Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 3 July 2024, pp: 943-954
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Analysis Network Security Based Point to Point Protocol Over Ethernet (PPPoE) Using Mikrotik

Analisis Keamanan Jaringan Berbasis Point to Point Protocol Over Ethernet (PPPoE) Menggunakan Mikrotik

Linna Oktaviana Sari[1], Ery Safrianti[2], Defvi Wahyuningtias[3*]

[1,3]Program Studi Teknik Informatika, Universitas Riau, Indonesia
[2]Program Studi Teknik Elektro, Universitas Riau, Indonesia

E-Mail: [1]linnaoasari@lecturer.unri.ac.id, [2]esafrianti@eng.unri.ac.id,
[3]defvi.wahyuningtias4596@student.unri.ac.id

Received Feb 28th 2024; Revised May 11th 2024; Accepted May 20th 2024
Corresponding Author: Defvi Wahyuningtias

Abstract

Network security is the process of actions to protect the network to avoid various types of attacks and data breaches, such as preventing cyber attacks, access control, detecting malicious software and other security measures. LAN networks have a protocol called Address Resolution Protocol (ARP). ARP is a protocol that is very vulnerable to exploitation, because any computer can provide manipulated ARP transaction packets. This vulnerability is exploited for a type of attack commonly called ARP spoofing. To secure the local network from ARP Spoofing attacks, a security mechanism is needed to minimize the risk of exploitation of communication protocols in the network. Therefore, in this research, a PPPoE-based network security analysis was carried out using Mikrotik as the right solution to overcome network security problems better. To determine the performance of PPPoE in terms of security, testing was carried out with ARP spoofing attacks using the netcut tools. Testing was carried out before and after implementing PPPoE with the result that before implementing PPPoE information was obtained regarding the IP address, MAC address and device name of the connected user so that cut-off could be carried out. Meanwhile, after implementing PPPoE, users connected to the PPPoE network were not detected so cut-off could not be carried out.

Keyword: ARP, Mikrotik, Network Security, PPPoE, Spoofing

Abstrak

Keamanan jaringan adalah proses tindakan untuk melindungi jaringan untuk menghindari berbagai jenis serangan dan pelanggaran data, seperti mencegah serangan *cyber*, kontrol akses, mendeteksi perangkat lunak berbahaya dan tindakan keamanan lainnya. Jaringan LAN memiliki protokol yang disebut *Address Resolusi Protocol* (ARP). ARP merupakan protokol yang sangat mudah untuk dieksploitasi karena paket transaksi ARP dapat dimanipulasi oleh komputer manapun. Serangan ARP *spoofing* dapat dieksploitasi pada kerentanan ini. Untuk mengamankan jaringan lokal dari serangan ARP *Spoofing*, diperlukan mekanisme keamanan yang dapat meminimalkan risiko eksploitasi protokol komunikasi dalam jaringan. Maka pada penelitian ini dilakukan analisa keamanan jaringan berbasis PPPoE dengan menggunakan Mikrotik sebagai cara terbaik untuk mengatasi permasalahan keamanan jaringan. Untuk mengetahui performa PPPoE dari segi keamanan, dilakukan pengujian dengan serangan ARP *spoofing* menggunakan *tools netcut*. Pengujian dilakukan sebelum dan sesudah penerapan PPPoE dengan hasil sebelum penerapan PPPoE diperoleh informasi mengenai alamat IP, alamat MAC dan nama perangkat pengguna yang terhubung sehingga dapat dilakukan *cut-off*. Sedangkan setelah penerapan PPPoE, pengguna yang terhubung ke jaringan PPPoE tidak terdeteksi sehingga *cut-off* tidak dapat dilakukan.

Kata Kunci: ARP, Keamanan Jaringan, Mikrotik, PPPoE, Spoofing

1. PENDAHULUAN

Teknologi informasi saat ini mengalami kemajuan yang sangat pesat, hal ini memberikan pengaruh terhadap setiap aspek kehidupan masyarakat dalam melakukan aktivitas, baik itu pekerjaan, pendidikan, bahkan mencari informasi pada saat ini membutuhkan peran serta teknologi informasi. Semakin bertambahnya teknologi-teknologi yang terbaru sekarang ini, mengakibatkan kebutuhan akan jaringan komputer menjadi semakin meningkat, baik yang bersifat publik maupun pribadi. Proses pertukaran data yang awalnya hanya

menggunakan dokumen, hardcopy berupa tulisan tangan, sekarang menjadi komunikasi yang menggunakan jaringan komputer dikarenakan lebih efisien.

Jaringan lokal merupakan salah satu jenis jaringan komputer yang hanya mencakup wilayah lokal tertentu atau terbatas seperti area sekolah, perkantoran, cafe, rumah pribadi dan yang lainnya [1]. Keamanan jaringan diperlukan untuk berbagi data di jaringan komputer lokal. Keamanan jaringan merupakan langkah-langkah untuk melindungi jaringan agar terhindar dari berbagai macam serangan dan pelanggaran data, seperti mencegah serangan *cyber*, kontrol akses, mendeteksi perangkat lunak berbahaya dan tindakan keamanan lainnya[2]. Keamanan jaringan sudah pasti sangat dibutuhkan seiring meningkatnya ilmu-ilmu tentang *hacking*. Semakin banyak akses ke jaringan menyebabkan meningkatnya peluang kejahatan. *Sniffing, spoofing*, serangan *Man-in-the-Middle*, *Distributed Denial of Service* (DDoS), dan kejahatan dunia maya lainnya bisa sangat berbahaya jika terjadi di jaringan komputer [3].

Kehilangan data, kerusakan pada perangkat komunikasi, dan peretas yang dapat menonaktifkan sumber daya jaringan yang bersangkutan adalah kemungkinan akibat dari kejahatan. Perangkat lunak ataupun *tools-tools* yang digunakan oleh *attacker* untuk menyusup suatu jaringan juga semakin bervarian. Akibatnya, serangan terhadap jaringan komputer dapat terjadi kapan saja dan berdampak buruk pada pengguna jaringan karena penyerang dapat memperoleh data target secara illegal [4].

Terdapat protokol yang disebut *Address Resolusi Protocol* (ARP) pada jaringan LAN. Mengubah alamat IP menjadi alamat MAC adalah fungsi ARP [5]. Setiap komputer yang akan berkomunikasi selalu melakukan transaksi terkait antara IP *address* dan MAC *address.* ARP adalah protokol yang sangat rentan untuk dieksploitasi, karena kemungkinan setiap komputer memberikan paket transaksi ARP palsu [6]. Kelemahan ini digunakan untuk melancarkan serangan yang dikenal dengan nama spoofing ARP. ARP *spoofing* adalah serangan yang bisa mengubah atau memblokir lalu lintas di jaringan lokal dengan mengendus *frames* data melalui media kabel atau jaringan area lokal nirkabel (WLAN) [7]. *Tools* yang bisa digunakan untuk melancarkan serangan yang memanfaatkan eksploitasi dari protokol tersebut yaitu *NetCut.* Untuk mengamankan jaringan lokal dari serangan *ARP Spoofing*, langkah-langkah keamanan diperlukan untuk mengurangi kemungkinan eksploitasi protokol komunikasi jaringan[8].

Oleh karena itu, pada penelitian ini dilakukan sebuah pengamanan pada jaringan lokal dengan memanfaatkan salah satu fitur pada Mikrotik [9]. Fitur tersebut yaitu *Tunneling,* dimana proses *tunneling* ini berbasis protokol IP. *Tunneling* merupakan sebuah proses transfer data yang dikirim akan di-*encaptulation* atau dibungkus oleh protokol lain. Untuk dapat melakukan pembungkusan suatu paket data, bisa dengan menggunakan protokol yang khusus dirancang untuk melakukan *tunneling* [10]. Pada penelitian ini yang akan digunakan adalah *Point to Point Protocol Over Ethernet* (PPPoE).

PPPoE membuat koneksi antar *frame* jaringan, membatasi akses ke internet untuk pengguna karena hanya yang memiliki *username* dan *password* yang bisa melakukan *login* pada jaringan [11]. Disamping itu, PPPoE akan menyembunyikan MAC *Address* dari host pada jaringan, yang membuat host lain tidak bisa menjalankan *tools* untuk melakukan serangan pada jaringan. Hal tersebut dilakukan untuk menghindari adanya gangguan pada jaringan yang disebabkan oleh penyusup yang berusahan memutus jaringan dan menyalahgunakan jaringan tersebut [12]. PPPoE adalah cara tepat untuk mengatasi masalah keamanan jaringan.

Sejumlah penelitian tentang PPPoE telah dilakukan, seperti yang tercantum di bawah ini. Analisis Pemanfaatan PPPoE penelitian yang dilakukan oleh [12] yang menggali lebih dalam fitur dan keunggulan PPPoE, khususnya terkait keamanan dan kerahasiaan data. Temuan penelitian ini menunjukkan seberapa efektif pemanfaatan PPPoE dalam melindungi transmisi data.

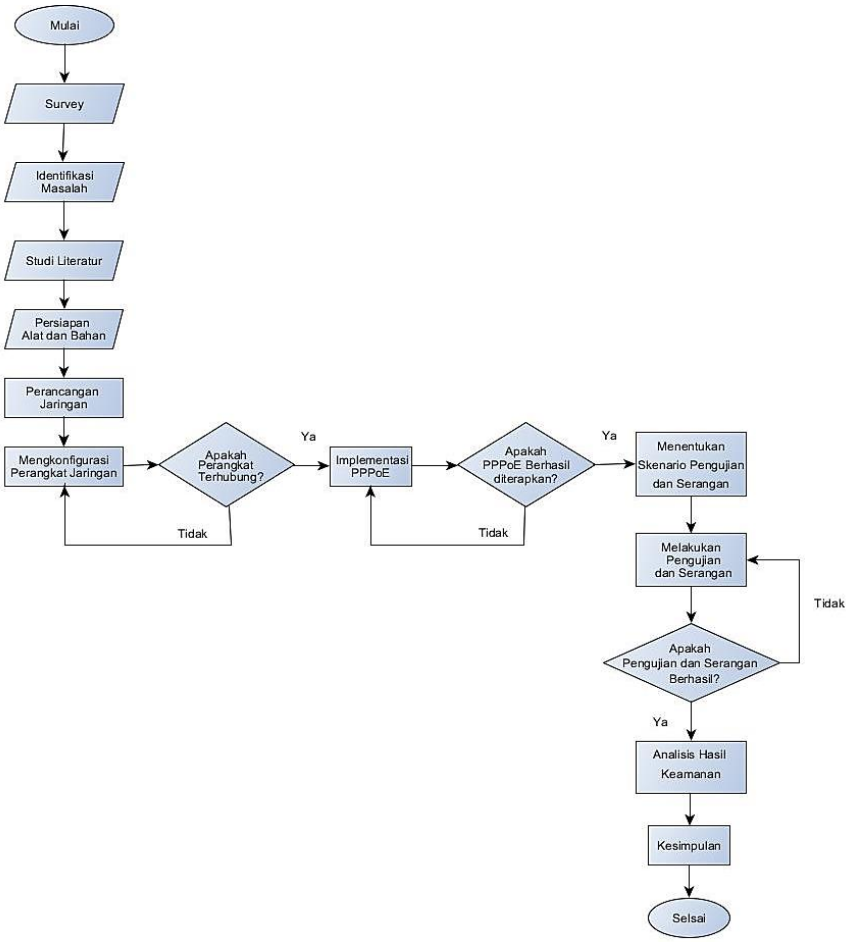
Penelitian yang dilakukan [13] mengenai analisia *Quality of Service* (QoS) terhadap kinerja PPPoE. Untuk menguji kualitas PPPoE, dalam penelitian ini digunakan ping untuk mengirimkan paket ICMP dengan muatan paket yang berbeda. Penelitian tentang kinerja PPPoE pada mikrotik juga dilakukan oleh [14]. Qos digunakan dalam pengujian kinerja PPPoE pada penelitian ini, yang menunjukkan keunggulan PPPoE dalam kehilangan paket. Di sini, keamanan PPPoE diuji dengan merangkum paket data yang dikirim melalui web menggunakan HTTP. Telah dibuktikan bahwa *Wireshake* tidak dapat menangkap http saat ditulis, yang menunjukkan bahwa PPPoE aman dalam pengujian ini sehubungan dengan enkripsi paket data http.

Penelitian mengenai desain tunneling dengan PPPoE menggunakan mikrotik RB-942 (Studi Kasus SMK Taruna Bhakti) [15]. Hasil penelitiannya adalah sebuah perancangan *Tunneling* dengan PPPoE, yang membuktikan bahwa sistem PPPoE memiliki otentikasi yang sangat aman karena menggunakan *username* dan *password*, proses *Dial-Up* lebih cepat dan mudah dikonfigurasi.

Berdasarkan latar belakang, maka pada penelitian ini dilakukan pengamanan pada jaringan lokal, agar *user* jaringan aman dari serangan yang memanfaatkan eksploitasi ARP. Serangan ARP *Spoofing* pada penelitian ini yaitu menggunakan *tools NetCut* dan *Ettercap.* Pengamanan dilakukan dengan memanfaatkan PPPoE yang ada pada Mikrotik untuk melihat seberapa besar pengaruh keamanan jaringan sebelum dan setelah diterapkan PPPoE. Maka pada tugas akhir ini, diangkat judul "Analisis Keamanan Jaringan Berbasis PPPoE Menggunakan Mikrotik".

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode eksperimen, dengan melakukan sebuah percobaan serta pengimplementasian dari kinerja PPPoE pada segi keamanan ketika menggunakan jaringan [12].



Gambar 1. Tahapan Penelitian

2.1. Survei

Survei dilakukan di Laboratorium Jaringan Komputer, Jurusan Teknik Elektro Fakultas Teknik, Universitas Riau. Survei dilakukan untuk dapat mengidentifikasi masalah yang terjadi. Terutama pada masalah keamanan jaringan. Setelah melakukan survei dengan menguji keamanan jaringan, ternyata pada jaringan tersebut masih bisa di *cut-off* atau dilakukan pemutusan jaringan. Hal tersebut bisa mengganggu aktifitas pengguna jaringan dan bisa menimbulkan serangan-serangan yang lainnya [16].

2.2. Identifikasi Masalah

Idenfikasi masalah pada penelitian ini adalah kurangnya pengamanan pada jaringan lokal, khususnya pengamanan terhadap ancaman dari penyerang yang bisa mengendus frames data di jaringan lokal atau melakukan modifikasi *traffic* serta bisa menghentikan jaringan (ARP *Spoofing*) [12].

2.3. Studi Literatur

Studi literatur dilaksanakan dengan beberapa cara yaitu melakukan studi pustaka dengan cara mempelajari *e-book*, serta buku-buku ataupun artikel yang berkaitan tentang jaringan komputer, keamanan dalam jaringan lokal, terutama yang berkaitan tentang kemanan menggunakan PPPoE [17]. Selanjutnya melakukan studi laboratorium untuk mengumpulkan data-data penelitian dengan melakukan percobaan di Laboratorium Jaringan Komputer Jurusan Teknik Elektro Fakultas Teknik Universitas Riau.

2.4. Persiapan Alat dan Bahan

Perihal utama yang diperlukan sebelum membuat perancangan sistem yaitu menganalisis kebutuhan perangkat dengan mempersiapkan alat dan bahan. Berdasarkan skema sistem yang telah dibuat, maka dapat

ditentukan perangkat-perangkat yang dibutuhkan dalam penelitian. Kebutuhan tersebut meliputi, kebutuhan perangkat keras (*hardware*) dan kebutuhan perangkat lunak (*software*) [5].

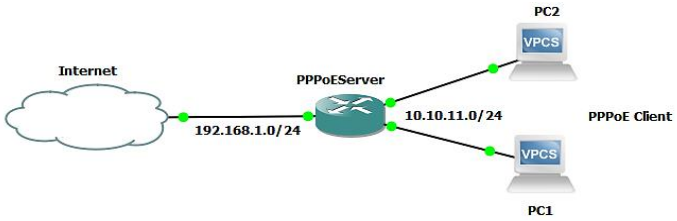
Tabel 1. Persiapan *Hardware* dan *Software*

No	*Hardware*	Keterangan
1	Laptop ACER *ASPIRE 3 A314-22* Prosesor AMD Ryzen en 3 3250U 2.60GHz Dual-core (2 Core™) Memory 4 GB	Sebagai komputer yang digunakan untuk menjalankan winbox
2	Laptop ASUS A516MA Prosesor Intel®Celeron® N4020 CPU 1.10GHz Memory 4 GB	Sebagai komputer *client* yang digunakan untuk melakukan serangan ARP *Spoofing*
3	Laptop ACER *ASPIRE 3 A314-22* Prosesor AMD Ryzen en 3 3250U 2.60GHz Dual-core (2 Core™) Memory 4 GB	Sebagai komputer *client* yang digunakan untuk target serangan
4	*Routerboard* Tipe Mikrotik 450	Sebagai *router server*
5	*Routerboard* Tipe Mikrotik RB-941	Sebagai *router client*
6	Winbox	Untuk melakukan konfigurasi mikrotik
7	*Netcut*	*Tools* untuk melakukan serangan ARP *Spoofing*

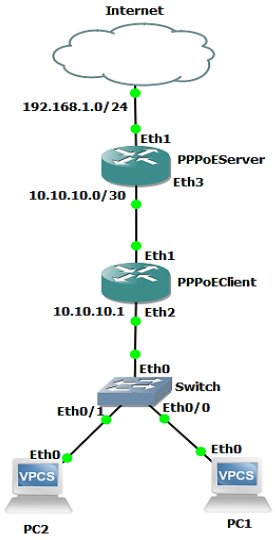
2.5. Perancangan Jaringan

2.5.1 Rancangan Topologi Jaringan

Rancangan topologi jaringan yang digunakan yaitu menggunakan topologi *tree*. Rancangan topologi jaringan dibuat dengan pengimplementasian fitur PPPoE pada fungsi *dial up* yang dilakukan pada mikrotik untuk melihat pengaruh dari kedua variasi topologi ini terhadap keamanan PPPoE. *Router* yang digunakan adalah *router* mikrotik dengan koneksi menggunakan kabel *ethernet* pada setiap koneksi antar *router server* dan *client.* Topologi yang akan digunakan pada penelitian ini yaitu seperti pada gambar dibawah ini:



Gambar 2. Rancangan Topologi Jaringan 1



Gambar 3. Rancangan Topologi Jaringan 2

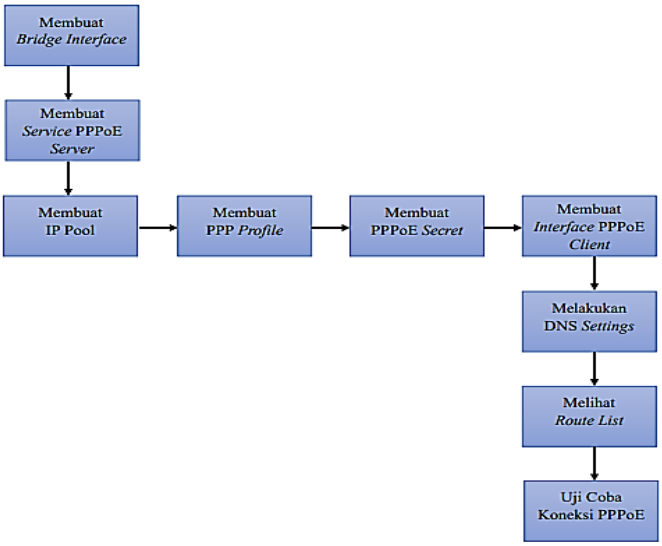
Pada gambar 2 merupakan rancangan topologi jaringan 1, pada topologi ini, router akan diimplementasikan sebagai PPPoE server, yang mendapatkan koneksi dari ISP dengan IP 192.168.1.0/24. PPPoE server mempunyai dua host, masing-masing host tersebut yaitu laptop yang akan berperan sebagai

PPPoE client. Karena antara server dan client memiliki jalur khusus maka harus menggunakan IP khusus pula untuk konektivitasnya. Pada PPPoE server memiliki IP 10.10.11.0/24

Pada gambar 3 merupakan rancangan topologi 2, yang memiliki 2 *router* mikrotik yang diimplementasikan sebagai PPPoE *server* dan PPPoE *client*, yang juga memiliki dua host yang diimplementasikan sebagai PPPoE *client*. PPPoE *server* mendapatkan koneksi dari ISP dengan IP 192.168.1.0/24. Sementara pada PPPoE *server* dibuat IP khusus untuk client dengan IP 10.10.10.0/24.

2.5.2 Perancangan Sistem Keamanan Menggunakan PPPoE

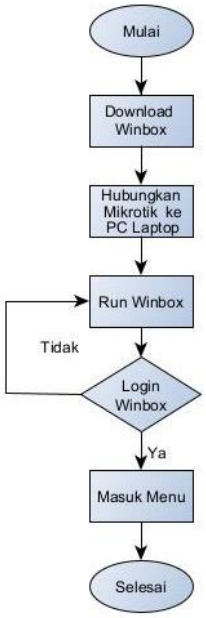
Proses ini merupakan alur perancangan sistem keamanan menggunakan PPPoE. Dalam perancangan ini, yang perlu dilakukan yaitu mulai dari membuat *bridge interface*, *service* PPPoE, IP *pool*, PPP *profile*, PPPoE *secret*, *interface* PPPoE *client*, melakukan DNS *settings*, *route list* dan melakukan uji coba koneksi. Pada penelitian ini, alur perancangan sistem keamanan menggunakan blok diagram sebagai berikut:



Gambar 4. Blok Diagram Perancangan PPPoE

2.6 Konfigurasi Perangkat Jaringan

Dalam tahap ini adalah melakukan konfigurasi perangkat jaringan yang digunakan, yaitu *routerboard* mikrotik, memastikan apakah perangkat telah terhubung atau terkoneksi ke internet dengan baik. Konfigurasi dilakukan pada mikrotik *server* dan mikrotik *client*. Konfigurasi dilakukan menggunakan *software winbox*, merupakan sebuah *utility* yang digunakan untuk melakukan *remote* ke *server* mikrotik ke dalam mode GUI.



Gambar 5. *Flowchart Login* Mikrotik

2.7 Implementasi PPPoE

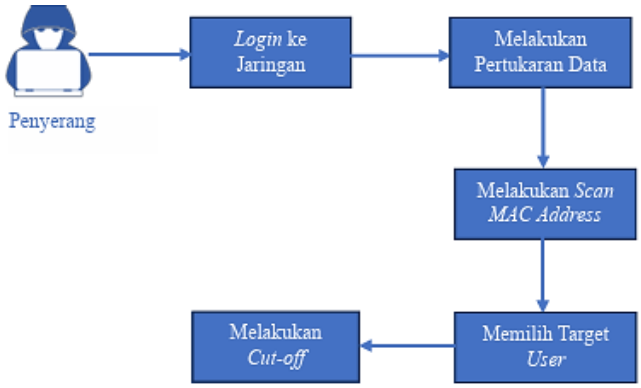
Pada penelitian ini, implementasi PPPoE dilakukan pada mikrotik di jaringan lokal (LAN) dengan menggunakan *software winbox*. Pada saat pengimplementasian ini, ada beberapa hal yang harus dilakukan yaitu sebagai berikut:

1. Melakukan setting PPPoE *server*
2. Melakukan setting PPPoE *client*

2.8 Skenario Pengujian

Skenario pengujian merupakan proses untuk mengetahui apakah keamanan jaringan yang diimplementasikan sesuai dengan tujuan penelitian. Pengujian dilakukan pada saat sebelum dan sesudah menerapkan PPPoE. Pengujian keamanan dilakukan untuk mengidentifikasi kerentanan keamanan pada jaringan. Serta untuk mengambil data dengan beberapa skenario serangan yang akan dilakukan untuk mengetahui kinerja dari PPPoE. Pada penelitian ini, pengujian keamanan jaringan dilakukan dengan serangan ARP *spoofing* menggunakan beberapa *tools* yaitu *Netcut* [18].

Skenario pengujian dilakukan menggunakan *tools netcut*. Pada skenario ini dilakukan pengujian keamanan jaringan tanpa PPPoE dan pengujian dengan PPPoE, tujuannya adalah untuk mendapatkan perbandingan dari sebelum dan setelah menerapkan PPPoE.



Gambar 6. Skenario Pertama dengan *Tools Netcut*

Langkah-langkah penyerangannya adalah sebagai berikut [19]:

1. 2 *user* masuk ke jaringan lokal dan melakukan pertukaran data
2. 1 *user* sebagai komputer penyerang melakukan *scan* MAC *Address*
3. Setelah penyerang melakukan *scanning*, penyerang memilih IP *address*/MAC *address* yang akan diputuskan koneksinya.

2.9 Analisis Hasil Keamanan

Pada tahap ini akan dilakukan analisis hasil dari pengujian keamanan jaringan berbasis PPPoE menggunakan mikrotik untuk melihat hasil yang didapatkan sesuai dengan penelitian yang telah dilakukan.

3. HASIL DAN PEMBAHASAN

Pada tahap konfigurasi perangkat jaringan ini adalah, melakukan konfigurasi pada mikrotik yang digunakan. Konfigurasi dilakukan dari sisi *server* dan *client* dan untuk memastikan semua perangkat telah terhubung atau terkoneksi ke internet dengan baik sebelum dilakukan pengimplementasian PPPoE [20].

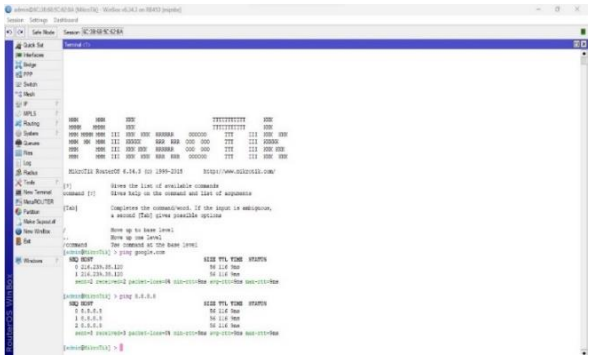
3.1 Hasil Konfigurasi Perangkat Jaringan

Pada tahap konfigurasi perangkat jaringan ini adalah, melakukan konfigurasi pada mikrotik yang digunakan. Konfigurasi dilakukan dari sisi *server* dan *client* dan untuk memastikan semua perangkat telah terhubung atau terkoneksi ke internet dengan baik sebelum dilakukan pengimplementasian PPPoE.

Langkah awal adalah dengan melakukan *login* pada *winbox* dari sisi *server*. Selanjutnya, memasukkan *ip address* pada masing-masing *interface*, melakukan *setting* DNS, melakukan *setting* pada *firewall*, dan melakukan *setting* pada *IP route*. Kemudian, melakukan *test* ping *google.com* dan *ip google* 8.8.8.8. Setelah berhasil tampilannya seperti gambar 7.

Setelah mikrotik *server* berhasil terkoneksi, selanjutnya dilakukan konfigurasi pada mikrotik *client*. Konfigurasi ini dilakukan untuk menghubungkan mikrotik *client* ke internet melalui *wifi*. Sebelum melakukan konfigurasi, mikrotik harus *login* ke *winbox*. Pada konfigurasi ini, yang dilakukan adalah mengaktifkan *wireless*, *security profile*, mengkonfigurasi *wireless* untuk melakukan *scan wifi*, mengkonfigurasi *wireless station*, mengkonfigurasi IP-DHCP *client*. Langkah terakhir adalah menguji konektivitasnya, untuk melihat

apakah sudah terhubung internet atau belum terhubung. Caranya dengan menuliskan *script* "*ping* google.com" dan "*ping* 8.8.8.8" di menu new terminal, ditunjukkan pada gambar 8.



Gambar 7. Mikrotik *Server* Telah Terkoneksi ke Internet

Gambar 8. Mikrotik *Client* Telah Terkoneksi ke Internet

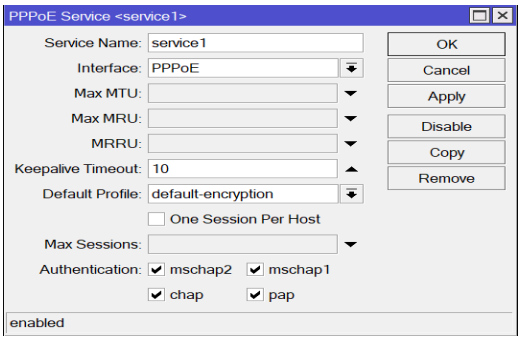
3.2 Hasil Implementasi PPPoE

Implementasi PPPoE adalah tahap menerapkan keamanan jaringan. Pada tahap ini, dilakukan konfigurasi dari sisi *server* dan *client*

.

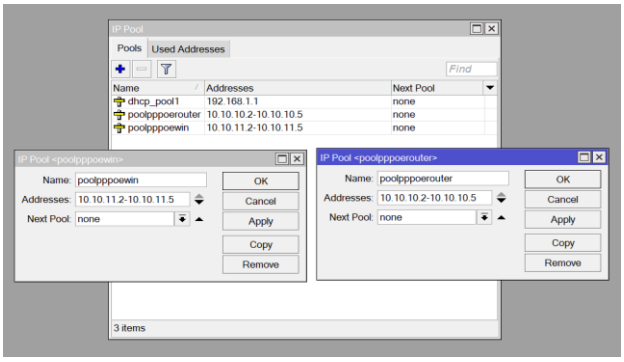
3.2.1 Hasil *Setting*-an *Router* PPPoE *Server*

Pada *setting-an* PPPoE *Server* ini, *bridge interface* dibuat sebelum membuat *service* PPPoE. Dengan membuat *bridge*, maka beberapa *interface* bisa digabungkan menjadi satu interface. Kemudian membuat *service* PPPOE *server* pada menu PPPoE *Server*. *Service name* diisi sesuai kebutuhan (disini *default* yaitu *service* 1), kegunaan *service name* yaitu untuk membedakan *server* karena pada bagian ini dibuat dua *server*. Pada *interface* diaktifkan di PPPoE sesuai yang dibuat pada *bridge*, serta mengaktifkan semua menu di bagian *authentication.*



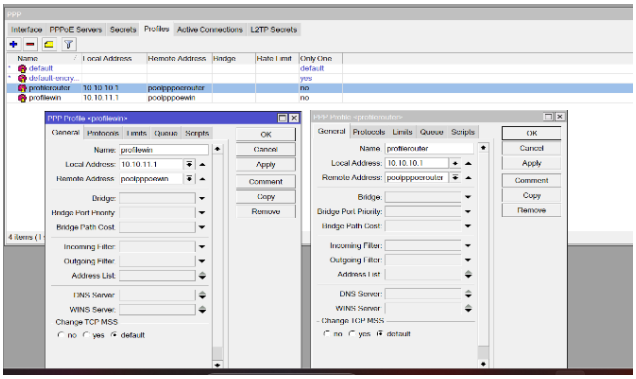
Gambar 9. Tampilan *Service* PPPoE *Server*

Membuat IP *Pool* untuk menentukan *range* IP yang bisa untuk membatasi *client* yang terkoneksi secara *wireless.* Gambar 10 adalah pembuatan IP pool, dimana dibuat 2 *range* IP untuk membedakan IP dari *server* 1 dan *server* 2. *Server* 1 diberi nama *poolpppoerouter* dengan *range* IP 10.10.10.2-10.10.10.5 sedangkan pada *server* 2 diberi nama *poolpppoewin* dengan *range* IP 10.10.11.2-10.10.11.5.



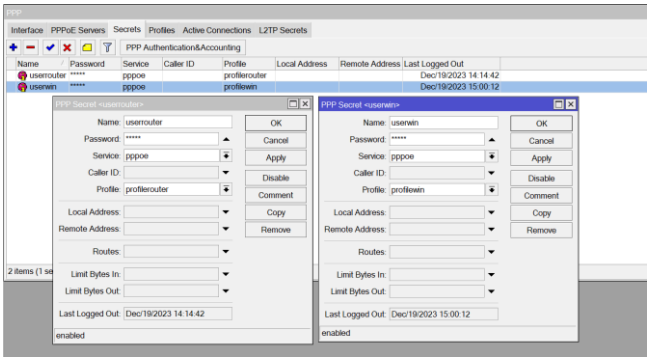
Gambar 10. Tampilan *Setting* IP Pool

PPP *profile* yaitu untuk mengatur nama *profile, local address* dan *remote address. Profile* yang dibuat yaitu diberi nama *profilerouter* dengan *local address* 10.10.10.1 serta *remote address* nya *poolpppoerouter*. Pada *profile* kedua diberi nama *profilewin* dengan *local address* 10.10.11.1 serta *remote address* nya *poolpppoewin* seperti gambar 11.



Gambar 11. Tampilan Menu *Profile*

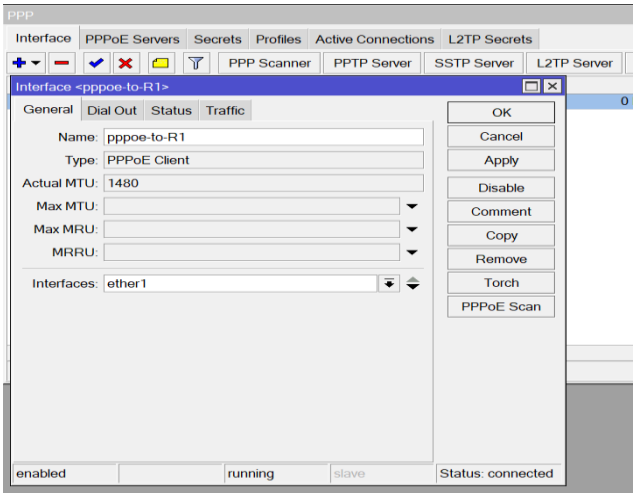
PPPoE akan memberikan IP secara otomatis, tetapi kinerjanya tidak seperti DHCP. Pemberian IP otomatis akan di *setting* dibagian *secret.* Di menu *secret* ini, bisa menentukan *username* dan *password* yang akan digunakan oleh *client* untuk bisa terkoneksi ke internet. Lalu, isi IP *Local* (IP PPPoE *Server*) dan *Remote* (IP PPPOE *Client*). Dimana IP ini nanti yang menjadi alamat *point to point* PPPoE nya.



Gambar 12. Tampilan Menu *Secret*

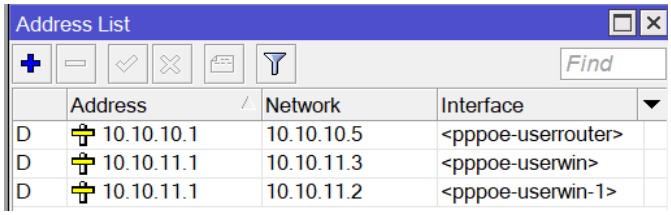
3.2.2 Hasil *Setting-an Router* PPPoE *Client*

Setting PPPoE *client* dilakukan pada R2 atau router *client.* Pada menu PPP, dengan menambahkan *interface* PPPoE *client* dan memilih menu *interface,* untuk melihat koneksi antara R1 dan R2 sudah berjalan.



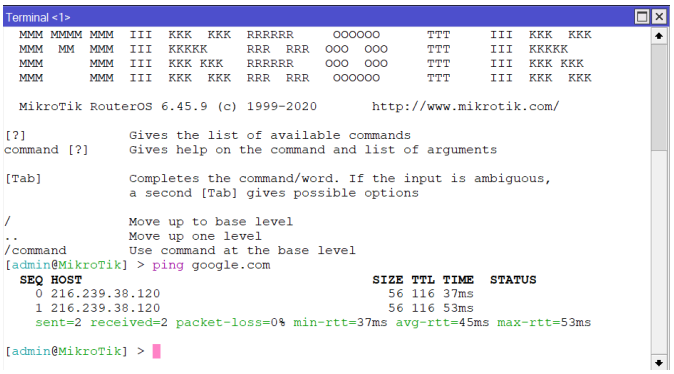
Gambar 13. Tampilan Menu *Interface* PPPoE *Client* (*General*)

Selanjutnya, pada tab *dial out*, mengisi *username* dan juga *password* yang sesuai dengan PPPoE *Server* (R1). Jika *interface* PPPoE *client* ini akan digunakan untuk koneksi internet, maka cek list pada *user peer* DNS dan *add default route*. Kemudian pada tab status, untuk melihat apakah status nya sudah *connect* atau belum. Jika *connected* berarti sudah ter *connect*. Lalu pada bagian *encoding*, menggunakan MPPE128 yang artinya bahwa selain ada fitur *authentication* (tidak semua orang bisa terkoneksi) disini juga ada fitur untuk *encryption* jadi datanya lebih aman. Kemudian untuk pengecekan, jika telah terkoneksi maka akan mendapatkan IP *address* secara otomatis.. Kemudian mengatur DNS *setting* yang dilakukan untuk memetakan *hostname* atau domain dari situs-situs yang ada diinternet menjadi IP *address*.



Gambar 14. Tampilan IP *Address Client* yang Terhubung

Setelah informasi IP telah didapatkan oleh router, maka PPPoE *client* sudah terkoneksi ke internet. Dengan melakukan pengecekan di terminal.



Gambar 15. PPPoE *Client* Terkoneksi ke Internet

3.3 Hasil Pengujian Keamanan

3.3.1 Hasil Pengujian Keamanan Jaringan tanpa PPPoE

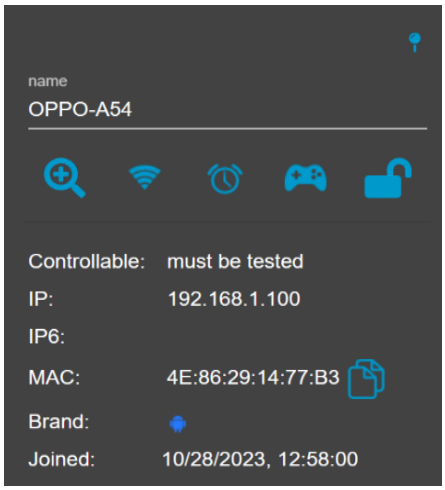
Pengujian keamanan jaringan tanpa PPPoE adalah untuk menganalisis keamanan jaringan sebelum diimplementasikan PPPoE. Pada pengujian ini yaitu 1 komputer penyerang melakukan penyerangan *ARP Spoofing* terhadap 3 target *user* yang sedang terkoneksi pada jaringan yang belum diterapkan PPPoE. Waktu penyerangan dilakukan secara bergantian dengan target IP yang telah ditentukan.

Penyerangan pertama dilakukan terhadap *user* 1, seperti pada gambar 16 saat tidak menggunakan PPPoE, *netcut* berhasil mendeteksi beberapa *host* terkait *IP* sekaligus *MAC Address* pasa setiap *host* yang terhubung pada jaringan yang sama. Selain bisa mendeteksi *IP* dan *MAC address*, penyerangan dengan *netcut* juga bisa mendeteksi aktivitas yang dilakukan oleh *user*, ditunjukkan pada gambar 17.

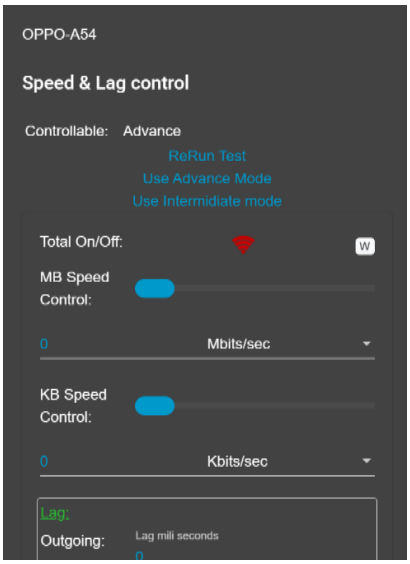
Setelah berhasil mendeteksi *IP address*, *MAC address* serta melihat aktivitas-aktivitas dari *user* 1 sebagai korban, selanjutnya adalah melakukan serangan dengan memutusan jaringan dari *user* 1, sehingga *user* 1 tidak bisa terkoneksi dan tidak bisa melakukan aktivitas apapun pada jaringan seperti pada gambar 17. Koneksi *user* 1 telah diputuskan dapat terlihat jaringan nya berwarna merah. Tabel 2 adalah hasil *ARP spoofing* sebelum penerapan PPPoE menggunakan *tools netcut*.

Tabel 2. Data Hasil Pengujian Keamanan Jaringan tanpa PPPoE menggunakan Tools Netcut

Target	IP Address	MAC Address	Nama Perangkat	Hasil
User 1	192.168.1.100	4E:86:29:14:77:B3	Oppo-A54	Berhasil di *cut-off*
User 2	192.168.1.106	70:BB:E9:6D:25:E8	Android	Berhasil di *cut-off*
User 3	192.168.1.107	DC:21:5C:E6:BD:6A	LAPTOP-TLAUPTV	Berhasil *di cut-off*



Gambar 16. Deteksi IP dan MAC Address User 1



Gambar 17. Pemutusan Koneksi *User* 1

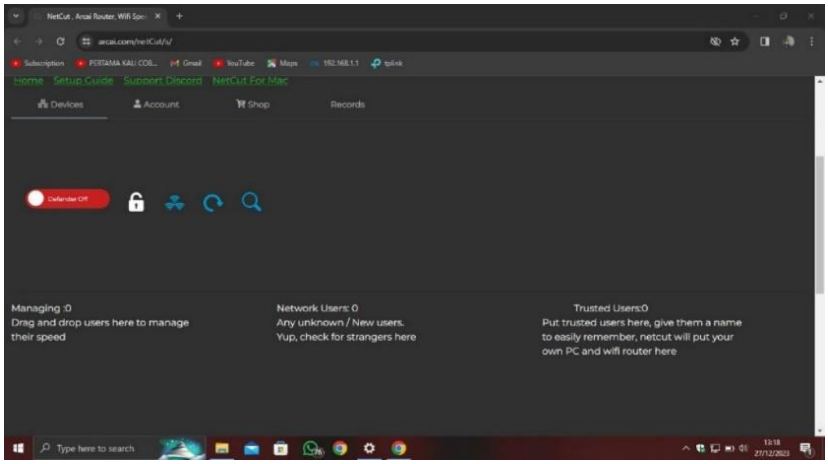
Tabel 2 merupakan data hasil serangan ARP *spoofing* menggunakan *tools netcut* saat belum diimplementasikan PPPoE. Berdasarkan data yang didapat, ada tiga *user* yang terhubung pada jaringan lokal yang sama. Setelah penyerang melakukan *scan* pada jaringan, diperoleh hasil berupa informasi IP *address*, MAC *address*, dan nama perangkat dari *user-user* yang terhubung pada jaringan.

1. *User* 1 terdeteksi dengan nama perangkat Oppo-A54, yang memiliki IP *address* 192.168.1.100 dengan MAC *address* 4E:86:29:14:77:B3 berhasil di *cut-off*. *User* tersebut telah terputus koneksinya ketika di *cut-off* oleh penyerang, dan tidak bisa terhubung dengan jaringan.
2. *User* 2 terdeteksi dengan nama perangkat Android, yang memiliki IP 192.168.1.106 dengan MAC *address* 70:BB:E9:6D:25:E8 berhasil di *cut-off*. Sama seperti *user* 1, ketika *user* berhasil di *cut-off*, maka koneksinya terputus dan tidak bisa terhubung ke jaringan.
3. *User* 3 terdeteksi dengan nama perangkat LAPTOP-TLAUPTV, yang memiliki IP *address* 192.168.1.107 dengan MAC *address* DC:21:5C:E6:BD:6A berhasil di *cut-off*. *User* 3 juga terputus koneksinya karena berhasil di *cut-off* oleh penyerang serta tidak bisa terhubung ke jaringan.

3.3.2 Hasil Pengujian Keamanan Jaringan dengan PPPoE

Pengujian keamanan jaringan dengan PPPoE dilakukan untuk mendapatkan data setelah diterapkan PPPoE, untuk melihat kinerja dari PPPoE dalam proses pengamanan jaringan dari serangan ARP *spoofing* menggunakan *tools netcut.*

Pengujian ini menggunakan 1 komputer penyerang dengan IP 10.10.11.3 melakukan penyerangan *ARP Spoofing* terhadap 1 *user* dengan IP 10.10.11.2 yang sedang terkoneksi pada jaringan PPPoE. Serangan dilakukan menggunakan *tools netcut.*



Gambar 18. Tampilan Serangan Menggunakan *Netcut*

Gambar 18 merupakan tampilan salah satu *user* PPPoE menyalakan *netcut* dengan tujuan untuk memutuskan jaringan *user* lain yang sedang terkoneksi dengan jaringan PPPoE. Tetapi, *netcut* tidak bisa mendeteksi *host* yang terkoneksi, terlihat tampilan pada *network user* di *netcut* yaitu kosong. Maka dengan adanya PPPoE tidak bisa dilakukan pemutusan (*cut-off*) pada jaringan. Berikut adalah tabel dari hasil *ARP spoofing* setelah penerapan PPPoE menggunakan *tools netcut*:

Tabel 3. Data Hasil Pengujian Keamanan Jaringan dengan PPPoE menggunakan Tools Netcut

Target	IP Address	MAC Address	Nama Perangkat	Hasil
User 1	-	-	-	Tidak bisa di *cut-off*
User 2	-	-	-	Tidak bisa di *cut-off*

Tabel 3 merupakan data hasil serangan ARP *spoofing* menggunakan *tools netcut* setelah diimplementasikan PPPoE. Ketika dua *user* berada pada jaringan yang sama, dan salah satu *user* melakukan serangan didapatkan hasil bahwa, *user* tidak terdeteksi ketika berada pada jaringan tersebut. Sehingga untuk informasi berupa IP *address*, MAC *address,* dan nama perangkat juga tidak diperoleh. Oleh karena itu, PPPoE berhasil melindungi *user* pada jaringan dari serangan pada pengujian ini.

4. KESIMPULAN

Kesimpulan yang didapat berdasarkan hasil penelitian yang dilakukan adalah Analisis Keamanan Jaringan Berbasis Point To Point Protocol Over Ethernet (PPPoE) Menggunakan Mikrotik telah berhasil dilakukan untuk mengamankan jaringan dari serangan ARP Spoofing menggunakan *Tools Netcut* serta mengamankan dari serangan *ARP Spoofing* menggunakan *Tools Ettercap*. PPPoE merupakan sebuah rekomendasi yang tepat sebagai solusi keamanan pada jaringan lokal, dapat dibuktikan saat dilakukan serangan diperoleh hasil bahwa user yang terhubung ke jaringan yang sama, tidak bisa menyerang user lain, tidak terdeteksi pula IP Address, MAC Address, bahkan nama perangkat yang terhubung. Koneksi pada PPPoE adalah point to point, dimana setiap user hanya akan terhubung dengan router. Oleh karena itu, proses management terhadap client lebih mudah.

REFERENSI

[1] V. Charnita, B. Ginting, M. Data, and D. P. Kartikasari, "Deteksi Serangan ARP Spoofing berdasarkan Analisis Lalu Lintas Paket Protokol ARP," 2019. [Online]. Available: http://j-ptiik.ub.ac.id

[2] D. Kurniawan, "Ilmu Hacking." Accessed: Dec. 14, 2023. [Online]. Available: https://www.google.co.id/books/edition/Ilmu_Hacking/0iGzEAAAQBAJ?hl=id&gbpv=1&dq=netcut&pg=PA93&printsec=frontcover

[3] E. Zam, "Buku Sakti Hacker - Google Books," *Media Kita, Jakarta Selatan*, 2011, Accessed: Jan. 24, 2024. [Online]. Available: https://www.google.co.id/books/edition/Buku_Sakti_Hacker/Ju6-xtLkzdEC?hl=en&gbpv=1&dq=crawling+adalah&pg=PA219&printsec=frontcover

[4] H. Muhammmad, K. Nasution, O. Nasution, and S. Krianto, *Implementasi Aplikasi Cain And Abel Dalam Penyadapan Paket Data Pada Jaringan Wifi*. 2021. [Online]. Available: www.yuksinau.id

[5] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," *Jurnal Telekomunikasi dan Komputer*, vol. 10, no. 2, p. 111, Aug. 2020, doi: 10.22441/incomtech.v10i2.8757.

[6] W. Najib, "PANDUAN PRAKTIKUM JARINGAN KOMPUTER - Google Books." Accessed: Jan. 15, 2024. [Online]. Available: https://www.google.co.id/books/edition/PANDUAN_PRAKTIKUM_JARINGAN_KOMPUTER/ouMHEAAAQBAJ?hl=id&gbpv=1&dq=pengertian+IP+address+adalah&pg=PA5&printsec=frontcover

[7] A. Rizal Fauzi, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," 2018.

[8] A. A. Zackiansyah, "Easy and Practice PPPoE Server, VPN PPTP, Bandwidth Management, Mikrotik Ho... - Google Books." Accessed: Dec. 18, 2023. [Online]. Available: https://www.google.co.id/books/edition/Easy_and_Practice_PPPoE_Server_VPN_PPTP/XP18EAAAQBAJ?hl=id&gbpv=1&dq=jenis+jenis+mikrotik+routerboard&pg=PA2&printsec=frontcover

[9] I. M. K. Karo, F. Ramadhani, N. A. A. Nasution, and S. N. Amalia, "Pengenalan Mikrotik bagi Pemula - Jejak Pustaka - Ichwanul muslim Karo Karo, Fanny Ramadhani, Nadrah Afiati Amalia Nasution, Sisti Nadia Amalia - Google Buku." Accessed: Jan. 24, 2024. [Online]. Available: https://books.google.co.id/books?id=jiruEAAAQBAJ&newbks=0&printsec=frontcover&pg=PA29&dq=definisi+dhcp+pada+jaringan&hl=id&source=newbks_fb&redir_esc=y#v=onepage&q=definisi%20dhcp%20pada%20jaringan&f=false

[10] Y. Habibi and B. Satya, "Analisis Dan Implementasi PPPoE Client Dan Server Dengan Menggunakan Mikrotik Studi Kasus ISP PT. Cobralink Yogyakarta," 2015.

[11] M. S. Laksono, “Mikrotik MTCNA TEACHER - Google Books.” Accessed: Dec. 20, 2023. [Online]. Available: https://www.google.co.id/books/edition/Mikrotik_MTCNA_TEACHER/lg_MDwAAQBAJ?hl=id&gbpv=1&dq=winbox+mikrotik&pg=PA16&printsec=frontcover

[12] E. Suryani, T. Kalsum, and Khairil, “Analisa Pemanfaatan Point To Point Protokol Over Ethernet (PPPoE) | PDF.” Accessed: Sep. 01, 2022. [Online]. Available: https://www.scribd.com/doc/287988544/Analisa-Pemanfaatan-Point-To-Point-Protokol-Over-Ethernet-PPPoE

[13] E. Prasetyo, A. Hamzah, and E. Sutanta, “(PDF) Analisa Quality Of Service (Qos) Kinerja Point To Point Protocol Over Ethernet (PPPoE) Dan Point To Point Tunneling Protocol (PPTP).” Accessed: Sep. 01, 2022. [Online]. Available: https://www.researchgate.net/publication/320383186_Analisa_Quality_Of_Service_Qos_Kinerja_Point_To_Point_Protocol_Over_Ethernet_PPPoE_Dan_Point_To_Point_Tunneling_Protocol_PPTP

[14] A. A. Slameto and R. Hidayat, “Comparative Analysis of PPPOE and SSTP Performance in Microtic (Analisis Perbandingan Kinerja PPPOE dan SSTP Pada Mikrotik),” *Jurnal KomtekInfo*, vol. 6, no. 2, 2019, doi: 10.35134/komtekinfo.v6i2.881.

[15] I. Wahyudi Siadi, I. Fitri, and R. Nuraini, “Desain Tunneling dengan Point to Point Protocol over Ethernet (PPPoE) menggunakan Mikrotik RB-941 (Studi Kasus SMK Taruna Bhakti),” 2020, [Online]. Available: https://iocscience.org/ejournal/index.php/mantik/index

[16] M. Gilang, H. Wibowo, J. Triyono, E. Sutanta, J. Teknik Informatika, and A. Yogyakarta, “Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika Diy.”

[17] W. A. Pamungkas, “Rancang Bangun Jaringan Internet Dengan Sistem Pppoe Dan Hotspot Dalam Satu Interface Menggunakan Mikhmon Sebagai User Management Hotspot (Studi Kasus: Gandaria, Pekayon),” 2021.

[18] N. Erzed, “Modul 6 Keamanan Informasi Ancaman Internal dan Eksternal Internal and External Attack,” 2020.

[19] H. Ussk and N. Hendrarini, “Implementasi Pencegahan ARP Spoofing menggunakan VLAN dan Bandwidth Management Setia Jul Ismail.”

[20] D. Mustofa, D. A. Mahendra, D. Intan, S. Saputra, and M. S. Amin, “Implementasi Point-to-Point Protocol Over Ethernet pada Jaringan RT/RW Net Menggunakan Mikrotik RB750 GR3,” *Jurnal IT CIDA*, vol. 8, no. 2, 2022.