Portabel *Intrusion Prevention System* Untuk Mengamankan Koneksi Internet Saat Menggunakan WiFi Publik

Yudhi Ardiyanto*
Program Studi Teknik Elektro
Universitas Muhammadiyah Yogyakarta
Jalan Brawijaya, Tamantirto, Kasihan, Bantul, Yogyakarta, Indonesia
yudhi.ardiyanto@umy.ac.id

***Abstract*—Almost all public places provide public Wireless Fidelity (WiFi) facilities today. Users who are connected through these facilities are often ignorant of data and network security factors; the most important thing for them is to enjoy free internet access. In terms of security, public WiFi is quite vulnerable because it can be misused by irresponsible parties to retrieve essential data from its users. After all, in terms of access, there are no restrictions. This research aims to develop a system that functions as a gateway router and a system that can prevent attacks from running on minicomputers. This study uses the Intrusion Prevention System (IPS) method, where this system can detect and prevent attacks. The study results found that the portable IPS has been successfully developed using the Raspberry Pi 4 Model B and Suricata equipped with a 3.50-inch TFT LCD and a power supply with a capacity of 10,000 mAh. The portable IPS successfully detected the attack in port scanning using the Zenmap application. In addition to functioning as an IPS device, this device is capable of being a gateway router. The IPS portable power supply can last for 34611.22 seconds with a smartphone as the client.**

***Keywords*— Portabel IPS, Raspberry Pi, Suricata**

***Abstrak*-- Saat ini hampir semua tempat umum menyediakan fasilitas *Wireless Fidelity* (WiFi) publik. Pengguna yang terkoneksi melalui fasilitas tersebut terkadang sering abai terhadap faktor keamanan data dan jaringan, yang terpenting bagi mereka adalah dapat menikmati akses internet secara gratis. Dari sisi keamanan WiFi publik cukup rentan karena jaringan ini bisa saja dipergunakan oleh pihak-pihak yang kurang bertanggung jawab untuk mengambil data penting dari para penggunanya, karena dari segi akses tidak ada pembatasan. Tujuan dari penelitian ini adalah untuk mengembangkan sistem yang berfungsi sebagai *router gateway* dan sistem yang mampu mencegah terhadap upaya serangan yang berjalan pada perangkat mini komputer. Penelitian ini menggunakan metode *Intrusion Prevention System* (IPS), dimana sistem ini mampu mendeteksi sekaligus melakukan pencegahan adanya serangan. Dari hasil penelitian diperoleh bahwa portabel IPS telah berhasil dikembangkan dengan menggunakan Raspberry Pi 4 Model B dilengkapi dengan LCD TFT 3,50 inch dan catu daya dengan kapasitas 10.000 mAh serta Suricata yang dikonfigurasi sebagai IPS. Serangan berupa port scanning menggunakan aplikasi zenmap berhasil dideteksi oleh portabel IPS. Selain berfungsi sebagai IPS perangkat ini mampu menjadi *router gateway*. Catu daya portabel IPS mampu bertahan selama 34611,22 detik dengan sebuah *smartphone* sebagai *client*.**

***Kata Kunci*—Portabel IPS, Raspberry Pi, Suricata**

I. PENDAHULUAN

Koneksi internet sudah merupakan kebutuhan primer bagi semua kalangan masyarakat. Saat ini hampir sebagian besar fasilitas umum seperti hotel, stasiun, sekolah, kampus, bandara bahkan di beberapa tempat wisata dapat ditemukan layanan *Wireless Fidelity* (WiFi) publik. Penyediaan fasilitas tersebut memungkinkan masyarakat dapat melakukan *browsing*, *upload*, *download*, belanja dan transaksi *online* secara gratis tanpa harus membeli paket internet. Kendati dari segi biaya gratis, akan tetapi dari sisi keamanan berpotensi dapat membahayakan privasi pengguna, karena dengan sifat aksesnya yang bebas maka siapapun yang berada dalam area tersebut akan dapat melakukan penyadapan terhadap lalu lintas paket data [1]. Cara lain untuk melakukan penyadapan terhadap privasi seseorang melalui jaringan WiFi yaitu dengan memasang *Fake Access Point* atau *Evil Twin*. Penyerang dengan sengaja memasang *access point* tersebut dengan meniru *Service Set Identifier* (SSID) aslinya [2].

Berbagai metode dikembangkan untuk meminimalisir adanya kerentanan keamanan pada jaringan WiFi yaitu melalui *Wired Equivalent Privacy* (WEP), *WiFi Protected Access* (WPA) dan *WiFi Protected Access 2* (WPA2), akan tetapi dengan ketiga protokol keamanan tersebut ternyata dapat diretas menggunakan beberapa teknik dan pengujian memanfaatkan aplikasi Aircrack [3]. Serangan dilakukan pada protokol keamanan *Wireless Fidelity Protected Access 2 - Pre-Shared Key* (WPA2-PSK) dengan memanfaatkan pengguna yang terhubung melalui jaringan WiFi tersebut. Metode yang digunakan adalah dengan menunggu pengguna terhubung ke jaringan WiFi untuk memperoleh *handshake* maupun informasi lain seperti *Media Access Control* (MAC) address, alamat IP, Channel yang digunakan. Beberapa teknik dan pengujian dilakukan dengan menggunakan berbagai *tool* yang ada pada Kali Linux untuk memecahkan kode enkripsi dari protokol WPA2-PSK tersebut [4].

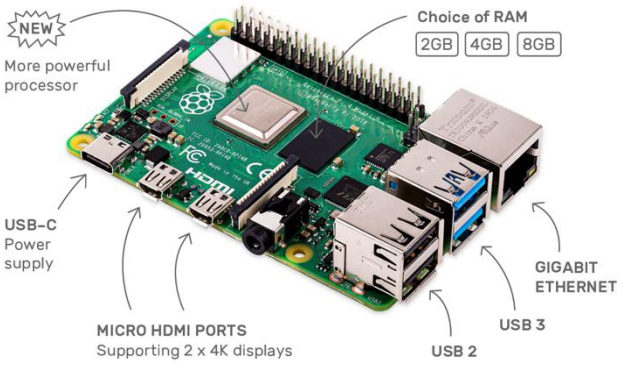
Beberapa langkah dikembangkan untuk meminimalisir adanya serangan siber adalah dengan mengaktifkan *firewall* dan

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022

antivirus terupdate pada perangkat yang digunakan. Cara selanjutnya adalah dengan menghubungkan jaringan WiFi publik di perangkat secara manual dan sebisa mungkin meminimalisir terhubung secara otomatis ke jaringan tersebut.

Upaya lain yang dapat dilakukan untuk mengamankan koneksi internet saat menggunakan WiFi publik adalah dengan mengimplementasikan *Intrusion Prevention System* (IPS). Bisa diimplementasikan pada jaringan komputer atau lebih dikenal sebagai *Network-based Intrusion Prevention System* (NIPS) maupun di host yang ingin dilindungi atau disebut sebagai *Host-based Intrusion Prevention System* (HIPS). Sistem ini mampu mendeteksi adanya serangan, sekaligus melakukan pencegahan terhadap adanya serangan. Sedikit berbeda dengan *Intrusion Detection System* (IDS), sistem ini tidak mampu melakukan pencegahan secara otomatis terhadap serangan dan hanya akan mengirimkan *alert* kepada administrator jaringan serta menyimpan aktivitas serangan kedalam *log*. Beberapa produk IPS yang bersifat *open source* diantaranya adalah Snort dan Suricata. Snort dapat diinstal pada berbagai paltform sistem operasi seperti Fedora, Windows, FreeBSD dan CentOS [5]. sedangkan Suricata IPS dapat diinstall pada sistem operasi Linux, Mac, FreeBSD, Unix dan Windows. Suricata juga dapat dikonfigurasi sebagai IDS [6]. Snort dan Suricata juga dapat dijadikan sebagai IDS. IPS seperti Snort dan Suricata dapat diinstal pada perangkat *single board computer*, seperti halnya Raspberry Pi [7], [8].

Dewasa ini perkembangan Raspberry Pi semakin meningkat kemampuan komputasinya dengan harga yang relatif terjangkau. Raspberry Pi 4 Model B menggunakan processor Broadcom BCM2711 dengan pilihan *Random Access Memory* (RAM) yang bervariasi, mulai dari 2 *Gigabyte* (GB), 4 GB dan 8 GB. Dari sisi display sudah mendukung 4K display dengan menggunakan dua buah *port* mini HDMI. Selain itu perangkat ini dilengkapi dengan port USB 3.0 sebanyak 2 buah dan *port* USB 2.0 juga 2 buah. Teknologi nirkabel yang dipakai yaitu *Bluetooth* 5.0 dan WiFi 802.11 ac dual band, serta dilengkapi dengan *Gigabit Ethernet*. Bentuk dari perangkat Raspberry Pi 4 Model B yang relatif kecil, *power input* yang digunakan juga tidak besar hanya 5 Volt DC. Dengan *power input* tersebut, maka Raspberry Pi 4 model B ini mampu dihidupkan menggunakan catu daya yang berasal dari *power bank*. Gambar 1 merupakan Raspberry Pi 4 model B.



Gambar 1. Perangkat Raspberry Pi 4 Model B [9]

Bentuk dari Raspberry Pi yang kecil memungkinkan perangkat ini mudah untuk dibawa kemana-mana. Kendati demikian, meski dari segi bentuk memiliki ukuran yang kecil, namun perangkat ini sudah teruji perfomanya untuk dijadikan sebagai *web server*. Raspberry Pi mampu dijadikan sebagai *web server* dan dapat melayani *client* sebanyak 1200, jumlah *client* diperoleh dengan menggunakan aplikasi Jmeter. Aplikasi *web server* yang digunakan untuk melakukan pengujian yaitu Apache Tomcat, Lighttpd Nginx, Jetty dan Apache. Lighttpd mengkonsumsi sumber daya, baik itu penggunaan CPU maupun memori paling rendah diantara *web server* yang lain [10]. Penggunaan Raspberry Pi sebagai *web server* yang digunakan untuk pengontrolan lampu secara jarak jauh. Lampu dapat dimatikan dan dihidupkan melalui tombol yang ada pada halaman web [11]. Penggunaan Raspberry Pi 3 dan Snort sebagai IDS, dari hasil implementasi sistem mampu mendeteksi adanya *Packet Internet Groper* (PING) *request* dan *File Transfer Protocol* (FTP) *request* [12]. Raspberry Pi 3 dapat digunakan sebagai IDS, honeypot server dan menjalankan analisa paket menggunakan Tshark, ketiganya mampu berfungsi dengan baik tanpa ada isu terkait penggunaan memori dan pemrosesannya [13]. Pengujian IDS Snort dan Bro yang diinstal dan dikonfigurasi pada *single board computer* Raspberry Pi 3 mampu berfungsi dengan baik, akan tetapi pada saat menggunakan IDS Bro perangkat tersebut mengalami *crash* hal ini terjadi karena proses penyerangan dilakukan secara masif. Pada saat menggunakan IDS Snort perangkat relatif lebih stabil [14].

Berdasarkan masalah yang ada serta beberapa penelitian terdahulu, maka penelitian ini bertujuan untuk mengembangkan IPS yang bersifat portabel dengan menggunakan perangkat Raspberry Pi 4 Model B. Selain dari sisi bentuk yang relatif kecil, catu daya dapat menggunakan *power bank* serta harganya yang relatif terjangkau. Perangkat ini akan dijadikan sebagai gateway bagi host yang ingin dilindungi, sehingga *host/client* tersebut tidak akan terekspose langsung oleh perangkat lain yang terhubung ke WiFi publik. Pengguna LCD TFT 3,5 inch memudahkan pengguna untuk menghubungkan portabel IPS ke jaringan WiFi publik.

II. METODE PENELITIAN

Terdapat beberapa metode dalam mengamankan jaringan komputer dari adanya serangan. Salah satunya adalah IPS, sistem ini selain mendeteksi adanya serangan juga dapat melakukan pencegahan secara aktif. Berbeda dengan *Intrusion Detection System* (IDS) yang hanya mampu mendeteksi adanya serangan tanpa bisa melakukan pencegahan. Metodologi yang dilakukan untuk mengembangkan portabel IPS ini terdiri dari berbagai tahapan, dan dapat dilihat sebagai berikut:

A. Studi Literatur

Pada tahapan ini bertujuan untuk mengetahui perangkat *development board* yang dapat diinstall dan dikonfigurasi sebagai IPS serta *wireless router*. Berdasarkan pada beberapa literatur yang ada, maka Raspberry Pi 4 dipilih sebagai perangkat yang akan dijadikan sebagai portabel IPS dengan sistem operasi Raspberry Pi OS (Raspbian) versi 10 Buster dan Suricata 6.0.1 yang nantinya akan dikonfigurasi sebagai IPS serta aplikasi pendukung lainnya.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022

B. *Topologi Jaringan*

Portabel IPS yang telah dilakukan instalasi dan konfigurasi kemudian akan dilakukan pengujian menggunakan topologi seperti yang ditunjukan pada Gambar 2.

Gambar 2. Topologi Jaringan

Pada Gambar 2 tampak skema jaringan untuk melakukan pengujian portabel IPS. Perangkat portabel IPS terhubung melalui *Wireless Router* dengan *Service Set Identifier* (SSID) berupa "admin" menggunakan interface wlan0 dengan mode client. Host 1 dan 2 merupakan perangkat yang ingin dilindungi dari adanya serangan, dapat berupa laptop dan *smartphone*. Perangkat tersebut terhubung secara tidak langsung ke WiFi publik, akan tetapi melalui portabel IPS yang dikonfigurasi sebagai *Access Point* mode dengan menggunakan *interface* uap0. SSID yang digunakan adalah "AP-IPS" dengan frekuensi mengikuti frekuensi yang ada pada *wireless router*. Catu daya portabel IPS diperoleh dari power bank dengan tegangan output 5 volt, arus 1 ampere, sedangkan kapasitasnya 10.000 mAh. Pengujian serangan ke *client* dilakukan menggunakan komputer Attacker yang sudah terinstall aplikasi Zenmap. Perangkat portabel IPS terdiri dari dua komponen utama yaitu Raspberry Pi 4 Model B dan *power bank*, seperti terlihat tampak pada Tabel 1 berikut ini.

TABEL 1. PERANGKAT PORTABEL IPS

No	Nama Perangkat	Spesifikasi
1	Raspberry Pi 4 Model B	• Broadcom BCM2711, Quad core Cortex-A72 (ARM versi 8) 64-bit SoC @ 1,5 GHz • 4 Gigabyte LPDDR4-3200 SDRAM • 2.4 GHz dan 5.0 GHz IEEE 802.11ac *wireless*, *Bluetooth* 5.0, BLE • Micro SD 64 GB • LCD TFT 3,5 inch
2	*Power bank* merek Kivee	• Kapasitas Baterai 10.000 mAh • *Input* 5 Volt, 2 Ampere • *Output* 5 Volt, 1 dan 2 Ampere

Wireless router dikonfigurasi sebagai *Dynamic Host Configuration Protocol* (DHCP) server dengan network 192.168.100.0/24. Alokasi alamat IP yang akan diberikan kepada *client* mulai dari 192.168.100.2 sampai 192.168.100.254. *Default gateway* dan *Domain Name System* (DNS) server adalah 192.168.100.1. Berdasarkan Gambar 2, maka *Attacker* dan portabel IPS akan memperoleh alamat IP dari *wireless router* tersebut, sehingga konfigurasi alamat *Internet Protocol* (IP) pada *interface* wlan0 portabel IPS dan laptop *Attacker* dikonfigurasi secara *dynamic*.

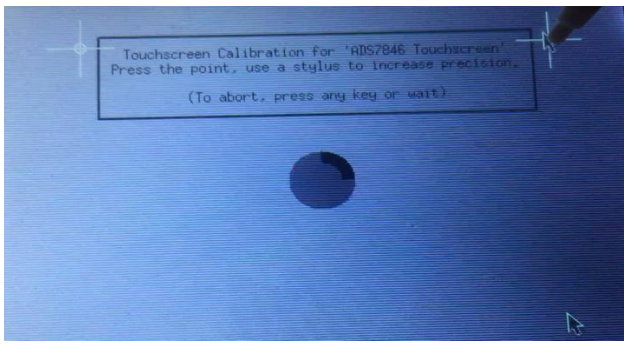
Portabel IPS selain berfungsi sebagai *Intrusion Prevention System* juga dijadikan sebagai router dengan menggunakan network 192.168.4.0/24. Virtual *interface* uap0 dijadikan sebagai *Access Point* dengan "AP-IPS" sebagai SSIDnya, frekuensi yang digunakan mengikuti frekuensi yang diterima oleh wlan0. Alokasi alamat IP setiap perangkat dapat dilihat pada Tabel 2 berikut ini.

TABEL 2. ALOKASI ALAMAT IP PADA SETIAP PERANGKAT

No	Nama Perangkat	Interface	Alamat IP
1	Wireless Router	*Wireless Local Area Network* (WLAN)	192.168.100.1/24
2	Raspberry Pi 4 model B	wlan0 uap0	Dynamic 192.168.4.2/24
3	Laptop Attacker	en0	Dynamic
4	Host 1 dan 2	WLAN	Dynamic

C. *Instalasi dan Konfigurasi Layar LCD TFT*

Tampilan dashboard sistem operasi Raspbian dari Raspberry Pi dapat dilihat secara langsung melalui layar LCD TFT 3.5 inch. Penggunaan LCD tersebut memudahkan bagi pengguna ketika ingin melakukan koneksi ke WiFi Publik yang diinginkan.



Gambar 3. Kalibrasi LCD TFT 3,5 inch

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022

Pada Gambar 3 merupakan salah satu langkah untuk melakukan kalibrasi LCD TFT yang telah terinstal dan terkonfigurasi, hal ini dilakukan agar presisi LCD ketika disentuh menjadi akurat.

D. Konfigurasi Raspberry Pi sebagai Gateway dan IPS

Perangkat Raspberry Pi nantinya akan dikonfigurasi untuk dijadikan *gateway* dan IPS bagi *host* yang akan dilindungi. *Interface* wlan0 akan dikonfigurasi sebagai mode *station*. *Interface* virtual uap0 dijadikan sebagai mode *access point* dengan SSID "AP-IPS" atau disebut sebagai *host access point daemon* (hostapd). Konfigurasi sebagai gateway menggunakan script https://github.com/idev1/rpihotspot.git [15]. Tujuan dari konfigurasi tersebut adalah untuk menjadikan Raspberry Pi selain sebagai AP, akan berfungsi sebagai DHCP server yang akan memberikan alamat IP secara otomatis mulai dari 192.168.4.10 - 192.168.4.15 dengan durasi *release* alamat IP selama 12 jam. Konfigurasi dilakukan dengan menambahkan script " dhcp-range=192.168.4.10,192.168.4.15,12h" pada file /etc/dnsmasq.com. Proses instalasi dan konfigurasi Suricata sebagai IPS mengacu pada dokumen manual instalasi dan konfigurasi yang ada [6].

E. Pengujian Serangan ke Portabel IPS dan Client

Serangan berupa *port scanning* dilakukan menggunakan aplikasi Zenmap. Skenario serangan dilaksanakan melalui mekanisme penyerangan terhadap portabel IPS dan client. Alamat IP Attacker mempunyai alamat IP jaringan yang sama dengan portabel IPS. *Rule* yang digunakan pada pengujian ini adalah Emerging Scan *Rule*.

F. Monitoring Unjuk Kerja Portabel IPS

Penggunaan CPU, memori serta temperatur core portabel IPS dimonitor menggunakan aplikasi RPi-Monitor. Aplikasi ini berfungsi untuk memonitor unjuk kerja dari sistem GNU/Linux secara *real time* [16].

G. Skema Pengujian Ketahanan Catu Daya Portabel IPS

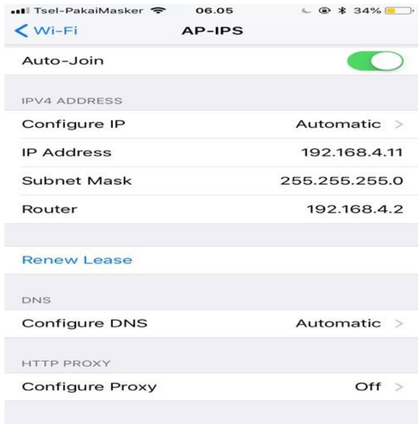
Pada tahapan ini akan dilakukan pengujian seberapa lama catu daya yang bersal dari power bank dengan kapasitas 10.000 mAh mampu bertahan. Selain difungsikan sebagai IPS, perangkat ini akan dijadikan sebagai *gateway*. Satu *client* berupa *smartphone* Iphone 6 akan terhubung ke perangkat tersebut melalui AP dengan SSID berupa AP-IPS.

III. HASIL DAN PEMBAHASAN

Pada tahapan ini akan dilakukan pengujian terhadap portabel IPS yang telah diinstal dan dikonfigurasi, hasil pengujian dapat dilihat sebagai berikut:

A. Pengujian Raspberry Pi Sebagai Gateway

Pada tahapan ini diperoleh hasil bahwa portabel IPS mampu dijadikan sebagai *gateway* dan DHCP server. Tampak pada Gambar 4 merupakan konfigurasi *network* yang menggambarkan bahwa *smartphone* sudah terkoneksi ke Access Point dengan SSID "AP-IPS" dan memperoleh alamat IP 192.168.4.11/24 dengan *default gateway* 192.168.4.2. Alamat IP yang diperoleh sudah sesuai dengan konfigurasi, yaitu mulai dari 192.168.4.10 sampai dengan 192.168.4.15.



Gambar 4. Status WiFi di *smartphone*

B. Pengujian Raspberry Pi sebagai Portabel IPS

Setelah proses instalasi dan konfigurasi Suricata IPS di Raspberry Pi 4 selesai dilakukan, maka dilakukan pengujian dengan menggunakan perintah seperti ditunjukkan pada Gambar 5.

```
pi@raspberrypi:~ $ sudo suricata -c /etc/suricata/suricata.yaml -q 0 -D
```

Gambar 5. Menjalankan Suricata IPS di Raspberry Pi dengan mode daemon

Portabel IPS tersebut diuji dengan menggunakan aplikasi scanner Zenmap yang berjalan di sistem operasi Mac OS Big Sur Versi 11.2.2. Emerging-scan *rule* digunakan dalam melakukan pengujian. Salah satu *rule* yang berfungsi mendeteksi adanya upaya *scanning* sistem operasi menggunakan Zenmap, dengan mengubah *alert* menjadi *drop* seperti terlihat pada Gambar 6.

```
drop udp $EXTERNAL_NET 10000: -> $HOME_NET 10000: (msg:"ET
SCAN NMAP OS Detection Probe"; dsize:300;
content:"CCCCCCCCCCCCCCCCCCCC"; fast_pattern;
content:"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC";
depth:255;
content:"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC";
within:45; classtype:attempted-recon; sid:2018489; rev:4;
metadata:created_at 2014_05_20, updated_at 2019_10_07;)
```

Gambar 6. Modifikasi Emerging-scan *rule* dari *alert* ke *drop* [17]

Kemampuan dalam mendeteksi adanya serangan dilakukan pengujian menggunakan *network* 192.168.100.0/24, dengan alamat ip 192.168.100.28 dengan target portabel IPS alamat IP adalah 192.168.100.18, terlihat pada Gambar 7 portabel IPS berhasil mendeteksi adanya serangan tersebut.

```
06/25/2021-08:11:24.256706 [wDrop] [**] [1:2018489:4] ET SCAN NMAP OS Detection Probe [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 192.168.100.28:34749 -> 192.168.100.18:41863
```

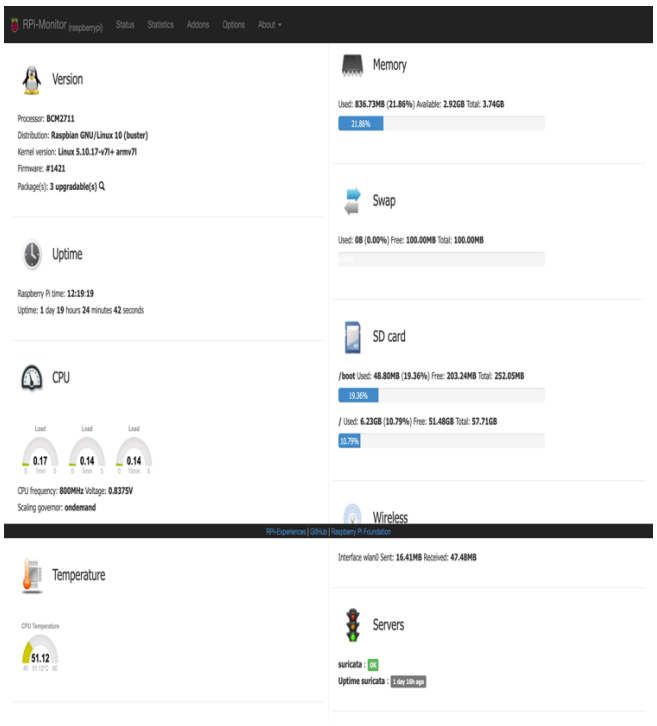
Gambar 7. Hasil deteksi penyerangan menggunakan Zenmap

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022

Pengujian berikutnya adalah dengan melakukan *port scanning* menggunakan aplikasi Zenmap dengan target *client* yang ingin dilindungi, dalam hal ini memiliki alamat IP 192.168.4.11. Hasilnya diperoleh bahwa *client* tidak akan dapat terekspose karena berada pada belakang router, sehingga relatif lebih aman. *Log* serangan *port scanning* dari laptop *Attacker* tidak terdeteksi oleh portabel IPS.

C. *Monitoring Kinerja Portabel IPS*

Kinerja dari portabel IPS dimonitor menggunakan perangkat lunak RPi-Monitor, karena perangkat lunak ini dikhususkan untuk memonitor perangkat embedded secara *real time*. Metrik dari sistem termasuk periperal yang terhubung dipantau dan datanya disimpan ke dalam *database* lokal RPi-Monitor, metrik tersebut dapat diakses melalui browser. Pemantaun metrik meliputi: penggunaan *Central Processing Unit* (CPU) dan *Random Access Memory* (RAM); paket data yang melewati *interface* wlan0; status Suricata dalam kondisi *running* atau tidak termasuk infromasi berapa lama *uptime* dari *service* tersebut. Pengguna dapat mengakses dashboard tersebut melalui http://192.168.4.2:8888. Tampilan dari dashboard RPi-Monitor dapat dilihat pada Gambar 8. Tampak pada dashboard uptime portabel IPS adalah 1 hari 19 jam 24 menit dan 42 detik, hal ini dapat terjadi karena Raspberry Pi 4 Model B masih menggunakan catu daya yang bersal dari adaptor, bukan berasal dari *power bank*.



Gambar 8. Tampilan *dashboard* pemantauan metrik portabel IPS

D. *Monitoring Status Service dan Uptime Portabel IPS*

Status *service* dan *uptime* dari Suricata dapat dimonitor melalui *dashboard* RPi-Monitor. Suricata sudah dikonfigurasi running secara otomatis pada saat perangkat dihidupkan. Konfigurasi dilakukan melalui file services.conf yang ada pada direktori /etc/rpimonitor/template, seperti terlihat pada Gambar 9.

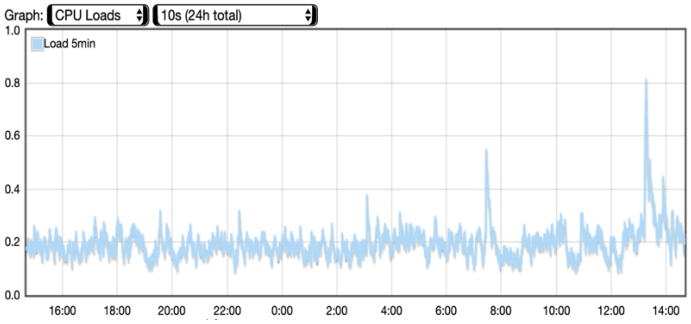
```
dynamic.4.name=suricata
dynamic.4.source=service suricata status | grep "Active: "
dynamic.4.regexp=(\(.*\))
dynamic.18.name=suricata_runtime
dynamic.18.source=service suricata status | grep "Active: "
dynamic.18.regexp=; (.*)
web.status.1.content.1.name=Servers
web.status.1.content.1.icon=daemons.png
web.status.1.content.1.line.1="<b>suricata</b> : "+Label(data.suricata,"=='(running)'","OK","success")+Label(data.suricata,"!='(running)'","KO","danger")
web.status.1.content.1.line.2="<b>Uptime suricata</b> : "+Label(data.suricata,"=='(running)'",data.suricata_runtime,"default")+Label(data.suricata,"!='(running)'","-","default")
```

Gambar 9. Konfigurasi pada file services.conf

Pengujian status *service* dan *uptime* dari Suricata dilakukan dengan cara menonaktifkan *service* yang telah berjalan. Perintah yang digunakan "sudo systemctl stop suricata.service", sedangkan *service* dari Suricata diaktifkan kembali dengan perintah ""sudo systemctl start suricata.service". Indikator berwarna merah dengan keterangan "KO" menandakan bahwa *service* Suricata tidak aktif dan uptime tidak tertampil waktunya, sedangkan jika *service* dalam keadaan aktif akan terlihat indikator berwarna hijau dengan keterangan "OK" dan *uptime service* akan terlihat, seperti ditunjukkan pada Gambar 10.

Gambar 10. Status *service* dan *uptime* Suricata tidak aktif (a), status aktif (b) pada *dashboard* RPi-Monitor

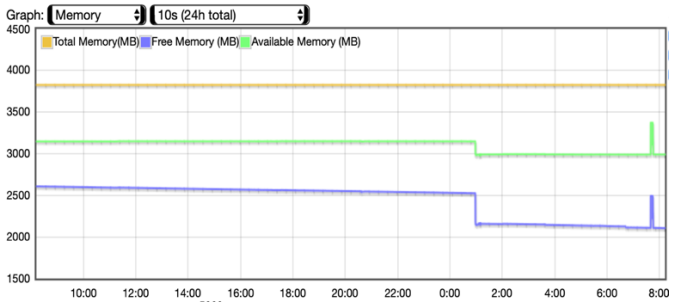
Data terkait dengan beberapa metrik diambil pada tanggal 6 - 7 Juli 2021. Informasi mengenai beban CPU secara terperinci dapat dilihat pada gambar 11 berikut ini.



Gambar 11. Beban CPU portabel IPS

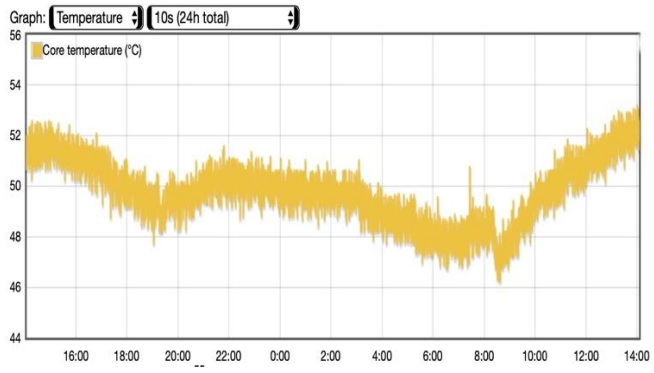
p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022

Beban CPU tertinggi terjadi tercatat sebesar 80%, sedangkan untuk beban terendah berada pada 9%. Beban CPU portabel IPS relatif stabil di sekitar 20%. Gambar 12 menunjukkan indikasi kapasitas memori. Ketersediaan memori yang masih dapat digunakan serta ketersediaannya. Ketersediaan memori relatif masih sangat cukup digunakan dari total memori sebesar 3827 MB.



Gambar 12. Total, ketersediaan dan kapasitas memori yang masih bisa digunakan

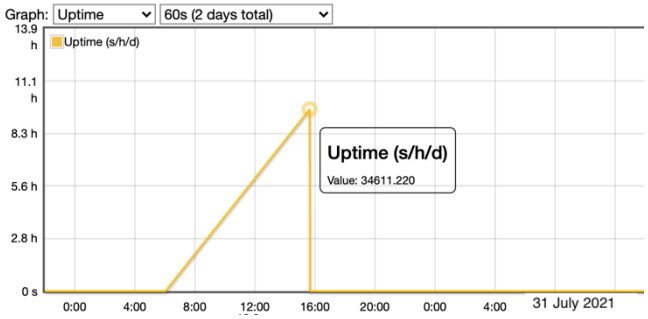
Temperatur *core* dari portabel IPS relatif cukup panas, hal ini dapat dilihat pada Gambar 13. Tampak bahwa temperatur terendah sebesar 46,20 ^{0}C, dan tertinggi di suhu 54,45 ^{0}C. Tampak temperatur *core* cukup tinggi, untuk itu kedepannya diperlukan pendingin atau kipas agar temperatur menjadi lebih dingin.



Gambar 13. Temperatur *core* portabel IPS.

E. Pengujian Durability Catu Daya Portabel IPS

Pada tahapan ini dilakukan pengujian ketahanan catu daya portabel IPS yang berasal dari *power bank* merek Kivee dengan kapasitas 10.000 mAh. Pengujian dilakukan pada tanggal 30 Juli 2021 sekitar pukul 06.00 - 16.00, dengan sebuah smartphone yang terhubung ke portabel IPS melalui interface uap0 menggunakan SSID "AP-IPS". *Smartphone* digunakan untuk aktivitas *browsing* dan *streaming*. Berdasarkan Gambar 14 dapat dilihat bahwa catu daya dari power bank 10.000 mAh mampu bertahan selama 34611.220 detik atau sekitar 9 jam.



Gambar 14. Hasil pengujian ketahanan catu daya portabel IPS

IV. KESIMPULAN

Pengembangan portabel IPS telah berhasil dikembangkan dengan menggunakan Raspberry Pi 4 model B dan Suricata dilengkapi dengan LCD TFT 3,50 inch dan catu daya dengan kapasitas 10.000 mAh. Serangan berupa *port scanning* menggunakan aplikasi Zenmap berhasil dideteksi dan dicegah oleh portabel IPS. Selain berfungsi sebagai IPS perangkat ini mampu menjadi router *gateway*. Penurunan perfoma baik penggunaan CPU dan memori relatif stabil. Catu daya portabel IPS mampu bertahan selama 34611.22 detik dengan sebuah *smartphone* sebagai *client*. Penelitian berikutnya dapat dilakukan pengujian serangan menggunakan metode selain *port scanning*. Penggunaan LCD dengan tipe yang lain, hal ini dikarenakan LCD TFT 3,50 inch dirasakan masih kurang sensitif ketika disentuh pada area tertentu. Penambahan kipas atau pendingin pada portabel IPS, sehingga temperatur *core* menjadi lebih dingin.

UCAPAN TERIMA KASIH

Penghargaan dan ucapan terima kasih kepada pihak Lembaga Penelitian, Publikasi dan Pengabdian Masyarakat Universitas Muhammadiyah Yogyakarta (LP3M UMY) yang telah memberikan dana melalui skema penelitian Dosen Pemula tahun anggaran 2020, sehingga penelitian ini dapat diselesaikan.

DAFTAR PUSTAKA

[1] N. Cheng, X. Oscar Wang, W. Cheng, P. Mohapatra, dan A. Seneviratne, "Characterizing privacy leakage of public WiFi networks for users on travel," *Proc. - IEEE INFOCOM*, no. April, hal. 2769–2777, 2013, doi: 10.1109/INFCOM.2013.6567086.

[2] F. Paramita, O. Alvina, R. E. Sentia, dan A. Kurniawan, "Analisis Unauthorized Access Point Menggunakan Teknik Network Forensics," vol. 14, no. 2, hal. 63–72, 2021.

[3] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, dan S. Shrawne, "Vulnerabilities of Wireless Security protocols (WEP and WPA2)," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 1, no. 2, hal. 2278–1323, 2012.

[4] . B., Y. Yanti, dan . Z., "Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi," *J. Serambi Eng.*, vol. 3, no. 1, hal. 248–254, 2018, doi: 10.32672/jse.v3i1.353.

[5] M. Roesch dan The Snort Team, "Snort 3 User Manual," hal. 1–312, 2018, [Daring]. Tersedia pada: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/008/468/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20190421%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190421T232324Z&X-Am.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022

[6] "Suricata User Guide — Suricata 6.0.3 documentation." https://suricata.readthedocs.io/en/suricata-6.0.3/ (diakses Jul 30, 2021).

[7] Parag Vadher, "Snort IDPS using Raspberry Pi 4," *Int. J. Eng. Res.*, vol. V9, no. 07, hal. 151–154, 2020, doi: 10.17577/ijertv9is070099.

[8] T. Zitta, M. Neruda, dan L. Vojtech, "The security of RFID readers with IDS/IPS solution using Raspberry Pi," *2017 18th Int. Carpathian Control Conf. ICCC 2017*, hal. 316–320, 2017, doi: 10.1109/CarpathianCC.2017.7970418.

[9] "Buy a Raspberry Pi 4 Model B – Raspberry Pi." https://www.raspberrypi.org/products/raspberry-pi-4-model-b/?resellerType=education (diakses Jul 31, 2021).

[10] A. D. Putra, W. Yahya, dan A. Bhawiyuga, "Analisis Kinerja Dan Konsumsi Sumber Daya Aplikasi Web Server Pada Platform Raspberry Pi," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 4, hal. 3513–3521, 2019.

[11] D. Prihatmoko, "Pemanfaatan Raspberry Pi Sebagai Server Web Untuk Penjadwalan Kontrol Lampu Jarak Jauh," *J. Infotel*, vol. 9, no. 1, hal. 84, 2017, doi: 10.20895/infotel.v9i1.159.

[12] O. Karahan dan B. Kaya, "Raspberry Pi Firewall and Intrusion Detection System," *J. Intell. Syst. Theory Appl.*, vol. 3, no. 2, hal. 21–24, 2020, doi: 10.38016/jista.653486.

[13] S. Tripathi dan R. Kumar, "Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer," *Proc. Int. Conf. Comput. Tech. Electron. Mech. Syst. CTEMS 2018*, hal. 80–85, 2018, doi: 10.1109/CTEMS.2018.8769135.

[14] Y. P. Atmojo, "Analisa Performa Raspberry Pi sebagai Intrusion Detection System: Studi Kasus IDS Pada Server Web," *Eksplora Inform.*, vol. 8, no. 1, hal. 24, 2018, doi: 10.30864/eksplora.v8i1.143.

[15] "GitHub - idev1/rpihotspot: Raspberry Pi - Hotspot (Access Point and WiFi Client/Station)." https://github.com/idev1/rpihotspot (diakses Jul 30, 2021).

[16] "Welcome to RPi-Monitor documentation ! — RPi-Monitor v2.13-r0." https://xavierberger.github.io/RPi-Monitor-docs/index.html (diakses Jul 31, 2021).

[17] "Proofpoint Emerging Threats Rules." https://rules.emergingthreats.net/open/suricata-5.0/rules/ (diakses Agu 02, 2021).

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1223, Copyright ©2020
Submitted : August 2, 2021; Revised : April 7, 2022; Accepted : April 8, 2022; Published : April 13, 2022