Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 340-347
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

MENGAMANKAN SERANGAN PACKET SNIFFING PADA JARINGAN KOMPUTER MENGGUNAKAN VPN TUNNEL

Rezi Elsya Putra[1], Nizwardi Jalinusl[2], Rijal Islami[3], Mohd. Iqbal[4]

[1]Teknik Informatika, Sekolah Tinggi Ilmu Komputer Muhammadiyah Batam, Batam, Kepulauan Riau
[2]Pendidkan Teknologi Kejuruan, Universitas Negeri Padang, Jl. Prof. Dr. Hamka, Padang, Sumatera Barat
[3]Pendidkan Teknologi Kejuruan, Universitas Negeri Padang, Jl. Prof. Dr. Hamka, Padang, Sumatera Barat
[4]Teknik Informatika, Sekolah Tinggi Ilmu Komputer Muhammadiyah Batam, Batam, Kepulauan Riau
[5]SMA Negeri 7 Solok Selatan, Solok Selatan, Sumatera Barat
Email: [1]rezielsyaputra91@gmail.com, [2]jnizwardi228@gmail.com, [3]rijal_a@ft.unp.ac.id, [4]rnpanay@gmail.com
Email Penulis Korespondensi: rezielsyaputra91@gmail.com

Article History:
Received Jun 12th, 202x
Revised Aug 20th, 202x
Accepted Aug 26th, 202x

Abstrak

Perkembangan teknologi sangat mempengaruhi dan mengontrol aktivitas kita dalam sehari-hari. Perkembangan Teknologi diikuti dengan zamannya Revolusi Industri 4.0. Dalam penggunaan teknologi ini tidak sedikit terjadinya ancaman, maka dibutuhkan sebuah jaringan komputer yang memadai dan terjaga keamannanya yang menjadi prioritas, seperti serangan packet sniffing. Dalam pengiriman data dalam suatu jaringan sangat penting untuk menjamin kerahasiaan data yang akan di kirim agar tidak jatuh ke tangan pihak ke tiga. Maka Pelitian ini memiliki tujuan untuk mengamankan serangan packet sniffing pada jaringan komputer menggunakan vpn tunnel. Hasil penelitian vpn tunnel dapat di gunakan untuk mengamakan packet sniffing dari serangan dan ancaman pada jaringan komputer yang tepat.

Kata Kunci : Packet Sniffing, Jaringan Komputer, VPN Tunnel, Serangan

Abstract

Abstract

Technological developments greatly affect and control our daily activities. Technological developments were followed by the era of the Industrial Revolution 4.0. In the use of this technology there are not a few threats, so we need an adequate and secure computer network that is a priority, such as packet sniffing attacks. In sending data in a network it is very important to ensure the confidentiality of the data to be sent so that it does not fall into the hands of third parties. So this research has the goal of securing packet sniffing attacks on computer networks using a VPN tunnel. The results of VPN tunnel research can be used to secure packet sniffing from attacks and threats on the right computer networks

Keyword : *Packet Sniffing, Computer Networks, VPN Tunnels, Attack*

1. PENDAHULUAN

Perkembangan teknologi saat ini sangat pesat, kita menggunakan teknologi dalam kegiatan kita sehari-hari contohnya internet, internet saat ini sangat dibutuhkan terutama dalam kaitannya dengan komunikasi [1]. Dengan meningkatnya jumlah pengguna Internet, masalah keamanan terus menjadi faktor penting dalam jaringan computer [2][3]. Dengan banyaknya komputer yang saling terhubung dan pesatnya perkembangan yang disebut jaringan komputer, muncul teknologi baru, yaitu teknologi yang menghubungkan komputer di dunia menjadi satu sehingga memungkinkan terjadinya pertukaran informasi dan data. bahkan saling berkomunikasi dan bertukar informasi. Informasi berupa gambar atau video [4].Keamanan saat mengirim dan menerima informasi sangat penting untuk memastikan bahwa informasi yang dikirim aman dan tidak bocor ke pihak ketiga, terutama bila informasi tersebut bersifat rahasia. . Oleh karena itu, penerapan metode keamanan informasi di Internet sangat penting. Banyak metode yang bisa diterapkan seperti *Tunneling* [5].

VPN dibutuhkan untuk dapat melakukan koneksi dial upterhadap proses komunikasi. PPTP bekerja dengan sebuah serveryang dapat berfungsi sebagai penghubung antar komputer yang dapat diketahui sebagai client, baik komputer yang berada di wilayah pusat maupun komputer yang berada di wilayah cabang [6][7]. Virtual Private Network (VPN)

adalah teknologi komunikasi jaringan yang memungkinkan Anda terhubung ke jaringan publik dan melaluinya ke jaringan lokal, memberi Anda hak dan pengaturan yang sama seperti di jaringan lokal itu sendiri, meskipun sebenarnya Anda menggunakan jaringan public [8]. VPN adalah teknologi komunikasi yang memungkinkan Anda terhubung ke jaringan publik dan menggunakannya untuk terhubung ke jaringan lokal. Ini memberi Anda hak dan peraturan yang sama seperti di kantor atau online, meskipun Anda menggunakan jaringan public [9][10].

Dalam arti tertentu, sniffing berarti mengintai, sementara dalam keamanan jaringan, mengintai menangkap paket data yang bergerak di sekitar jaringan. Sniffing itu sendiri biasanya digunakan untuk mencuri informasi penting seperti kata sandi, badan email, dan transfer file dari jaringan. Sniffing biasanya menyerang protokol seperti Telnet, HTTP, POP, IMAP, SBM, FTP dan lain-lain. Dalam metode peretasan, pengintaian dibagi menjadi dua bagian: pengintaian pasif dan pengintaian aktif [11][12]. Keamanan jaringan adalah jenis keamanan informasi yang tidak terlihat secara fisik tetapi memainkan peran penting dalam menjaga keamanan jaringan suatu sistem [13].

Sekolah Tinggi Ilmu Komputer Muhammadiyah Merupakan sebuah perguruan tinggi yang bergerak di bidang pendidikan pada level sekolah tinggi bidang ilmu komputer. Sekolah Tinggi Ilmu Komputer Muhammadiyah Batam memiliki beberapa gedung yang dimana pengolahan data menggunakan jaringan *internet*. Pusat jaringan yang ada di Sekolah Tinggi Ilmu Komputer Muhammadiyah Batam terpusat di gedung biro yang menghubungkan beberapa gedung. Jaringan *internet* di Sekolah Tinggi Ilmu Komputer Muhammadiyah Batam bisa di akses oleh mahasiswa dan dosen dengan bebas. Kelamahan yang terdapat tidak bisa tercegahnya data yang dikirim bisa di sadap oleh orang yang ada di dalam jaringan itu sendiri [14]. Dengan menerapkan keamanan dengan vpn tunnel bisa mengatasi permasalahan tersebut. Dimana VPN masih digunakan saat ini [15][16]Tapi dengan segalanya Internet juga memiliki kelebihan kelemahan Mudah untuk menggunakan internet semua orang melakukannya tidak Pasti akan membagikan info ini sifat rahasia. Selain itu, ada banyak dari mereka aplikasi baru yang bisa menyampaikan berita dengan sangat mudah, yang tidak dilakukan oleh peretas bertanggung jawab [17][18].

2. METODOLOGI PENELITIAN

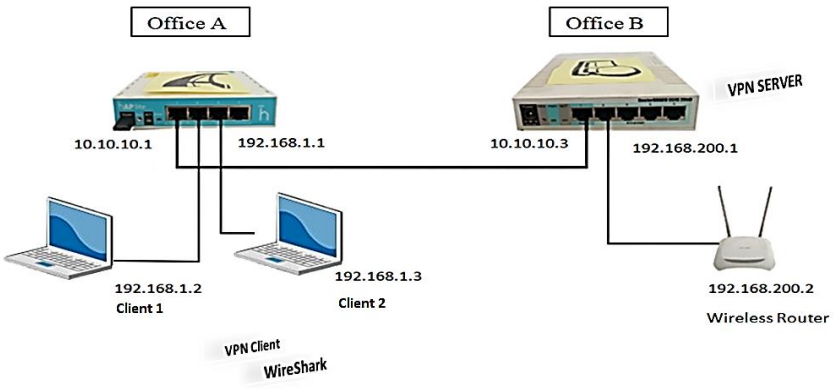
2.1 Tahapan Penelitian

Untuk mempermudah pemahaman dalam melakukan penelitian dan untuk menjelaskan sebuah permasalahan penulis membuat sebuah kerangka pemikiran atau alur penelitian sebagai berikut dapat dilihat pada Gambar 1:

Gambar 1. Flowchart Diagram Alur

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 340-347
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

2.2 Topologi Statik Router



Gambar 2. Topologi Statik Router

Ada 2 Mikrotik dimana Mikrotik A dipakai sebagai office A dan Mikrotik B sebagai office B, dimana office A mempunyai Ip Address 10.10.10.1 dan bridge di eth2 dan eth3 dengan Ip 192.168.1.1 dan ada 2 laptop dengan masing-masing Ip 192.168.1.2 dan Ip 192.168.1.3. Di office B dengan Ip Address 10.10.10.3 dan Ip 192.168.200.1 di eth2. Ada perangkat Wereless Router dengan Ip 192.168.200.2.

2.3 Pengalamatan IP Address

Berikut adalah pengalamatan Ip yang digunakan seperti yang bisa dilihat di Tabel 1:

Tabel 1. Ip Address yang digunakan

No	Komponen	Ip	Ket
1	Mikrotik A	10.10.10.1	Ether 1
2	Bridge	192.168.1.1	Ether 2 dan ether 3
3	Client 1	192.168.1.2	Wireshark, VPN Client
4	Client 2	192.168.1.3	Wireshark, VPN Client
5	Mikrotik B	10.10.10.3	Ether 1
6	Mikrotik B	192.168.200.1	Ether 2
7	Wireless Router	192.168.200.2	

3. HASIL DAN PEMBAHASAN

Sebelum masuk dan melakukan konfigurasi ke sistem, terlebih dahulu digunakan aplikasi WinBox untuk me-remote Router. Penggunaan aplikasi WinBox membutuhkan alamat IP Router, IP User berserta Password dari Router yang akan di remote, dan setelah melakukan konfigurasi diketahui IP Router adalah 10.10.10.1. Banyaknya komponen yang terdapat dalam MikroTik Router sehingga perlu dilakukan observasi lokasi dimana letak informasi yang dapat digunakan sebagai bukti digital. Dalam penelitian ini, tahapan observasi dan pemetaan Router dilakukan melalui CLI (Command Line Interface). Menu utama Router pada Terminal CLI. Setelah melakukan Observasi pada Router diketahui terdapat banyak menu dan submenu dalam jaringan MikroTik Router. Selanjutnya untuk keperluan menganalisa serangan Packet Sniffing.

3.1 Proses Observasi pada Mikrotik Router

Komponen Router yang bisa digunakan dan berpotensi dijadikan sebagai barang bukti digital dari Router adalah IP Address List, PPTP, Router list, Bridge, Firewall, ARP List, Router Version, Log Aktivity, user. Berikut adalah komponen-komponen isi Router pada menu dan submenu WinBox yang bisa digunakan dalam proses penarikan data forensik, dapat dilihat pada Tabel 2.

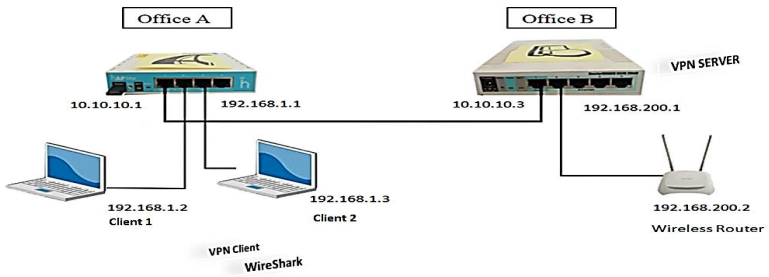
Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 340-347
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

2 Komponen-Komponen Winbox

No	Komponen	Lokasi
1	Log Akses	/log
2	Log Aktivity	/log
3	Pengguna	/User
4	IP Address List	/Ip/address
5	Mac Address Client	/ip/arp
6	Router Version	/System/resource
7	ARP	/ip/arp
8	PPTP	/bridge

3.2 Perancangan Skenario Pengujian Serangan Sniffing

Ada 2 Mikrotik dimana Mikrotik A dipakai di office A dan Mikrotik B sebagai office B, Office A mempunyai Ip Address 10.10.10.1 dan bridge di eth2 dan eth3 dengan Ip 192.168.1.1 dan ada 2 laptop sebagai berikut: laptop yang digunakan sebagai Client 1 dengan Ip 192.168.1.2 dan laptop yang digunakan sebagai Client 2 dengan Ip 192.168.1.3. Untuk Office B dengan Ip Address 10.10.10.3 dan Ip 192.168.200.1 di eth2 ada perangkat Wireless Router dengan Ip 192.168.200.2 dapat dilihat pada Gambar 3.



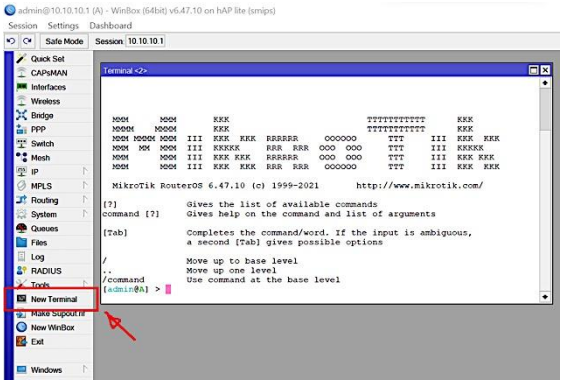
Gambar 3. Simulasi serangan Sniffing

4.1. Implementasi Serangan Sniffing

Konsep simulasi serangan Sniffing, yaitu penyerang akan mengirimkan data secara terus-menerus atau memanfaatkan kelemahan sistem dengan memaksa kapasitas pemprosesan yang berakibat sistem tidak lagi beroperasi secara normal yang merupakan tipe serangan menggunakan Protocol TCP, UDP atau ICMP.

4.3.1 Pengujian Settingan Ip Address

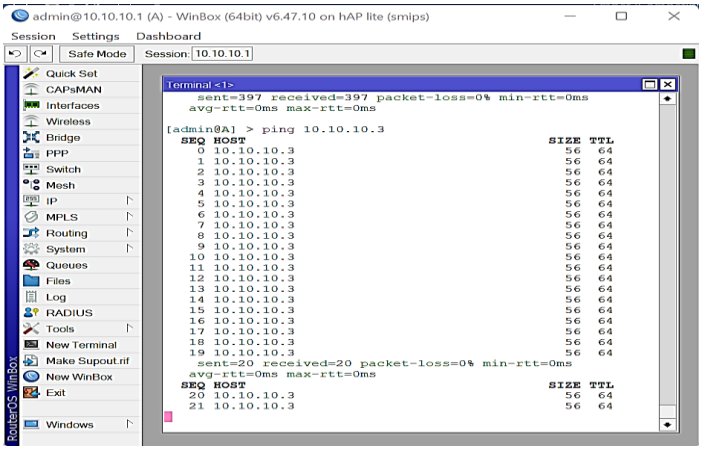
Untuk mengetahui apakah Settingan Ip terkoneksi maka kita lakukan pengetesan dengan membuka menu New Terminal lalu melakukan Ping test ke alamat yang dituju, seperti Gambar 4:



Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 340-347
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

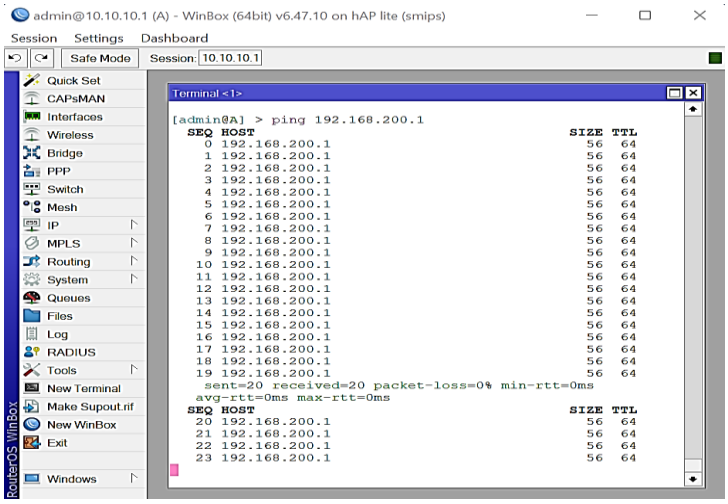
Gambar 4. New Terminal

Gambar 5 memastikan Mikrotik A sudah terkoneksi di Mikrotik B.



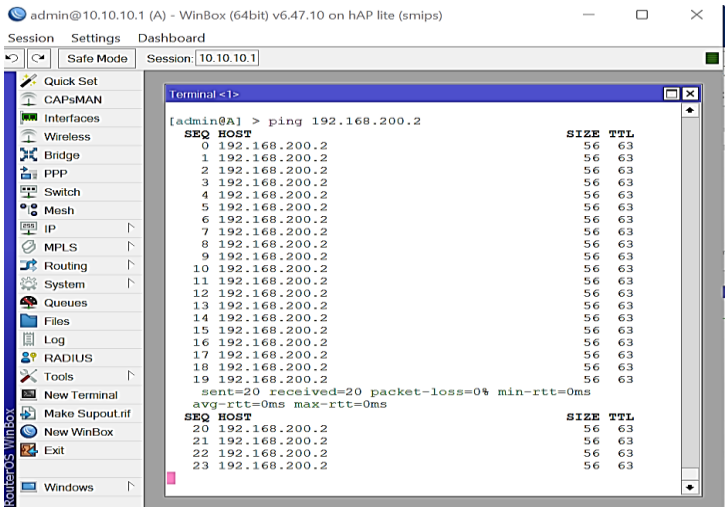
Gambar 5. Mikrotik A terkoneksi di Mikrotik B

Gambar 6 memastikan Mikrotik A sudah terkoneksi di Ether 2 Mikrotik B.



Gambar 6. Mikrotik A terkoneksi di Ether 2 Mikrotik B.

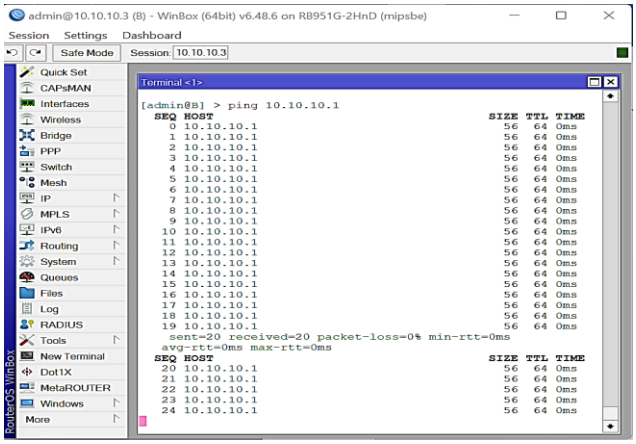
Gambar 7 memastikan Mikrotik A sudah terkoneksi di Wireless Router (Mikrotik B).



Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 340-347
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

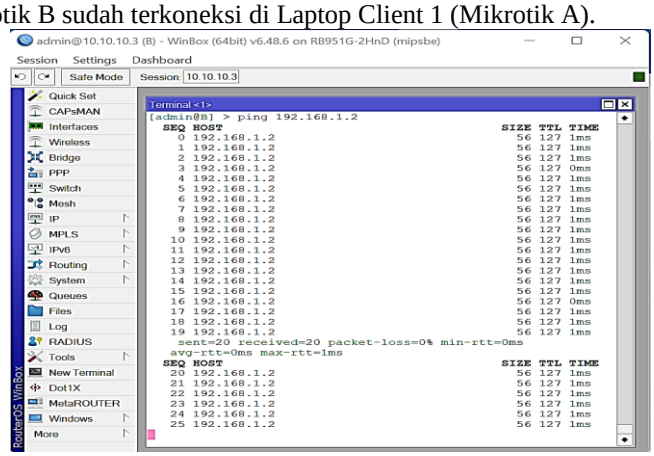
Gambar 7. Mikrotik A terkoneksi di Wireless Router (Mikrotik B)

Gambar 8 memastikan Mikrotik B sudah terkoneksi di Mikrotik A.



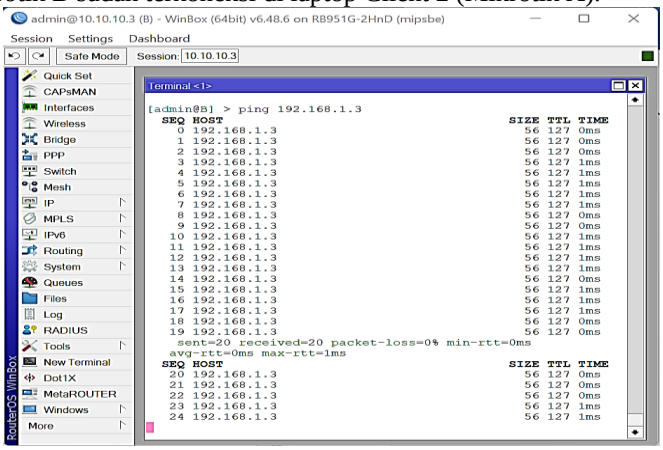
Gambar 8. Mikrotik B terkoneksi di Mikrotik A

Gambar 9 memastikan Mikrotik B sudah terkoneksi di Laptop Client 1 (Mikrotik A).



Gambar 9. Mikrotik B terkoneksi di Laptop Client 1 (Mikrotik A)

Gambar 10 memastikan Mikrotik B sudah terkoneksi di laptop Client 2 (Mikrotik A).

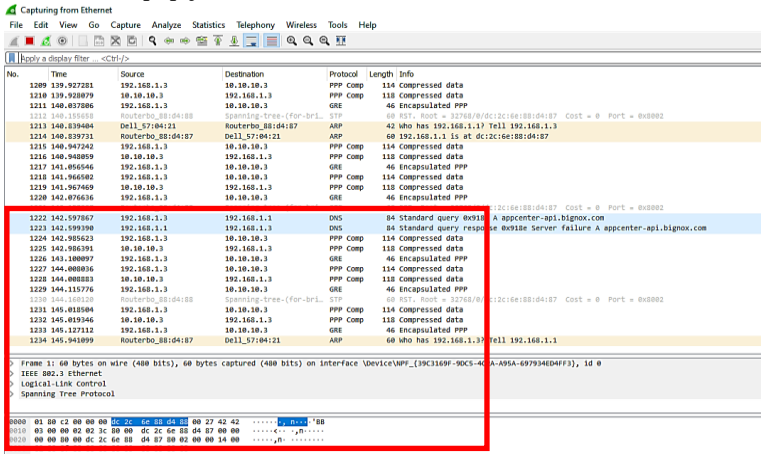


Gambar 10. Mikrotik B terkoneksi di laptop Client 2 (Mikrotik A)

4.3.2 Hasil Pengujian

Setelah dilakukan pengujian settingan Ip Address, maka berikutnya dilakukan pengujian jaringan dengan menggunakan Wireshark. Pertama-tama buka aplikasi Wireshark yang sudah di install pada computer, Kemudian capture dan tentukan interface, Selanjutnyaklik *start*. Untuk hasil sniffing real time menggunakan Wireshark dengan VPN, dimana ping test dari laptop Client 2 dengan IP 192.168.1.3 ke Wireless Router dengan IP 192.168.200.2 tidak dapat terdeteksi, seperti pada Gambar 11.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 340-347
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index



Gambar 11. Routing dengan VPN

4. KESIMPULAN

Selama proses penelitian serta melakukan simulasi serangan Sniffing pada menganalisa data yang terdeteksi, maka dapat disimpulkan dari penelitian ini yaitu :

a. Pada Implementasi VPN Tunnel berbasis Mikrotik dapat digunakan kapan saja dibutuhkan.untuk menjaga kerahasiaan data.
b. Dengan menggunakan VPN Tunnel aktivitas lalu lintas data tidak dapat terlihat dan sehingga dapat terhindar atau mengurangi dari pencurian data (Sniffing).

DAFTAR PUSTAKA

[1] Erawati, Wati, And Sujiliani Heristian. "Implementasi Virtual Private Network (VPN) Menggunakan Protokol PPTP Mikrotikrouter Pada Yayasan Muhamadiyah Parung." *Jurnal Teknik Informatika* 4.1 (2018): 28-32.

[2] WATMAH, SRI WATMAH. "Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang." *INSANTEK-Jurnal Inovasi Dan Sains Teknik Elektro* 1.1 (2020): 6-12.

[3] Rahino, Bayu Gagat, And Atang Susila. "Implementasi Jaringan VPN (L2TP/Ipsec) Mikrotik Untuk Remote Access Sebagai Security Selama Work From Home." *OKTAL: Jurnal Ilmu Komputer Dan Sains* 1.11 (2022): 1911-1918.

[4] Ismail, Mohd Nazri. "Analysis Of Secure Real Time Transport Protocol On Voip Over Wireless LAN In Campus Environment." *International Journal On Computer Science And Engineering (IJCSE)* 2.02 (2010): 898-902.

[5] Albar, Ahmad Rinaldi, Alex Wijaya, And Hutrianto Hutrianto. "Analisis Keamanan Jaringan Dengan Endekatan Protokol Authentication Header (Ah) Dan Encapsuating Securtiy Payload (Esp) Tunneling Studi Kasus Universitas Muhammadiyah Palembang." *Bina Darma Conference On Computer Science (BDCCS)*. Vol. 3. No. 1. 2021.

[6] Alfarizi, Nauval, Tengku Mohd Diansyah, And Risko Liza. "Simulasi Pengamanan Virtual Server Menggunakan Dionaea Honeypot Dan Tunneling Sebagai Proses Pengamanan Komunikasi Data." *SNASTIKOM* 1.01 (2022): 41-48.

[7] M. Noviansyah And H. Saiyar, "Pencegahanpacket Sniffing Menggunakan Metode Vpn Tunnel Untuk Keamanan Jaringan Komputer Berbasis Mikrotik," Vol. 6, No. November, P. 6, 2021

[8] Supendar, Hendra. "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik." *Bina Insani ICT Journal* 3.1 (2016): 85-98.

[9] Mufida, Elly, Dedi Irawan, And Giatika Chrisnawati. "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta." *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer* 16.2 (2017): 9-19.

[10] Budi Santoso, Rizki. Perbandingan Kinerja Jaringan Vpn Berbasis Mikrotik Menggunakan Protokol Pptp Dan L2tp Sebagai Media Transfer Data. Diss. Universitas Muhammadiyah Jember, 2019.

[11] Agustiara, Windi, Ade Pratama, And Satrio Junaidi. "Analisis Keamanan Protokol Secure Socket Layer Terhadap Serangan Packet Sniffing Pada Website Portal Berita Harian Umum Koran Padang." Jtik *(Jurnal Teknik Informatika Kaputama)* 6.1 (2022): 10-15.

[12] Nugroho, Irwan, Bebas Widada, And Kustanto Kustanto. "Perbandingan Performansi Jaringan Virtual Private Network Metode Point To Point Tunneling Protocol (PPTP) Dengan Metode Internet Protocol Security." *Jurnal Teknologi Informasi Dan Komunikasi (Tikomsin)* 3.2 (2015).

[13] Mulyanto, Yudi, And Akbar Algi Fari. "Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration Testing (Studi Kasus: Smk Negeri 2 Sumbawa)." *Jurnal Informatika Teknologi Dan Sains* 4.3 (2022): 145-155.

[14] Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains Dan Manajemen*, *8*(1).

[15] Ikhwan, Syariful, And Ahya Amalina. "Analisis Jaringan VPN Menggunakan PPTP Dan L2TP." *Jurnal Infotel* 9.3 (2017): 265-270.

[16] Farly, Kaseger Arthur, Xaverius BN Najoan, And Arie SM Lumenta. "Perancangan Dan Implementasi Vpn Server Dengan Menggunakan Protokol Sstp (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi." *Jurnal Teknik Informatika* 11.1 (2017).

[17] Audrey, Berby Febriana. "Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik: Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik." *Journal Of Network And Computer Applications (ISSN: 2964-6669)* 1.1 (2022): 1-8.

[18] Alviendra, Ilmalik Muhammad, Eko Setijadi, And Gatot Kusrahardjo. "Pengembangan Dan Penerapan Sistem Virtual Private Network (VPN) Pada Internet Of Things (IOT) Menggunakan Simulasi." *Jurnal Teknik ITS* 11.1 (2022): A15-A22.