghubungi admin jaringan di SMK Telkom Jakarta
- c. Setelah menghubungi admin jaringan, lalu diberikan data berupa data log CCR (*Cloud Core Router*)
- d. Selanjutnya adalah data yang di screenshot ini akan di analisa keamanan jaringannya.

## IV. HASIL DAN ANALISA

### A. Analisa Permasalahan Keamanan Jaringan pada SMK Telkom Jakarta

1. Status Red (*System Error*), Status Red yaitu status yang berwarna merah Maksudnya dari status red terjadi karena user yang memasuki sistem login dari SMK Telkom Jakarta adalah user yang salah dan kode authentication salah, sehingga ditolak dan terjadi login failed.
2. Status Blue (*Offering Lease*) Status yang berwarna biru Status ini masih menjadi hal ambigu dan membingungkan, biasanya DHCP *client* ada *double mac adres* dan mungkin di memori nya belum sepenuhnya hilang.
3. Status Black (Normal), Status berwarna hitam Status ini dapat diabaikan karena tidak ada kendala yang berarti, dikarenakan *user* berhasil masuk dan kode *authentication* nya sesuai.

### B. Sistem Login pada SMK Telkom Jakarta (*System, info, account*)

#### 1. Login Via API

Login Via API selama periode 1-4 September didapatkan ada 6 kali percobaan *login* yang dilakukan oleh *user* dan semuanya berhasil. Persentase untuk login via API adalah sebagai berikut :

$$\frac{\text{jumlah data login via API}}{\text{jumlah data (tanggal 1 - 4 september)}} \times 100\%$$

$$= \frac{6}{134} \times 100\% = 4,47\%$$

## 2. Login Via Winbox

Login Via Winbox selama periode 1-4 September didapatkan ada 12 kali percobaan login berhasil dan 1 *login failure* yang pada kasus ini kemungkinan ada *user* yang berusaha masuk ke mikrotik tetapi tidak berhasil dan ada kemungkinan lain yaitu kesalahan admin daam memasukkan *password* karena biasanya admin tidak hanya menangani 1 mikrotik saja. Persentase untuk login via Winbox yang berhasil adalah sebagai berikut :

$$= \frac{\text{jumlah data login via winbox}}{\text{jumlah data (tanggal 1-4 september)}} \times 100\%$$

$$= \frac{12}{134} \times 100\% = 8,95\%$$

Sedangkan untuk persentase *login failure* adalah sebagai berikut :

$$= \frac{\text{jumlah data login failure via winbox}}{\text{jumlah data (tanggal 1-4 september)}} \times 100\%$$

$$= \frac{1}{134} \times 100\% = 0,74\%$$

## 3. Login Via Telnet

Login Via Telnet selama periode 1-4 September didapatkan ada 2 kali percobaan *login* yang dilakukan oleh *user* dan semuanya berhasil. Persentase untuk login via Telnet adalah sebagai berikut:

$$= \frac{\text{jumlah data login via telnet}}{\text{jumlah data (tanggal 1-4 september)}} \times 100\%$$

$$= \frac{2}{134} \times 100\% = 1,49\%$$

## C. Analisa Critical

*Critical* adalah *warning* untuk *admin* bahwa topik ini mengartikan ada yang berusaha tembus dengan contoh *message* yang ada di tabel 4.1 “*user 1 authentication failed*” yang artinya ada atas nama “*user 1*” ada yang akses *pptp* tapi notifikasinya *failed*. Lalu *ccr* meneruskan pesan *login failure* yang artinya ada *user* yang berusaha masuk tapi tidak bisa dikonfirmasi oleh *ccr* dan langsung otomatis ada *warning* merah. Jika *user* tersebut berhasil tembus maka ambil tindakan merubah *password* dan *active connectionnya* diputuskan.

## D. Analisa DHCP Warning

Kondisi ini terjadi dikarenakan ingin masuk menggunakan *address* yang sudah ada, namun dalam mikrotik secara *system* tidak kebagian *leasing* (sewa IP). Sebab terjadinya pada kondisi ini karena bentrok dengan pc lain. Biasanya terdapat *message* dari log berupa *offering lease* yang masih jadi masalah ambigu atau membingungkan biasanya di *DHCP Client* ada *double MAC Address* mungkin di memorinya belum sepenuhnya hilang. Pada kasus ini *DHCP Warning*

dalam periode tanggal 1 september sampai tanggal 4 september 2020 sebanyak 2 kali Yang dimana presentase nya itu sekitar 1,49% saja untuk muncul *DHCP Warning* dalam waktu 4 hari.

## E. Analisa PPTP (Point-to-Point Tunneling Protocol) Error

Pada data log *CCR* terdapat topik *pptp,ppp,error* dengan pesan *user authentication failed* dimana maksud dari pesan ini adalah *warning* sebagai admin, ada yang berusaha masuk ke mikrotik tetapi tidak berhasil, Pada kasus ini dalam periode tanggal 1-4 september 2020 sebanyak 24 kali Yang dimana presentase nya itu sekitar 1,49% saja untuk muncul *DHCP Warning* dalam waktu 4 hari.

$$= \frac{\text{jumlah data pptp,ppp,error}}{\text{jumlah data (periode tanggal 1-4 september)}} \times 100\%$$

$$= \frac{24}{134} \times 100\% = 17,91\%$$

## F. Interface,info

Biasanya topik ini memberikan pesan antara *link up* dan *link down*. Jika pesan tersebut isinya *link up* maka artinya status normal, ada respon di sisi *client/perangkat* yang terhubung sedangkan pesan tersebut isinya *link down* maka artinya ada sisi *client* yang tidak aktif.

## G. Alternatif Penyelesaian Masalah

### 1. Diperlukan Tambahan Keamanan Jika Login Failure

Untuk keamanan ini SMK Telkom Jakarta sudah cukup aman, namun ketika terjadi masalah seperti *user* tidak dikenal ingin masuk sehingga *login failed*. Maka cara mengatasinya adalah segera di non-aktifkan perangkat nya. Namun harus menginfokan kepada *user* yang menggunakan hal tersebut. Dalam hal ini SMK Telkom Jakarta perlu meningkatkan enkripsi.

### 2. Melakukan Reboot/Restart Router Secara Rutin

Seperti yang kita ketahui dalam kondisi ini admin harus membuat jadwal rutin untuk melakukan *reboot/restart*. Jadwal rutin nya adalah setiap 12 jam sekali. Namun sebelum itu melakukan *screenshot* atau simpan sebagai data. Hal ini dilakukan karena kondisi yang cukup panas yang bisa mengakibatkan router *over heat*.

### 3. Mengupdate Sistem Operasi

Pengupdatean sistem operasi pun sama pentingnya dengan mengupdate *anti virus* dikarenakan didalam sistem operasinya pun adanya lobang keamanan dari sistem operasi tersebut. Lubang keamanan ini sering dimanfaatkan oleh *virus* untuk masuk dan merusak sistem operasi komputer. Disamping mengamankan dari serangan *virus*, melakukan update sistem operasi juga akan membuat komputer berjalan dalam keadaan stabil.

## DAFTAR PUSTAKA

- [1] F. Alwafi, "ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN PADA PT . DAE MYUNG HIGHNESS INDONESIA Pendahuluan Kemajuan di bidang teknologi lainnya instansi dan bentuk usaha dengan dalam berinteraksi karyawan informasi khususnya internet kantor cabang , maupun di lapanga," vol. 3, no. 1, pp. 1–10, 2015.
- [2] A. Supriyadi and D. Gartina, "Memilih Topologi Jaringan dan Hardware dalam Desain Sebuah Jaringan Komputer," *Inform. Pertan.*, vol. 16, no. 2, pp. 1037–1053, 2007.
- [3] Madcoms, *Membangun Sistem Jaringan Komputer*, 1st ed. Yogyakarta: C.V Andi Offset, 2009.
- [4] I. Anugrah and R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 5, no. 2, pp. 91–106, 2018, doi: 10.33558/piksel.v5i2.271.
- [5] W. Kurniawan, *Jaringan Komputer*, 1st ed. Yogyakarta: C.V Andi Offset, 2007.
- [6] R. Budi, *Praktik Membuat Jaringan LAN dan Wireless*. Yogyakarta: Skripta, 2019.
- [7] U. Mulawarman, "Analisis usabilitas sistem operasi windows 10 pada pengguna expert dan novice (studi kasus : mahasiswa fakultas teknik universitas mulawarman)," *Manaj. dan Tek. Ind.*, no. September 2014, pp. 16–23, 2017.
- [8] B. Shinugi, *Mengenal Perangkat Lunak Komputer*, Kelima. Jakarta: PT Mediantara Semesta, 2018.
- [9] I. R. Rahadjeng, "Analisis Jaringan Local Area Network (LAN) pada PT. Mustika Ratu Tbk Jakarta Timur," vol. 5, no. 1, 2018, doi: 10.31219/osf.io/htxwe.