Journal of Informatics and Computer Science Vol.7 No.2 Oktober 2021
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius

Design And Security Analysis On Freeradius Centralized Authentication System

Aulia Syarif Aziz[1], Safriatullah[2]
Program Studi Ilmu Komputer, Fakultas Sains, Teknologi, dan Ilmu Kesehatan, Universitas Bina Bangsa Getsempena,
Jl. Tanggul Krueng Lamnyong No.34 Rukoh Kec. Syiah Kuala, Kota Banda Aceh, Indonesia[1,2]
e-mail **:** as.sektim@gmail.com[1], safriatullah@gmail.com[2]

Abstrak – Pengguna Internet di Indonesia meningkat pesat sejak menyebarnya wabah COVID-19, dari 175,4 juta orang pada tahun 2020 menjadi 202,6 juta orang pada tahun 2021. Laporan Digital 2020 menunjukkan bahwa 54,6% pengguna mengakses Internet menggunakan telepon genggam, 44,9% menggunakan laptop, dan sisanya menggunakan komputer desktop serta perangkat lainnya. Saat ini pengguna Internet memiliki mobilitas yang tinggi, sebab itu banyak digunakan sistem autentikasi terpusat di sekolah-sekolah maupun kantor-kantor agar pengguna yang memakai Internet menggunakan WiFi bisa tetap terhubung tanpa harus *login* berulang-ulang. Salah satu aplikasi yang bisa digunakan secara gratis dalam membangun sistem autentikasi terpusat adalah FreeRADIUS. Dalam penelitian ini penulis melakukan analisis keamanan terhadap FreeRADIUS dengan membandingkan prokol autentikasi yang bisa digunakan serta ketersediaan layanan ketika terjadi serangan pada jaringan. Hasil dari penelitian ini diharapkan dapat membantu administrator jaringan dalam meningkatkan keamanan jaringan terutama pada jaringan dengan sistem autentikasi terpusat yang menggunakan RADIUS.

Kata kunci: ***Keamanan Jaringan, RADIUS, FreeRADIUS, MikroTik, Autentikasi***

Abstract - Internet users in Indonesia have increased rapidly since the COVID-19 outbreak, from 175.4 million people in 2020 to 202.6 million people in 2021. Digital Report 2020 shows that 54.6% of users access the Internet using mobile phones, 44, 9% use laptops, and the rest use desktop computers and other devices. Currently Internet users have high mobility, that's why centralized authentication systems are widely used in schools and offices so that users using the Internet using WiFi can stay connected without having to log in repeatedly. One application that can be used for free in building a centralized authentication system is FreeRADIUS. In this study, the authors conduct a security analysis on FreeRADIUS by comparing the authentication protocols that can be used and the availability of services when an attack occurs on the network. The results of this study are expected to assist network administrators in improving network security, especially on networks with a centralized authentication system that uses RADIUS.

Keywords: ***Network Security, RADIUS, FreeRADIUS, MikroTik, Authentication***

I. PENDAHULUAN

Sejak menyebarnya wabah COVID-19, penggunaan Internet dalam kehidupan masyarakat telah meningkat pesat. Hal ini terlihat dari mulai diterapkannya sistem kerja *work from home* hingga pembelajaran daring. Pada tahun 2021 pengguna internet di Indonesia meningkat 11 persen dari tahun sebelumnya, yaitu dari 175,4 juta menjadi 202,6 juta pengguna (Pratiwi, 2021). Seiring peningkatan tersebut, keamanan jaringan menjadi aspek yang sangat penting untuk diperhatikan sebab setiap orang pasti berusaha menjaga kerahasiaan, keaslian, dan integritas data mereka (Fachri, Fahmi, Abdul Fadlil, dan Imam Riadi, 2021).

Berdasarkan laporan Digital 2020 yang disampaikan oleh Hootsuite dan We Are Social, 54.6% pengguna Internet menggunakan telepon genggam, 44.9% menggunakan laptop, dan sisanya menggunakan komputer desktop (PC) serta perangkat lainnya (Kemp, 2020). Telepon genggam dan laptop sendiri umumnya menggunakan teknologi jaringan nirkabel untuk terhubung ke Internet. Menurut Bulbul, Batmaz, dan Ozel (2008), jaringan nirkabel merupakan teknologi yang sangat membantu untuk meningkatkan produktivitas penggunanya. Namun teknologi tersebut juga membawa beberapa risiko keamanan yang baru dalam jaringan komputer, walaupun teknologi jaringan nirkabel terus berkembang dengan pesat dan banyak produk serta fitur baru yang terus bermunculan. Produk dan fitur baru tersebut dirancang untuk mengatasi kelemahan lama maupun kelemahan yang baru ditemukan (Karygiannis & Owens, 2002).

Dalam keamanan jaringan komputer, setidaknya ada tiga aspek utama yang perlu diperhatikan yaitu kerahasiaan, keaslian, dan ketersediaan. Autentikasi adalah salah satu cara membuktikan keaslian, yaitu melalui proses pembuktian terhadap identitas pengguna ketika akan memasuki sebuah sistem. Dalam beberapa tahun ini, banyak penelitian yang melakukan perancangan sistem autentikasi terpusat menggunakan FreeRADIUS. Oleh sebab itu, dalam penelitian ini peneliti mengkaji aspek keamanan pada FreeRADIUS, terutama pada faktor keaslian dan ketersediaan.

II. TINJAUAN PUSTAKA

A. Jaringan Komputer

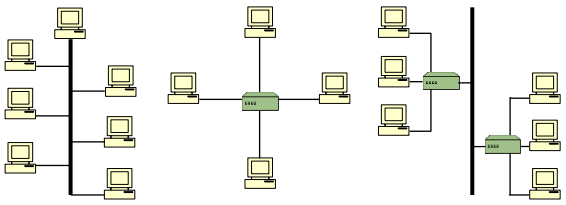
Stair & Reynolds (2012) menjelaskan bahwa jaringan komputer terdiri dari media komunikasi, perangkat keras, dan perangkat lunak yang dibutuhkan untuk menghubungkan dua komputer atau lebih. Setiap komputer dan perangkat dalam jaringan tersebut disebut titik (node). Berdasarkan jarak antara setiap titik, jaringan komputer dapat diklasifikasikan ke dalam personal area network (PAN), local area network (LAN), metropolitan area network (MAN), dan wide area network (WAN).

- Personal Area Network (PAN) merupakan jaringan yang menghubungkan beberapa perangkat dalam lingkup sekitar 10-meter untuk keperluan pribadi. PAN memungkinkan seseorang menghubungkan laptop, kamera digital, dan printer.
- Local Area Network (LAN) adalah jaringan yang menghubungkan beberapa komputer dan perangkat lainnya dalam area kecil seperti kantor, rumah, dan sekolah. Semua pengguna dalam kantor dapat terhubung dan berkomunikasi dengan mudah.
- Metropolitan Area Network (MAN) adalah jaringan telekomunikasi yang menghubungkan pengguna dengan perangkat dalam lingkup geografis yang mencakup kampus atau kota. MAN menggabungkan banyak jaringan kecil menjadi sebuah jaringan yang lebih besar, misalnya menggabungkan LAN di kampus.
- Wide Area Network (WAN) merupakan jaringan telekomunikasi yang menghubungkan wilayah yang luas. Sebuah WAN biasanya memungkinkan terjadinya komunikasi data antar negara, hal ini melibatkan aturan-aturan nasional dan internasional.

B. Topologi Jaringan

Topologi adalah peta dari sebuah jaringan. Topologi menjelaskan rancangan penghubungan jaringan dan lokasi komponen yang menyusunnya (Groth & Skandier, 2005). Beberapa bentuk topologi adalah sebagai berikut:

- Topologi *Bus*
  Pada topologi ini, setiap komputer terhubung ke sebuah kabel utama. Kelebihan topologi ini yaitu kabel yang digunakan tidak banyak sehingga menghemat biaya. Kekurangannya adalah sering terjadi antrean data dan jika terjadi gangguan pada satu komputer bisa mengganggu jaringan di komputer lain.
- Topologi *Star*
  Berbeda dengan topologi *bus*, setiap komputer pada topologi *star* terhubung ke sebuah titik tengah. Perangkat tengah yang digunakan bisa seperti hub, switch, maupun *access point*. Kelebihan topologi ini yaitu mudah untuk melakukan penambahan atau pengurangan komputer tanpa mengganggu komputer lain. Kekurangannya adalah jika titik di tengahnya mengalami gangguan, maka seluruh jaringan akan terganggu.
- Topologi *Tree*
  Topologi ini merupakan gabungan dari topologi *star* dan topologi *bus*. Biasanya dalam topologi ini terdapat beberapa tingkatan jaringan. Kekurangannya adalah jika terjadi kesalahan pada jaringan tingkat tinggi, maka jaringan tingkat rendah akan terganggu juga.



Gambar 1. Topologi bus, star, dan tree

C. Internet Protocol Suite (TCP/IP)

Internet protocol suite adalah kumpulan protokol komunikasi yang digunakan dalam jaringan komputer dan Internet, biasanya disebut juga TCP/IP. Protokol merupakan aturan-aturan yang dipakai oleh komputer agar dapat melakukan interaksi dengan komputer lainnya yang terhubung dalam sebuah jaringan (Zam, 2011). TCP/IP adalah gabungan dari TCP (*Transmission Control Protocol*) dan IP (Internet *Protocol*). TCP/IP berfungsi untuk mengatur mekanisme komunikasi data dari sebuah perangkat ke perangkat lainnya yang terhubung dalam sebuah jaringan. Bonaventure (2011) menjelaskan lapisan (*layer*) pada TCP/IP sebagai berikut:

- *Application layer* adalah lapisan yang paling terlihat dalam jaringan komputer. Aplikasi yang bekerja pada lapisan ini berinteraksi secara langsung dengan pengguna. Contoh protokol yang bekerja dalam lapisan ini adalah *hypertext transfer protocol* (HTTP), *file transfer protocol* (FTP), dan *simple mail transfer protocol* (SMTP).
- *Transport layer* adalah lapisan yang terletak di atas *network layer*. Ada 2 macam servis pada lapisan ini, yaitu *connectionless* dan *connection-oriented*. *User datagram protocol* (UDP) menyediakan servis transpor *connectionless*. UDP tidak bisa mengirim data yang lebih besar dari 65507 bytes dan tidak menjamin pengiriman paket data ke tujuan. UDP biasanya digunakan oleh aplikasi yang membutuhkan *delay* yang kecil. Contoh umum penggunaan UDP adalah *domain name system* (DNS). *Transmission control protocol* (TCP) merupakan protokol yang *connection-*

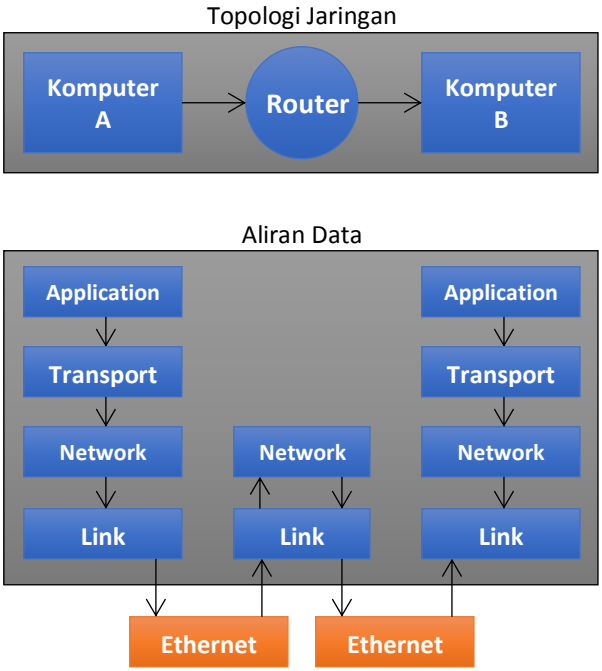
oriented, artinya protokol ini menjamin pengiriman data. Aplikasi yang menggunakan protokol ini antara lain: email (SMTP, POP, IMAP), *world wide web* (HTTP, HTTPS), *file transfer protocol* (FTP), *remote* akses komputer (SSH, Telnet), dll.

- *Network layer* memungkinkan aplikasi untuk bertukar data secara efisien, tanpa harus mengetahui apapun tentang teknologi *subnetworks*. *Network layer* menghubungkan *subnetworks* dengan *transport layer*, dan menjamin pertukaran data antara *host* yang terhubung dengan *subnetworks* yang berbeda. Fungsi utama dari *network layer* adalah untuk memungkinkan terjadinya pertukaran data dari jaringan berbeda melalui sebuah sistem yang disebut *router*. Unit informasi yang dikirimkan melalui *network layer* disebut paket data.
- *Data link layer* adalah lapisan paling bawah dari *Internet protocol suite*. Beberapa protokol yang bekerja dalam *layer* ini yaitu *point-to-point protocol* (PPP), *address resolution protocol* (ARP), dan *media access control* (MAC). *Data link layer* menggunakan servis yang disediakan oleh *physical layer* untuk bertukar data.

D. Internet Protocol Address

Syafarani (2012) menyebutkan bahwa *Internet protocol* (IP) merupakan sebuah protokol jaringan yang secara umum dijalankan bersama protokol TCP/IP. Setiap perangkat yang terhubung ke Internet dan ingin berkomunikasi dengan perangkat lain menggunakan TCP/IP harus memiliki alamat IP sebagai alat identifikasi diri. Oleh sebab itu, alamat IP harus bersifat unik, tidak boleh ada alamat IP kembar yang digunakan oleh 2 perangkat (host) berbeda dalam sebuah jaringan yang sama. Penggunaan alamat IP di seluruh dunia diatur oleh IANA (*Internet Assigned Numbers Authority*).

Menurut Zam (2011) alamat IP adalah identitas tersendiri yang dimiliki oleh perangkat yang terhubung ke sebuah jaringan. Format penulisan alamat IP adalah A.B.C.D. Masing-masing huruf tersebut terdiri dari angka 8 bit, sehingga nilai yang mungkin adalah 0 sampai 255. Alamat IP sebuah komputer yang tidak terhubung ke sebuah jaringan adalah 127.0.0.1 atau disebut juga dengan nama *localhost*. Ada 2 macam alamat IP, yaitu *public* dan *private*. Alamat IP *public* adalah alamat IP yang digunakan pada jalur umum (publik) Penggunaan alamat IP publik harus melalui proses registrasi ke organisasi yang menangani masalah pemakaian IP, tujuannya supaya tidak ada dua perangkat *host* yang memiliki IP yang sama. Alamat IP *private* adalah alamat IP yang digunakan pada jaringan lokal, sehingga tidak memerlukan proses registrasi.



Gambar 2. Diagram pengiriman data melalui *Internet protocol suite*

E. MikroTik

MikroTik merupakan sistem operasi berbasis Linux yang dibuat khusus untuk router jaringan. Mikrotik didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows application (WinBox). Selain itu, instalasinya dapat dilakukan pada komputer biasa (Handriyanto, 2009).

Menurut Ardhitya (2010), Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk membuat komputer menjadi *router* jaringan yang handal. Mikrotik didirikan pada tahun 1995. Pada awalnya Mikrotik ditujukan untuk Penyelenggara Jasa Internet (PJI) atau Internet *Service Provider* (ISP). Terdapat 2 jenis mikrotik, yaitu:

- Mikrotik RouterOS yang berbentuk perangkat lunak dan dapat diunduh di http://www.mikrotik.com. Perangkat lunak ini bisa diinstal pada komputer.

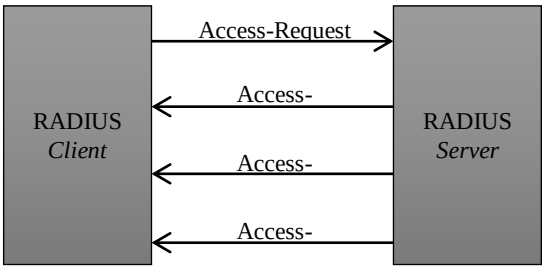
Gambar 3. Tampilan Mikrotik RouterOS

- *Built-in hardware* Mikrotik dalam bentuk perangkat keras yang khusus dikemas dalam *routerboard* yang di dalamnya sudah terinstal Mikrotik RouterOS.

F. RADIUS

Mengacu pada Vollbrecht (2006), Remote Authentication Dial In User Service (RADIUS) adalah sebuah protokol jaringan yang menyediakan manajemen Authentication, Authorization, dan Accounting (AAA) secara terpusat bagi pengguna layanan jaringan. RADIUS dikembangkan pada tahun 1991 oleh Livingston Enterprises, Inc sebagai autentikasi akses server dan protokol penghitungan, hingga pada akhirnya dijadikan standar Internet Engineering Task Force (IETF). Menurut Xiao (2008), RADIUS bisa menjaga sebuah jaringan dengan menolak akses dari pengguna ilegal.

Protokol ini telah banyak diimplementasikan dan digunakan. Pengamatan yang dilakukan menunjukkan bahwa RADIUS dapat mengalami penurunan kinerja dan kehilangan data bila digunakan dalam sistem dengan skala besar karena tidak mencakup ketentuan untuk pengendalian kemacetan. S*erver* RADIUS sendiri berkomunikasi dengan NAS menggunakan protokol UDP. RADIUS mendukung beberapa mekanisme autentikasi, seperti PPP CHAP atau PAP, UNIX *login*, dll. (Rigney, et al., 2000).

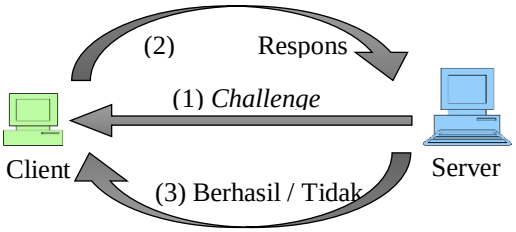


Gambar 4. Skema autentikasi pada RADIUS

G. Protokol Autentikasi PAP dan CHAP

Protokol autentikasi adalah protokol kriptografi yang bertujuan untuk autentikasi, agar komunikasi dapat dilakukan dengan aman. Beberapa contoh protokol autentikasi yaitu PAP, EAP, CHAP, dan Kerberos.

CHAP (*Challenge Handshake Authentication Protocol*) dan PAP (*Password Authentication Protocol*) adalah mekanisme autentikasi yang digunakan dalam PPP (*Point-to-Point Protocol*). Forouzan (2007) mengemukakan bahwa PAP merupakan protokol autentikasi simpel yang bekerja dengan dua langkah sederhana (*two-way handshake*), pertama client mengirimkan permintaan autentikasi dengan mengirimkan nama pengguna dan kata sandi, kemudian server mengidentifikasi permintaan tersebut dan memberikan respons yang sesuai (penerimaan atau penolakan). Sementara CHAP merupakan protokol autentikasi yang tingkat keamanannya lebih tinggi dan bekerja melalui tiga langkah. Pertama server akan mengirimkan sebuah paket *challenge* ke *client*, kemudian *client* menggabungkan paket tersebut dengan kata sandinya, selanjutnya server akan membandingkan data yang diterima dari *client* dengan yang dimilikinya dan mengirimkan respons yang sesuai.



Gambar 5. Proses autentikasi CHAP

III. METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini adalah penelitian kombinasi yang dilakukan dengan cara eksperimen dan studi literatur. Peneliti bertujuan untuk mendeskripsikan serta menjelaskan fenomena dengan menganalisis kejadian berdasarkan data yang diperoleh.

B. Alat dan bahan

Perangkat keras yang digunakan dalam penelitian ini adalah sebagai berikut:

a. 1 unit PC dengan spesifikasi:
   - CPU Intel Pentium Dual-Core E5500
   - RAM 2 GB
   - *Harddisk* 320

b. 1 unit server
   - CPU Intel Xeon Dual-Core 5110
   - RAM 1 GB
   - Harddisk 73.4 GB

Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:

a. FreeRADIUS 2.1.0
b. MikroTik RouterOS 5.20
c. SSH 5.9p1

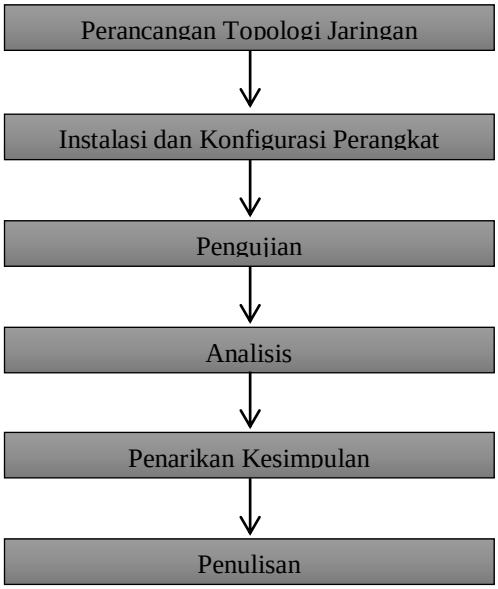
C. Pengumpulan Data

Pada metode ini akan dilakukan pengumpulan data dan informasi sebagai bahan yang dibutuhkan dalam penelitian. Peneliti melakukan beberapa tahapan untuk mengumpulkan data dan informasi. Tahapan yang dilakukan adalah sebagai berikut:

1. Metode Studi Literatur
   Pada tahap ini peneliti mempelajari penelitian terdahulu yang berkaitan dengan permasalahan yang diangkat melalui buku, jurnal, majalah, dokumen, serta sumber lain yang layak dijadikan referensi.
2. Metode Pengujian
   Metode pengujian adalah cara atau teknik untuk menguji perangkat lunak, mempunyai mekanisme untuk menentukan data uji yang dapat menguji perangkat lunak. Dalam penelitian ini ada dua parameter yang akan diuji, yaitu protokol autentikasi dan daya tahan terhadap serangan DoS.

D. Cara Kerja

Penelitian ini difokuskan untuk melakukan analisis keamanan pada sistem autentikasi terpusat FreeRADIUS. Alur pengerjaan penelitian ini dapat dilihat pada gambar berikut:

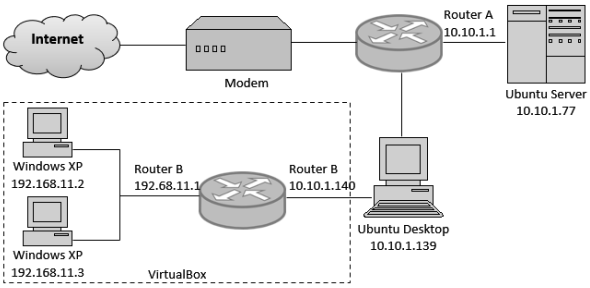


Gambar 6. Skema alur penelitian

IV. HASIL DAN PEMBAHASAN

A. Perancangan Topologi Jaringan

Dalam penelitian ini digunakan topologi jaringan dengan bentuk tree seperti pada gambar berikut:



Gambar 7. Rancangan topologi jaringan

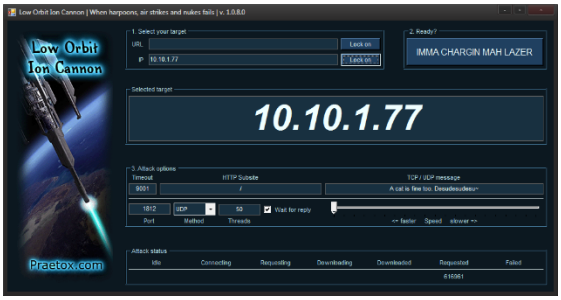
B. Instalasi dan Konfigurasi Perangkat

Untuk membangun sistem autentikasi terpusat, diperlukan perangkat lunak FreeRADIUS dan MikroTik. MikroTik berperan sebagai *router* dan FreeRADIUS sebagai server autentikasinya. Pengaturan yang perlu dilakukan di MikroTik adalah menambahkan RADIUS server. Kemudian file konfigurasi yang perlu diatur pada FreeRADIUS adalah dapat terhubung ke mirotik adalah clients.conf.

C. Pengujian

Pertama dilakukan pengujian keamanan autentikasi pada PAP dan CHAP. Pengujian dilakukan dengan mengamati paket data menggunakan aplikasi Wireshark. Mode *monitoring* diaktifkan pada Wireshark sebelum pengguna melakukan *login*, lalu pengguna melakukan *login* menggunakan masing-masing protokol autentikasi, setelah itu diamati hasil paket data yang telah diambil.

Pengujian selanjutnya dilakukan dengan melakukan serangan DoS dari komputer *client* ke server yang berada di jaringan lokal yang sama, kemudian diamati *response time* dari server RADIUS tersebut dan dibandingkan dengan *response time* dalam keadaan normal. *Response time* adalah total waktu tunggu yang dibutuhkan ketika sebuah permintaan dikirimkan hingga permintaan tersebut menerima balasan (Madalina, 2007). Serangan DoS dilakukan menggunakan aplikasi Low Orbit Ion Cannon (LOIC) dengan mengisikan alamat IP dan *port* yang digunakan oleh server.



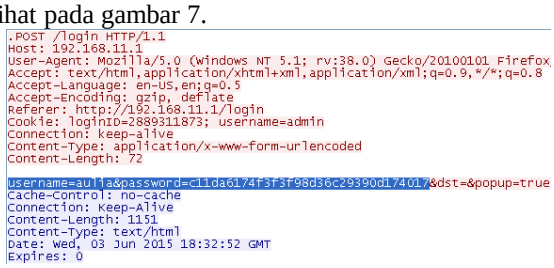
Gambar 8. Antarmuka aplikasi LOIC

D. Analisis

Pengujian autentikasi menggunakan PAP memperlihatkan bahwa kata sandi yang dikirimkan dari *client* ke server dapat terlihat jelas dalam bentuk aslinya, seperti terlihat pada gambar 6.

Gambar 9. Hasil pengamatan paket data pada autentikasi menggunakan PAP

Sementara itu pada autentikasi yang menggunakan CHAP, kata sandi sudah diacak menggunakan algoritma tertentu hingga sulit untuk dibaca. Kata sandi yang dihasilkan dari CHAP bisa dilihat pada gambar 7.



Gambar 10. Hasil pengamatan paket data pada autentikasi menggunakan CHAP

Hasil pengukuran *response time* server RADIUS dalam keadaan normal berkisar antara 15 sampai 32 ms dengan nilai rata-rata 20.5 ms, serta modus dan mediannya adalah 16 ms. *Response time* server RADIUS pada keadaan normal dapat dilihat pada tabel berikut:

Tabel 1. *Response time* server RADIUS pada keadaan normal

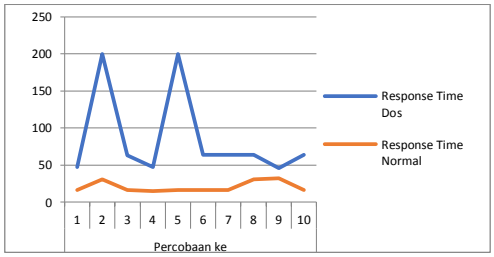
Percobaan ke-	1	2	3	4	5	6	7	8	9	10
Response time (ms)	16	31	16	15	16	16	16	31	32	16

Response time server RADIUS ketika dilakukan serangan DoS mengalami peningkatan yang signifikan. Nilainya berkisar dari 46 sampai 200 ms dengan rata-rata 85.9 ms (terjadi peningkatan 319%), serta modus dan mediannya adalah 64 ms.

Tabel 2. *Response time* server RADIUS dalam serangan DoS

Percobaan ke-	1	2	3	4	5	6	7	8	9	10
Response time (ms)	47	200	63	47	200	64	64	64	46	64

Perbandingan *response time* dalam keadaan normal dengan dalam serangan DoS bisa dilihat pada gambar 9.



Gambar 9. Grafik perbandingan *response time* server RADIUS

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan mulai dari studi literatur, perancangan, pengujian, hingga analisis, maka dapat disimpulkan bahwa:

1. FreeRADIUS mendukung banyak protokol autentikasi, diantaranya adalah PAP dan CHAP.
2. Dalam melakukan autentikasi, PAP bekerja dengan dua langkah dan mengirimkan data dalam bentuk mentah, sehingga kata sandi pengguna dapat terlihat dengan mudah bila ada pengguna lain yang meretas jaringan.
3. CHAP melakukan autentikasi melalui tiga tahap. Data yang dikirimkan telah dienkripsi sehingga tidak mudah terbaca oleh pihak lain.
4. Response time server RADIUS yang menggunakan FreeRADIUS berkisar antara 15 ms sampai 32 ms dalam jaringan lokal.
5. Serangan DoS yang dilakukan mempengaruhi *response time* server RADIUS. Terjadi peningkatan *response time* sebanyak 319%, nilai rata-rata awal 20.5 ms meningkat hingga 85.9 ms.
6. Diperlukan konfigurasi yang baik agar server RADIUS dapat berjalan dengan baik serta data pengguna bisa terjaga dengan aman. Hal ini bisa dilaksanakan dengan cara seperti menggunakan protokol autentikasi terkini yang sudah teruji keamanannya, serta mengganti port autentikasi untuk menghindari hal-hal yang tidak diinginkan.

REFERENSI

Ardhitya, A.I. 2010. Pengertian dan Penjelasan Mikrotik. Tersedia di http://ilmukomputer.org/2013/01/04/pengertian-dan-penjelasan-mikrotik/. Diakses 20 Juli 2021.

Agustini, Pratiwi. 2021. Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di Internet. Tersedia di: https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/. Diakses 11 September 2021.

Bonaventure, Olivier. 2011. *Computer Networking : Principles, Protocols and Practice*. The Saylor Foundation, Washington D.C.

Bulbul, H.I., Batmaz, I., & Ozel, M.. 2008. "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols." *E-Forensics 2008 - Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop* (Icv):1–6. doi: 10.4108/e-forensics.2008.2654.

Fachri, Fahmi, Abdul Fadlil, & Imam Riadi. 2021. "Analisis Keamanan Webserver Menggunakan Penetration Test." *Jurnal Informatika* 8(2):183–90. doi: 10.31294/ji.v8i2.10854.

Forouzan, B.A. 2007. *Data Communications and Networking* 4th ed. McGraw-Hill, New York.

Handriyanto, D.F. 2009. Kajian Pengguanaan Mikrotik Router OS Sebagai Router pada Jaringan Komputer. Universitas Sriwijaya.

Karygiannis, T., & Owens, L. 2002. *Wireless Network Security:*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Kemp, S. 2020. Digital 2020: Global Digital Overview. Tersedia di: https://datareportal.com/reports/digital-2020-global-digital-overview. Diakses 2 Agustus 2021.

Madalina. 2007. *Analyzing the Network Response Time and Load Balancing. Revista Informatica Economica* Vol. 11 (44): 64-67.

Rigney, C., Willens, S., Rubens, A., & Simpson, W. 2000. Remote Authentication Dial In User Service (RADIUS). Tersedia di https://tools.ietf.org/html/rfc2865. Diakses 22 Mei 2021.

Stair, R.M. & Reynolds, G.W. 2012. *Fundamentals of Informations Systems 6th ed*. Course Technology, Boston.

Syafarani, A.R. 2012. *E-book Dasar-Dasar Jaringan*

Komputer. Tersedia di: http://www.andimicro.com/2011/02/ebook-dasar-dasar-jaringan-komputer.html. Diakses 7 Juni 2021.

Vollbrecht, John. 2006. The Beginnings and History of RADIUS. Interlink Networks, Ann Arbor.

Xiao, Luo. 2008. The Realization of the RADIUS Security Authentication. Wireless Communications, Networking and Mobile Computing (WiCOM), 4th International Conference On. IEEE, Dalian.

Zam, Efvy. 2011. Buku Sakti Hacker. Mediakita, Jakarta.