

SISTEM KEAMANAN PADA JARINGAN WIRELESS MENGGUNAKAN PROTOKOL RADIUS

Aldi Sigit Saputra¹⁾, Dadan Irwan²⁾

¹Fakultas Teknik, Universitas Islam 45
Email: aldyputra020@gmail.com

²Fakultas Teknik, Universitas Islam 45
Email: dadanirwan@gmail.com

Abstract

Wireless networks require a security system to protect servers from attacks such as Port Scanning and Denial of Service. This research aims to design a wireless network security system using Remote Authentication Dial-In User Service or RADIUS protocol. The research stages include analysis of system requirements, preparation of completeness of system requirements, installation and configuration of the network and RADIUS protocol, detection and prevention testing of attacks, and analysis of test results. The design system used is to implement a single authentication, authorization, and accounting protocol that supports the internal and external networks of the Bahana Taruko Santosa Company. The results of implementing the RADIUS protocol on a wireless network server service can perform a DoS attack filter properly and block unauthorized users from accessing Internet services. Data analysis results show DoS attacks with the type of ICMP Flooding attack and UDP Flooding attack can be blocked with a percentage of 98%. In addition, there is a reduction in unauthenticated user access rights with the result of reducing the amount of bandwidth usage.

Keywords: *Wireless, RADIUS, Authentication, Authorization, Accounting.*

1. Pendahuluan

Teknologi jaringan *wireless* memungkinkan para pengguna atau *user* tetap terhubung dalam jaringan secara *mobile* tanpa harus menghubungkan kabel apapun (Rumalutur, 2014). Komunikasi pada jaringan *wireless* memiliki kesamaan dengan jaringan menggunakan kabel tetapi pada jaringan *wireless* memiliki kelebihan pada aspek pemasangan perangkat akhir seperti komputer dan perangkat lainnya yang berada pada lingkup area tertentu (Supriadi, Fahmi, & Imtihan, 2018) (Haerudin, Aksara, & Yamin, 2017). Namun dibalik semua keuntungan dan kemudahan yang diberikan setiap teknologi pasti memiliki kekurangan dan keterbatasan. Salah satu sisi kelemahan pada jaringan *wireless* yaitu pengguna yang tidak berhak dapat masuk ke dalam jaringan (Kuswanto, 2017). *Authentication* merupakan sebuah sistem keamanan yang bertujuan untuk melakukan pencatatan

setiap *user* yang akan mengakses ke dalam jaringan *wireless* (Setiawan, Jazuli, Listyorini, Sari, & Widodo, 2012). Sementara autentikasi yaitu proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan (Gaol & Pramarta, 2012). *Remote Acces Dial in User* (RADIUS) adalah protokol yang digunakan untuk otentikasi pengguna jaringan, dengan menyediakan fungsi *authentication, authorization, and accounting* (AAA) (Hidayat, 2015). Protokol RADIUS memiliki kelebihan dibandingkan dengan protokol lainnya seperti *Wired Equivalent Privacy* (WEP) dan *Wi-fi Protected Access* (WAP) (Stiawan & Rini, 2009). Penelitian sebelumnya berjudul “Celah Keamanan Sistem Autentikasi *Wireless* Berbasis RADIUS” yang bertujuan untuk menutup celah kelemahan pada sistem autentikasi Jaringan *Wireless* menggunakan RADIUS

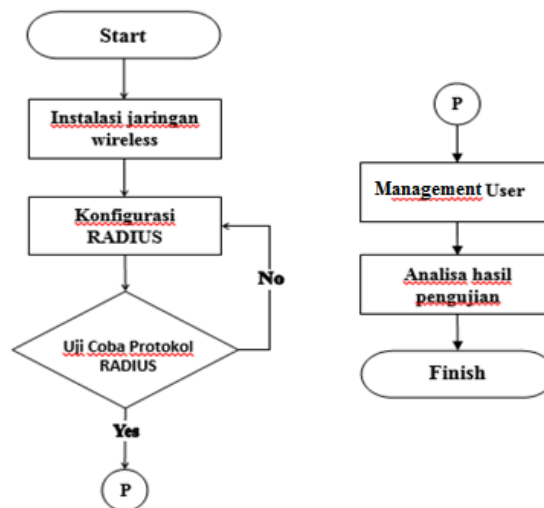
(Kunang & Ibadi, 2013). Penelitian lain berjudul “Perancangan Sistem Otentikasi RADIUS pada Pengguna Jaringan Wireless untuk Meningkatkan Keamanan Jaringan Komputer”. Model otentikasi yang digunakan yaitu PAP (*Password Authentication Protocol*) sehingga pengguna dapat mengakses jaringan Internet ketika sudah memiliki *username* dan *password* pada RADIUS server (Darmadi, 2018). Pada penelitian ini telah diimplementasikan protokol RADIUS

untuk melindungi dan melengkapi kinerja dari jaringan *wireless* LAN, sehingga diperoleh tingkat keamanan dan *rate* data yang baik serta dapat dimonitoring performanya. Implementasi protokol RADIUS dilakukan pada jaringan di PT. Baroka Taroka Santosa. Pada perusahaan tersebut saat ini belum memiliki jaringan *wireless* LAN dan sistem keamanannya, sehingga dimungkinkan pengguna yang setiap pengguna dapat masuk ke dalam jaringan tersebut.

2. Metode Penelitian

Beberapa tahapan pada penelitian ini meliputi: 1) analisis kebutuhan sistem; 2) persiapan kelengkapan kebutuhan sistem; 3) instalasi dan konfigurasi jaringan dan protokol RADIUS; 4) skenario pengujian

mendeteksi dan pencegahan serangan; 5) analisa dari hasil pengujian sistem. Proses-proses tersebut dapat dilihat pada Gambar 1.

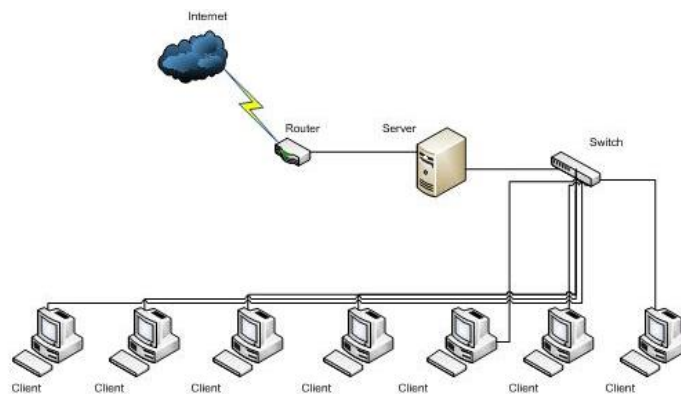


Gambar 1. Diagram alir penelitian

2.1 Analisis Jaringan

Jaringan saat ini pada awalnya merupakan sebuah titik akses langsung dihubungkan ke sebuah *switch*, dan *switch*

tersebut berhubungan dengan jaringan lokal *server* seperti pada Gambar 2.



Gambar 2. Topologi jaringan berjalan

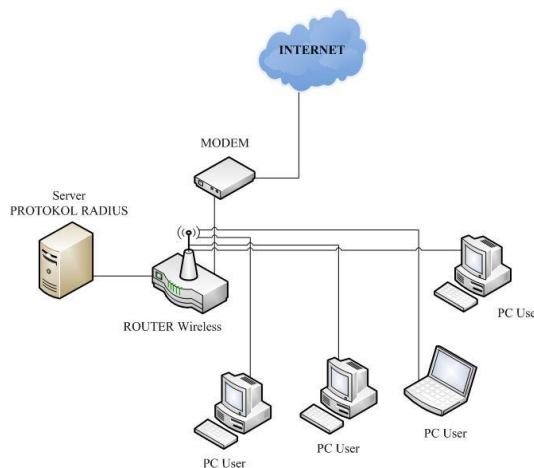
Beberapa permasalahan terjadi yang disebabkan oleh tidak ada sistem jaringan yang memadai, kurangnya keamanan pada proses pertukaran data antara divisi karena masih bergantung dengan sistem keamanan

yang diberikan *server*, tidak adanya media monitoring untuk pembatasan pengguna jaringan dalam area kerja, serta belum tersedianya jaringan *wireless* yang terklasifikasi.

2.2 Desain Jaringan Usulan

Beberapa pengembangan yang dilakukan yaitu, menambahkan jaringan *wireless* dengan memanfaatkan layanan dari protokol RADIUS yang menyediakan autentikasi *user*, otorisasi *user*, serta

penghitungan nilai *service* yang digunakan oleh *user*, dan membuat portal hotspot untuk memudahkan pengawasan pada setiap pengguna dengan topologi seperti Gambar 3.



Gambar 3. Topologi rancangan

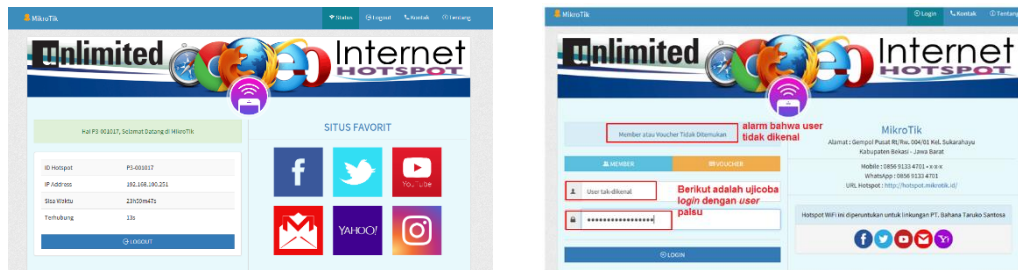
3. Hasil Pengujian

Pengujian pertama adalah melakukan login pada jaringan *wireless* ini dengan membuat kategori pengguna dengan

hak akses dan pengguna yang tidak memiliki hak akses klasifikasi *login user*. Prinsip ujicobanya adalah, saat ada

pengguna yang ingin terhubung atau mendapatkan koneksi internet harus terlebih dahulu melakukan *login* di portal atau laman *website* yang telah sinkron pada protokol RADIUS, dan proses itu disebut

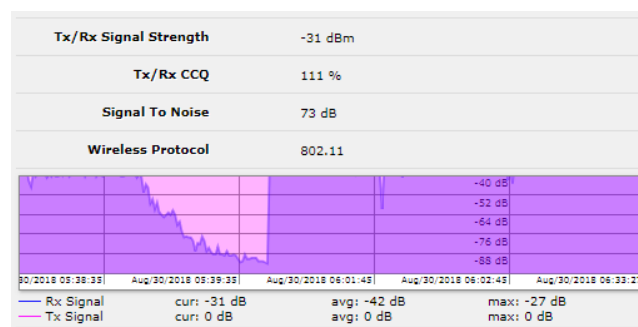
dengan AAA. Pada Gambar 4 ditampilkan hasil pengujian pada jaringan *wireless* (Hotspot) dengan *user* terdaftar dan *user* yang tidak terdaftar.



Gambar 4. Pengujian login dengan *user* terdaftar dan tidak terdaftar

Pada pengujian *wireless* tanpa RADIUS yang dilakukan yaitu berupa data monitoring *logging* sistem *resource* pada *server* terhadap serangan DoS yang

dilakukan sebelum menerapkan teknik RADIUS dengan menggunakan *tool* Vmstat.



Gambar 5. *Logging* sistem *resource* pada *server* Sebelum dilakukan serangan dos

Pada Gambar 5 merupakan monitoring *logging* sistem *resource* pada router *firewall* Mikrotik RouterOS 5.16 dalam keadaan normal sebelum dilakukan

serangan DoS menggunakan *tool* Torch untuk dijadikan pembanding *logging* sistem *resource* pada *server* saat terjadi serangan DoS.

```
[admin@MikroTik] > tool torch interface=ether1<INTERNET> ip-protocol=any
IP-PROTOCOL      TX          RX TX-PACKETS RX-PACKETS
tcp                3.3kbps    1056bps         2           2
icmp              784bps     784bps         1           1
                  4.1kbps    1840bps         3           3
[-] [Q quit|D dump|C-z continue]
```

Gambar 5. *Tool* Torch Mikrotik RouterOS 5.16

3.1 Perbandingan Data Hasil

Tabel 1. Merupakan data hasil pengujian yang telah dilakukan ini, yaitu

berupa data perbandingan *logging server* saat terjadi DoS *attack* dari tiga jenis pengujian

DoS *attack* sebelum dan sesudah *server* diimplementasi teknik RADIUS.

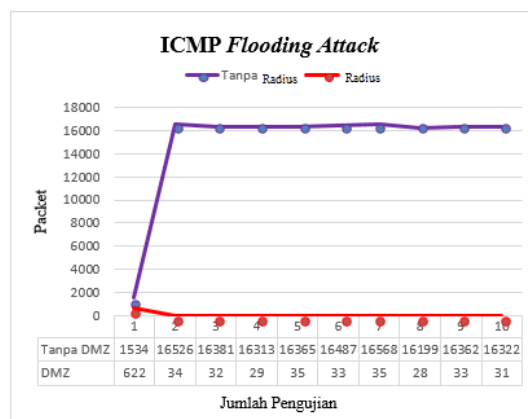
Tabel 1. Data perbandingan *logging server*
Hasil *Logging Sistem Resource server* pada *system in (Packet)*

No.	Packet ICMP flooding attack		Packet UDP flooding attack		Packet SYN flooding attack	
	Tanpa RADIUS (satuan bit)	RADIUS (satuan bit)	Tanpa RADIUS (satuan bit)	RADIUS (satuan bit)	Tanpa RADIUS (satuan bit)	RADIUS (satuan bit)
1.	1534	622	2066	616	2053	606
2.	16526	34	7582	35	7383	7681
3.	16381	32	7561	30	8109	7695
4.	16313	29	7613	75	7242	7802
5.	16365	35	7676	26	7374	7534
6.	16487	33	7771	29	7607	7319
7.	16568	35	7526	26	7410	7238
8.	16199	28	7638	29	7224	7143
9.	16362	33	7744	30	6861	7133
10.	16322	31	7656	28	7264	7126

4. Analisa Hasil dan Pembahasan

Pada Gambar 6 merupakan grafik perbandingan hasil *logging ICMP flooding attack* pada *server* tanpa RADIUS rata-rata menunjukkan jumlah *packet* yang diterima sebanyak 16391,4 *packet* dan rata-rata *packet* yang diterima saat RADIUS sebanyak 32,2 *packet*, sehingga didapatkan perbandingan penurunan jumlah *packet* saat

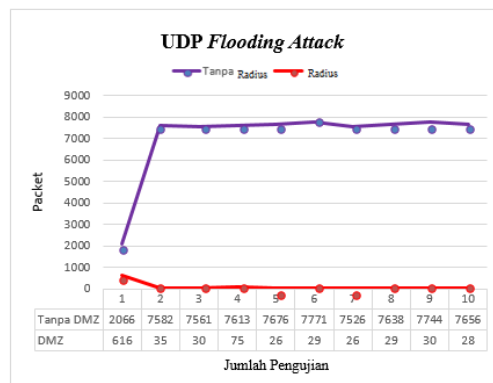
terjadi DoS *attack* sebesar 16359,2 *packet* setelah implementasi teknik RADIUS, artinya RADIUS berhasil melakukan *filter* sebesar 16359,2 *packet* pada DoS *attack* tersebut. Sebagai informasi data pengujian 1 (satu) tidak dihitung karena data tersebut bukan merupakan data yang *valid*.



Gambar 6. Grafik perbandingan ICMP flooding attack

Pada Gambar 7 merupakan grafik perbandingan hasil *logging UDP flooding attack* pada *server* tanpa RADIUS rata-rata menunjukkan jumlah *packet* yang diterima sebanyak 7640,7 *packet* dan rata-rata *packet* yang diterima saat RADIUS sebanyak 34,2 *packet*, sehingga didapatkan perbandingan penurunan jumlah *packet* saat

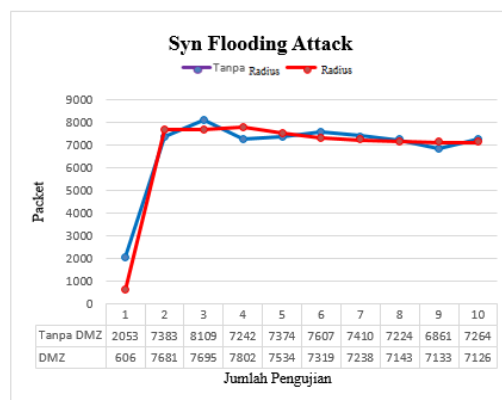
terjadi DoS *attack* sebesar 7606,5 *packet* setelah implementasi teknik RADIUS, artinya RADIUS berhasil melakukan *filter* sebesar 7606,5 *packet* pada DoS *attack* tersebut. Sebagai informasi data pengujian 1 (satu) tidak dihitung karena data tersebut bukan merupakan data yang *valid*.



Gambar 7. Grafik perbandingan UDP flooding attack

Pada Gambar 8 merupakan grafik perbandingan hasil *logging* Syn flooding attack pada server tanpa RADIUS rata-rata menunjukkan jumlah *packet* yang diterima sebanyak 7386 *packet* dan rata-rata *packet* yang diterima saat RADIUS sebanyak 7407,8 *packet*, sehingga didapatkan perbandingan jumlah *packet* yang hampir

sama pada server sebelum dan setelah implementasi teknik RADIUS, artinya RADIUS tidak berhasil melakukan filter pada jenis DoS Syn flooding attack tersebut karena server masih terkena flooding. Sebagai informasi data pengujian 1 (satu) tidak dihitung karena data tersebut bukan merupakan data yang valid.



Gambar 8. Grafik perbandingan syn flooding attack

5. Kesimpulan

Berdasarkan implementasi dari protokol RADIUS maka dapat diambil kesimpulan bahwa protokol RADIUS dapat melakukan otentikasi user melalui serangkaian komunikasi antara client dan

server. Rekaman accounting akses internet terdokumentasi secara baik dan realtime pada database server RADIUS.

Referensi

Darmadi, E. A. (2018). *Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless*. 2(3), 9–16.

Gaol, E. B. L., & Pramarta, C. R. A. (2012). *Implementasi dan Analisis Autentikasi Jaringan Wireless Menggunakan Metode Extensible Authentication Protocol Transport*

- Layer Security*. Jurnal Ilmu Komputer. Haerudin, D. I., Aksara, L. M. B., & Yamin, M. (2017). *Implementasi Wireless Distribution System Pada Hostspot*. SemanTIK, 3(2), 105–112.
- Hidayat, R. N. (2015). *Implementasi Tomato Firmware Pada Linksys Wireless Router Dengan Proses Authentication , Authorization , Accounting*. 2010(Snati), 51–55.
- Kunang, Y. N., & Ibadi, T. (2013). *Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS*. SNATI, 34(2), 1907–5022.
- Kuswanto, H. (2017). *Sistem Autentikasi Hotspot Menggunakan Radius Server Mikrotik Router*. Informatics for Educators and Professionals, 2(1), 234369.
- Rumalutur, S. (2014). *Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong*. Jurnal Teknologi Dan Rekayasa, 19(100), 48–60.
- Setiawan, R., Jazuli, A., Listyorini, T., Sari, R., & Widodo, A. (2012). *Implementasi Protokol Radius Untuk IEEE 802 . 11 Wireless Pada SMK Muhammadiyah Kudus*. 5, 7–13.
- Stiawan, D., & Rini, D. P. (2009). *Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS pada Jaringan Publik Wireless Hotspot*. Seminar Nasional Electrical, Informatics, and IT'S Educations, 1–5.
- Supriadi, D., Fahmi, H., & Imtihan, K. (2018). *Analisa Dan Perancangan Infrastruktur Jaringan Wireless Local Area Network (Wlan) Pada Dinas Perindustrian Dan Perdagangan Kabupaten Lombok Tengah*. Jurnal Informatika Dan Rekayasa Elektronik, 1(2), 1. <https://doi.org/10.36595/jire.v1i2.53>