BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

Berdasarkan proses elaborasi pengumpulan data, penelitian ini menggunakan metode *port mirroring* untuk pendeteksian *malicious traffic* pada lampu cerdas menggunakan apliaksi Maltrail, dimulai dengan proses *pairing* lima merek lampu cerdas berbeda yang dikontrol menggunakan *tools* aplikasi. Proses *pairing* dilakukan selama 1 hari (1x24 jam) pada masing-masing lampu cerdas tersebut yang kemudian akan diambil nomor IP lampu tersebut dan dilakukan deteksi *maliciuos traffic*. Rangkaian pengambilan nomor IP dimulai dengan dilakuakan proses pengoneksian raspbery pi yang sudah terinstal aplikasi Maltrail menggunakan Putty dengan *set up* dan *convigurasi* MikroTik dasar menggunakan WinBox.

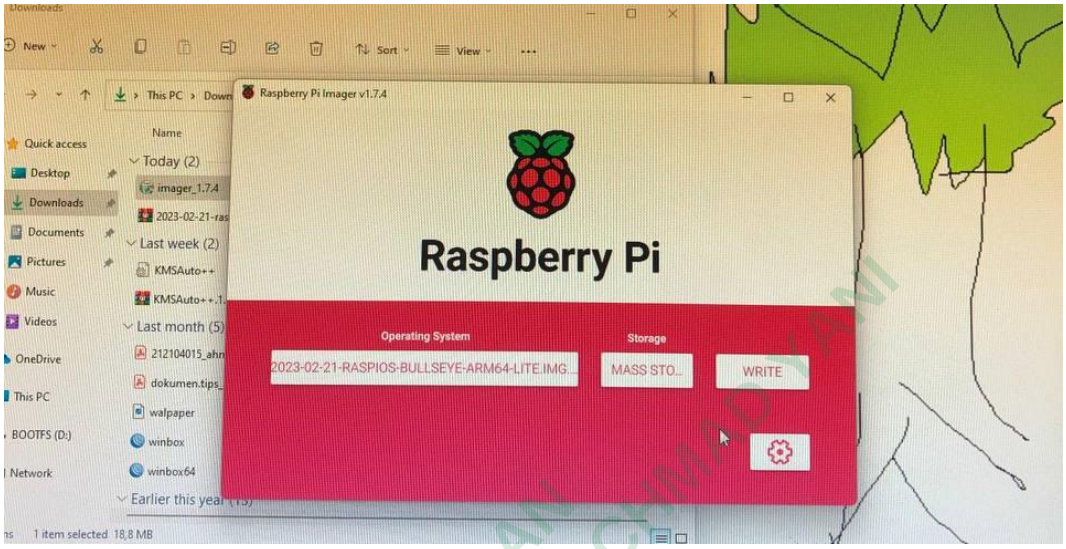
4.1.1 Proses Pengunpulan Data

A. Proses *Pairing*

Proses *pairing Smart Lamp* merupakan langkah dalam menghubungkan lampu pintar pada jaringan nirkabel, kemudian dikendalikan melalui perangkat Smartphone. Pengguna dapat menyalakan, mematikan, dan mengatur kecerahan lampu dengan mudah melalui perangkat yang digunakan. Lampu pintar juga dilengkapi dengan fitur tambahan seperti perubahan warna atau pola pencahayaan yang dapat disesuaikan dengan kebutuhan.

Selain itu, beberapa lampu pintar juga menyediakan fitur pengawasan, sehingga pengguna dapat melacak dan mengelola penggunaan. Dalam proses *pairing* peneliti membutuhkan lampu cerdas, fitting saklar colok, dan aplikasi pengontrol lampu. Setiap lampu akan terkoneksikan pada aplikasi pengontrol dan terkoneksi pada *instenet* yang sudah diatur menggunakan pengaturan MikroTik dasar sehingga akan terdeteksi nomor IP pada setiap perangkat lampu cerdas tersebut yang digunakan dalam mengidentifikasi *malicious traffic* menggunakan aplikasi Maltrail.

B. Instalasi Raspbery



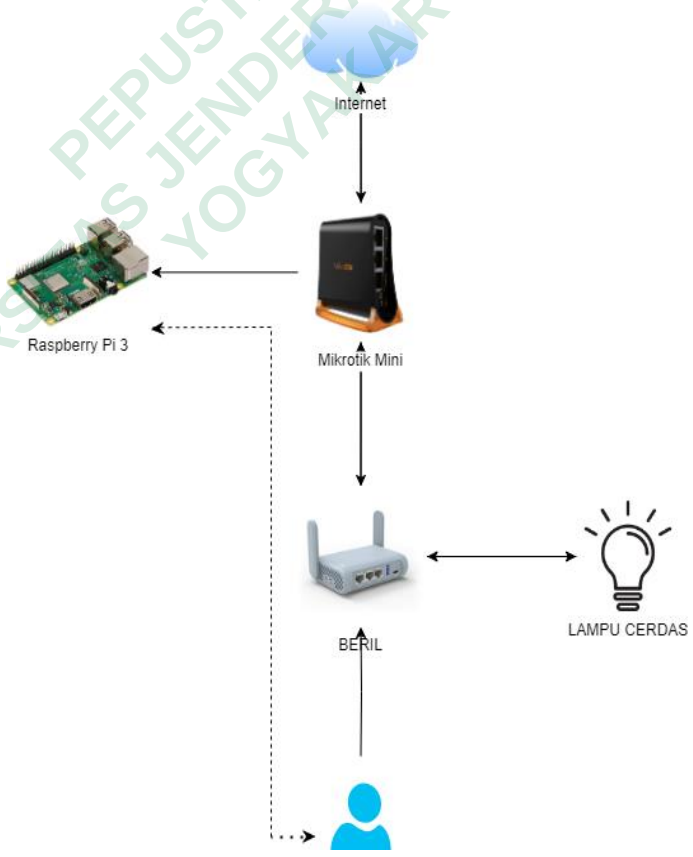
Gambar 4.1 Tampilan Imager Raspberry Pi

Dalam penelitian ini penulis melakukan instalasi Raspberry Pi dimulai dengan instal Imager seperti pada **Gambar 4.1**, 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 16GB sebagai penyimpan aplikasi Maltrail. Ada beberapa model Raspberry Pi yang tersedia, dalam penelitian ini penulis mengunakan Raspberry Pi 3 model B+.

Raspberry Pi membutuhkan sistem operasi (OS) agar dapat berfungsi. OS yang digunakan pada penelitian ini adalah Ubuntu 20.4. 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.

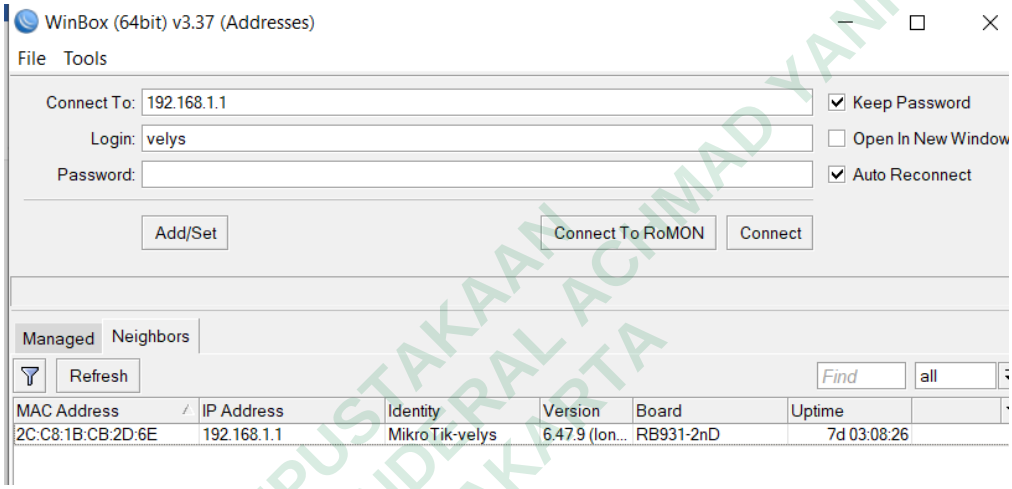
C. Setup Mikrotik

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 rauter 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 privat dengan menggunakan nomor IP 10.10.10.5/24 dan membuat disain topologi MikroTik. Pada **Gambar 4.2** dibawah ini merupakan design topologi yang penulis gunakan :



Gambar 4.2 Topologi Pengujian

Perlu diperhatikan beberapa hal yang dilakukan dalam setup MikroTik pada WinBox yaitu masukkan nama pengguna (username) dan kata sandi (password) untuk mengautentikasi 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.

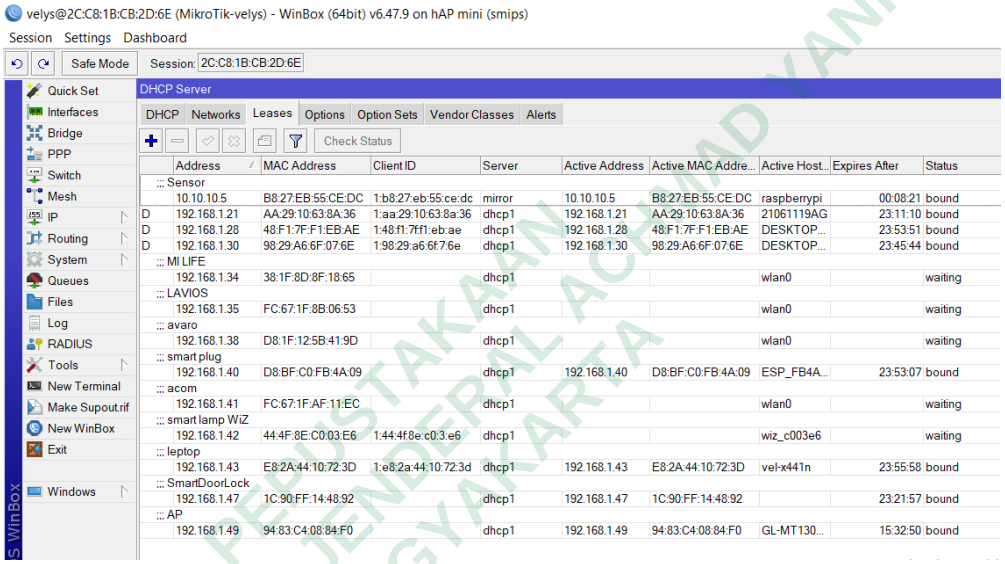


Gambar 4.3 Tampilan WinBox

Gambar 4.3 merupakan tampilan pada WinBox setelah *username* dan *password* telah diganti. Setelah itu dilakukan juga penggantian *identity* pada WinBox untuk meminimalisir kesalahan dalam *setup* rangkaian tersebut. Kemudian dilakukan beberapa konfigurasi berikut :

1. Konfigurasi IP Address pada antarmuka Ethernet pada MikroTik yaitu Ether 1 sebagai Firewall – NAT ,Ether 2 sebagai DHCP server, dan Ether 3 sebagai Network.
2. MikroTik digunakan sebagai router dengan mengubungkan 3 kabel Ethernet hitam sebagai internet, ethernet putih untuk distribusi dan biru sebagai *port mirroring.*
3. MikroTik mengaktifkan fitur DHCP (*Dynamic Host Configuration Protocol*) server. DHCP ini digunakan untuk memudahkan dalam pendistribuan IP secara otomatis keperangkat lain.

Setelah *setup* MikroTik dilakukan akan ada tampilan pada gambar dibawah ini yang menujukan nomor IP lampu yang sudah terkoneksi pada internet yang telah dikoneksikan dengan rangkaian setup MikroTik. Kemudian dilakukan proses pengidentifikasian lampu yang sudah memiliki nomor IP, penulis akan menandai lampu sesuai nomor IP. Selain nomor IP lampu, tersambung juga nomor IP raspberry pi, acces point GL-MT dan segala sesuatu yang terkoneksi internet pada server penulis akan terdeteksi alamat IP.



Gambar 4.4 Tampilan Nomor IP

Gambar 4.4 menunjukan tampilan nomor IP perangkat IoT yang terkoneksi pada *setup* MikroTik. Alamat IP akan digunkan sebagai pendeteksian *malicious taffic* pada aplikasi maltrail. IP digunakan sebagai komunikasi untuk mengirim dan menerima data melalui jaringan komputer. IP berperan penting dalam mengatur pengiriman paket data antar perangkat yang terhubung ke internet.

Dalam rangkaian setup MikroTik perlu diperhatikan dalam menyambungkan koneksi.

D. Port Mirroring

Port mirroring adalah sebuah teknik dalam jaringan komputer yang digunakan untuk memantau lalu lintas jaringan yang melewati satu atau beberapa port pada switch atau router. Dalam skenario 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.

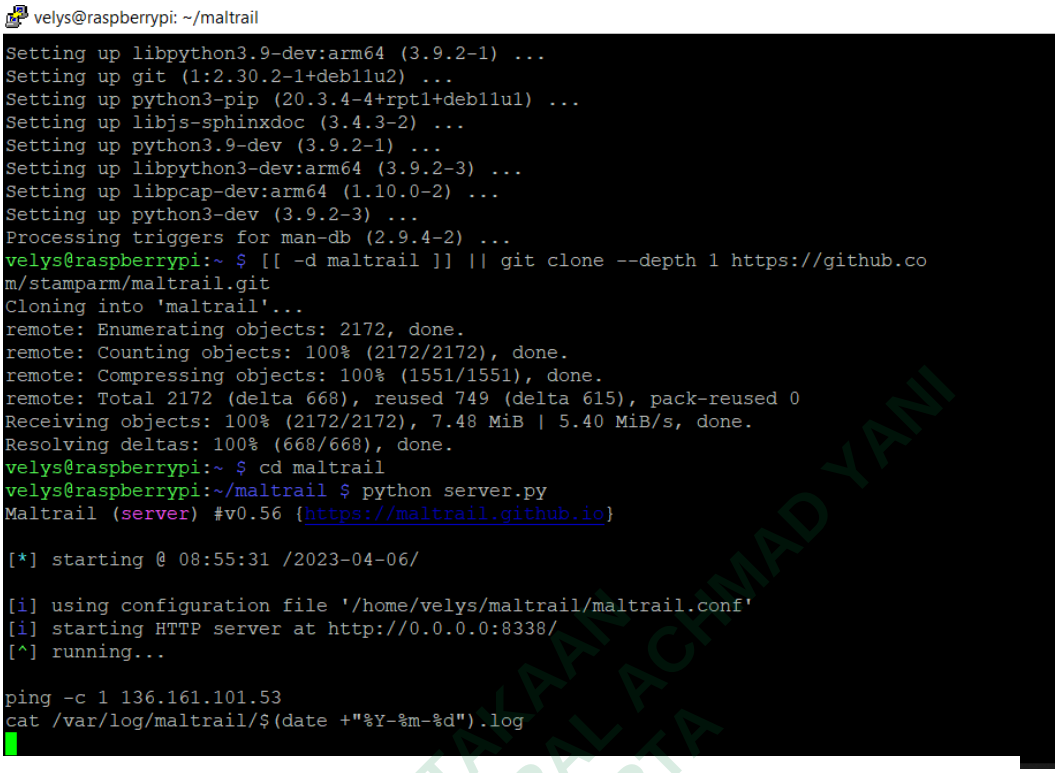
Menunjukan rangkaian *setup* MikroTik yang berperan dalam proses *port mirroring* dengan menggunakan 3 kabel ethernet yaitu kabel putih merupakan kabel distribusi internet dari swicth kemudian dikoneksikan pada MikroTik untuk mendapatkan internet yang kemudian didistribusikan kembali menggunakan kabel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

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 lalu lintas berbahaya yang menggunakan daftar jejak berbahaya dan umumnya mencurigakan, serta jejak statis yang disusun dari berbagai laporan dan daftar kustom khusus, di mana jejak dapat berupa apa pun seperti nama domain. Aktivitas jaringan yang mencurigakan tersebut terdapat pada perangkat lunak atau software deteksi sebagai pencegahan intrusi jaringan (*network intrusion detection and prevention system* atau NIDS/NIPS) yang bersifat *open-source*. Maltrail juga menggunakan mekanisme heuristik

canggih yang dapat membantu menemukan ancaman yang tidak diketahui misalnya malware baru. 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. Unduh aplikasi Maltrail dari repositori resmi yaitu pada situs web Maltrail (*`https://github.com/stamparm/maltrail`*) untuk mendapatkan tautan unduhan terbaru dan instruksi instalasi yang lebih rinci. Gunakan perintah git atau unduh sebagai file ZIP.
c. Ekstrak file unduhan ke direktori yang diinginkan di sistem.
d. Buka terminal atau konsol dan navigasikan ke direktori Maltrail yang baru saja Anda ekstrak.
e. Buka file *"`config/production.py`"* dengan editor teks dan sesuaikan pengaturan. Pastikan untuk mengatur variabel `INTERFACE` ke antarmuka jaringan yang digunakan untuk pemantauan.
f. Selanjutnya, mempersiapkan basis data untuk Maltrail. Jalankan perintah berikut: *"`python db_init.py`"*.
g. Setelah basis data siap, jalankan Maltrail dengan perintah: "`python server.py`".
h. Aplikasi Maltrail akan berjalan dan memantau aktivitas jaringan. Pemantauan dapat dilakukan dengan mengakses antarmuka web Meltrail menggunakan peramban web di "`http://localhost:8338`". seperti yang ada pada **Gambar 4.5**
i. . Yang kemudian akan dilampilkan mealui HTTP server dengan menuliskan starting http://10.10.10.5:8338/ kemudian di *running.*



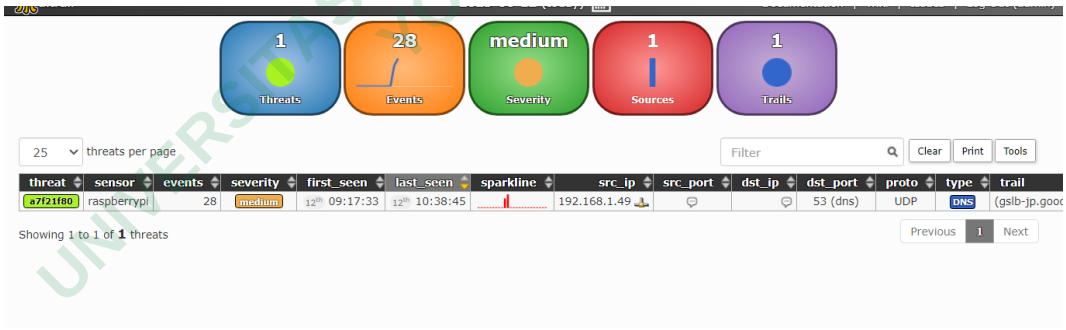
Gambar 4.5 Tampilan Kode *starting* HTTP server Maltrail

Proses pengambilan data dilakukan dengan melakukan pengujian 1x24 jam pada masing lampu sehingga dilakukan selama 5 hari pendeteksian *malicious traffic*. Dari rangkaian proses tersebut dihasilkan data berikut :

1. Analisis *malicious trafic* pada lampu PILIPS WiZ Tuneable White *Connected Wiffi* 8W. Pada **Gambar 4.6** merupakan tampilan deteksi *malicious traffic* lampu PILIPS WiZ Tuneable White *Connected* Wiffi 8W dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi nomor IP lampu PILIPS WiZ Tuneable White *Connected* Wiffi 8W yaitu 192.168.1.42

Gambar 4.6 Deteksi *malicious traffic* lampu PILIPS WiZ Tuneable White Connected Wiffi 8W

2. Analisis *malicious trafic* pada lampu AVARO smart blub 12W. Pada **Gambar 4.7** merupakan tampilan deteksi *malicious traffic* lampu AVARO smart blub 12W dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi nomor IP lampu IP : 192.168.1.35. Malicious terjadi pada Raspbery Pi dengan nomor IP 192.168.1.49, penyerangan bersifat medium.



Gambar 4.7 Deteksi malicious traffic lampu AVARO smart blub 12W

3. Analisis *malicious traffic* pada lampu ACOME Smart Wiffi LED Bulb 14W. Pada **Gambar 4.8** merupakan tampilan deteksi *malicious traffic* lampu AVARO smart blub 12W dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi nomor IP lampu IP 192.168.1.41.

Gambar 4.8 Deteksi *malicious traffic* pada lampu ACOME Smart Wiffi LED Bulb 14W

4. Analisis *malicious traffic* pada lampu LOVIS Smart Wiffi LED 15W. Pada **Gambar 4.9** merupakan tampilan deteksi *malicious traffic* lampu AVARO smart blub 12W dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi nomor IP lampu IP 192.168.1.35.

Gambar 4.9 Deteksi *malicious traffic* pada lampu MI LIFE Smart Wiffi LED10W pada Maltrail

5. Analisis *malicious traffic* pada lampu MI LIFE Smart Wiffi LED 10W. Pada **Gambar 4.10** merupakan tampilan deteksi *malicious traffic* lampu lampu MI LIFE Smart Wiffi LED 10W dengan pendeteksian menggunakan aplikasi Maltrail. Dalam gambar tersebut tidak terdeteksi nomor IP lampu IP 192.168.1.34

Gambar 4.10 Deteksi malicious traffic lampu MI LIFE Smart Wiffi LED 10W pada Maltrail

Keterangan :

Gambar 4.11 Grafik Maltrail

1. *Treats box* merupakan kotak ancaman yang mewakili persentase ancaman teratas dalam bentuk diagram lingkaran (Catatan: jika terdapapat warna abu-abu, warna tersebut menyimpan semua ancaman yang masing-masing memiliki <1% dalam total peristiwa), dengan jumlah total ancaman di atas.
2. *Events box* merupakan kotak acara yang mewakili jumlah total acara dalam periode 24 jam yang dipilih, di mana garis merah mewakili acara berbasis IP, garis biru mewakili acara berbasis DNS, dan garis kuning mewakili acara berbasis URL. Dalam **Gambar 4.1.11** pada bagian events hanya terdapat dua warna yaitu biru dan kuning.
3. *Severity box* menunjukan evaluasi tingkat keparahan ancaman (Catatan: dihitung berdasarkan nilai dalam kolom info dan referensi, memprioritaskan lalu lintas yang dihasilkan malware.
4. *Sources box* merupakan kotak sources mewakili jumlah peristiwa per Sources teratas dalam bentuk bagan kolom bertumpuk, dengan jumlah total sources.
5. *Trails box* merupakan kotak lintasan mewakili persentase lintasan teratas dalam bentuk bagan.

Gambar 4.12 Grafik Maltrail

Kolom *threat* menyimpan ID unik ancaman (misalnya a7f21f80) dan warna (Catatan: dikeluarkan dari ID ancaman), sensor menyimpan nama sensor tempat peristiwa dipicu (misalnya raspberrypi), *events* menyimpan jumlah total peristiwa untuk ancaman saat ini, tingkat keparahan yang dievaluasi dan tingkat keparahan ancaman (Catatan: dihitung berdasarkan nilai dalam kolom info dan referensi, memprioritaskan lalu lintas yang dihasilkan *malware*).

First_seen merupakan waktu peristiwa pertama dalam periode (24 jam) yang dipilih (misalnya 12 th 09:17:33), last_seen menyimpan waktu peristiwa terakhir dalam periode (24j) yang dipilih (misalnya 12 th 10:38:45), *sparkline* menyimpan grafik *sparkline* kecil yang mewakili aktivitas ancaman dalam periode yang dipilih, *src_ip* menyimpan IP sumber ancaman (misalnya 192.168.1.49).

Src_port menyimpan port sumber, *dst_ip* menyimpan IP tujuan, *dst_port* menyimpan port tujuan (misalnya 53 (DNS)), *proto* menyimpan protokol, (UDP), *trail* menyimpan entri daftar hitam (atau heuristik) yang memicu peristiwa, info menyimpan lebih banyak informasi tentang ancaman/jejak (mis. penyerang yang dikenal untuk alamat IP penyerang yang dikenal atau ipinfo untuk layanan informasi IP yang dikenal yang biasa digunakan oleh malware selama *startup*), *reference* memegang sumber entri daftar hitam (misalnya (statis) untuk jejak statis atau myip.ms untuk umpan dinamis yang diambil dari sumber yang sama) dan tag memegang tag yang ditentukan pengguna untuk jejak yang diberikan (misalnya APT28).

Tabel 3 Tabel Hasil Penelitian

No	Nama Lampu	Aplikasi yang digunakan	Tanggal penelitian	Hasil
1.	PILIPS WiZ Tuneable White *Connected* Wiffi 8W	WiZZ	Rabu, 05 April 2023	Aman
2.	AVARO smart blub 12W	AVARO	Senin, 10 April 2023	Aman
3.	ACOME Smart Wiffi LED Bulb 14W	ACOM IoT	Selasa, 11 April 2023	Aman
4.	LOVIS Smart Wiffi LED 15W	Tuya Smart Life	Rabu, 17 Mei 2023	Aman
5.	MI LIFE Smart Wiffi LED10W	Tuya Smart LIfe	Senin, 12 juni 2023	Aman