BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

Berdasarkan proses pengumpulan data, penelitian ini menggunakan metode *Port mirroring* untuk pendeteksian *malicious traffic* pada ponsel android *"China Brand"* menggunakan aplikasi Maltrail dengan ponsel android *"China Brand"* yang berbeda sebagai obyek penelitian. Proses ini dilakukan selama 1 hari (1x24 jam) pada masing-masing ponsel android *"China Brand"* data yang dikumpulkan adalah trafik akses internet dari ponsel android *"China Brand"* tersebut. Ponsel android *(China Brand)* yang digunakan dalam keadaan *fresh install* atau setelan pabrik. Rangakain pengambilan trafik dimulai dengan proses pengoneksian raspberry pi yang sudah terinstall aplikasi Maltrail menggunakan terminal linux dengan *set up* dan *configuration* MikroTik dasar menggunakan WinBox. Kemudian dilakukan analisis hasil dari penelitian tersebut.

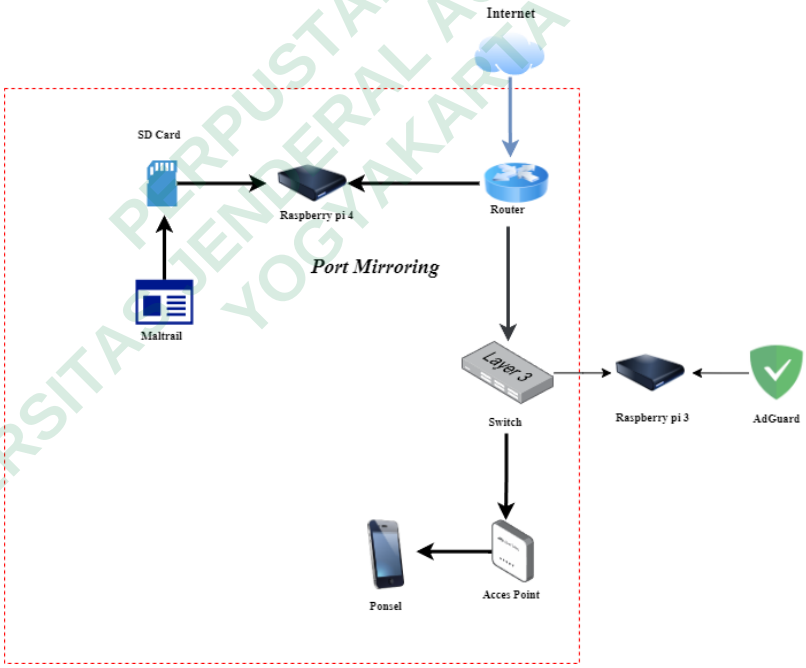
4.1.1 Proses Pengumpulan Data

4.1.1.1 *Port Mirroring*

Port Mirroring adalah sebuah teknik dalam jaringan komputer yang digunakan untuk memantau lalu lintas jaringan yang melewati satau atau beberapa port pada switch atau router. Dalam port mirroring, lalu lintas dari satu atau lebih port yang ditentukan akan disalin atau "dimirroring" ke port lain yang disebut sebagai port tujuan atau port monitor. Port monitor ini kemudian dapat digunakan untuk memantau atau menganalisis lalu lintas jaringan tersebut. Port mirroring digunakan untuk tujuan pemecahan masalah jaringan, analisis lalu lintas, atau keamanan jaringan. Dengan menggunakan port mirroring, administrator jaringan dapat memantau aktivitas jaringan secara real-time, menganalisis paket data, dan mengidentifikasi masalah jaringan atau ancaman keamanan. Dalam pengaturan *port mirroring*, lalu lintas yang disalin ke port berfungsi agar

dapat mencakup semua paket yang melewati port sumber atau hanya paket yang memenuhi kriteria tertentu, seperti paket yang berasal dari atau menuju ke alamat IP atau port tertentu (Christandl et al., 2021)

Menunjukan rangkaian setup MikroTik yang berperan dalam proses port mirroring dengan menggunakan 3 kabel ethernet yaitu kabel abu-abu merupakan kabel distribusi internet dari swicth kemudian dikoneksikan pada MikroTik untuk mendapatkan internet yang kemudian didistribusikan kembali menggunakan kabel putih yang digunakan untuk mengoneksikan internet kedalam Raspberry, dan kabel abu- abu merupakan kebel yang dikoneksikan dari MikroTik menuju Mi Router 4C untuk menjalankan proses *port mirroring*.



Gambar 4.1 Metode *Port Mirroring*

4.1.1.2 IDS *(Intrusion Detection System)*

Intrusion Detection System (IDS) adalah perangkat atau aplikasi yang dirancang untuk memantau jaringan atau sistem komputer guna mendeteksi aktivitas mencurigakan atau tidak sah. IDS mengidentifikasi

potensi ancaman dengan menganalisis lalu lintas jaringan atau perilaku sistem. Ketika mendeteksi sesuatu yang mencurigakan, IDS akan memberikan peringatan kepada administrator sehingga tindakan pencegahan bisa segera diambil. IDS dapat memanfaatkan *port mirroring* dengan cara pemantuan lalu lintas jaringan, analisis lalu lintas yang detail, keamanan jaringan, mengurangi beban pada jaringan, dan meningkatkan efisiensi respon(Varghese & Muniyal, 2021)

4.1.1.3 Instalasi Raspberry

Gambar 4.2. Tampilan imager Raspberry Pi

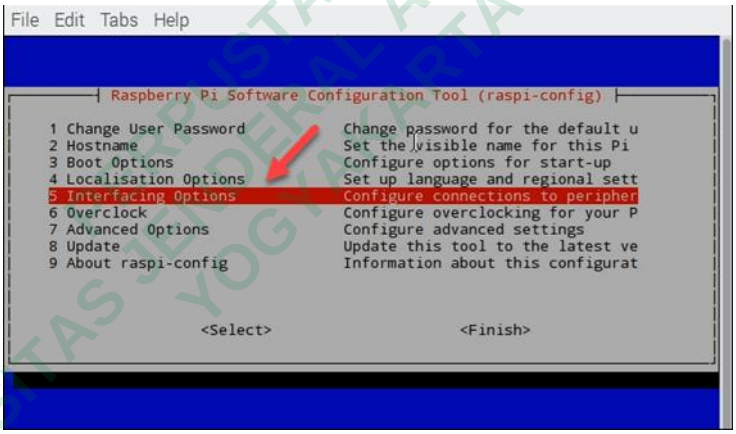
Dalam penelitian ini penulis melakukan instalasi Raspberry Pi dimulai dengan instalasi *Imager* seperti pada Gambar 4.2**.** Pengunduhan dan penginstalan dilakukan dengan mengunjungi situs resmi Raspberry Pi atau situs distribusi OS Raspberry Pi. Pengunduhan Imager dilakukan pada situs resmi Raspberry Pi. Kemudian di ekstrak pada mikroSD Card sebagai media penyimpanan utama. Kartu mikroSD yang digunakan adalah V-GEN 32GB sebagai penyimpan aplikasi Maltrail. Ada beberapa model Raspberry Pi yang tersedia, dalam penelitian ini penulis mengunakan Raspberry Pi 4. Raspberry Pi membutuhkan sistem operasi (OS) agar dapat berfungsi. OS yang digunakan pada penelitian ini adalah Ubuntu 22.04.3LTS. Dibutuhkan juga hardware seperti monitor, keyboard, dan mouse sebagai komponen untuk menghubungkan ke Raspberry Pi. Setelah Raspberry Pi selesai

Booting, akan diarahkan ke antarmuka konfigurasi OS untuk mengatur pengaturan jaringan, bahasa, zona waktu, dan konfigurasi lainya.

Setelah melakukan penginstalan Raspberry, kemudian mengaktifkan SSH dengan raspi-config. . Berikut adalah langkah-langkah mengkatifkan SSH pada Raspberry Pi di Terminal linux :

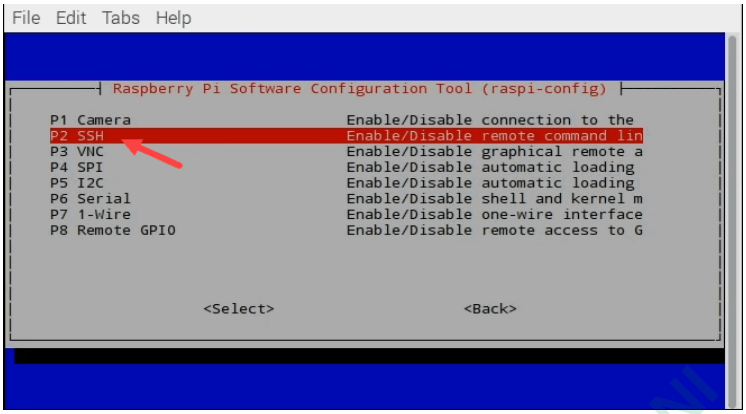
1. Buka terminal pada Raspberry Pi dan jalankan alat dengan mengetik: "`sudo raspi-config`"

2. setelah itu akan muncul opsi antarmuka, kemudian Pilih "`Interfacing Options`" seperti pada **Gambar 4.3** dibawah ini:



Gambar 4.3 konfigurasi SSH

3. Pilih opsi P2 SSH, seperti pada **Gambar 4.4** dibawah ini

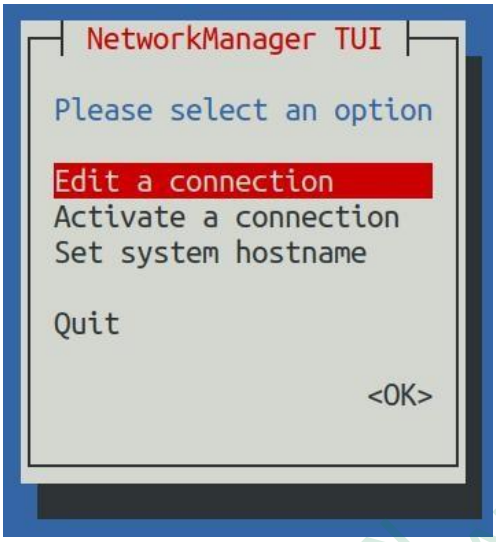


Gambar 4.4 SSH diaktifkan

4. Pilih **<Ya>** pada "Apakah Anda ingin server SSH diaktifkan?" mengingatkan.
5. Tekan **Enter** pada kotak konfirmasi "Server SSH diaktifkan".
6. Arahkan ke bawah dan pilih **Selesai** untuk menutup *raspi-config*.

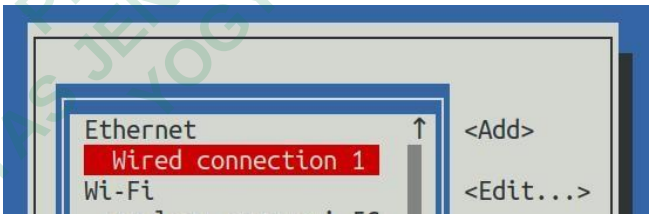
Untuk terhubung melalui SSH ke Raspberry Pi dari terminal, gunakan perintah ini: `"ssh -l username Raspberry Pi_ip address"`. SSH (*secure shell*) adalah protokol jaringan yang memberikan cara aman untuk mengakses dan mengelola perangkat jarak jauh melalui jaringan yang tidak aman. SSH menyediakan enkripsi data, yang berarti data yang dikirimkan antara client dan server dienkripsi untuk mencegah penyadapan dan serangan lainnya (Park et al., 2021). Setelah Mengaktifkan SSH dengan raspi-config, kemudian mengatur alamat IP statis, Berikut adalah langkah-langkah mengkatifkan SSH pada Raspberry Pi di Terminal linux :

1. Pertama jalankan perintah "nmtui"
2. Kemudian pilih Edit koneksi dan tekan Enter, seperti pada **Gambar 4.5** dibawah ini



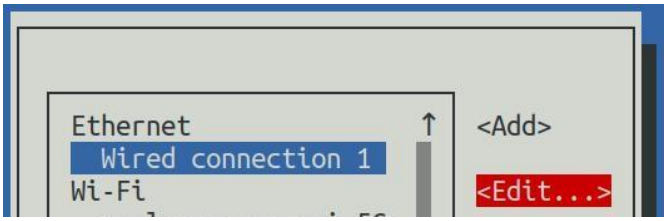
Gambar 4.5 menu antarmuka nmtui

3. Kemudian pilih antarmuka jaringan yang perlu diatur alamat IP statisnya, misalnya untuk mengatur alamat IP statis antarmuka Ethernet, pilih Koneksi kabel 1, seperti pada **Gambar 4.6** dibawah ini



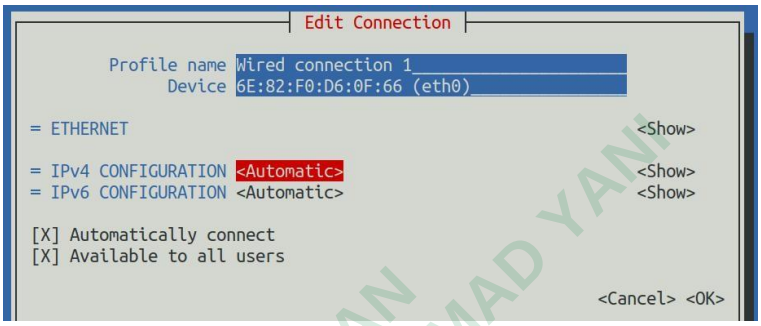
Gambar 4.6 menu antarmuka jaringan

4. setelah itu pilih Edit melalui tombol Tab dan tekan tombol Enter, seperti pada **Gambar 4.7** dibawah ini



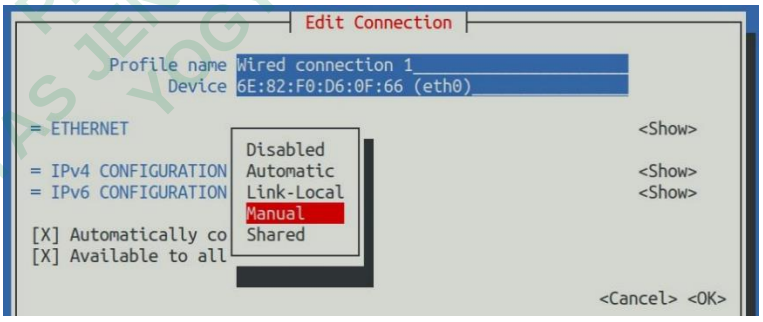
Gambar 4.7 menu antarmuka jaringan

5. Kemudian, gunakan tombol Tab untuk memindahkan kursor ke posisi <Automatic> yang ditunjukkan pada gambar di bawah ini untuk mengonfigurasi IPv4. Seperti pada **Gambar 4.8** dibawah ini



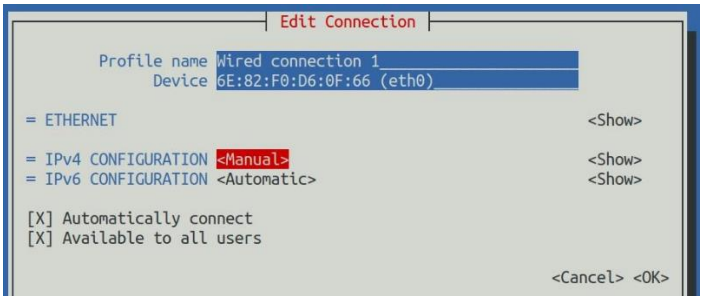
Gambar 4.8 mengatur konfigurasi IPv4

6. Lalu tekan Enter, pilih Manual melalui tombol panah atas dan bawah, lalu tekan Enter untuk konfirmasi, seperti pada **Gambar 4.9** dibawah ini



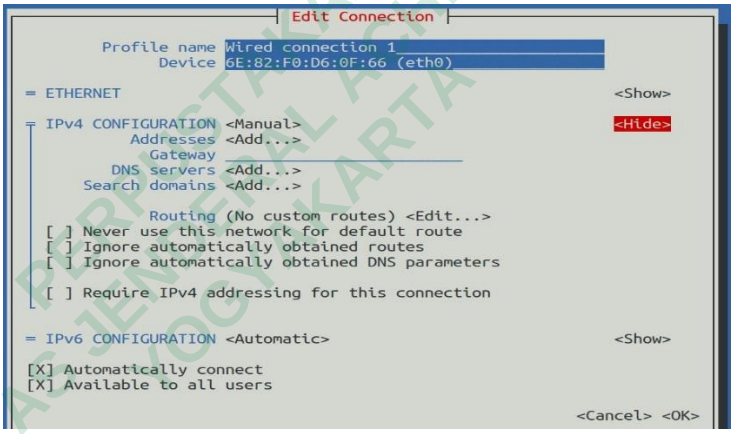
Gambar 4.9 mengatur konfigurasi IPv4

7. Tampilan setelah pemilihan ditunjukkan pada **Gambar 4.10** di bawah ini



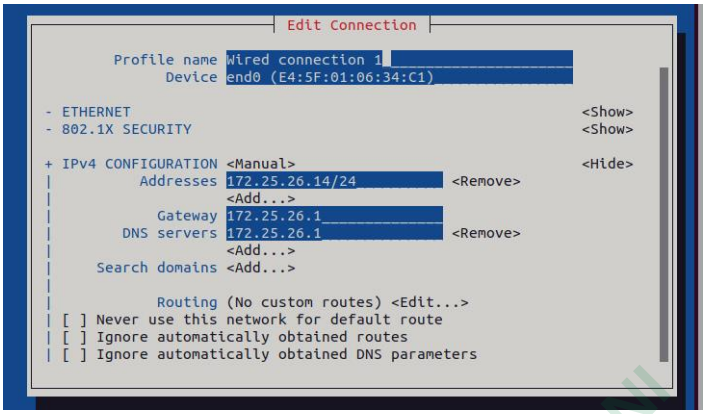
Gambar 4.10 Tampilan setelah pemilihan

8. Kemudian pindahkan kursor ke <Show> melalui tombol Tab lalu tekan **Enter**, dan antarmuka pengaturan berikut akan munul setelah masuk, seperti **Gambar 4.11** dibawah ini



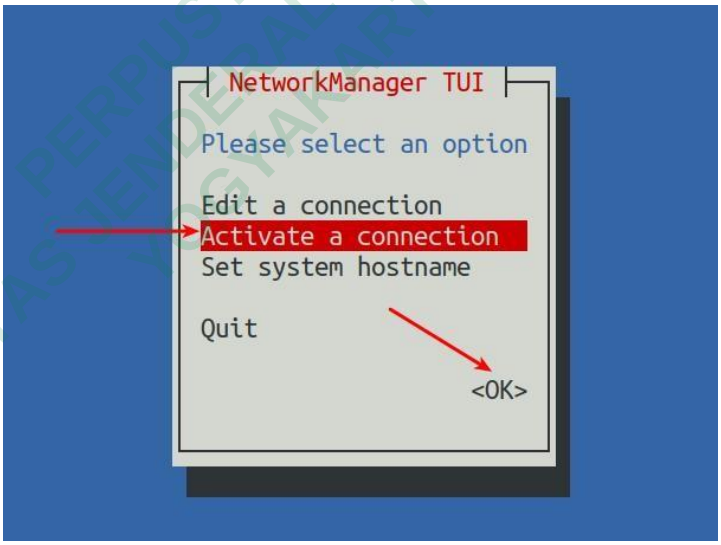
Gambar 4.11 mengatur konfigurasi IPv4

9. kemudian mengatur IP Address, Gateway, dan DNS server Setelah melakukan setting IP address, Gateway dan DNS server, pindahkan kursor ke <OK> disudut kanan bawah, dan tekan Enter. Nanti akan muncul ke menu antar muka Ethernet kemudian klik <Back> untuk kembali ke menu antar muka pilihan, seperti **Gambar 4.12** di bawah ini



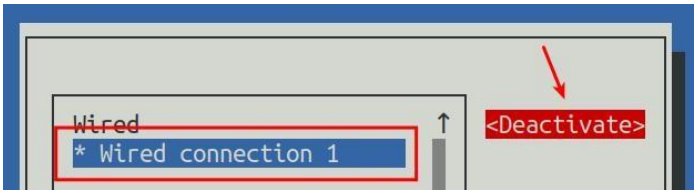
Gambar 4.12 Mengatur IP Address, Gateway, dan DNS server

10. Lalu pilih Activate a connection, kemudian pindahkan kursor ke <OK> setelah itu klik enter, seperti **Gambar 4.13** di bawah ini



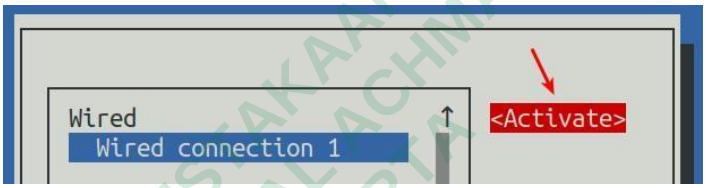
Gambar 4.13 tampilan anatarmuka nmtui

11. kemudian pilih antarmuka jaringan yang perlu diatur, seperti Wired connection 1, lalu Gerakan kursor ke <Deactivate> dan tekan enter untuk menonaktifkan Wired connection 1, seperti pada **Gambar 4.14** dibawah ini



Gambar 4.14 Pengaturan antarmuka jaringan

12. kemudian tekan tombol Enter untuk mengaktifkan kembali Wired connection 1, sehingga Alamat IP statis yang ditetapkan sebelumnya akan berlaku, seperti pada **Gambar 4.15** dibawah ini



Gambar 4.15 Pengaturan antarmuka jaringan

Setelah melakukan seting IP statis, kemudian dapat keluar dari nmtui melalui tombol <back> dan keluar.

Setelah mengatur alamat IP statis, kemudian mengaktifkan *promiscuous.* Cara mengaktifkan mode *promiscuous* pada antarmuka jaringan menggunakan perintah `ifconfig` atau `ip`. Berikut cara menggunakan kedua metode tersebut :

1. Menggunakan `ifconfig`: “`sudo ifconfig <interface_name> promisc`”. Misalnya, jika ingin mengaktifkan mode promiscuous pada `eth0` antarmuka, maka dapat dijalankan seperti berikut:
   “`sudo ifconfig eth0 promisc`”
2. Menggunakan `ip :`” `sudo ip link set <interface_name> promisc on`”. untuk mengaktifkan mode promiscuous pada `eth0` antarmuka menggunakan `ip` perintah : “`sudo ip link set eth0 promisc on`”

Promiscuous adalah fitur dalam jaringan komputer yang memungkinkan kartu jaringan (NIC) menangkap dan membaca semua paket data yang melewati jaringan (Net_traffic_monitors3, n.d.). Beberapa kegunaan dari *promiscuous*:

a. Pemantauan Jaringan *(Network Monitoring)*: Administrator jaringan menggunakan mode promiscuous untuk memantau lalu lintas jaringan dan menganalisis kinerja serta mendeteksi masalah.

b. Penangkapan Paket *(Packet Sniffing)*: Alat seperti Wireshark dapat digunakan dalam mode promiscuous untuk menangkap dan menganalisis paket data yang melewati jaringan, membantu dalam troubleshooting jaringan dan analisis keamanan.

c. Deteksi Intrusi *(Intrusion Detection)*: Sistem deteksi intrusi (IDS) menggunakan mode *promiscuous* untuk mendeteksi aktivitas mencurigakan atau serangan di jaringan dengan memeriksa semua paket yang masuk dan keluar.

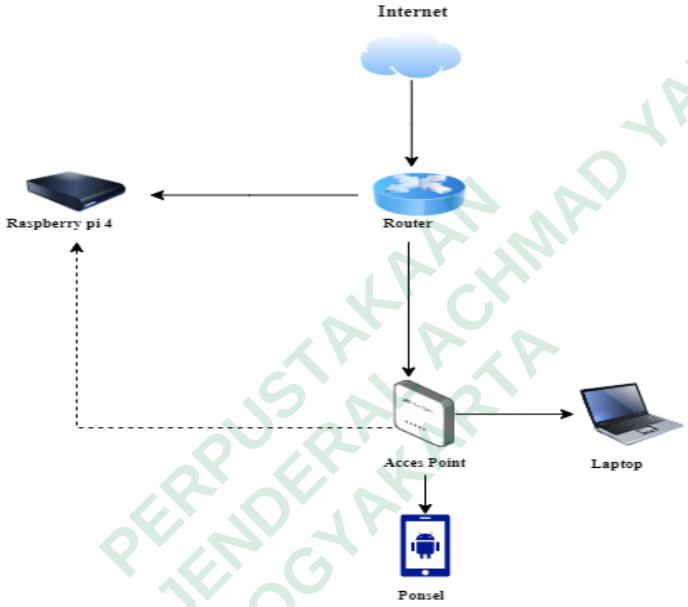
d. Pengujian Penetrasi *(Penetration Testing)*: Dalam pengujian penetrasi, mode promiscuous digunakan untuk mengidentifikasi kelemahan dan kerentanan di jaringan dengan menangkap dan menganalisis paket data

e. Pemantauan Performa *(Performance Monitoring)*: Alat pemantauan performa jaringan dapat menggunakan mode promiscuous untuk mendapatkan gambaran lengkap tentang penggunaan *bandwidth* dan pola lalu lintas di jaringan.

4.1.1.4 *Setup* MikroTik Dasar

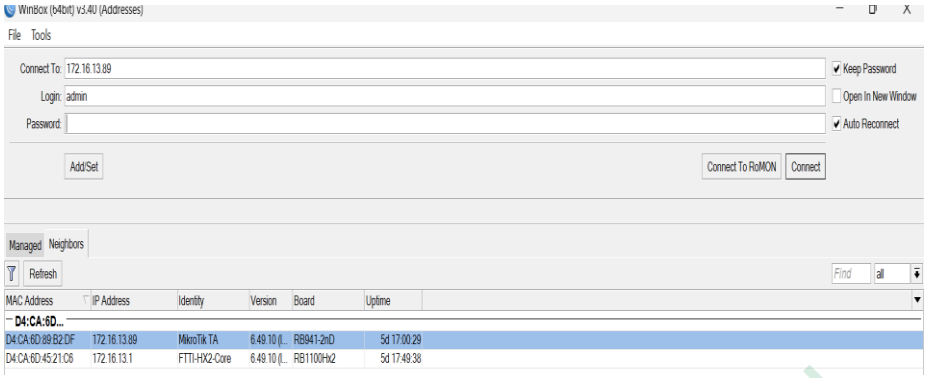
Setup dasar MikroTik adalah langkah-langkah awal dalam mengkonfigurasi perangkat MikroTik untuk keperluan jaringan. Perlu diperhatikan perangkat MikroTik terhubung dengan sumber daya listrik dan jaringan komputer yang sesuai. Dalam penelitian ini peneliti mengoneksikan MikroTik pada router yang sudah teroneksi jaringan

menggunakan kabel Ethernet dan diperlukan manajemen remote agar dapat mengakses dan mengkonfigurasi perangkat tersebut dari jarak jauh melalui program WinBox. Sebelum mengatur MikroTik menggunakan WinBox, penulis menentukan IP dengan menggunakan nomor IP 172.16.13.89 dan membuat desain topologi MikroTik. Dibawah ini merupakan desain topologi yang penulis gunakan :



Gambar 4.16 Topologi Jaringan

Perlu diperhatikan beberapa hal yang dilakukan dalam *set up* MikroTik pada Winbox yaitu masukan nama pengguna (Username) dan kata sandi (Password) untuk mengindetifikasi ke perangkat MikroTik. Dalam memasukan *username* dan kata sandi, diawal akan menggunakan username admin dan tanpa *password*. Ketentuan ini sudah ada dari setup bawaan sehingga perlu diubah sebagai upaya mengamankan rangkaian setup MikroTik dari serangan kejahatan. Dibawah ini merupakan tampilan pada Winbox setelah username dan password telah diganti



Gambar 4.17 Tampilan WinBox

Gambar 4.17 merupakan tampilan pada WinBox setelah *username* dan *password* telah diganti. Setelah itu dilakukan juga penggantian *identity* pada WinBox untuk meminalisir kesalahan dalam *setup* rangkaian tersebut. Kemudian dilakukan beberapa konfigurasi berikut:

1. konfigurasi IP Adrdress pada antarmuka Ethernet pada MikroTik yaitu Ether 1 sebagai Internet, Ether 2 sebagai Maltrail, dan ether 3 sebagai DHCP server

2. Mikrotik digunakan sebagai router dengan menghubungkan 3 kabel Ethernet biru sebagai internet, ethernet putih sebagai *port mirroring*, dan abu-abu sebagai distribusi

3. MikroTik mengaktifkan fitur DHCP (*Dynamic Host Configuration Protocol)* server. DHCP ini digunakan untuk memudahkan dalam pendistribuan IP secara otomatis keperangkat lain.

4.1.2 Pelaporan hasil analisis

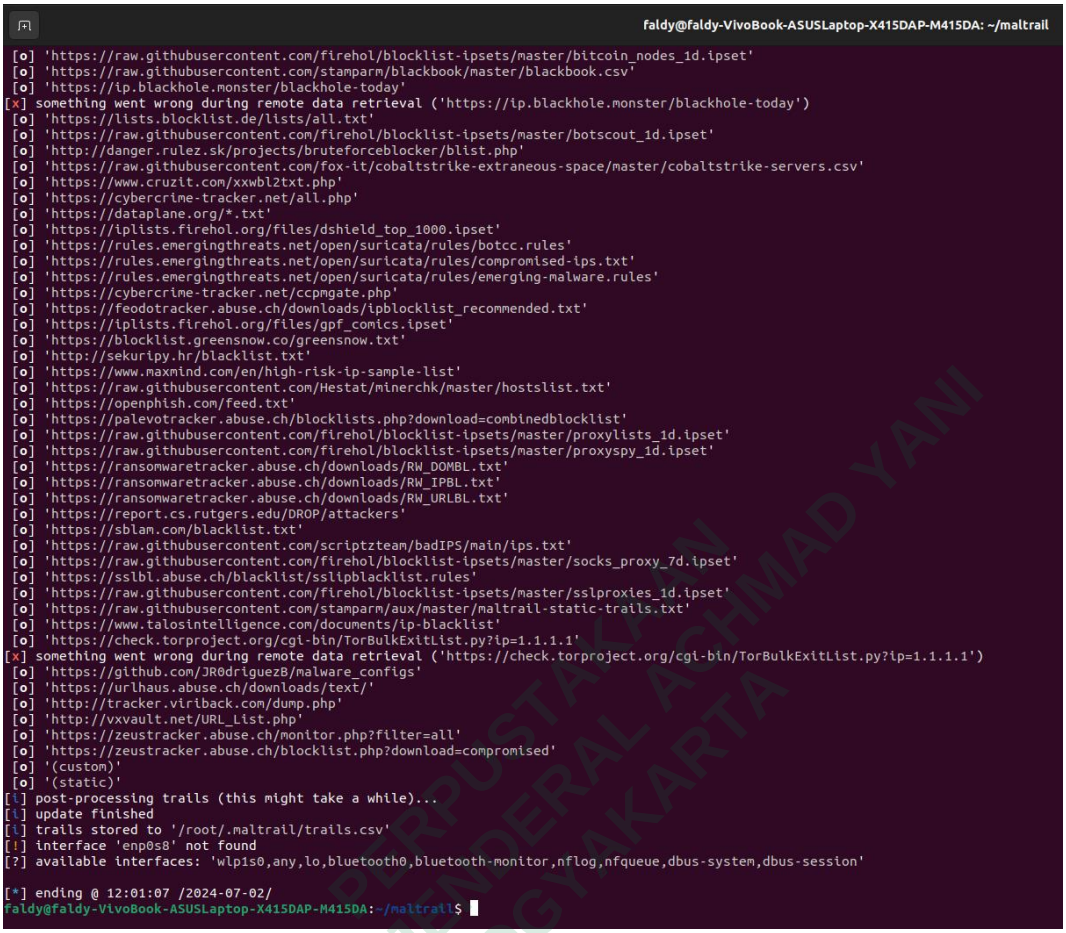
Untuk menjalankan aplikasi Maltrail ada beberapa tahap yang perlu dilakukan. Menjalankan maltrail dimulai dengan melakukan konfigurasi pada putty. Maltrail adalah sistem deteksi ancaman jaringan berbasis *Suricata* yang mendeteksi aktivitas jaringan yang mencurigakan. perangkat lunak atau software deteksi dan pencegahan intrusi jaringan *(network intrusion detection and*

prevention system atau NIDS/NIPS) yang bersifat open-source. Berikut adalah langkah-langkah umum untuk menjalankan aplikasi Maltrail :

a. Pastikan memiliki sistem operasi yang kompatibel. Maltrail dapat dijalankan di sistem operasi Linux, termasuk distribusi seperti Ubuntu, Debian, CentOS, dan lainnya.
b. Buka terminal atau command prompt, kemudian jalankan perintah berikut untuk menginstal phyton versi 3

   `"sudo apt-get install git python3 python3-dev python3-pip python-is-python3 libpcap-dev build-essential procps schedtool"`
c. Instal depedensi yang diperlukan oleh Maltrail dengan menjalankan perintah : "`sudo pip3 install pcapy-ng`"
d. Setelah perintah selesai, selanjutnya melakukan kloning dengan menjalankan perintah:

   `"git clone https://github.com/stamparm/maltrail.git"`
e. Lalu pindah ke direktori Maltrail dengan perintah : `"cd maltrail"`
f. Jika sudah terinstal lakukan konfigurasi Maltrail dengan menyunting file "maltrail.conf " yang terletak di dalam direktori Maltrail dan sesuaikan pengaturan. Pastikan untuk mengatur INTERFACE ke antarmuka jaringan yang digunakan untuk pemantauan.
g. Selanjutnya jalankan Maltrail dengan perintah : `"sudo python3 server.py"`
h. Aplikasi Maltrail akan berjalan dan memantau aktivitas jaringan. Pemantauan dapat dilakukan dengan mengakses antarmuka web Maltrail menggunakan peramban web di http://localhost:8338 seperti yang ada pada Gambar 4.4. pada HTTP server dengan menuliskan starting http://172.25.26.14:8338/ kemudian di *running.*



Gambar 4.18 Instalasi Maltrail

Proses pengambilan data dilakukan dengan melakukan pengujian selama 1x24 jam pada masing-masing ponsel android *(China Brand))* yang digunakan dalam keadaan *fresh install* atau setelan pabrik, dan dilakukan selama 5 hari untuk pendeteksian *Malicious traffic.* Dari rangkaian proses tersebut dihasilkan data sebagai berikut:

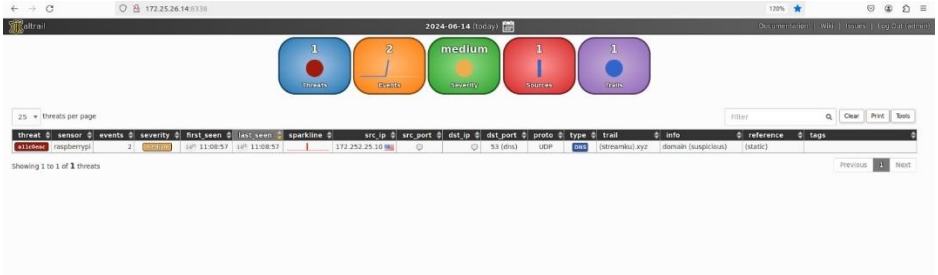
1. Analisis *Malicious traffic* pada ponsel android X1 Pada **Gambar 4.19** merupakan hasil *Malicious traffic* ponsel android X1 dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi trafik ponsel android X1 yaitu 172.252.25.113

Gambar 4.19 Hasil *Malicious traffic* ponsel android X1

2. Analisis *Malicious traffic* pada ponsel android X2 pada **Gambar 4.20.** merupakan hasil *Malicious traffic* ponsel android X2 dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi trafik ponsel android X2 yaitu 172.252.25.114. *Malicious* terjadi pada Raspberry Pi dengan nomor IP 172.252.25.10, dan penyerangan bersifat medium

Gambar 4.20 Hasil *Malicious traffic* ponsel android X2

3. Analisis *Malicious traffic* pada ponsel android X3. pada **Gambar 4.21** merupakan hasil *Malicious traffic* ponsel android X3 dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi trafik ponsel android X3 yaitu 172.252.25.115

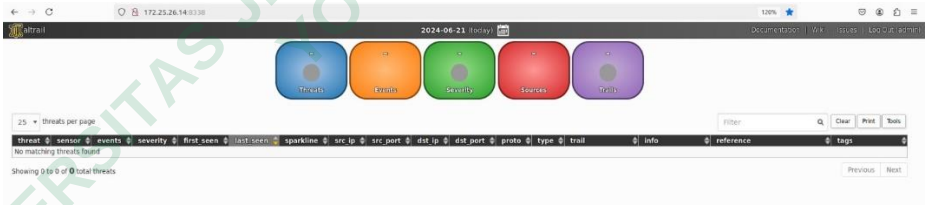


Gambar 4.21 Hasil *Malicious traffic* ponsel android X3

4. Analisis *Malicious traffic* pada ponsel android X4. pada **Gambar 4.22** merupakan hasil *Malicious traffic* ponsel android X4 dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi trafik ponsel android X4 yaitu 172.252.25.108

Gambar 4.22 Hasil *Malicious traffic* ponsel android X4

5. Analisis *Malicious traffic* pada ponsel android X5 pada **Gambar 4.23** merupakan hasil *Malicious traffic* ponsel android X5 dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi trafik ponsel android X5 yaitu 172.252.25.109



Gambar 4.23 Hasil *Malicious traffic* ponsel android X5

Dari hasil penelitian *Malicious traffic* pada ponsel android *"China Brand"* menunjukkan hasil jumlah trafik pada ponsel Android selama beberapa periode waktu. Tabel ini mencakup informasi mengenai tanggal, alamat IP, waktu, tipe, dan jumlah *Malicious traffic* berbahaya yang terdeteksi. Berikut adalah rincian dari hasil penelitian *Malicious traffic* pada ponsel android *"China Brand"* pada table 2 dibawah ini :

Table 2 Hasil jumlah trafik pada ponsel Android

No	Tanggal	IP	Waktu	Tipe	Jumlah *Malicious Traffic*
1.	04-05 Juni 2024	172.252.25.113	15:26	X1	0
2.	13-14 Juni 2024	172.252.25.114	08:28	X2	0
3.	14-15 Juni 2024	172.252.25.115	16:44	X3	0
4.	19-20 Juni 2024	172.252.25.108	10:56	X4	0
5.	19-20 Juni 2024	172.252.25.109	10:59	X5	0