e-ISSN: 2685-7006 | p-ISSN: 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 10, Nomor 3, Tahun 2021

Performa Raspberry PI Wireless Intrusion Detection System (RAPWIDS) Mendeteksi Serangan Cracking WPA2 HandShake

Gede Arna Jude Saskara[1], I Made Edy Listartha, Gede Saindra Santyadiputra
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
Singaraja, Bali, Indonesia
jude.saskara@undiksha.ac.id[1]

***Abstract*—Pada jaringan wireless kita tidak bisa mengetahui siapa yang berada di dalam jaringan tersebut, sehingga secara tidak langsung memunculkan permasalahan keamanan. Kejahatan yang kemungkinan terjadi pada jaringan wireless adalah pemutusan jaringan, membuat jaringan menjadi lambat dengan membanjiri jaringan dengan paket sampah atau DDos. untuk mengatasi permasalah tersebut diperlukan sebuah system untuk dapat memonitoring dan dapat mendeteksi ketika terdapat masalah keamanan. System yang dapat mendeteksi dan memonitoring tersebut dikenal dengan nama Intrusion Detection System, salah satu software Intrusion Detection System adalah kismet. Pada penelitan ini software kismet Intrusion Detection System yang digunakan untuk mengamankan jaringan wireles akan di pasangkan pada sebuah Raspberry Pi. sehingga nantinya dapat mengukur performa kismet intrusion detection sistem yang dipasangkan pada Raspberry Pi. metode yang digunakan pada penelitian ini adalah pertama melakukan kajian pustaka, kemudian dilanjutkan dengan perancangan system dari merancang topologi dan juga merancang pengujian, kemudian mengimplementasikan sistem, dan melakukan pengujian performa dari Intrusion Detection System. Berdasarkan hasil pengujian Performa Intrusion Detection System menggunakan software Kismet yang dipasangkan pada Raspberry Pi, didapatkan bahwa Kismet yang dipasangkan pada Raspberry Pi dapat mendeteksi 10 serangan Cracking WPA2 handkshake dari 10 kali penyerangan dengan rata-rata deteksi dari serangan dikirimkan hingga dideteksi oleh kismet adalah 3,41 detik. Dapat dikatakan performa intrusion detection system kismet yang dipasangkan pada Raspberry Pi sangat akurat dan dapat mendeteksi serangan dengan sangat cepat.**

Keywords—RAPWIDS; WPA2; Cracking; Handshake;

I. INTRODUCTION

Saat ini jaringan tersedia hampir di setiap rumah, tempat makan, perkantoran, cafe, sekolah, kampus maupun tempat umum [1]. Jaringan wireless merupakan jaringan yang paling mudah untuk di setting untuk terhubung ke internet. Sebuah perangkat dapat terhubung pada wireless hanya dalam waktu hitungan menit [2]. Selain itu juga tidak menggunakan kabel sehingga perangkat dari user dapat terhubung ke jaringan internet, selama masih dalam cakupan area dari jaringan wireless tersebut. Wi-fi merupakan istilah yang biasa digunakan pada sistem Wireless Local Area Network (WLAN). WLAN menggunakan standar komunikasi IEEE 802.11. IEEE 802.11 pertama kali diperkenalkan pada tahun 1999 dan dikembangkan untuk keperluan perangkat di rumah dan kantor untuk konektivitas WLAN. Pasa saat pertama kali di kembangkan kecepatan maksimum transfer datanya adalah 2 Mbps, yang kemudian terus berkembang yang saat ini sudah bisa melakukan transfer data dengan kecepatan 540Mbps. Untuk menjaga keamanan jaringan wireless biasanya pengelola jaringan menambahkan konfigurasi authentication pada perangkat wireless yang digunakan. Terdapat beberapa jenis authentication yang tersedia namun yang paling sering digunakan adalah Wired Equivalent Privacy (WEP) dan Wi-Fi Protection Access (WPA). WPA ada 2 versi WPA dan WPA2 yang nantinya ditambahkan enkripsi untuk mengamankan authentication dari wi-fi [3].

Seiring perkembangan teknologi banyak pengembang perangkat lunak mengembangkan perangkat lunak yang digunakan untuk memcahkan authentication dari Wi-Fi ini sehingga dapat dengan mudah untuk terhubung ke jaringan. Jika sudah masuk kedalam jaringan bisa saja jaringan tersebut digunakan untuk melakukan tindak kejahatan mencari lokasi server maupun melakukan serangan DDos. Selain DDos Masih banyak serangan yang dapat dilakukan pada jaringan wireless yaitu Eavesdropping Attack, Node Capture Attack, Sybil attack, Byzantine attack [4]. Pada penelitian S and Pavithran [5] melakukan serangan bruteforce attack dengan meggunakan perangkat lunak aircrack untuk dapat masuk ke dalam jaringan wireless yang sudah diberikan authentication. Dengan adanya perangkat lunak yang dapat memecahkan authentication pada wi-fi maka sangat diperlukan sebuah pengamanan tambahan

e-ISSN: 2685-7006 | p-ISSN: 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 10, Nomor 3, Tahun 2021

untuk melindungi jaringan wi-fi tersebut. Pada jaringan wi-fi tersebut bisa saja terdapat sebuah server yang menyimpan data yang sangat penting atau bisa saja digunakan untuk mengirimkan data penting.

Untuk dapat membantu mengingkatkan keamanan dari wi-fi, pada jaringan perlu ditambahkan sebuah keamanan tambahan seperti pada penelitian sebelumnya yaitu menambahkan captive portal pada jaringan wi-fi sehingga penyerang tidak dapat melakukan serangan ke dalam jaringan [6]. Selain hal tersebut pada jaringan perlu juga ditambahkan server yang digunakan untuk memonitoring dan memberikan informasi jika pada jaringan terjadi suatu tindakan kejahatan. Proses monitoring dan pemberian informasi tersebut dikenal dengan nama Intrusion Detection System [7][8]. Beragam penelitian terkait Intrusion Detection System telah dilakukan seperti yang dilakukan oleh Agarwal et al. 2013 menambahkan Intrusion Detection System pada jaringan wi-fi untuk mendeteksi serangan de-authentication. [9], selain itu juga pada penelitian Sobari, 2015 menambahkan intrusion detection sistem pada jaringan wireless, dimana intrusion detection system yang digunakan adalah Snort yang menggunakan metode Hierarchical Clustering sehingga dapat mendeteksi serangan baru pada jaringan[10]. Nizam et al, 2017 membuat RaspyAir yaitu Raspberry Pi yang telah dipasangkan Intrusion Detection System yang kemudian diuji coba dengan melakukan segala jenis serangan yang dapat dilakukan melalui jaringan wi-fi [2]. Adapun peneliti lain yaitu Wibowo, Triyono, dan Sutanta, 2017 melakukan pengujian keamanan jaringan wireless yang dimiliki oleh Dinas Kominfo Yogyakarta serangan yang dilakukan yaitu Aircrack, ARP Spoofing, Cracking WPA/WPA2 [11]. Pranata, Kunang and Saputri, 2019 melakukan penelitian peningkatan keamanan jaringan nirkabel dengan pendeteksi serangan yang berbasis kismet DD-WRT dimana didapakan hasil software kismet dapat mendeteksi serangan pada jaringan [12]. Penelitian terakhir yang dilakukan oleh Haninda dan Swari, 2020 yang menggunakan Raspberry Pi 3 yang telah dipasangkan Intrusion Detection System Snort untuk mengamankan jaringan Wi-Fi di Kampus STMIK STIKOM Indonseia [13].

Dari permasalahan yang pada jaringan wireless yang sudah terdapat authentication berupa WEP maupun WPA/WPA2 namun penyerang masih tetap bisa melakukan aksinya, dan didukung oleh penelitian-penelitian sebelumnya, maka perlu dilakukan penelitian Performa Intrusion Detection System menggunakan software Kismet yang dipasangkan pada Raspberry Pi. Intrusion Detection System yang digunakan adalah Kismet dikarenakan kismet mendukung monitoring terhadap jaringan wireless dan dipasangkan pada Raspberry agar pengelola jaringan dapat menyediakan pengamanan jaringan yang murah dibandingkan dengan membeli sebuah komputer server. Adapun kontribusi dalam penelitian ini adalah menggunakan Intrusion Detection System Kismet yang nantinya dapat mendeteksi serangan Cracking WPA2 Handshacking, selain itu juga diuji performanya pada sebuah mini komputer yaitu raspberry pi yang pada penelitian-penelitian sebelumnya belum diterapkan.

II. KAJIAN PUSTAKA

Wi-fi merupakan istilah yang biasa digunakan pada sistem Wireless Local Area Network (WLAN). WLAN menggunakan standar komunikasi IEEE 802.11. IEEE 802.11 pertema kali diperkenalkan pada tahun 1999 dan dikembangkan untuk keperluan perangkat di rumah dan kantor untuk konektivitas WLAN. Pasa saat pertama kali di kembangkan kecepatan maksimum transfer datanya adalah 2 Mbps, yang kemudian terus berkembang yang saat ini sudah bisa melakukan transfer data dengan kecepatan 540Mbps.

Untuk mengamankan jaringan wireless biasanya pengelola jaringan menambahkan konfigurasi authentication pada perangkat wireless yang digunakan. Terdapat beberapa jenis authentication yang tersedian namun yang paling sering digunakan adalah Wired Equivalent Privacy (WEP) dan Wi-Fi Protection Access (WPA). WPA ada 2 versi WPA dan WPA2 yang nantinya ditambahkan enkripsi untuk mengamankan authentication dari wi-fi.

A. Intusion Detection System

Intrusion Detection System (IDS) merupakan sebuah aplikasi atau perangkat lunak yang dapat mendeteksi aktivitas yang mecurigakan pada sebuah sistem atau jaringan. IDS akan memonitor lalulintas data pada sebuah jaringan atau mengambil data dari bekas log.IDS akan menganalisa dengan algoritma tertentu yang kemudian nantinya ditentukan jenis serangannya dan kemudian memberikan peringatan kepada administrator jaringan.

IDS umumnya berdasar pada arsitektur multi-tier dari :

1. Teknologi deteksi, yang bergantung pada :
   a. Sensor: biasanya disebut engine/probe, merupakan teknologi yang memungkinkan IDS untuk memantau sejumlah besar traffic
   b. Agents: Software yang di install pada suatu PC untuk memantau file atau fungsi tertentu dan melakukan pelaporan jika terjadi sesuatu.
   c. Collector: Seperti agent, tetapi lebih kecil, dan tidak membuat keputusan, tetapi hanya menyampaikan ke manager pusat.
2. Analisis Data: Proses analisis data dan data mining sejumlah besar data dilakukan oleh lapisan(layer), kadang diletakkan pada pusat data/server.
3. Manajemen Konfigurasi/GUI: Biasanya disebut juga console merupakan antarmuka operator dengan IDS.

Sensor bertugas untuk memfilter informasi dan mendiscard data yang tidak relevan dari sekumpulan kejadian yang terhubung dengan sistem terproteksi, misalnya mendeteksi aktivitas-aktivitas yang mencurigakan. Analisis dilakukan dengan menggunakan database yang berisi kebijakan dalam

e-ISSN: 2685-7006 | p-ISSN: 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 10, Nomor 3, Tahun 2021

mendeteksi. Database ini mengatur konfigurasi parameter IDS, termasuk mode komunikasi dengan modul tanggap.

Sensor diintegrasikan dengan sejumlah komponen yang bertanggung jawab untuk pengumpulan data. Metode pengumpulan ini ditentukan oleh kebijakan dari event generator yang akan menjelaskan mode filtering dari suatu deskripsi informasi. Event Generator (misalnya: sistem operasi, jaringan, dan aplikasi) akan membuat sebuah kebijakan yang konsisten dalam mengeset sekumpulan kejadian yang mungkin seperti adanya sebuah log atau audit dari sistem atau paket jaringan.

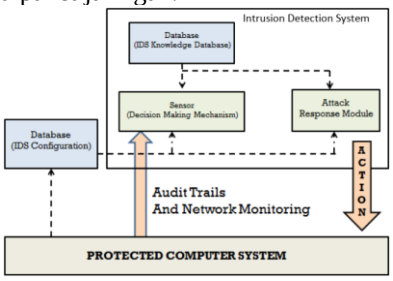

Fig. 1 Arsitektur IDS

IDS pada umumnya memiliki beberapa sifat diantaranya :

a. Suitability
   Suitabiliy artinya aplikasi IDS lebih berfokus pada skema manajemen dan arsitektur jaringan.
b. Flexibility
   IDS mampu beradaptasi dengan berbagai spesifikasi jaringan yang akan dideteksi oleh aplikasi.
c. Protection
   Proteksi pada IPS sangat ketat dalam memproteksi ganguan yang sifatnya berbahaya dan utama.
d. Interoperability
   IDS dapat beropreasi dengan baik dengan perangkat-perangkat keamanan jaringan serta manajemen jaringan lainnya.
e. Comprehensiveness
   Kelengkapan yang dimili oleh aplikasi IDS mampu melakukan sistem pendeteksian secara menyeluruh seperti pemblokiran semua yang berbentuk Java Applet, memonitor isi dari suatu e-mail.
f. Event Management
   Konsep IDS mampu melakukan proses manajemen suatu jaringan serta proses pelaporan pada saat dilakukan setiap pelacakan, bahkan aplikasi ini mampu melakukan updating pada sistem basis data pola suatu ganguan.
g. Active Response
   Pendeteksi gangguan ini mampu secara cepat untuk mengkonfigurasi saat munculnya suatu ganggoan, biiasanya aplikasi ini berintegrasi dengan aplikasi lainnya seperti aplikasi Firewall serta aplikasi IDS ini dapat mengkonfigurasi ulang spesifikasi router pada jaringannya.
h. Supprot
   Lebih bersifat mendukung pada suatu jenis produk apabila diintegrasikan dengan aplikasi lain.

Berikut adalah teknik deteksi yang digunakan dalam IDS :

a. Teknik Deteksi Anomali (Anomaly Detection/Behavior Based)
   Behaviour base adalah cara kerja IDS dengan mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan – kejanggalan pada sistem, yaitu adanya keanehan dan kejanggalan dari kondisi pada saat sistem normal, sebagai contoh : adanya penggunaan memory yang melonjak secara terus menerus atau terdapatnya koneksi secara parelel dari satu IP dalam jumlah yang banyak dan dalam waktu yang bersamaan. Kondisi tersebut dianggap kejanggalan yang selanjutnya oleh IDS Anomaly Based ini dianggap sebagai serangan.
b. Teknik Deteksi Penyalahgunaan (Misuse Detection/Knowledge Based)
   Knowled Based adalah IDS mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule pada IDS tersebut. Dabase rule tersebut dapat berisi signature paket serangan. Jika pattern atau pola paket data tersebut memiliki kesamaan dengan rule pada database rule pada IDS maka paket data dapat dianggap sebagai serangan,

IDS dapat dikategorikan menjadi

a. Network-based Intrusion Detection System (NIDS)
   Memantau anomaly di jaringan dan mampu mendeteksi seluruh host yang berada dalam satu jaringan. Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Contoh: Melihat adanya network scanning.
b. Host-based Intrusion Detection System (HIDS)
   Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke internet. Contoh: memonitor logfile, process dan file ownership.

Terdapat beberapa program yang bisa digunakan untuk IDS diantaranya adalah

a. Tcplogd
   Program yang mendeteksi stealth scan. Stealth scan adalah scanning yang dilakukan tanpa harus membuat sebuah sesi tcp. Sebuah koneksi tcp dapat terbentuk jika klient mengirimkan paket dan server

e-ISSN: 2685-7006 | p-ISSN: 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 10, Nomor 3, Tahun 2021

mengirimkan kembali paketnya dengan urutan tertentu, secara terus menerus hingga sesi tcp dapat berjalan. Stealth scan memutuskan koneksi tcp sebelum klien menerima kembali jawaban dari server. Scanning model ini biasanya tidak terdeteksi oleh log umum di linux.

b. Snort
Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort merupakan sebuah produk terbuka yang dikembangkan oleh Marty Roesch dan tersedia secara gratis. Snort merupakan IDS berbasis jaringan yang menggunakan metode deteksi rule based, menganalisis paket data apakah sesuai dengan jenis serangan yang diketahui olehnya.

c. Kismet
Kismet juga mmerupakan suatu perangkat lunak analisis jaringan yang dapat mengidentifikasi jaringan dengan cara mengumpulkan paket dan mendeteksi jaringan secara pasif. Kismet Wireless Intrusion Detection System memiliki kemampuan untuk mendeteksi nama SSID yang tersembunyi dan keadaan jaringan non-beaconing melalui lalu lintas data.

III. METODE PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan, diantaranya adalah dengan kajian pustaka, perncangan, implementasi, pengujian, dan pemeliharaan. Alur penelitian dapat dilihat pada Gambar Fig. 2.

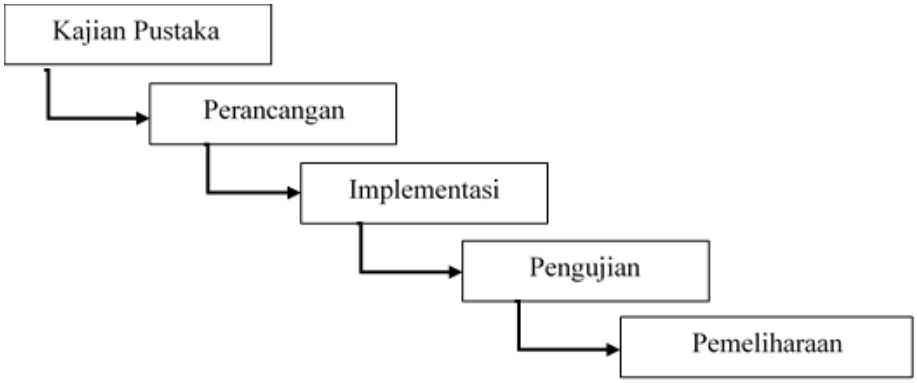

Fig. 2 Alur Penelitian

Berikut penjelasan dari masing-masing tahapan penelitian.

A. Kajian Pustaka

Tahap kajian pustaka merupakan tahap melakukan pencarian terhadap berbagai sumber tertulis, baik berupa buku-buku, arsip, majalah, artikel, dan jurnal, atau dokumen-dokumen yang relevan dengan permasalahan yang dikaji. Tahapan ini memiliki tujuan untuk memperoleh informasi mengenai hal-hal yang telah dilakukan oleh peneliti sebelumnya, aspek apa saja yang telah diteliti, teknik yang diterapkan, bagaimana hasil dan hambatan yang ditemui dalam melakukan penelitian, dan perbedaan rumusan masalah yang hendak dipecahkan dengan masalah-masalah yang sudah dipecahkan oleh peneliti sebelumnya. Sehingga informasi yang didapat dari kajian pustaka ini dijadikan rujukan untuk memperkuat argumentasi-argumentasi yang ada. Penelitian ini nantinya akan melakukan pengkajian beberapa literatur yang berkaitan dengan Intrusion Detction System, Wireless Network dan Kismet.

B. Perancangan

Tahapan selanjutnya adalah melakukan perancangan topologi jaringan yang akan digunakan. Selain itu, terdapat skenario dalam implementasi Intrusion Detection System ini. Skenario simulasinya adalah dengan menggunakan Akses point yang sudah diberikan Autentication dengan WPA2/PSK yang terhubung dengan dengan switch dan terhubung dengan Intusion Detection System dan juga terhubung ke internet. Konfigurasi yang dilakukan pada Raspberry Pi adalah konfigurasi aplikasi intrusion detection system yaitu kismet sehinga dapat memberikan notifikasi jika ada seseorang yang ingin berusaha masuk ke dalam jaringan dengan melakukan brouteforce WPA2/PSK.

e-ISSN: 2685-7006 | p-ISSN: 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 10, Nomor 3, Tahun 2021

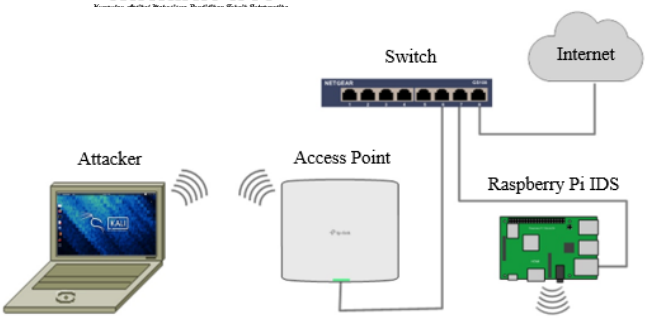

Fig. 3 Topologi Jaringan

C. *Implementasi*

Pada tahapan ini adalah melakukan konfigurasi pada Raspberry Pi dan juga pada aplikasi Intrusion Detection System sehingga dapat memberikan informasi ketika terjadi serangan

D. *Pengujian*

Tahap pengujian merupakan tahapan lanjutan dari tahapan implementasi. Adapun tahapan pengujian adalah dengan melakukan serangan bruteforce attack password pada wifi sebanyak 10 kali dan juga menghitung waktu dari melakukan serangan hingga dideteksi oleh Kismet Intrusion Detection System.

E. *Pemeliharaan*

Dari hasil pengujian yang kemudian dijadikan dasar untuk tahapan terakhir yaitu pemeliharaan. Pada tahapan ini merupakan tahapan memperbaiki dan memelihara sistem sehingga dapat berjalan dengan baik

IV. HASIL DAN PEMBAHASAN

A. *Implementasi*

Penelitian diawali dengan membuat rancangan topologi sesuai yang sudah dijelaskan pada bab sebelumnya, kemudian melakukan implementasi dari topologi tersebut. Implementasinya tidak jauh berubah dari perancangany yang sudah dibuat. Dimana terdapat sebuah switch yang terhubung ke internet dan juga terhubung ke access point dan juga raspberry pi. Rasberry Pi yang terhubung ke switch dan internet tersebut kita pasangkan aplikasi Kismet dan pada access point kita atur agar dapat menyebarkan jaringan internet dengan menggunakan password yaitu WPA2/PSK. Gambaran hasil implementasinya dapat dilihat pada gambar Fig 4.

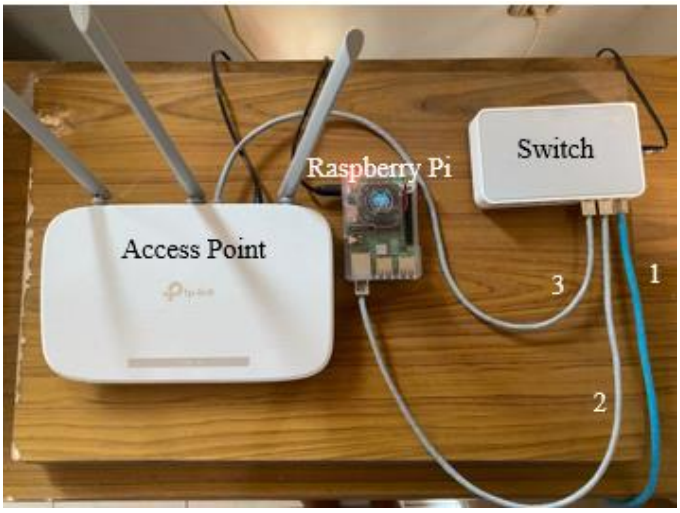

Fig. 4 Implementasi Perancangan

Terdapat 3 kabel UTP yang terhubung pada Switch. Kabel UTP yang diberi nomor 1 pada gambar terhubung ke Internet, kemudian kabel UTP yang diberi nomor 2 terhubung ke Raspberry Pi yang nantinya akan dipasangkan Kismet untuk mendeketsi serangan yang dialami oleh Access Point. Terakhir kabel UTP yang diberi nomor 3 pada gambar terhubung dengan Access Point yang nantinya akan memancarkan sinyal wifi yang terhubung ke internet dan sudah di beri password dengan security WPA2-AES, dan WPA Authentication: PSK dan dengan nama SSID Kemuning4_A.

Setelah semua terhubung dan sesuai dengan topologi yang dirancang, kemudian dilanjutkan dengan memasangkan Operating System pada Raspberry Pi. Pada penelitian kali ini Operating System yang digunakan pada Raspberry Pi adalah Kali Linux, dikarenakan pada Kali Linux ini sudah terpasang aplikasi Intrusion Detection System yang akan digunakan yaitu Kismet. Untuk menjalankan Kismet pada Kali Linux, harus masuk ke user Rootnya terlebih dahulu, kemudian menjalankan perintah kismet -c wlan0. Setelah itu kismet intrusion detection system dapat diakses melalui browser dengan alamat http://localhost:2501/ atau bisa menggunakan alamat IP dari raspberry pi.

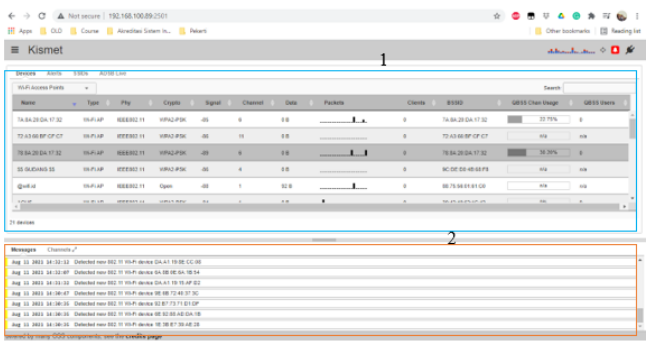

Fig. 5 Monitoring Wifi dengan Kismet Intrusion Detection System

e-ISSN: 2685-7006 | p-ISSN: 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 10, Nomor 3, Tahun 2021

Pada Fig. 5 dibagian 1 dapat dilihat bahwa dengan menggunakan Kismet kita dapat melihat seluruh Access point dan juga Device yang terhubung ke Access point yang berada dalam jangkauan Raspberry Pi, dan juga pada bagian 2 dapat melihat alert (pemberitahuan ketika ada perangkat baru yang terhubung dengan access point hingga ketika ada perangkat yang melakukan serangan) jika terdapat serangan pada Wifi di sebuah access point kismet akan meberikan pemberitahuan dengan memberi warna merah pada kolom nomor 2 pada gambar Fig. 5 atau bisa dilihat pada gambar Fig. 6. Pemberitahuan itu juga dapat dilihat pada pemberitahuan di pojok kanan atas pada web kismet. Selain memberikan pemberitahuan kismet juga akan langusng memutuskan jaringan perangkat yang melakukan serangan.

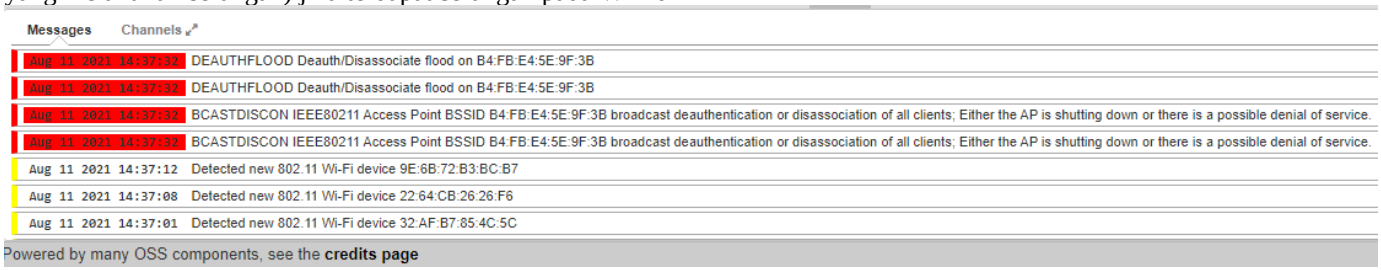

Fig. 6 Alert pada Kismet ketika Terjadi Serangan

B. Pengujian

Setelah perancangan topologi sudah semua terhubung dan aplikasi intrusion detection system Kismet yang sudah terpasang dan berjalan pada Raspberry Pi. Selanjutnya adalah melakukan pengujian terhadap performa dari Kismet intrusion detection system pada Raspberry. Pengujian yang dilakukan adalah dengan melakukan serangan bruteforce attack password pada Access Point atau biasa dikenal dengan Cracking Wifi WPA2 Handshake dan serangan tersebut akan dilakukan sebanyak 10 kali dan dicatat waktu dari proses penyeranngan hingga dapat dideteksi oleh kismet.

C. Hasil

Pada penelitian ini untuk melakukan serangan menggunakan komputer yang sudah terpasang system operasi Kali Linux, sehingga ketika melakukan serangan Cracking Wifi WPA2 handshake dapat dilakukan dengan menjalankan perintah berikut sudo airodump-ng -w Password -c 11 --bssid B4:FB:E4:5E:9F:3B wlan0mon, keterangan dari perintah tersebuh -w merupakan perintah untuk menyimpan data hasil handshaking, Password merupakan file tempat menyimpan hasil handshacking, -c merupakan perintah untuk memasukkan channel wifi access point yang akan diserang, dan diikuti dengan 11 yang merupakan channel wifi access point yang diserang dan --bssid B4:FB:E4:5E:9F:3B merupakan mac address dari access point yang diserang dan terakhir wlan0mon adalah perangkan yang digunakan untuk melakukan serangan yang pada sistem operasi linux wlan0 merupakan perangkat wifi pada komputer maupun raspberry pi. Perintah tersebut dilakukan sebanyak 10 kali sehingga didapatkan hasil sebagai berikut.

TABLE I. HASIL PERCOBAAN

Percobaan ke-	Berhasil/Tidak	Waktu (dalam detik)
1	Berhasil	3,49 detik
2	Berhasil	3,23 detik
3	Berhasil	4,01 detik
4	Berhasil	3,36 detik
5	Berhasil	2,92 detik
6	Berhasil	3,58 detik
7	Berhasil	3,45 detik
8	Berhasil	2,98 detik
9	Berhasil	3,80 detik
10	Berhasil	3,28 detik

Setelah melakukan pengujian tahapan terakhir adalah melakukan pemeliharaan, dari hasil pengujian didapatkan bahwa Kismet dapat mendeteksi dan mengantisipasi serangan Cracking WPA2 Handshacking.. Untuk dapat mendeteksi dan mengantisipasi serangan tersebut membuat kinerja Raspberry Pi semakin berat sehingga membuat kismet berhenti setiap kurang lebih 1 jam dijalankan. Untuk itu diperlukan pemeliharaan yaitu melakukan pemindahan log dari kismet ke cloud kemudian menghapus dari raspberry lalu melakukan boot ulang system operasi atau Restart dan langsung menjalankan Kismet.

D. Pembahasan

Hasil dari tahapan pengujian memperlihatkan bahwa Kismet sangat efektif untuk mendeteksi serangan Cracking WPA2 Handshaking. Dari 10 kali pengujian serangan

Cracking WPA2 Handshaking, Kismet dapat mendeteksi dan mangantisipasi semua serangan tersebut dengan rata-rata waktu mendeteksi dari serangan dikirimkan hingga dideteksi adalah 3,41 detik.

V. KESIMPULAN

Berdasarkan penelitian Performa Intrusion Detection System menggunakan software Kismet yang dipasangkan pada Raspberry Pi, diperoleh kesimpulan bahwa Kismet yang dipasangkan pada Raspberry Pi dapat mendeteksi 10 serangan Cracking WPA2 handkshake dari 10 kali penyerangan dengan rata-rata deteksi dari serangan dikirimkan hingga dideteksi oleh kismet adalah 3,41 detik. Dapat dikatakan performa intrusion detection system kismet yang dipasangkan pada Raspberry Pi sangat akurat dan dapat mendeteksi serangan dengan sangat cepat. Namun yang menjadi kendala adalah Ketika Kismet Intrusion Detection System dijalankan selama kurang lebih 1 jam makan aplikasi akan tidak dapat mendeteksi serangan dan perlu melakukan restart pada raspberry pi dan menjalankan kembali kismet. Hal tersebut dikarenakan procecor dan memory penyimpanan yang kecil sehingga cepat penuh oleh log kismet, sehingga diperlukan pemindahan log secara berkala setiap jamnya..

Adapun saran untuk kedepannya, Kismet dapat dijalankan pada raspberry yang dibuat dalam cluster sehingga memberpesar daya untuk menjalankan kismet dan tidak perlu melakukan restart setiap kurang lebih 1 jam. Mengembangkan sistem untuk memberikan notifikasi kepada administrator jaringan melalui over the top (OTT) seperti whatsapp ataupun telegram. Selain itu juga melakukan pengukuran Intrusion Detection yang lain pada Raspberry Pi.

ACKNOWLEDGMENT

Terima kasih saya ucapkan kepada Lembaga Peneilitan dan Pengabdian Kepada Masyarakat (LPPM) Universitas Pendidikan Ganesha. Karena telah memberikan bantuan dana untuk penelitian dengan Nomor Kontrak penelitian 265/UN48.16/LT/2021.

REFERENCES

[1] R. Haryunarendra, M. N. Al-Azam, and D. Rizaluddin, "Performa Jaringan Free Wireless di Taman Kota Surabaya," J. Link, vol. 26, no. 2, pp. 25–29, 2017.

[2] M. Nizam et al., "RaspyAir : Self-Monitoring System for Wireless Intrusion Detection using Raspberry Pi RaspyAir : Self-Monitoring System for Wireless," vol. 1, no. February, pp. 20–31, 2017.

[3] S. Banerji and R. S. Chowdhury, "On IEEE 802 . 11 : Wireless LAN Technology," no. July 2013, 2015, doi: 10.5121/ijmnct.2013.3405.

[4] S. D. Kanawat and P. S. Parihar, "Attacks in Wireless Networks," Int. J. Smart Sens. Adhoc Network., no. 1, pp. 113–116, 2011, doi: 10.47893/ijssan.2011.1033.

[5] M. P. S and S. Pavithran, "Advanced Attack Against Wireless Networks Wep , Wpa / Wpa2-Personal And Wpa / Wpa2- Enterprise," no. August, 2015, doi: 10.13140/RG.2.2.35107.91686.

[6] G. Arna, J. Saskara, I. P. O. Indrawan, and P. M. Putra, "KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN CAPTIVE PORTAL DAN WPA / WPA2 DI POLITEKNIK GANESHA GURU," J. Pendidik. Teknol. dan Kejuru., vol. 16, no. 2, pp. 236–247, 2019, doi: 10.23887/jptk-undiksha.v16i2.18559.

[7] A. Hamdan, M. N. Rafidah, B. Bahaa, and A. A. Zaidan, "Intrusion Detection System: Overview," J. Comput., vol. 2, no. 2, pp. 130–133, 2010.

[8] S. Saini Yogesh Kumar Sharma, "A Research Study of Wireless Network Security: A Case Study," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 6, no. 3, p. 2277, 2016, [Online]. Available: www.ijarcsse.com.

[9] M. Agarwal, S. Biswas, and S. Nandi, "Detection of De-authentication Denial of Service," 2013.

[10] I. A. Sobari, "Rancangan Wireless Intrusion Detection System Menggunakan Snort," J. Techno Nusa Mandiri, vol. 12, no. 1, pp. 1–9, 2015.

[11] M. G. H. Wibowo, J. Triyono, and E. Sutanta, "Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika Diy," Semin. Nas. Call Pap. Pengemb. Smart City menuju Pembang. Kota yang Cerdas dan Berkelanjutan, vol. 1, no. 1, pp. 2–9, 2017.

[12] D. Pranata, Y. N. Kunang, and N. A. O. Saputri, "Peningkatan Keamanan Jaringan Nirkabel Dengan Pendeteksi Serangan Berbasis Kismet DD-WRT," Bina Darma Conf. Comput. Sci., vol. 1, no. 5, pp. 1126–1132, 2019.

[13] M. Hanindia and P. Swari, "Intrusion Detection System (Ids) Menggunakan Raspberry Pi 3 Berbasis Snort Studi Kasus : Stmik Stikom Indonesia," J. SCAN, vol. XV, pp. 2–7, 2020.