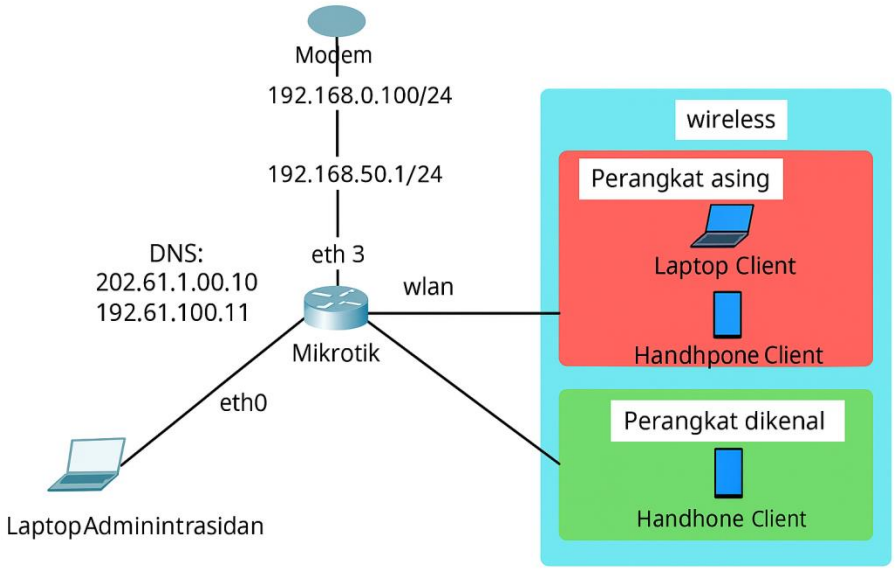
BAB IV
HASIL DAN PEMBAHASAN

4.1 Rangkaian Alat Sistem Segmentasi Jaringan MikroTik

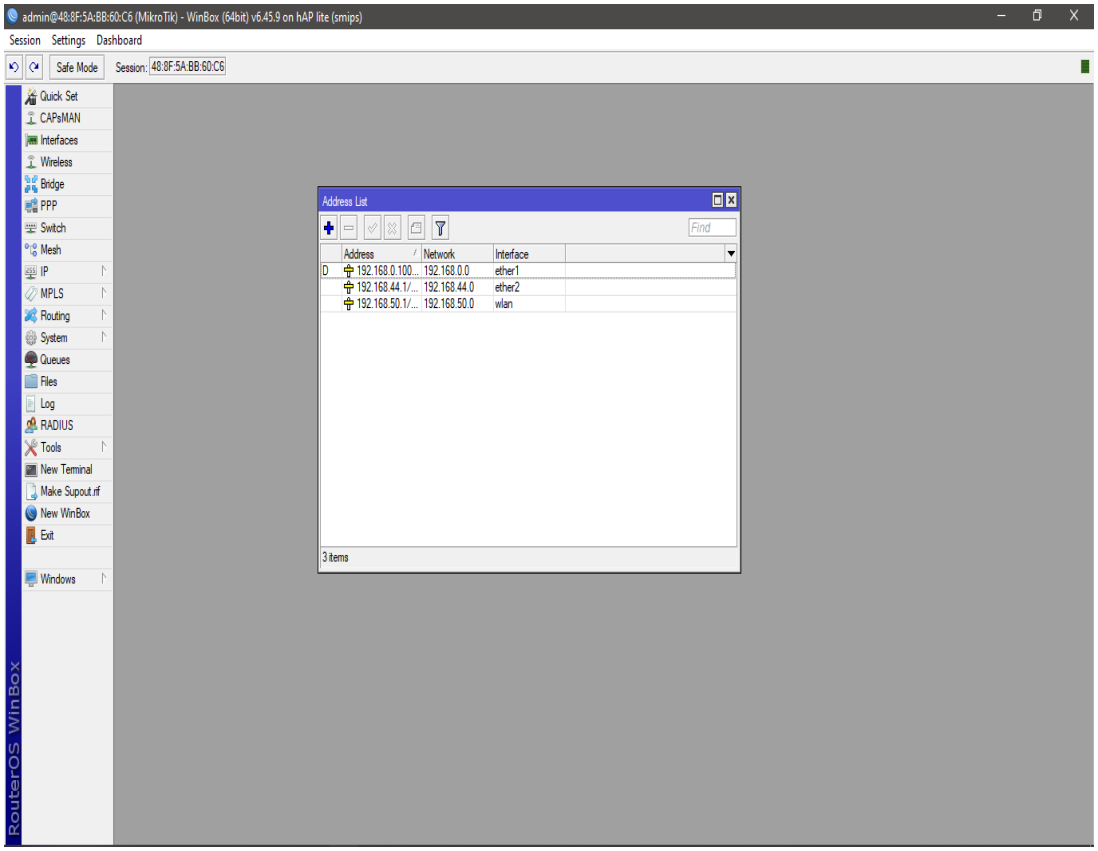
Pada penelitian ini akan dibahas tentang Implementasi *Port Knocking* Pada Mikrotik Untuk Meningkatkan Segmentasi Jaringan Menggunakan Metode *Access Control List* (ACL). Berikut ini adalah rangkaian alat sistem segmentasi jaringan dapat dilihat pada gambar 4.1.

Gambar 4. 1 Rangkaian Alat Sigmentasi Jaringan Mikrotik



Gambar 4. 2 Hasil Implementasi Segmentasi Jaringan MikroTik

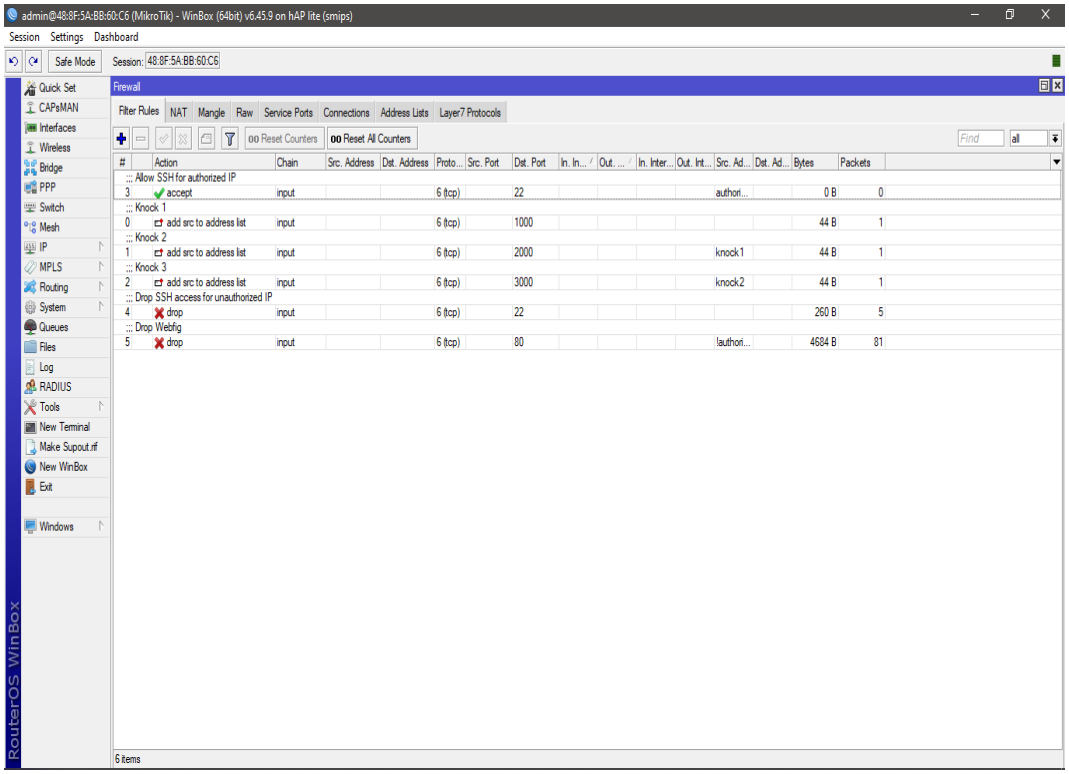
Pada tahap ini, dilakukan penerapan strategi keamanan jaringan di lingkungan Kantor Pengadilan Agama Rantauprapat Kelas I B dengan menggunakan teknik Port Knocking. Penerapan ini dilakukan pada komputer yang memiliki dua alamat IP berbeda, dengan memanfaatkan perangkat *Routerboard* Mikrotik hAP lite RB941-2nD sebagai media utama. Perangkat tersebut kemudian dikoneksikan dengan klien. Konfigurasi firewall serta akses ke sistem Mikrotik diatur melalui aplikasi *Winbox* yang telah disiapkan oleh peneliti. Dalam skema ini, *Port Knocking* berperan sebagai lapisan keamanan lanjutan, yang akan aktif setelah perangkat klien berhasil melewati tahapan *Access Control List*. Klien diharuskan melakukan ping ke IP Mikrotik terlebih dahulu agar dapat mengakses menu *Winbox* dan mengelola konfigurasi jaringan di dalamnya.



Gambar 4. 3 Pembuatan Alamat IP *Adress*

Penerapan segmentasi jaringan yang dilakukan pada MkroTik mengunakan winbox dibuat menjadi dua alamat IP berbeda :

1. Untuk alamat IP yang di *interface ether* 1 adalah IP DHCP Modem (atau sebagai penyedia *Internet*)
2. Untuk alamat IP yang ada di *interface ether* 2 adalah IP yang terhubung ke perangkat Mikrotik Menggunakan Kabel LAN
3. Untuk alamat IP yang ada di *interface wlan* adalah IP yang bisa terhubung ke perangkat tanpa kabel.



Gambar 4. 4 Mengkonfigurasi *Port Knocking* di MikroTik

Selanjutnya Konfigurasi *Port Knocking* yang sesuai dengan Gambar 4.3 menunjukkan tabel *Firewall – Filter Rules* pada *RouterOS* MikroTik (hAP lite RB941-2nD) yang diakses melalui WinBox. Konfigurasi ini menggunakan metode *port knocking* untuk mengamankan akses SSH, serta menutup akses *Webfig* dari pihak yang tidak berwenang.

Rincian *Rule*:

1. *Allow SSH for authorized IP*

   Action : *accept*

   Chain : *input*

   Protocol : TCP *port* 22

   Src. Address List : *authorized*

   Fungsinya : Mengizinkan koneksi SSH hanya dari IP yang sudah masuk daftar *authorized*.

2. *Knock* 1

   Action : *add src to address list knock1*

   Chain : *input*

Protocol : TCP *port* 1000

Fungsinya : Menambahkan IP pengirim ke daftar *knock1* setelah mengetuk (mengakses) *port* 1000.

3. *Knock* 2

Action : *add src to address list knock2*

Chain : *input*

Protocol : TCP *port* 2000

Src. Address List : *knock1*

Fungsinya : Hanya IP yang sudah melakukan Knock 1 yang dapat melanjutkan ke Knock 2.

4. *Knock* 3

Action : *add src to address list authorized*

Chain : *input*

Protocol : TCP *port* 3000

Src. Address List : *knock*2

Fungsinya : Jika sudah melewati *Knock* 1 dan *Knock* 2, mengetuk *port* 3000 akan membuat IP masuk ke daftar *authorized*.

5. *Drop SSH unauthorized*

Action : d*rop*

Chain : *input*

Protocol : TCP *port* 22

Fungsinya : Memblokir akses SSH dari IP yang tidak ada di daftar *authorized*.

6. *Drop Webfig*

Action : *drop*

Chain : *input*

Protocol : TCP *port* 80

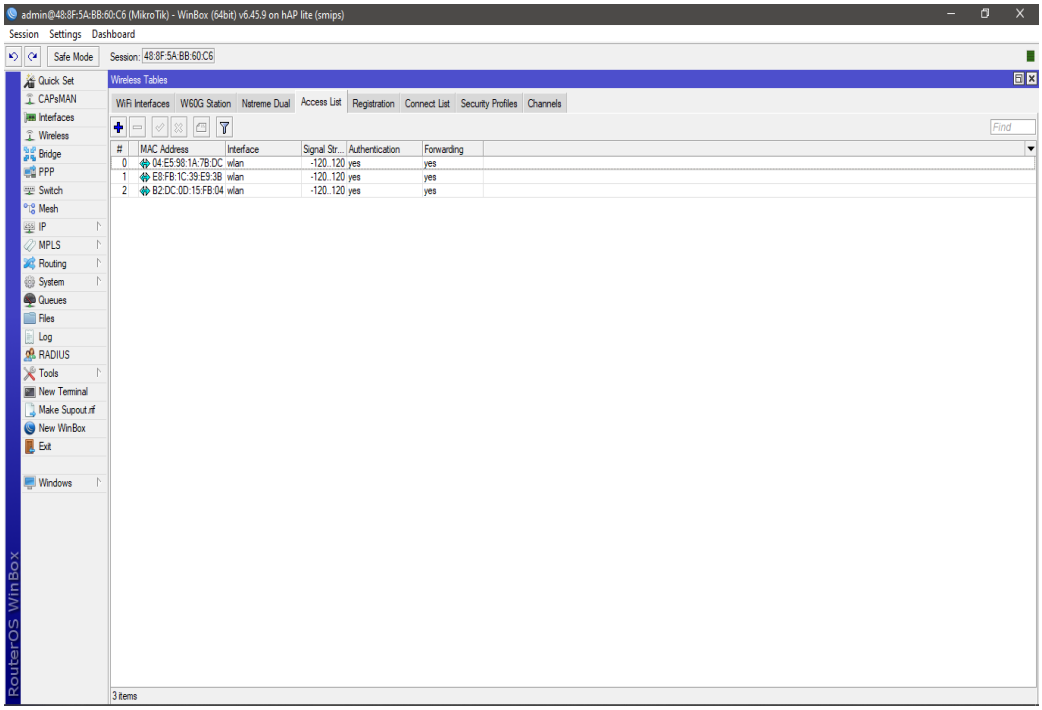
Src. Address List : *authorized* (tidak ada di rule ini berarti semua yang tidak *authorized* akan diblokir)

Fungsinya : Memblokir akses ke *Webfig* (*port* 80) dari pihak luar.

Hasil kesimpulan dari konfigurasi *port knocking* pada MikroTik:

- Keamanan meningkat: Hanya pengguna yang tahu urutan *port knocking* (1000 → 2000 → 3000) yang bisa mengakses SSH.
- Akses *Webfig* diblokir: Mengurangi risiko serangan melalui antarmuka *web* MikroTik.
- Efektivitas: *Port knocking* mencegah pemindaian *port* langsung oleh *attacker* karena *port* SSH (22) hanya terbuka setelah urutan *knock* yang benar.
- Monitoring: Nilai *Bytes* dan *Packets* menunjukkan sudah ada beberapa percobaan *knock* dan akses SSH.

Sementara itu, pada metode kedua yaitu *Access Control List* (ACL), pengamanan jaringan dilakukan melalui jaringan *WiFi* yang telah dikonfigurasi pada Mikrotik agar hanya memancarkan sinyal pada area terbatas, yaitu ruang *server*. Setelah Mikrotik diatur untuk menyiarkan jaringan nirkabel, dilakukan konfigurasi *Access List* guna menentukan perangkat yang diizinkan terkoneksi. Hanya perangkat dengan MAC *Address* tertentu yang diizinkan bergabung ke dalam jaringan tersebut. Selain itu, pengaturan tambahan seperti kekuatan sinyal, durasi koneksi, serta kecepatan akses turut dimanajemen demi meningkatkan keamanan dan efisiensi jaringan seperti pada Gambar 4. 3 dibawah ini.



Gambar 4. 5 Konfigurasi *Access Control List* (ACL)

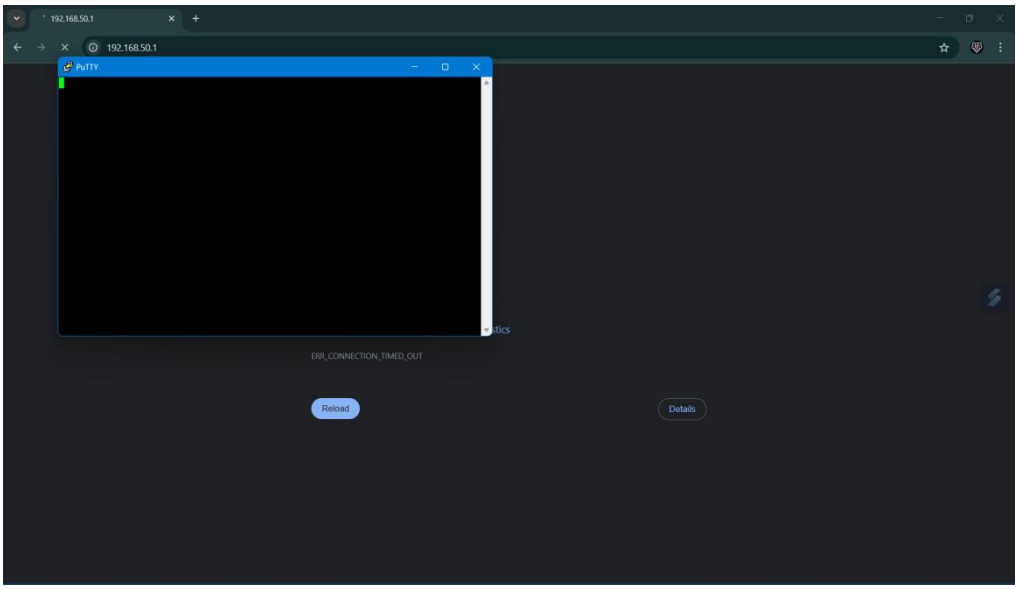
4.2 Pengujian Sistem Segmentasi Jaringan MikroTik

Pengujian merupakan tahapan krusial yang bertujuan untuk menilai efektivitas implementasi dari konfigurasi jaringan yang telah dirancang sebelumnya. Tujuan utama dari proses ini adalah untuk memastikan bahwa konfigurasi baru dapat diterapkan secara optimal dan memberikan kemudahan bagi administrator jaringan dalam pengelolaan sistem, khususnya pada objek penelitian yang telah ditentukan. Setelah melalui tahap perancangan dan implementasi, pengujian dilakukan guna mengevaluasi sejauh mana metode yang digunakan dapat mendukung peningkatan kualitas layanan jaringan di Kantor Pengadilan Agama Rantauprapat Kelas I B.

Adapun skenario pengujian dilakukan dengan menggunakan satu unit laptop administrator yang telah dikonfigurasi menggunakan metode *Port Knocking,* satu perangkat Mikrotik hAP lite RB941-2nD sebagai pusat pengendali jaringan, serta satu unit laptop *clien* yang digunakan untuk mensimulasikan akses tanpa melalui mekanisme keamanan *Port Knocking* khususnya terhadap akses ke aplikasi *Winbox.*

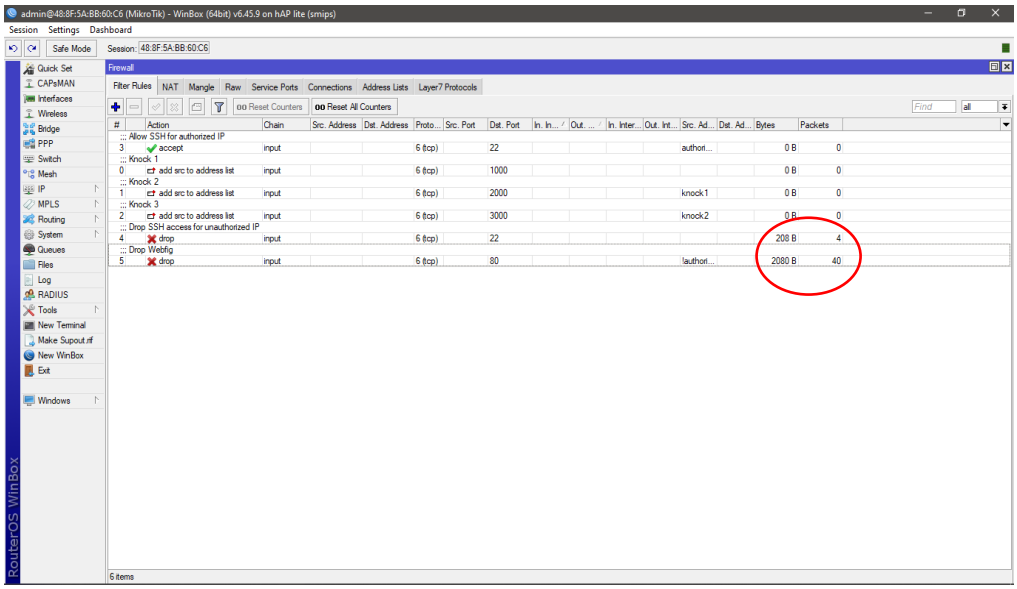
4.2.1 Pengujian *Port Knocking* di Mikrotik

1. Pengujian *Webfig* dengan membuka *webbrouser/Chrome* dengan tujuan ke IP Mikrotik sekaligus meremote dengan Aplikasi *Putty* dengan tujuan ke IP MikroTik sudah di berik akses atau tidak.



Gambar 4. 6 Tampilan dari perangkat komputer *clien*

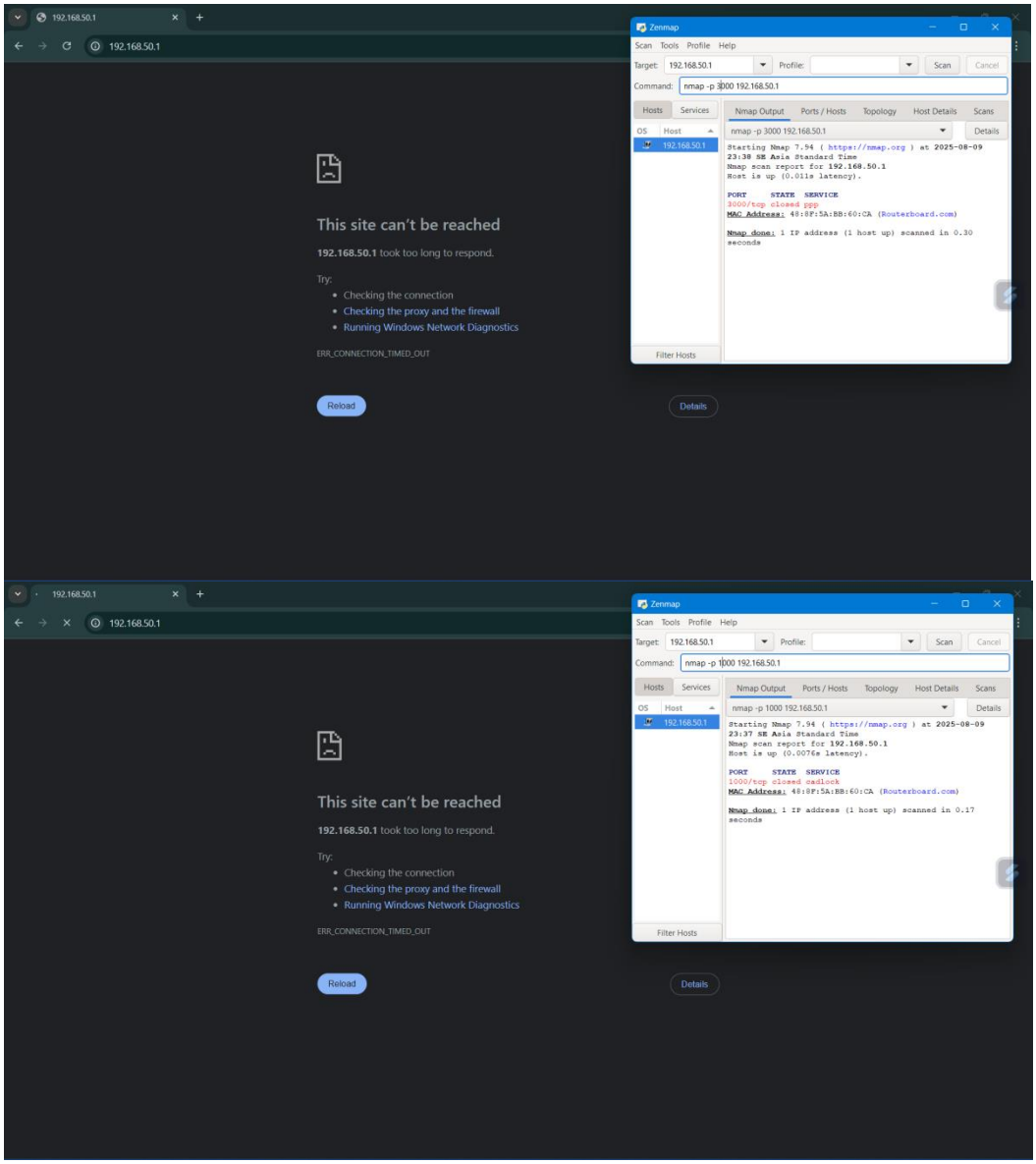
Dari gambar 4. 5 menjelaskan bahwa IP clien masuk ke daftar knock atau IP masih belum sudah masuk daftar *authorized* dan belum di beri izin akses sebelum menyelesaikan langkah-langkah memasuki port yang sudah berurutan.



Gambar 4. 7 Tampilan *winbox* dari perangkat komputer admin

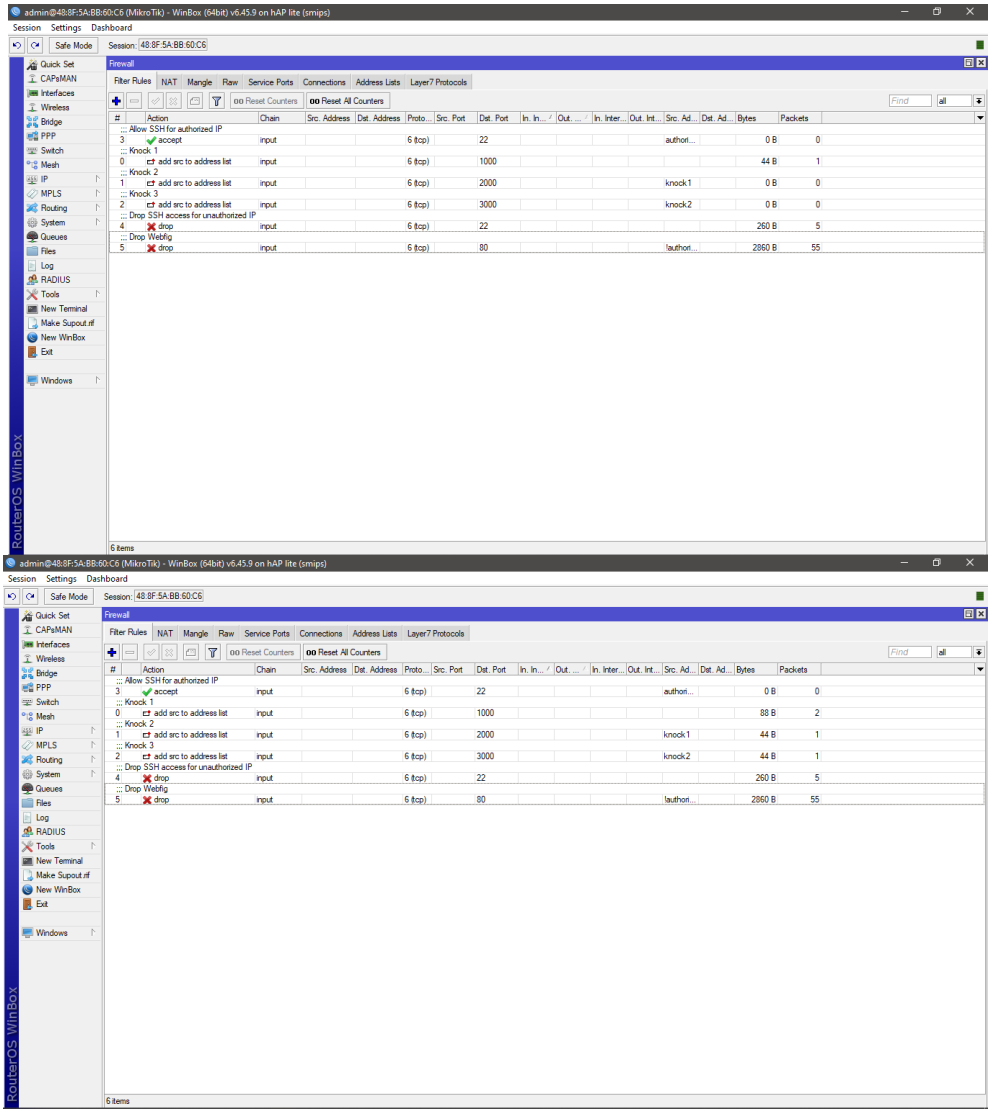
Dari gambar 4. 6 menjelaskan bahwa dari perangkat komputer admin ada IP *clien* yang mencoba masuk dan masih ter*knock* atau IP masih belum di beri izin akses sebelum menyelesaikan langkah-langkah memasuki *port* yang sudah berurutan.

2. Mengetuk *Port* yang benar secara berurutan



Gambar 4. 8 Mengetuk *Port* yang benar secara berurutan

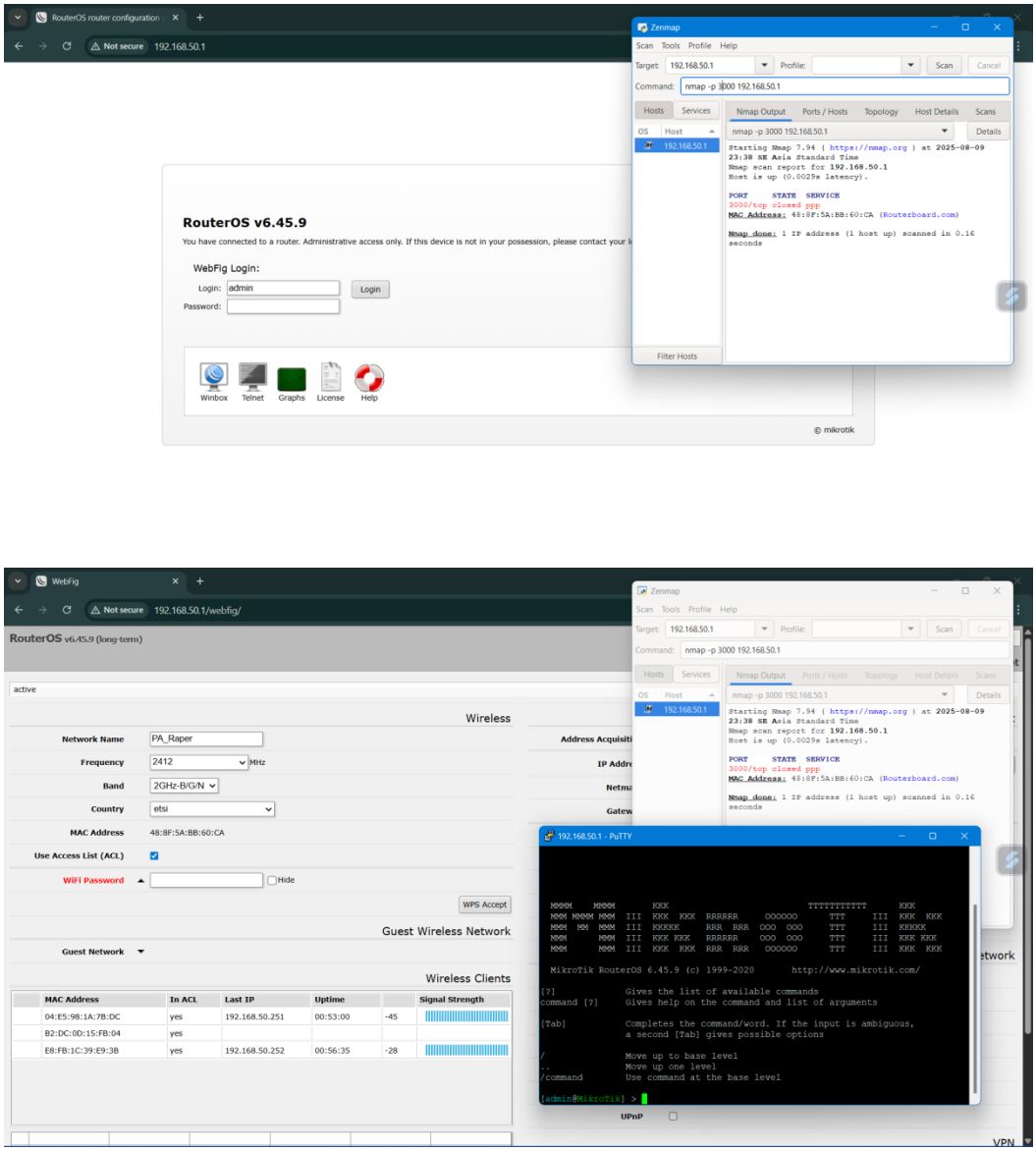
Dari gambar 4. 7 menjelaskan bahwa perangkat clien harus mengetuk *port* yang benar secara berurutan agar diberi izin akses masuk dan masuk ke daftar *authorized.*



Gambar 4. 9 Tampilan *winbox* di laptop admin mengecek *port* yang masuk

Dari gambar 4. 8 Menjelaskan bahwa perangkat laptop *clien* sudah mengetuk port yang benar dan sesuai dengan urutannya maka IP *clien* akan di beri izin masukkan ke dalam daftar *authorized*.

3. Tampilan laptop *clien* sudah diberi izin mengakses *webfiq* dan jaringan mikrotik

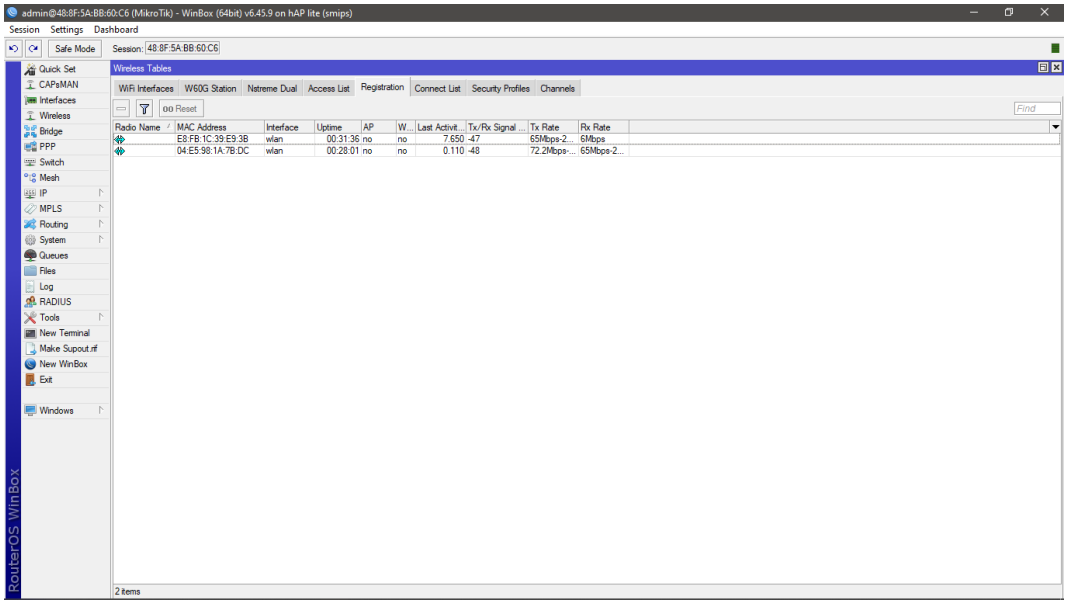


Gambar 4. 10 Tampilan di latop *clien* bahwa sudah diberi izin akses

Dari gambar 4. 9 menjelaskan bahwa laptop *clien* sudah diberi izin mengakses *webfiq* dan jaringan mikrotik.

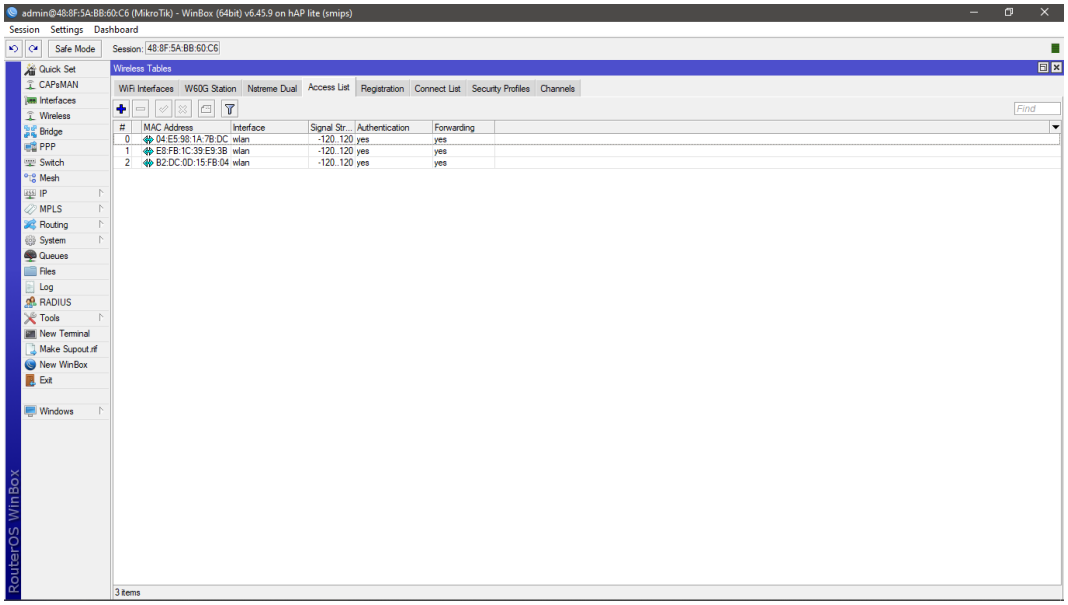
4.3.2 Pengujian *Access Control List* di MikroTik

Pengujian metode *Access Control List* (ACL), digunakan satu perangkat laptop (merk Asus CoreI5) dan *handphone* (redmi 9c) yang disesuaikan konfigurasinya untuk mengelola perangkat klien yang terkoneksi melalui jaringan *WiFi.* Konfigurasi dilakukan berdasarkan prinsip dan aturan yang telah ditetapkan dalam metode ACL, seperti pengaturan hak akses perangkat berdasarkan MAC *Address* serta pengelolaan kekuatan sinyal, durasi koneksi, dan kecepatan akses.



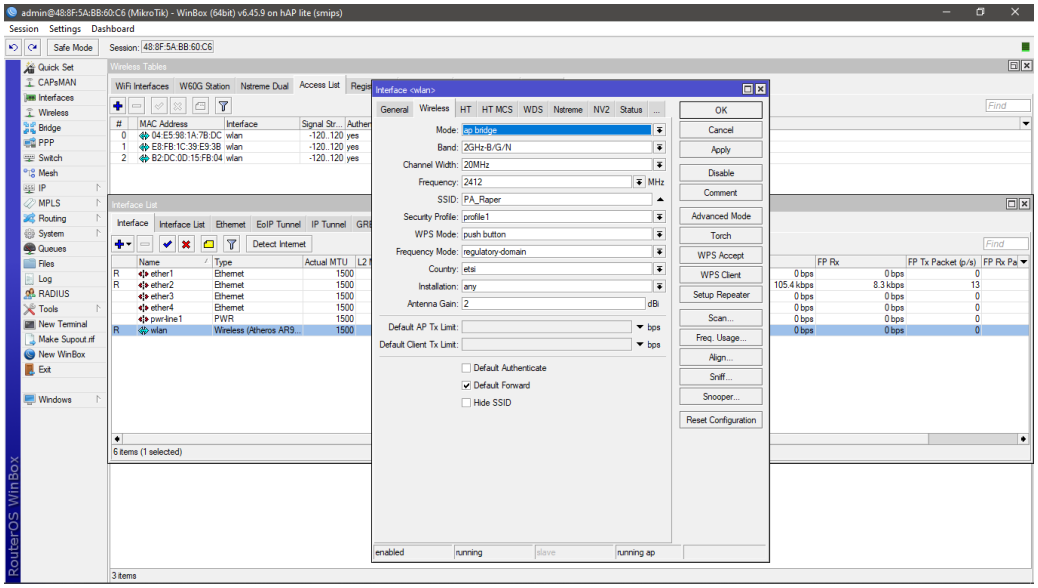
Gambar 4. 11 *Registrasi* MAC *Address* yang akan diberi izin *Access List*

MAC *address* setiap perangkat akan terdaftaftar ke mikrotik bila perangkat clien ingin mencoba masuk ke jaringan internet, MAC *address* yang belum terdaftar ke daftar *Access List* akan masuk ke menu *Registrasion* . MAC *address* yang belum di pindahkan ke daftar *Access List* tidak akan diberi izin akses *internet*/akses ditolak.



Gambar 4. 12 MAC *Address* yang sudah dipendahkan ke menu *Address List*

MAC *Address* yang sudah di pindahkan ke menu *address list* dan sudah terdaftar akan otomatis diberi akses jaringan tanpa harus menunggu izin akses dari perangkat laptop administrasion.



Gambar 4. 13 Pengaturan Menutup *access* dari perangkat luar yang masuk

Pengaturan *Access Control List* dari *winbox – interface* agar *Access* ditutup untuk MAC *Address* yang tidak terdaftar di menu *Access List* yang mencoba masuk dan hanya MAC *Address* yang terdaftar di menu *Access List* saja yang bisa mengakses jaringan *internet*.

4.3 Keunggulan Sistem Segmentasi Jaringan MikroTik

Tabel 4. 1 Keunggulan Segmentasi jaringan Mikrotik menggunakan ACL dan *Port Knocking*

No	Aspek	Keunggulan	Kekurangan
1	Keamanan	Meminimalkan akses tidak sah antar segmen jaringan melalui ACL dan *Port Knocking*	Konfigurasi keamanan membutuhkan pemahaman teknis yang mendalam
2	Manajemen	Mudah mengelola pengguna dan perangkat berdasarkan segmen	Pengaturan banyak segmen dapat menjadi rumit tanpa dokumentasi yang baik
3	Performa	Mengurangi broadcast dan meningkatkan efisiensi jaringan	Jika salah konfigurasi, dapat menyebabkan segmentasi tidak berfungsi optimal
4	Skalabilitas	Mudah dikembangkan sesuai kebutuhan jaringan	Perlu *upgrade hardware* untuk jaringan besar dengan banyak segmentasi
5	Fleksibilitas Konfigurasi	Bisa diterapkan secara fisik maupun *virtual* (VLAN, *port*)	Penggunaan VLAN memerlukan perangkat yang mendukung VLAN tagging
6	Integrasi Wireless	Dapat membedakan akses WiFi antara tamu dan staf melalui Virtual AP/VLAN	Perlu pengaturan ekstra untuk integrasi SSID dengan VLAN
7	*Monitoring* dan *Logging*	Mendukung pengawasan trafik antar segmen menggunakan fitur monitoring bawaan	Membutuhkan server log eksternal untuk skala monitoring yang besar