Volume 3 No. 2 (July - December 2023), pp. 110-123 | ISSN 2962-2360 (online) | ISSN 2962-3669 (print)
Arcitech: Journal of Computer Science and Artificial Intelligence
http://journal.iaincurup.ac.id/index.php/arcitech/article/view/8181 | DOI : http://dx.doi.org/10.29240/arcitech.v3i2.8181

Implementasi dan Analasis Keamanan Jaringan Pada STIA Lancang Kuning Dumai Menggunakan Port Scanning dan Firewall Tarpit

Mustazzihim Suhaidi[1], Nurhadi[2]
[1] Program Studi Teknik Informatika, STT DUMAI, Dumai, Indonesia
[2] Program Studi Teknik Komputer, Universitas Dumai, Dumai, Indonesia
Email : muja.1708@gmail.com, flinkdumai@gmail.com

Article Information

Article history

Received 8 August 2023
Revised 5 December 2023
Accepted 29 December 2023
Available 31 December 2023

Keywords

Network Security
Port Scanning
Tarpit Firewalls

Corresponding Author:

Nurhadi,
Universitas Dumai,
Email : flinkdumai@gmail.com

Abstract

This study aims to implement and analyze network security at STIA Lancang Kuning Dumai in Dumai City using the port scanning method and tarpit firewall. The main purpose of this research is to identify security holes in the network and protect the system from threats that may arise. The method used in this research is the SDLC method. The results of the analysis show that the implementation of port scanning and firewall tarpit at STIA Lancang Kuning Dumai has succeeded in significantly increasing network security. The port scan was able to identify several security holes which were then able to be fixed and strengthened. Tarpit firewalls are also effective in inhibiting attacks by slowing down and limiting attacker access. This research makes an important contribution to securing the network at STIA Lancang Kuning Dumai and provides valuable guidance for similar institutions in strengthening their security systems. However, it is important to continuously monitor new technology developments and security threats to keep systems well-protected and ready for more sophisticated attacks in the future.

Keywords : *Network Security, Port Scanning, Tarpit Firewalls.*

Abstrak

Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis keamanan jaringan pada STIA Lancang Kuning Dumai di Kota Dumai dengan menggunakan metode port scanning dan firewall tarpit. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi celah keamanan dalam jaringan dan melindungi sistem dari ancaman yang mungkin timbul. Metode penelitian pada riset ini adalah menggunakan metode SDLC. Hasil analisis menunjukkan bahwa implementasi port scanning dan firewall tarpit pada STIA Lancang Kuning Dumai berhasil meningkatkan keamanan jaringan secara signifikan. Pemindaian port berhasil mengidentifikasi beberapa celah keamanan yang kemudian dapat diperbaiki dan diperkuat. Firewall tarpit juga efektif dalam menghambat serangan dengan memperlambat dan membatasi akses penyerang. Penelitian ini memberikan kontribusi penting dalam mengamankan jaringan di STIA Lancang Kuning Dumai dan memberikan panduan yang berharga bagi institusi serupa dalam memperkuat sistem keamanan mereka. Namun, penting untuk terus memantau perkembangan teknologi dan ancaman keamanan yang baru agar sistem tetap terlindungi dengan baik dan siap menghadapi serangan yang lebih canggih di masa depan.

Kata Kunci : Keamanan Jaringan, Port Scanning, Firewall Tarpit

1. Pendahuluan

Dalam era digital saat ini, keamanan jaringan merupakan aspek kritis yang harus diperhatikan oleh organisasi dan lembaga pendidikan. Serangan terhadap jaringan dapat mengakibatkan kerugian yang serius, termasuk pencurian data sensitif, gangguan operasional, dan kerusakan reputasi (Laksamana, 2022). Oleh karena itu, penting bagi institusi seperti STIA Lancang Kuning di Kota Dumai untuk mengimplementasikan langkah-langkah yang efektif dalam menjaga keamanan jaringan mereka. Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis keamanan jaringan pada STIA Lancang Kuning dengan menggunakan dua metode utama, yaitu port scanning dan firewall tarpit. Port scanning digunakan untuk mengidentifikasi port-port yang terbuka pada sistem jaringan, sedangkan firewall tarpit digunakan untuk memperlambat serangan dan membuat penyerang terjebak dalam perangkap yang tidak produktif. Dalam penelitian ini, fokus diberikan pada STIA Lancang Kuning sebagai studi kasus.

STIA Lancang Kuning adalah sebuah institusi pendidikan yang menyediakan layanan jaringan bagi mahasiswa dan stafnya. Keamanan jaringan menjadi prioritas bagi STIA Lancang Kuning untuk melindungi data mahasiswa, informasi administrasi, dan sumber daya jaringan lainnya. Melalui penelitian ini, diharapkan dapat diidentifikasi celah keamanan yang mungkin ada dalam jaringan STIA Lancang Kuning. Dengan mengeksplorasi metode port scanning, penelitian ini akan mengungkapkan potensi kerentanan yang mungkin dimanfaatkan oleh penyerang. Selain itu, penerapan firewall tarpit akan memberikan perlindungan tambahan dengan memperlambat serangan dan membatasi akses penyerang. Hasil dari riset ini dapat memberikan rekomendasi dan panduan kepada STIA Lancang Kuning dalam memperkuat keamanan jaringan mereka. Sisi lain, riset ini juga dapat menjadi sumber informasi bagi institusi serupa yang ingin meningkatkan keamanan jaringan mereka. Dengan memperkuat keamanan jaringan, STIA Lancang Kuning dapat melindungi data sensitif, menjaga kontinuitas operasional, dan meningkatkan kepercayaan pengguna jaringan.

2. Kajian Terdahulu

Pada penelitian ini penulis merujuk beberapa jurnal ilmiah yang membahas permasalahan serupa dan selanjutnya dijadikan tinjauan pustaka. Adapun jurnal yang pertama diambil dari (Sartomo, 2022) yang berjudul "Model Keamanan Jaringan Menggunakan *Firewall Port Blocking*". Riset ini dicoba buat membatasi akses dari pihak satu ke pihak lain buat menghindari terbentuknya perampokan informasi dari orang tidak dikenal maupun yang diketahui. Dari pengujian yang dicoba diketahui bahwapenerapan firewall security port bisa melaksanakan kelakuan block pada koneksi jaringan itu kala terjalin perpindahan hak akses. Menurut (Wicaksono, 2022) yang berjudul "Sistem Keamanan Jaringan Menggunakan *Firewall* Dengan Metode *Port Blocking* Dan *Firewall Filtering*". Hasil penelitian ini dicoba menggunakan aplikasi Nmap

Zenmap untuk melihat sisa port komunikasi yang terbuka serta memakai browser untuk mengakses website web yang dialihkan serta di block.

Dengan mengoptimalkan serta memaksimalkan kemampuan firewall suatu jaringan internet hendak lebih aman serta meminimalisir bahaya serbuan dari luar. Menurut (Purwaningrum, 2018) yang bertajuk" Optimalisasi Jaringan Mengggunakan Firewall". Riset ini dicoba buat optimalisasi sistem firewall security memakai dual home host, screened host, serta screened subnet pada wide zona jaringan. Firewall ialah sesuatu fitur keamanan jaringan yang memperbolehkan bermacam bagian ruas jaringan buat melakukan komunikasi antara satu dengan yang yang lain cocok dengan arti kebijaksanaan keamanan yang sudah diaplikasikan lebih dahulu. Firewall liabel kepada kekeliruan bentuk serta kekalahan buat mempraktikkan kebijaksanaan, alhasil dibutuhkan bonus ataupun kenaikan keamanan lain.

2.1 Analisis

Penafsiran analisa merupakan aktivitas berasumsi buat menguraikan sesuatu totalitas jadi bagian alhasil bisa memahami isyarat bagian, hubungannya satu serupa lain serta guna tiap- tiap dalam satu keseluruhan yang terstruktur(Azwar, 2019).

2.2 Keamanan Jaringan

Banyak hal keterjaminan (*security*) dari suatu sistem jaringan PC yang tersambung ke internet kepada bahaya serta kendala yang tertuju pada sistem itu. Penyelinap (intruder) ialah orang ataupun berkas orang yang melaksanakan aksi yang tidak tepat, yang menyimpang (*anomaly*), serta tidak layak (*inappropriate*) kepada sesuatu jaringan pc. Sebagian tujuan dari seseorang penyelinap ialah:

1. Hanya mau ketahui sistem serta informasi yang terdapat pada sesuatu sistem jaringan pc yang dijadikan target. Penyelinap ini disebut *The Curius*.
2. Membuat sistem jaringan jadi down, ataupun mengganti bentuk dari sesuatu web website. Penyelinap ini disebut *The Malicious*.
3. Mau ketahui informasi apa saja yang terdapat di dalam jaringan pc buat memperoleh uang.
4. Berupaya buat memakai sumber energi di dalam sistem jaringan pc buat mendapatkan ketenaran. Penyelinap ini disebut The High Profile Intruder. (Madcoms, 2020)

2.3 Jenis Serangan Terhadap Keamanan

Pada dasarnya, berdasarkan serangan kepada sesuatu informasi dalam sesuatu jaringan bisa dikategorikan jadi 2, ialah:

1. Serangan Pasif (*Passive Attacks*)

   Serangan pasif merupakan serangan pada sistem autentikasi yang tidak menyelipkan informasi pada aliran data(data stream), namun cuma mencermati ataupun memantau pengiriman data ke tujuan. Data ini bisa dipakai di lain durasi oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil sesuatu bagian

informasi serta setelah itu menggunakanya untuk memasuki tahap autentikasi dengan berpura- pura jadi user autentik atau asli disebut dengan replay attack. Sebagian data autentikasi semacam password ataupun informasi biometric yang dikirim lewat transmisi elektronik bisa direkam serta setelah itu dipakai buat memanipulasi informasi yang sesungguhnya. Serangan pasif ini susah buat dideteksi sebab penyerbu tidak melaksanakan pergantian informasi. Oleh karena itu buat menanggulangi serangan pasif ini lebih dipusatkan pada penangkalan dari pendeteksiannya.

2. Serangan Aktif (*Active Attacks*)

   Serangan aktif merupakan serangan yang berupaya memodifikasi informasi, berupaya memperoleh autentikasi, ataupun memperoleh autentikasi dengan mengirimkan paket- paket informasi yang salah ke data stream ataupun dengan memodifikasi paket- paket yang melampaui data stream. Kebalikan dari serangan pasif, serangan aktif susah buat dilindungi sebab buat melaksanakannya diperlukan perlindungan fisik buat seluruh sarana komunikasi serta jalur- jalurnya setiap saat. Yang dapat dilakukan adalah mengetahui serta memperbaiki kondisi yang diakibatkan oleh serangan ini.

2.4 Aspek dan Ancaman Terhadap *Security*

Adapun aspek dan ancaman terhadap *security* diantaranya yaitu:

1. Privacy merupakan suatu yang karakter rahasia ataupun private. Intinya merupakan sesuatu penangkalan biar data itu tidak bisa diakses oleh orang yang tidak diketahui ataupun tidak berkuasa. Ilustrasinya merupakan, e- mail ataupun file- file lain yang tidak bisa dibaca orang lain walaupun beliau merupakan administrator.
2. Confidentiality merupakan informasi yang diserahkan pada pihak lain dengan tujuan spesial tetapi senantiasa dilindungi penyebarannya. Ilustrasinya merupakan informasi yang bertabiat individu semacam: Julukan, Tujuan, Nomor KTP, Telepon serta lain serupan.
3. Integrity ataupun penekanannya merupakan sesuatu data tidak bisa diganti lain oleh owner data itu. Sering- kali informasi yang telah terenskripsi juga tidak terpelihara integritasnya sebab terdapatnya sesuatu mungkin chaper text dari enkripsi itu yang berganti. Ilustrasi: Penyerangan integritas pada dikala suatu e- mail dikirimkan di tengah jalur setelah itu disadap serta ditukar isinya, alhasil e- mail itu yang hingga ketujuan sudah berganti.
4. Authentication ini hendak dicoba sewaktu user login dengan memakai julukan user dan password- nya. Perihal ini umumnya hendak berkaitan dengan hak akses seorang, apakah ia pengakses yang legal ataupun bukan.
5. Availability, dalam pandangan ini berhubungan dengan apakah sesuatu informasi ada kala diperlukan ataupun dibutuhkan oleh konsumen. Bila suatu informasi atau data sangat kencang pengamanannya hingga hendak mengalutkan dalam akses informasi itu. Tidak hanya itu akses yang lelet pula bisa membatasi terpenuhinya pandangan availability. Serbuan yang kerap dicoba pada pandangan ini merupakan

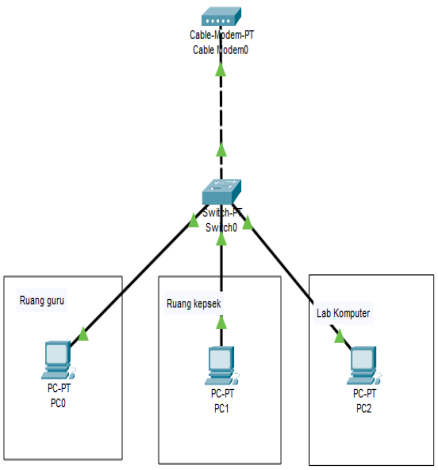
Denial of Service(DoS), ialah ialah penggagalan dari service sewaktu terdapatnya permohonan informasi alhasil pc tidak bisa melayaninya. Ilustrasi lain dari Denial of Service ini merupakan mengirimkan sesuatu request yang kelewatan alhasil bisa menimbulkan pc tidak bisa lagi menampung bobot itu serta sampai pada kesimpulannya pc down(Rendro, 2020)

3. Metodologi Penelitian

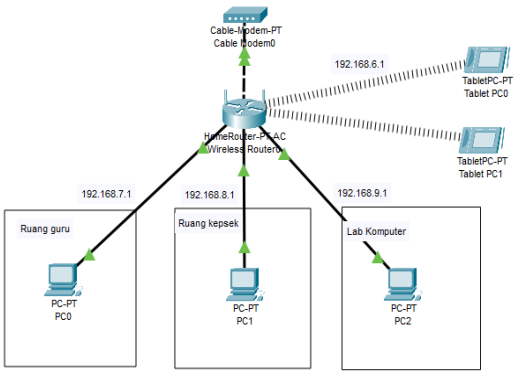
Analisa penelitian yang dilakukan dengan metode SDLC terdiri dari :

1. Analisa Kebutuhan (*Requiremenents Analysis*)
   Pada langkah ini dicoba analisa kebutuhan hal detail jaringan internet ialah dengan menetapkan kebutuhan riset yang menguraikan mengenai strategi pengembangan jaringan, menganjurkan suatu rancangan arsitektur jaringan dengan topologi yang pas dengan mengidentifikasikan eksploitasi teknologi yang bisa membagikan sokongan konsep sampai aplikasi.
2. *Design* (Desain)
   Konsep jaringan dibesarkan bersumber pada persyaratan teknis, serta bidang usaha yang didapat dari situasi lebih dahulu. Detail konsep jaringan merupakan konsep yang bertabiat menyeluruh serta mendetail, yang penuhi persyaratan teknis serta bidang usaha dikala ini. Jaringan itu haruslah sediakan ketersediaan, kehandalan, keamanan, skalabilitas(keterluasan) serta kemampuan.
3. *Implement* (Implementasi)
   Pada tahap ini, peralatan-peralatan terkini dilakukan instalasi dan di konfigurasi, sesuai spesifikasi desain. Perangkat-perangkat terkini ini akan mengubah ataupun menambah prasarana yang ada. Pemograman proyek juga wajib diiringi sepanjang tahap ini, bila terdapat pergantian sepatutnya di informasikan dalam pertemuan rapat, dengan persetujuan yang dibutuhkan untuk dilanjutkan.

Pada tahap ini, Penulis akan membuat skema jaringan menggunakan *Cisco Packet Tracer*, sebelum dan akan dibangun jaringan Wireless.



Gambar 1. Skema jaringan yang sedang berjalan
Sumber : Hasil Rancangan



Gambar 2. Skema jaringan yang diusulkan
Sumber : Hasil Rancangan

Alat dan Perancangan

1. *Wireless*

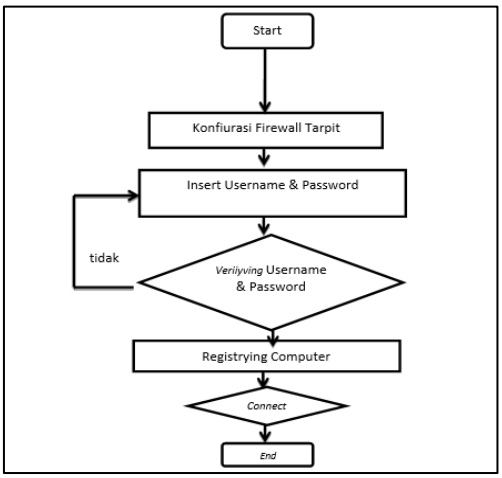
Gambar 3. *Wireless*
Sumber: Hasil Rancangan, 2023

2. *Router*

Gambar 4. Router

4. Hasil dan Pembahasan

Adapun tahapan dalam jenis data yang dikumpulkan yaitu *flowchart,* memberikan gambaran suatu bagan yang melakukan proses satu dengan lainnya secara detail. dapat dilihat pada gambar 5 berikut:

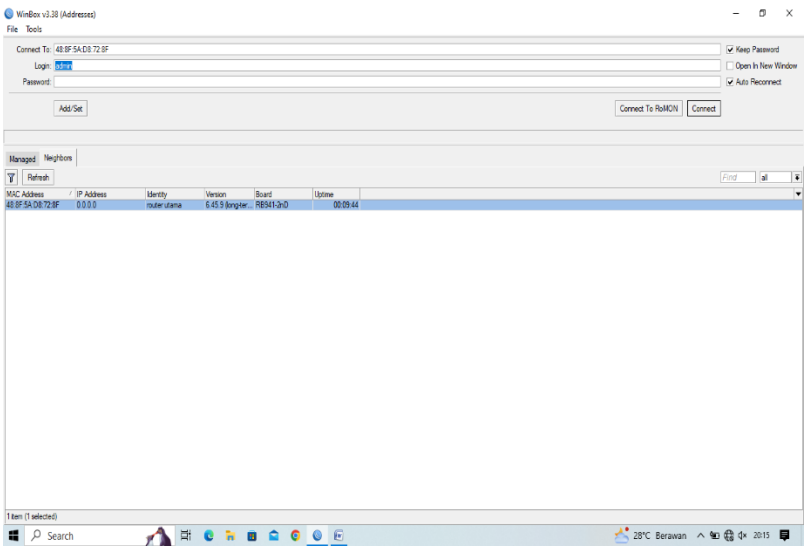


Gambar 5. Flowchart
Sumber : Hasil Penelitian, 2023

4.1 Implementasi Jaringan

1. Login Winbox

Pertama yang harus dilakukan adalah membuka aplikasi *WinBox* pada laptop yang akan digunakan untuk menyetting *Router* Mikrotik. Kemudian klik *neighbors -> address-> Connect*

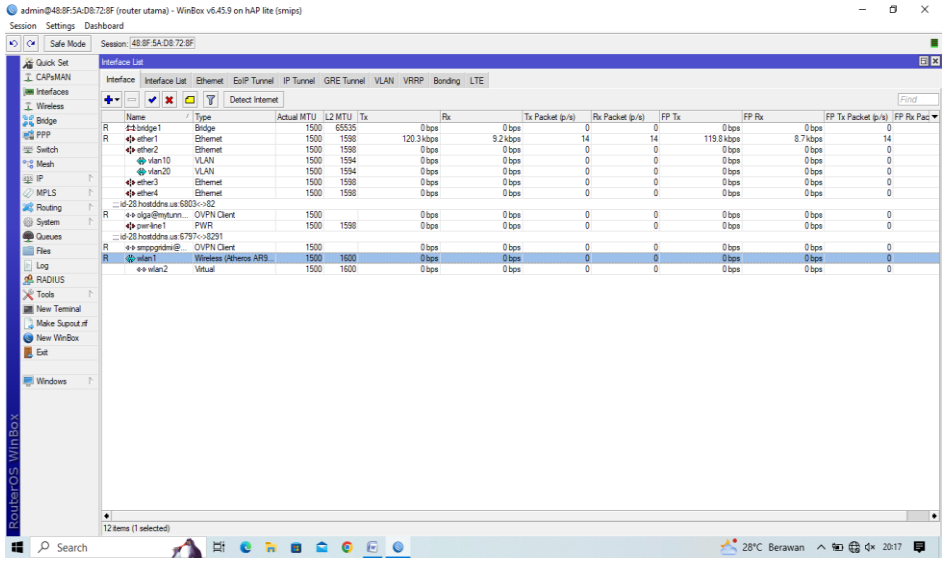


Gambar 6. *Login WinBox* (*neighboard)*
Sumber: Hasil Rancangan, 2023

2. Konfigurasi Wireless pada winbox

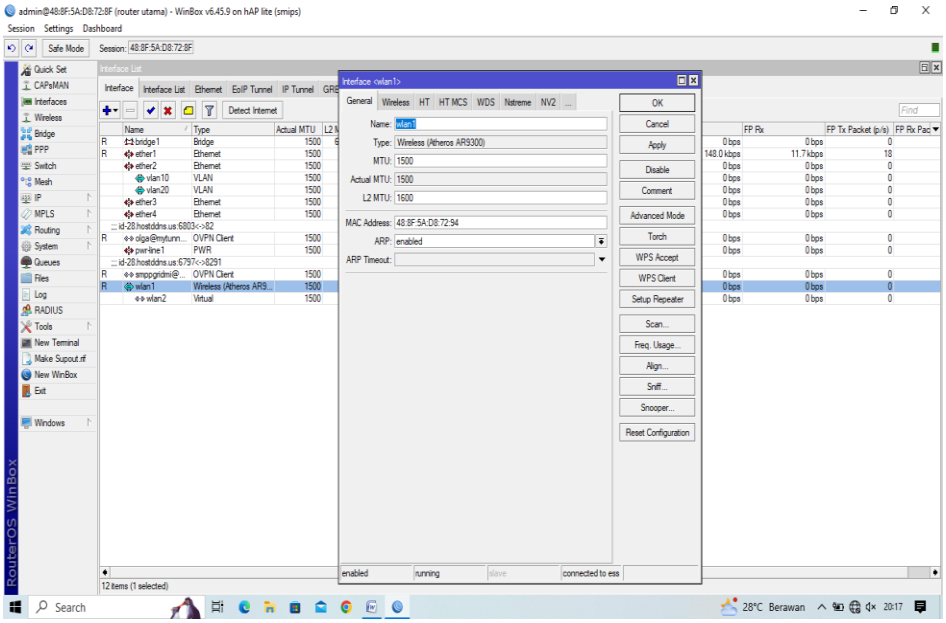
Pada proses instalasi dan konfigurasi ini, penulis melakukan konfigurasi *wireless* pada mikrotik. Lanjut, begini cara setting nya:

a. Klik menu *wireless*-> *interface list* -> double klik pada wlan1



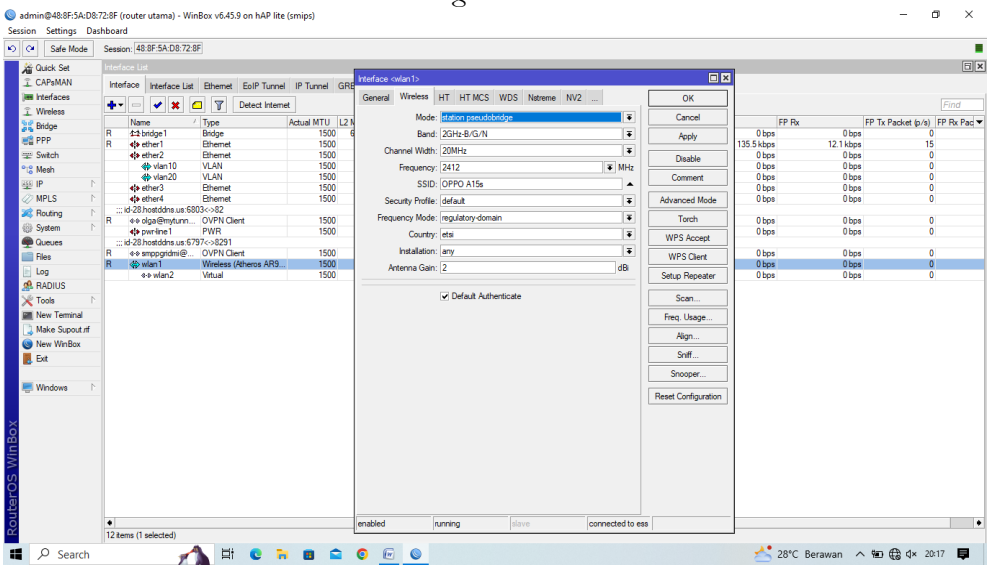
Gambar 7. Menu *Interface List*
Sumber: Hasil Rancangan, 2023

b. Setelah itu menampilkan menu *interface* wlan1->*general* ->apply->OK



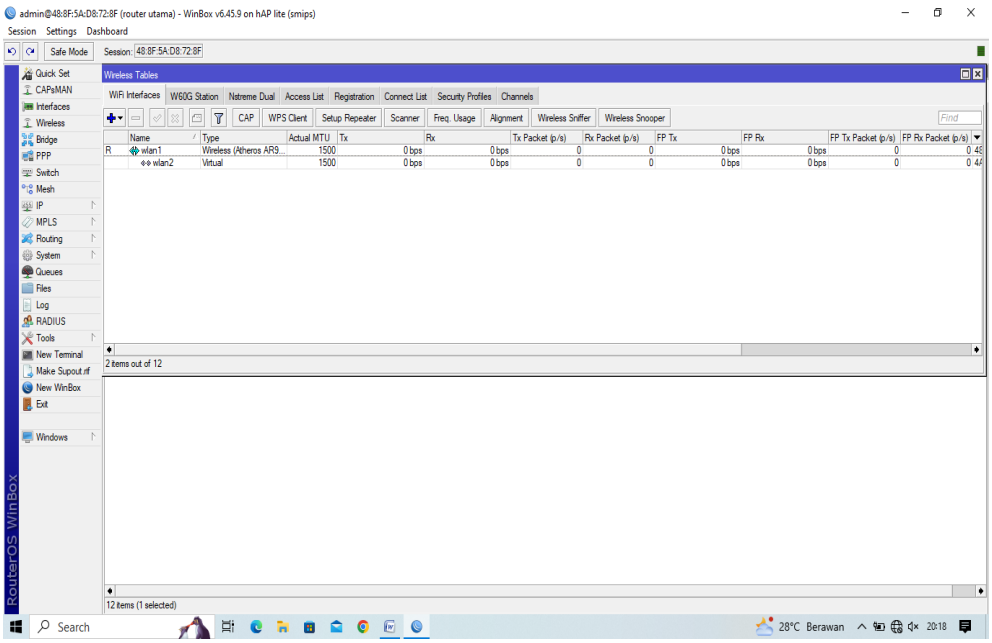
Gambar 8. *Interface Wlan1*
Sumber: Hasil Rancangan, 2023

3. Kemudian menampilkan menu *interface* wlan1->wirelass->Apply->Ok dimana:
   Mode : *Station-Psudobridge*



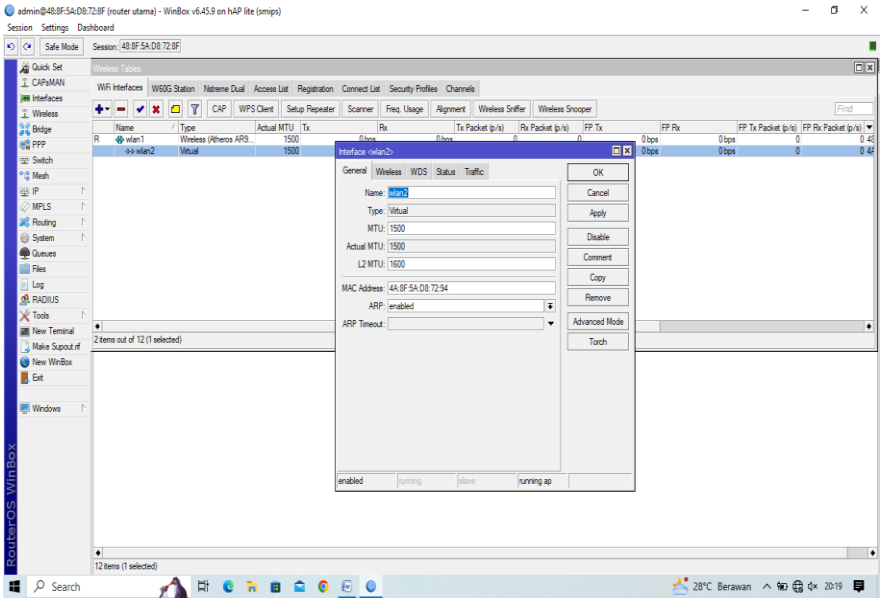
Gambar 9. *Interface Wlan1*
Sumber: Hasil Rancangan, 2023

4. Setelah itu, menampilkan *wifi interfaces*



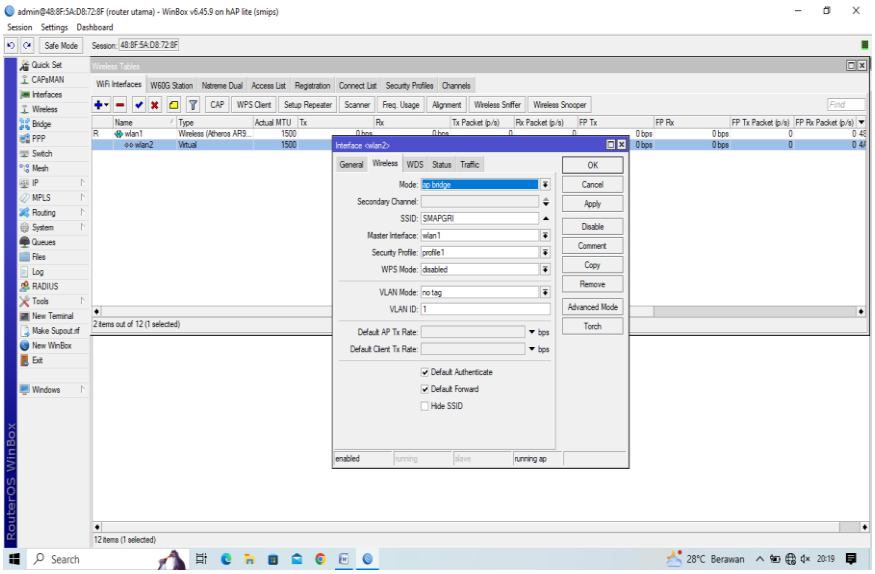
Gambar 10. *Wifi Interfaces*
Sumber: Hasil Rancangan, 2023

5. Kemudian menambahkan *interface* wlan2->Klik "+"->general->apply->OK
   Dimana: Name : Wlan2



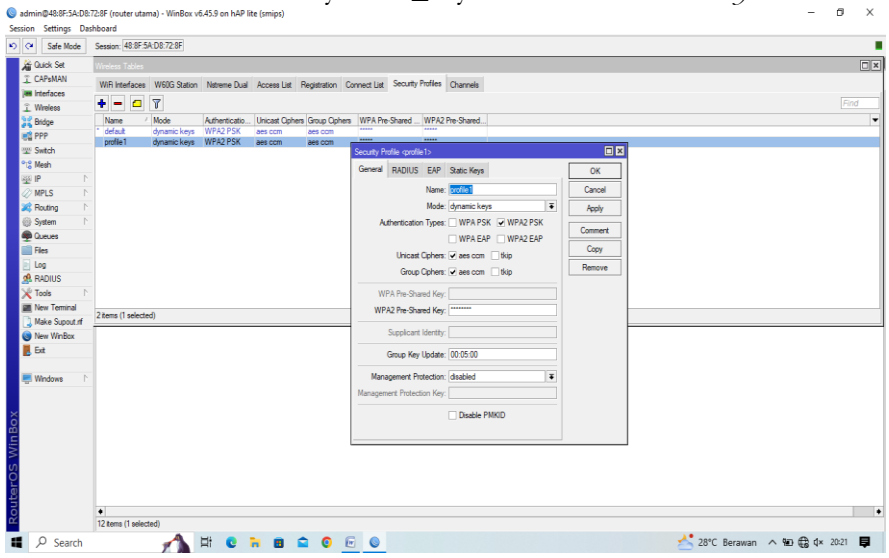
Gambar 11. *Interface* Wlan2
Sumber: Hasil Rancangan, 2023

6. Setelah itu menambahkan *interface* wlan2-> *Wireless*->apply->OK
   Dimana:
   Mode : Ap-*bridge* *Security Profile* : profile 1
   SSID : STIA-LK-DMI *Master Interface* : wlan1
   Security Profile : profile 1 *WPS Mobile* : *disabled*



Gambar 12. *Interface Wlan2*
Sumber: Hasil Rancangan, 2023

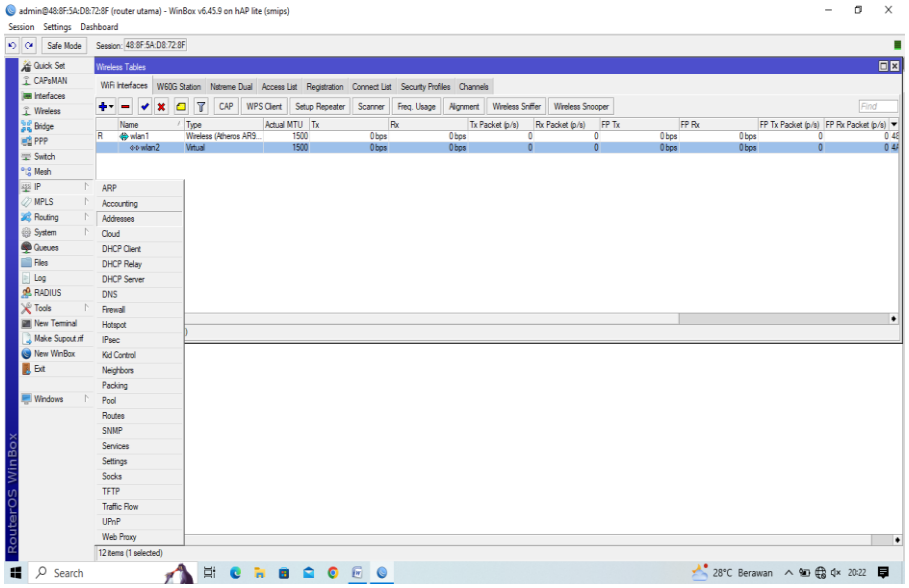
7. Setelah itu memberikan *security profile,* melakukan langkah pada menu *wireless tables* -> *security profile*-> klik "+"-> Apply -> Ok
   Dimana:
   Name : Profile1 *Autentication Types* : WPA2 PSK
   Mode : dynamic_keys WPA2 *Pre Shared Key* : 123456789



Gambar 13. *Security Profile1*
Sumber: Hasil Rancangan, 2023

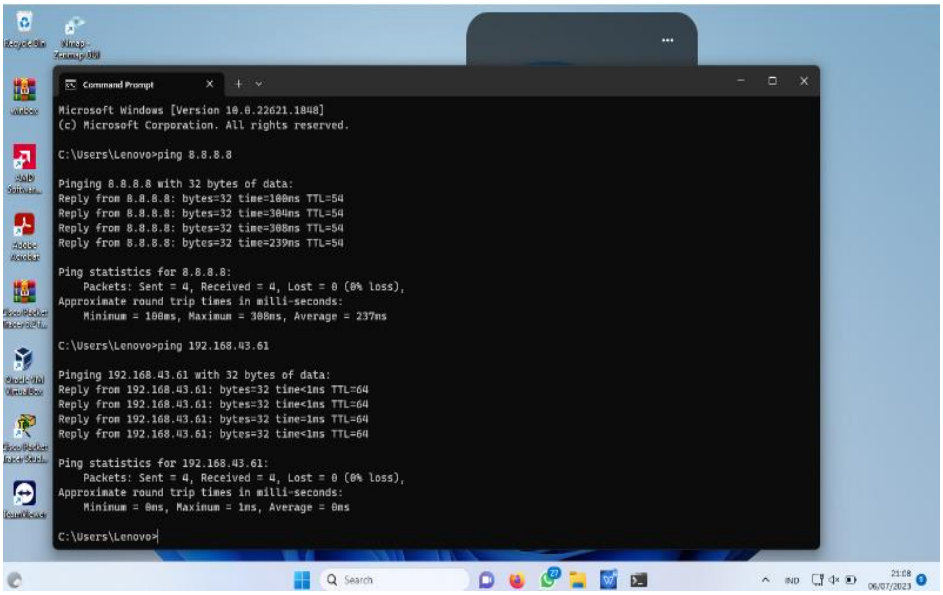
4.2 Konfigurasi IP *Adress* Pada Mikrotik

1. Pada Tampilan *winbox,* pilih menu ip->*address*



Gambar 14. Tampilan Menu Winbox
Sumber: Hasil Rancangan, 2023

4.3 Hasil Pengujian



Gambar 15. Pengujian Command Prompt
Sumber: Hasil Rancangan, 2023

5. Kesimpulan

Pemindaian port berhasil mengidentifikasi celah keamanan yang ada dalam jaringan STIA Lancang Kuning. Dengan mengetahui kerentanan ini, tindakan perbaikan dan penguatan dapat dilakukan untuk mengurangi risiko serangan. Selain itu, penerapan firewall tarpit membantu dalam memperlambat serangan dan membatasi akses penyerang, sehingga memberikan perlindungan tambahan terhadap sistem jaringan. Dalam konteks institusi pendidikan seperti STIA Lancang Kuning, keamanan jaringan sangat penting untuk melindungi data mahasiswa, informasi administrasi, dan sumber daya jaringan lainnya. Dengan mengimplementasikan metode yang efektif seperti port scanning dan firewall tarpit, STIA Lancang Kuning dapat meningkatkan keamanan jaringan mereka dan mengurangi risiko terhadap serangan dan pencurian data.

Pertimbangkan Penggunaan Teknologi Keamanan Tambahan: Selain port scanning dan firewall tarpit, pertimbangkan penggunaan teknologi keamanan tambahan seperti IDS (Intrusion Detection System) atau IPS (Intrusion Prevention System) untuk meningkatkan deteksi dan pencegahan serangan yang lebih lanjut.

6. Ucapan Terima Kasih

Terima kasih kepada Ketua STIA Lancang Kuning Dumai yang telah berkontribusi dan memberikan fasilitas/membantu dalam penelitian ini.

7. Pernyataan Penulis

Penulis menyatakan bahwa tidak ada konflik kepentingan terkait publikasi artikel ini. Penulis menyatakan bahwa data dan makalah bebas dari plagiarisme serta penulis bertanggung jawab secara penuh atas keaslian artikel.

Bibliografi

Asnawi, M.F. (2018) *Aplikasi Konfigurasi Mikrotik Sebagai Manajemen Bandwidth Dan Internet Gateway Berbasis Web.* Jurnal PPKM I(2018) 42-48

Azwar, S. (2019). *Reliabilitas dan Validitas* Edisi 4. Yogyakarta: Pustaka Pelajar

Dewi, L.P. Budihardjo, E.W (2020) *Pembuatan Konfigurasi SSL Yang Aman Untuk Diimplementasikan Pada Apache Dan Nginx.*

Efendi, I. (2019) *Topologi Jaringan Bandung* : Informasi Bandung.

Indrajani, 2015, *Database Design*, Jakarta : PT Elex Media Komputindo

Irawan, M., & Simargolang, S. (2018). *Implementasi E-Arsip Pada Program Studi Teknik Informatika.* Jurnal Teknologi Informasi, 67

R. Laksamana, E. Naf, E. Praja, and W. Mandala, "Protokol L2TP dan IPsec Sebagai Keamanan Jaringan Pada Dinas Kominfotik Sumatera Barat," vol. 10, no. 3, pp. 162–171, 2022.

Madcoms. (2020). *Manajemen Sistem Jaringan Komputer dengan Mikrotik RouterOS*. Jl. Letjend, Haryono 63 Madiun.

Purwaningrum, F. A, Purwanto, A. Darmadi, E.A. (2018) *Optimalisasi Jaringan Menggunakan Firewall.* Jurnal IKRA-IT. Vol.2 No.3

Rendro, D. W, Ngatomo, Aji, W. N (2020) *Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP* (Studi Kasus di SMK Negeri 1 Kota Serang) Vol. 7 No. 2

Sartomo, Sulistyo, W (2022). *Model Keamanan Jaringan Menggunakan Firewall Port Blocking.* Jurnal Teknik Informatika. Vol. 10. No.1

Syafrizal, M. (2018). Pengantar Jaringan Komputer. Yogyakarta: ANDI.

Tampi, S. S. Raharjo, S. Sholeh, M. (2019) *Perancangan Jaringan Komputer Pada Rumah Sakit Soedarsono Darmosoewito Di Batam.* Vol. 7 No. 1

Wicaksono, D. Widiasari, I.R. (2022) *Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering* . Jurnal Teknik Informatika Vol.9 N0.2