Jurnal Teknik Informatika vol.17 no. 1 January – March 2021, pp. 19-26
p-ISSN : 2301-8364, e-ISSN : 2685-6131 , available at : https://ejournal.unsrat.ac.id/index.php/informatika

An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs

Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa

Astri Saraun, Arie S.M. Lumenta, Daniel Febrian Sengkey
Teknik Elektro Universitas Sam Ratulangi Manado, Jl. Kampus Bahu-Unsrat Manado, 95115, Indonesia
E-mails: 17021106005@student.unsrat.ac.id, al@unsrat.ac.id, danielsengkey@unsrat.ac.id
Received: 23 July 2021; revised: 18 October 2021; accepted: 18 October 2021

***Abstract* — Wireless network is a technology that is rapidly developing in the field of data transmission. Wireless network make use of radio waves as a medium for data transmission. Kantor Dinas Pendidikan Kabupaten Minahasa has provided facilities in the form of a wireless network as office facilities to search for information, access the internet, manage data, communicate and others. However, wireless network still has many weaknesses and loopholes hence why it is very vulnerable to threats from irresponsible parties that can cause harm to others.**

This research aims to analyze the network security system in Kantor Dinas Pendidikan Kabupaten Minahasa. This research conducted testing with cracking the encryption, ARP poisoning, denial of service and wireless router password cracking attacks on wireless networks. This research uses the penetration test method. Attacks carried out against the wireless network have the status of being successful because the security system implemented by Kantor Dinas Pendidikan Kabupaten Minahasa is still not secure. The result of this study can be used by network managers as materials in repairing or improving the network security system in Kantor Dinas Pendidikan Kabupaten Minahasa.

***Keywords* — Network Security; Penetration test; Wireless Network; Wireless Local Area Network**

Jaringan nirkabel merupakan teknologi yang berkembang di bidang transmisi data. Jaringan nirkabel memanfaatkan gelombang radio sebagai media transmisi data. *Wireless fidelity* atau yang sering kita sebut Wi-Fi merupakan perangkat standar yang digunakan untuk komunikasi lokal tanpa penggunaan kabel (*wireless local area network*). Pada Kantor Dinas Pendidikan Kabupaten Minahasa telah menyediakan fasilitas berupa jaringan nirkabel sebagai fasilitas kantor untuk digunakan dalam mencari informasi, mengakses internet, pengelolaan data, berkomunikasi dan lainnya. Namun jaringan nirkabel masih memiliki banyak kelemahan atau celah sehingga sangat rentan terhadap ancaman - ancaman serangan dari pihak yang tidak bertanggung jawab yang bisa menyebabkan kerugian pada orang lain.

Penelitian ini untuk menganalisis sistem keamanan jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa. Melakukan pengujian dengan serangan *cracking the encryption*, ARP *poisoning* dan *denial of service* terhadap jaringan nirkabel. Penelitian ini menggunakan metode *penetration test.* Serangan – serangan yang dilakukan terhadap jaringan nirkabel berstatus berhasil karena sistem keamanan yang diterapkan oleh Kantor Dinas Pendidikan Kabupaten Minahasa masih kurang aman. Hasil dari penelitian ini bisa digunakan oleh pengelola jaringan sebagai bahan dalam perbaikan atau meningkatkan sistem keamanan jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa.

***Kata kunci* — Jaringan Nirkabel; Keamanan Jaringan; *Penetration Test*; *Wireless LAN*.**

I. PENDAHULUAN

Di era digital ini, teknologi informasi dan komunikasi telah berkembang sangat pesat sehingga memiliki peran penting bagi masyarakat. Jaringan komputer merupakan salah satu teknologi yang berkembang di bidang transmisi data. Jaringan komputer memiliki 2 jenis media transmisi data, yaitu kabel dan nirkabel. Jaringan nirkabel memanfaatkan gelombang radio sebagai media transmisi data, sehingga jaringan nirkabel tidak memerlukan kabel untuk bisa saling terhubung antara perangkat yang satu dengan perangkat yang lainnya [1]. Jaringan nirkabel atau *wireless* yang saat ini sangat sering digunakan bahkan dikembangkan karena jaringan nirkabel bisa digunakan pada setiap aspek skenario [2]-[3]. Adapun *wireless fidelity* atau yang sering kita sebut dengan Wi-Fi merupakan perangkat standar yang dipakai untuk komunikasi jaringan lokal tanpa menggunakan kabel (*Wireless Local Area Network*/WLAN) yang didasari pada spesifikasi IEEE 802.11 [4].

Namun penggunaan jaringan nirkabel tidak luput dari kejahatan – kejahatan siber yang dilakukan dari pihak yang tidak bertanggung jawab yang bisa berakibatkan merugikan orang lain. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), pada tahun 2020 terdapat jumlah 495,4 juta upaya kejahatan siber di Indonesia, jauh lebih tinggi di bandingkan tahun 2019 yang hanya berkisar 290,3 juta upaya kejahatan siber. Terjadinya kenaikan serangan siber pada tahun 2020 [5]-[6].

Maka dari itu pentingnya menerapkan suatu sistem keamanan jaringan yang cukup aman, sehingga bisa meminimalisir serangan – serangan terhadap jaringan, berupa, pencurian data, ketidak tersediaan data atau informasi, hilangnya integritas atau keaslian data atau informasi dan lainnya yang berakibat merugikan [7]-[8]. Untuk menerapkakan sistem keamanan jaringan yang cukup aman perlu dilakukan analisa terhadap sistem keamanan jaringan. Hasil dari analisa terhadap sistem keamanan bisa dijadikan sebagai bahan untuk melakukan evaluasi terhadap sistem keamanan jaringan [4].

Kantor Dinas Pendidikan Kabupaten Minahasa yang telah menyediakan fasilitas berupa jaringan nirkabel untuk digunakan sebagai media dalam membantu memenuhi kebutuhan informasi,

mengakses internet, berkomunikasi satu sama lain, melakukan transaksi *online*, pengelolaan pengirimandata dan lainnya [9]. Untuk meminimalisir serangan – serangan yang bisa berakibat merugikan, Kantor Dinas Pendidikan Kabupaten Minahasa perlu menerapkan sistem keamanan jaringan yang cukup aman.

A. Penelitian Terkait

Penelitian yang dilakukan oleh Desi Maya Sari, Muh Yamin, LM. Bahtiar Aksara dengan menggunakan pendekatan *action research* dan metode *penetration test*. Melakukan uji *penetration* dengan serangan *cracking the encryption* dan *bypassing* WLAN *authentication*. Dari hasil uji penetrasi yang dilakukan pada sistem keamanan WEP dengan serangan *cracking the encryption* dan MAC *address filtering* dengan serangan *bypassing* WLAN *authentication* berhasil dilakukan dan sistem keamanan WPAPSK/WPA2/PSK dengan serangan *cracking the encryption* berhasil dilakukan pada pengujian yang kedua dengan menggunakan huruf sebagai *pre-shared-key* (PSK). Pada pengujian yang pertama gagal dengan menggunakan kombinasi huruf dan angka pada kata sandi dan pengujian yang ketiga gagal dengan menggunakan kombinasi huruf, simbol dan angka pada kata sandi. Dari pengujian tersebut dapat ditarik kesimpulan bahwa sistem keamanan WPA merupakan sistem keamanan yang bisa terbilang aman. Namun sistem keamanan yang menggunakan WPA juga harus dibarengi dengan penggunaan kata sandi yang kuat dimana berisikan kata yang panjang dan dikombinasi dengan huruf kecil, huruf besar, angka dan simbol agar kata sandi tidat mudah ditebak [10].

He-Jun Lu dan Yang Yu, melakukan pengujian penetrasi Wi-Fi dengan menggunakan metode *penetration test* yang di bagi menjadi 4 tahapan yaitu persiapan, pengumpulan informasi, simulasi serangan dan pelaporan. Uji penetrasi yang dilakukan berupa Wi-Fi *password cracking*, dan pseudo-AP *spoofing*. Wi-fi *password cracking* yang dilakukan menggunakan serangan *brute-force* dan serangan ARP pada *client* untuk mengambil sejumlah paket data yang valid untuk dipecahkan, dan serangan ini pun berstatus berhasil. Serangan pseudo-AP, membuat adanya *access point* palsu untuk melakukan *phishing* Wi-Fi. Serangan – serangan yang dilakukan dapat mengukur tingkat keamanan yang ada, dan dijadikan sebagai acuan untuk meningkatkan sistem keamanan yang ada [11].

Renas R. Asaad, mengimplementasikan serangan pada jaringan nirkabel dengan melakukan serangan *crack password* pada kali linux dengan menggunakan teknik hashcat. Serangan *brute-force* dan *straight attack* yang dilakukan untuk mengidentifikasi kelemahan keamanan jaringan dengan menggunakan metode *penetration test*. Penelitan ini berfokus pada pembelajaran berbagai aspek pengujian *penetration* atau serangan yang dilakukan [12].

Fikriyadi, Ritzkal, Bayu Adhi Prakosa (2020), melakukan pengujian terhadap keamanan jaringan untuk melihat kualitas jaringan wireless. Metode yang digunakan adalah penetration test, metode ini dapat digunakan untuk mengevaluasi jaringan dengan mensimulasikan serangan – serangan terhadap jaringan wireless tersebut. Untuk melakukan simulasi serangan – serangan yang akan dilakukan terhadap jaringan wireless mempunyai 4 tahapan. Tahapan pertama yaitu tahap perencanaan, di mana penyerang akan menyusun perencanaan yang akan dilakukan. Tahap kedua adalah tahap penemuan, di mana penyerang akan mengumpulkan data dan informasi yang dibutuhkan dan melakukan analisis. Tahap ketiga adalah tahap serangan, penyerang akan melakukan aksi penyerangan terhadap jaringan *wireless*. Penyerang melakukan serangan – serangan meliputi *cracking the encryption*, *Bypassing MAC address*, *Attacking the Infrastructure* dan *man in the middle*. Penelitian yang dilakukan mendapatkan hasil dimana serangan – serangan yang di simulasikan berhasil dilakukan dengan status berhasil dan penggunaan *server radius* yang menggunakan otentikasi cukup aman digunakan karena hanya *user* yang terdaftar yang bisa mengakses jaringan tersebut. Serangan – serangan yang di simulasikan berhasil dilakukan dengan status berhasil [1].

B. Penetration Test (pentest)

Penetration testing merupakan upaya untuk menilai suatu kerentanan dengan melakukan eksploitasi ke dalam sistem. Uji penetrasi yang dilakukan oleh penguji diharapkan bisa untuk meniru tindakan yang dilakukan oleh penyerang. Hasil dari uji penetrasi yang dilakukan mampu membuktikan bahwa kerentanan yang ditemukan dapat menyebabkan kerusakan atau merugikan bagi orang lain dan bisa di atasi sebagaimana mestinya untuk ditangani [13]. Dalam melakukan pengujian *penetration testing* ada beberapa teknik yang dilakukan oleh penguji yaitu antara lain :

1) *Black-box test*, penguji penetrasi tidak memiliki pengetahuan sebelumnya tentang perusahaan jaringan. penguji diminta untuk mencoba meretas situs web atau jaringan seolah-olah dia adalah peretas jahat dari luar [13].
2) *White-box test,* penguji memiliki pengetahuan lengkap mengenai jaringan internal. Penguji mungkin diberikan diagram jaringan atau daftar sistem operasi dan aplikasi sebelum melakukan pengujian, meskipun bukan yang paling mewakili serangan luar, ini bisa dikatakan yang paling akurat karena menyajikan senario terburuk di mana penyerang memiliki pengetahuan lengkap mengenai jaringan [13].
3) *Grey-box test,* penguji mensimulasikan karyawan dalam. Penguji diberikan akun di jaringan internal dan akses standarke jaringan. Tes ini menilai ancaman internal dari karyawan di dalam perusahaan [13].

C. Wireless Local Area Network

Wireless local area network merupakan sistem komunikasi datanya memanfaatkan gelombang radio sebagai media tranmisi [4].

TABEL 1
802.11 IEEE

IEEE *Standard*	802.11 a	802.11 b	802.11 g	802.11 n	802.11 ac	802.11 ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5 Ghz	2.4 GHz	2.4 GHz	2.4 Ghz & 5GHz	2.4 Ghz & 5GHz	2.4 Ghz & 5GHz
Maximum Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1.3 Gbps	10-12 Gbps

The Institute of Electrical and Electronics atau sering disebut dengan IEEE telah mendefinisikan spesifikasi untuk wireless LAN, yang disebut IEEE 802.11, yang mencakup lapisan fisik dan data link. Standar arsitektur tersebut mendefinisikan dua jenis layanan yaitu *basic service set* (BSS) dan *extended service set* (ESS). Standar yang dikeluarkan oleh IEEE 802.11 untuk jaringan nirkabel, dapat dilihat pada tabel 1 [14].

Layanan *basic service set* ini bisa digambarkan sebagai blok prinsip kerja pada jaringan nirkabel LAN [14]. *Basic service set* terdiri dari beberapa piranti atau PC dan stasiun pusat atau yang biasa disebut dengan *access point* (AP). Adapun *basic service set* namun tanpa terdiri dari *access point*. Jaringan ini merupakan jaringan yang berdiri sendiri [14]. Perangkat – perangkat komputer membentuk sebuah jaringan tanpa menggunakan *access point*, jaringan ini dikenal dengan jaringan ad-hoc. *Basic service set* yang terdiri dengan *access point* biasa disebut dengan jaringan infrastruktur (*infrastructure network*). Layanan *extended service set* merupakan jaringan yang terdiri dari dua atau lebih dari beberapa *basic service set* (BSS) dengan *access point* (AP) [14]. Adapun *wireless fidelity* atau yang disingkat dengan Wi-Fi merupakan protokol jaringan nirkabel yang digunakan perangkat untuk berkomunikasi jaringan tanpa koneksi kabel (*wireless local area network* /WLAN) yang berdasarkan dari spesifikasi IEEE 802.11.

D.Keamanan Jaringan

Sistem keamanan mengarah pada perlindungan atau pertahanan yang diberikan untuk menjaga kerahasiaan, integritas dan ketersediaan layanan data dan informasi. Adapun aturan dasar yang digunakan untuk menetapkan sistem keamanan dikatakan aman, yaitu CIA *tria*d dengan kepanjangan *confidentiality*, *integrity* dan *availability* [15].

1) *Confidentiality*

Hanya orang – orang yang memiliki hak atau wewenang untuk dapat bisa mengetahui atau mengubah data dan informasi [15].

2) *Integrity* (integritas)

Terjaminnya keaslian atau keakuratan dari data dan informasi dari pemilik data dan informasi tersebut [15].

3) *Availability* (ketersediaan)

Ketersediaannya data dan informasi ketika ingin di akses oleh penggunanya [15].

Dan adapun aturan dasar pendukung lainnya antara lain yaitu :

1) Authentication

Validitas dari pengguna ketika akan mengakses suatu data dan informasi tersebut [15].

2) Akses Kontrol

Hanya orang yang benar – benar punya hak dan wewenang untuk dapat mengatur terhadap data dan informasi [15].

3) Non-Repudiation

Pencatatan pengguna agar tidak dapat melakukan penyangkalan terhadap transaksi atau aksi yang dilakukan [15].

E. Cracking The Encryption

WPA dan WPA2 merupakan protokol keamanan yang dibuat untuk mengatasi permasalahan dan kekurangan dari WEP. Penggunaan WPA dan WPA2 akan menyulitkan *hacker* dalam melakukan injeksi paket, dengan mengirimkan paket yang telah diambil sebelumnya (*replay attack*) atau serangan lain yang mengancam jaringan yang menggunakan WEP. *Hacking* terhadap jaringan yang telah menggunakan WPA atau WPA2 menjadi jauh lebih sulit dilakukan. WPA dan WPA2 bisa dijalankan dengan dua modusyaitu personal menggunakan PSK atau dengan kepanjangan *pre-shared-key* dan enterprises menggunakan *server radius*. Kemungkinan serangan *hacking* hanya bisa dilakukan pada WPA dan WPA2 PSK yang paling banyak digunakan oleh pengguna rumahan maupun perusahaan. WPA dan WPA2 PSK menggunakan *passphrase* yang harus diatur di setiap komputer seperti halnya WEP. Berbeda dengan *hacking* WEP, metode yang digunakan untuk melakukan serangan *hacking* terhadap WPA dan WPA2 tidak bisa menggunakan metode statistik. WPA dan WPA2 mempunyai IV (*initial vector*) yang dapat berubah-ubah sehingga tidak ada gunanya mengumpulkan paket data sebanyak-banyaknya seperti pada WEP untuk mendapatkan keys yang digunakan. Serangan *hacking* dengan cara ini membutuhkan waktu yang sangat lama sehingga metode yang paling memungkinkan adalah teknik *brute force* berdasarkan *dictionary file* yang dimiliki. Serangan *brute force* membutuhkan sebuah *file dictionary* yang berisi *passphrase* yang akan dicoba satu persatu kata dengan paket handshake untuk mencari *passphrase* yang digunakan pada *access point* [16].

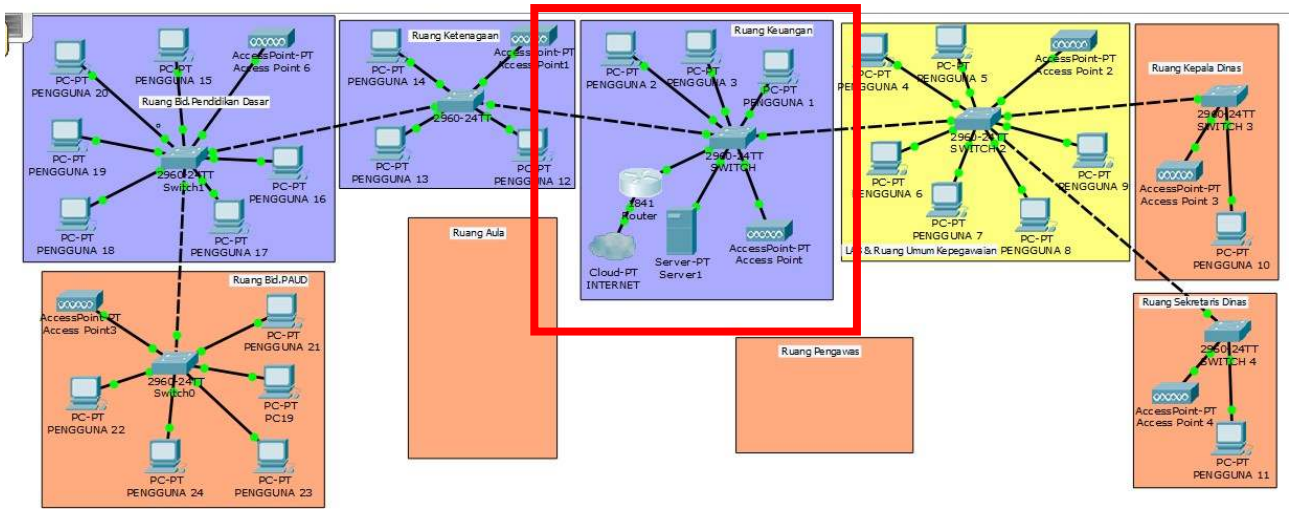
F. Denial Of Service

Dalam CIA *triad* (*confidentiality*, *integrity*, dan *availability*), serangan DoS atau *denial of service* memiliki tujuan untuk meniadakan layanan data atau informasi yang dibutuhkan oleh pengguna sehingga mengakibatkan pengguna tidak bisa mengakses data atau informasi tersebut. Serangan *denial ofservice* merupakan tindakan kejahatan di mana serangan ini membuat pengguna yang sah tidak bisa mengakses ke sistem, jaringan, perangkat lunak aplikasi, data atau informasi. Serangan *denial of service* memiliki banyak jenis tipe. Salah satu tipe dari *denial of service* adalah *deauthentication attack*. *Deauthentication attack* merupakan serangan yang melumpuhkan *access point* sehingga pengguna yang sedang terhubung ke jaringan *access point* akan dipaksa untuk terputus [17].

G.ARP Poisoining

Pada LAN, dua *host* bisa berkomunikasi jika para *host* mengetahui MAC *address* mereka , jika tidak, pesan ARP *broadcast* yang berisikan permintaan MAC *address* pada host tujuan akan dikirim ke semua *host* lain di jaringan dan ketika pesan tersebut diterima, setiap *host* yang menerima pesan akanmembalas pesan tersebut dengan pesan yang berisikan MAC *address* yang sesuai dengan permintaan. *Host* jahat dalam jaringan dapat melakukan serangan ARP *poisoning* [18].

ARP atau singkatan dari *address resolution protocol poisoning* merupakan suatu teknik serangan yang menyerang pada jaringan komputer lokal yang menggunakan media tranmisi kabel atau nirkabel. Teknik ini memungkinkan penyerang bisa mengendus *frames* data pada jaringan lokal dan bisa melakukan modifikasi *traffic* atau bahkan hingga bisamenghentikannya. ARP *poisoning* adalah konsep dari seranganpenyadapan antara dua perangkat yang sedang berkomunikasi atau biasa yang dikenal dengan MITM singkatan dari *man in the middle attack*. Prinsip serangan ARP *poisoning* merupakanmemanfaatkan kelemahan pada teknologi



Gambar 1. Topologi Jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa

jaringan komputer yang menggunakan ARP *broadcast*. ARP berada pada layer 2, pada layer 2 berisikan MAC *address*. Sebagai contoh, pengguna (PC) yang terhubung pada sebuah jaringan nirkabel ingin menghubungi pengguna lain pada jaringan nirkabel tersebut, maka dia membutuhkan informasi MAC *address* dari *host* atau pengguna tujuan [18].

II. METODE PENELITIAN

A. Topologi Jaringan Kantor Dinas Pendidikan Kabupaten Minahasa

Topologi jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa terlihat pada gambar 1. Uji penetrasi dengan menggunakan serangan *cracking the encryption*, ARP *poisoning* dan *denial of service* yang dilakukan pada Kantor Dinas Pendidikan Kabupaten Minahasa dilakukan pada ruangan keuangan.

B. Metode Penelitian

Metode penelitian yang digunakan adalah metode *penetration test*. *Penetration test* merupakan suatu kegiatan di mana seseorang mencoba untuk melakukan simulasi serangan – serangan terhadap sistem keamanan jaringan tersebut. Orang yang melakukan kegiatan ini disebut *penetration tester* [19].

III. HASIL DAN PEMBAHASAN

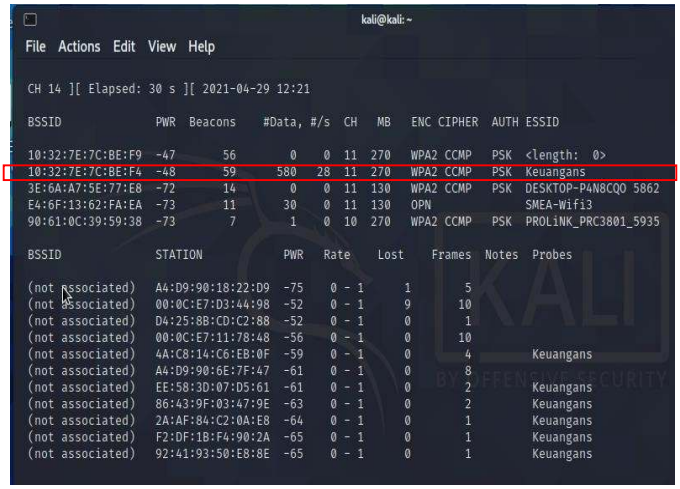
A. Serangan Cracking the Encryption

Serangan *Cracking the encryption* merupakan serangan yang bertujuan untuk mendapatkan kata sandi dari *access point* yang digunakan, sehingga bisa mengakses jaringan LAN pada Kantor Dinas Kabupaten Minahasa secara ilegal. Serangan *cracking the encryption* menggunakan teknik *brute force.* Penggunaan tools dan informasi yang dibutuhkan pada *serangan cracking the encryption* dapat dilihat pada tabel 2. Sesuai dengan informasi – informasi yang diperlukan untuk mensimulasikan serangan ini, pertama perlunya membuat *file wordlist*. Pembuatan

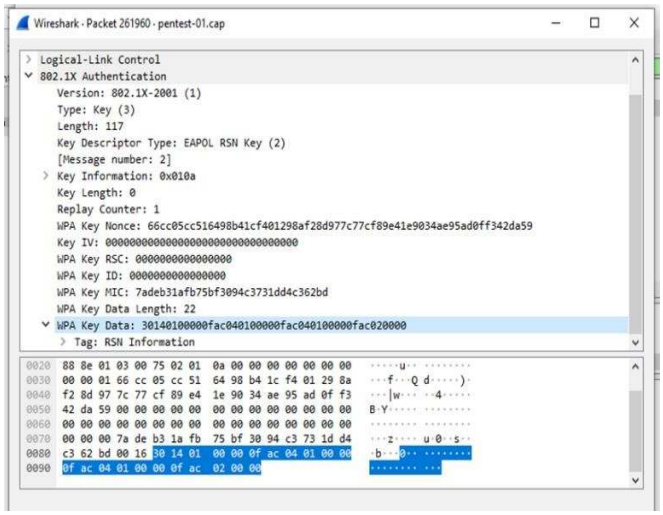
TABEL 2
CRACKING THE ENCRYPTION

Nama Serangan	*Tools*	Informasi yang Dibutuhkan
Cracking the encryption	Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng, Wireshark,	*Wordlist,* MAC *Address* dan Saluran *Access point,* WPA *handshake*

wordlist dengan menggunakan *tools crunch*. *Wordlist* ini berisikan kata – kata dengan berbagai macam kombinasi yang berkemungkinan adalah kata sandi yang digunakan pada *access point.* Kemudian akan dilanjutkan dengan mengaktifkan *monitor mode* pada *interface wireless adapter* dengan menggunakan *tools* airmon-ng. *Monitor mode* ini diaktifkan dengan tujuan untuk bisa melakukan *monitoring* lalu lintas jaringan aktif yang berada disekitar. Ketika *monitor mode* telah diaktifkan akan dilanjutkan dengan melakukan *monitoring* pada jaringan untuk menemukan jaringan *access point* yang akan dijadikan target untuk di simulasikan serangan *cracking the encryption.* Pada gambar 2 terlihat beberapa jaringan *access point* beserta jaringan *access point* yang akan dipilih untuk di simulasikan serangan *cracking the enkryption*. Jaringan *access point* yang dipilih untuk melakukan simulasi serangan *cracking the encryption* yaitu jaringan dengan ESSID Keuangans, memilikiMAC *address* 10:32:7E:7C:BE:F4, menggunakan enkripsi WPA2 dan berada pada saluran 11. Setelah itu akan dilanjutkan dengan penangkapan paket – paket data pada jaringan target yang berisikan data informasi WPA *handshake* ke dalam 1 file dengan menggunakan *tools* airodump-ng. Data informasi WPA *handshake* inilah yang memuat kunci WPA yang terenkripsi. Paket data informasi WPA *handshake* bisa didapatkan ketika ada pengguna melakukan autentikasi kembali pada jaringan nirkabel. Untuk membuat pengguna melakukan autentikasi kembali pada jaringan nirkabel, memerlukan melakukan serangan tambahan yaitu serangan deauthentication *attack* (*denial of*

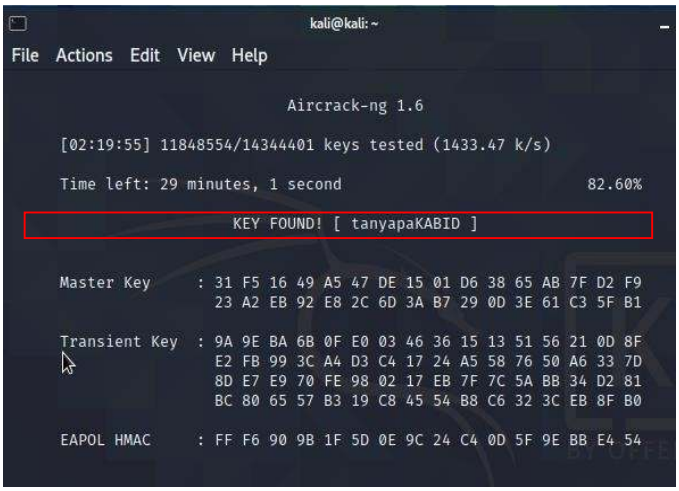


Gambar 2. Jaringan Access Point Target



Gambar 3. WPA Handshake

service) dengan menggunakan *tools* aireplay-ng. Serangan ini akan membuat pengguna dan jaringan *access point* terputus, sehingga pengguna akan melakukan autentikasi kembali pada jaringan *access point.* Salah satu pengguna yang melakukan autentikasi kembali pada jaringan adalah pengguna yang memiliki MAC *address* 6E:C4:C2:59:CE:4D. *File* paket WPA *handshake* yang ditemukan ketika pengguna melakukan autentikasi kembali akan dilihat dan dibuka dengan menggunakan *tools* wireshark untuk melihat isi paket WPA *handshake*. Pada gambar 3 terlihatisi paket *WPA handshake.* Isi paket pada bagian 802.1X *authentication,* bagian WPA *Key* Data memuat informasi kunci WPA yang terenkrip dengan kode ASCII sehingga perlu di dekripsi agar bisa memecahkan kata sandi yang digunakan padajaringan. setelah itu akan dilanjutkan dengan tahap pemecahan *passphrase* yang digunakan oleh jaringan target dengan menggunakan *tools* aircrak-ng. Diperlukan MAC *address* dari jaringan target yaitu 10:32:7E:7C:BE:F4, jaringan target di saluran 11, *file* yang berisi informasi WPA *handshake* dan *wordlist* yang berisikan kata – kata dengan berbagai macam kombinasi yang sudah



Gambar 4. Passphrase yang ditemukan

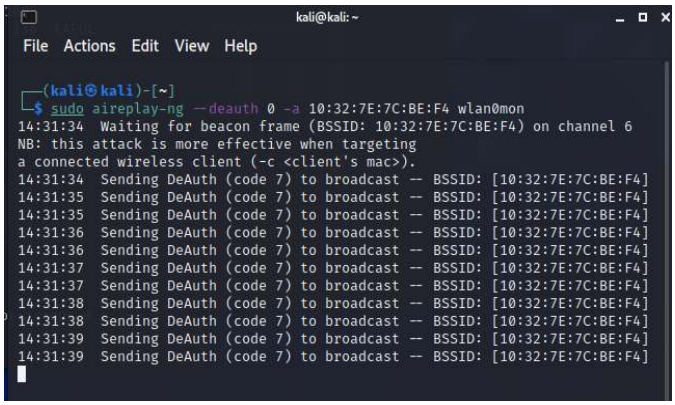
TABEL 3
DENIAL OF SERVICE

Nama Serangan	*Tools*	Informasi yang dibutuhkan
Denial of service	Airmon-ng, Airodump-ng, Aireplay-ng	MAC *Address* dan saluran *Access point*

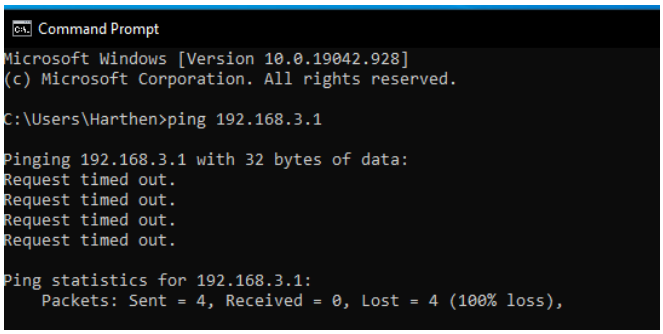
dibuat. Dalam pencarian *passphrase* yang tepat. Aircrack bekerja secara otomatis melakukan pencocokan kata per kata dengan berbagai macam kombinasi seperti angka dan simbol yang ada pada *wordlist*, sampai setiap kata per kata yang dicoba cocok dengan *passphrase* yang digunakan oleh *access point*. Pencarian *passphrase* pada jaringan *access point* target menghabiskan waktu selama 2 jam 19 menit 55 detik hingga bisa mendapatkan *passphrase* yang benar. Pada gambar 4 menampilkan *passphrase* yang ditemukan dengan menggunakan *tools* aircrack-ng. *Passphrase* yang ditemukan menggunakan *tools* aircrack-ng menggunakan 11 huruf dengan kombinasi huruf kecil dan huruf besar.

B. Serangan Denial of Service

Serangan *denial of service* bertujuan untuk meniadakan layanan jaringan sehingga membuat setiap pengguna yang berada pada jaringan terputus atau tidak bisa terhubung. Serangan ini menggunakan teknik *deauthentication*. Penggunaan *tools* dan informasi yang dibutuhkan pada serangan *denial of service* dapat dilihat pada tabel 3. Sesuai dengan informasi – informasi yang diperlukan untuk mensimulasikan serangan ini, pertama perlunya mengaktifkan *monitor mode* pada *interface wireless adapter* eksternal yang digunakan dengan menggunakan *tools* airmon-ng. *Monitor mode* ini diaktifkan untuk bisa melakukan *monitoring* lalu lintas jaringan aktif yang berada di sekitar. Setelah diaktifkan akan dilanjutkan dengan tahap *scanning*. Tahap ini untuk mencari jaringan aktif yang tersedia di sekitar dengan menggunakan *tools* airodump-ng. Setelah melakukan *scanning,* akan dilanjutkan dengan memilih jaringan *access point* yang akan di simulasikan



Gambar 5. Proses Serangan Denial of Service



Gambar 6. Koneksi Terputus

serangan *denial of service*. Dari beberapa jaringan yang ditemukan ketika melakukan *scanning*, salah satujaringan adalah jaringan dengan ESSID Keuangans. Jaringan Keuangans memiliki MAC *Address* 10:32:7E:7C:BE:F4. Jaringan inilah yang akan menjadi target untuk mensimulasikan serangan *denial of service*. Kemudian akan dilanjutkan dengan serangan *denial of service* yang dilakukan dengan menggunakan teknik *deauthentication* dengan menggunakan *tools* aireplay-ng pada jaringan *access point* yang dijadikan target yaitu jaringan *access point* dengan ESSID Keuangans. *Deauthentication* ini merupakan bagian dari *frame management* di protokol 802.11 dan dipakai untuk memutuskan asiosasi antara pengguna dan *access point*. Serangan ini akan ditujukan langsung ke *access point* sehingga mengakibatkan semua pengguna terputus koneksi pada jaringan *access point*. serangan ini akan membanjiri *access point* dengan *deauthentication frame* yang dikirimkan ke *broadcast address*dan *broadcast address* ini akan mengirimkan semua *deauthentication frame* ke semua pengguna yang sementara terhubung ke jaringan *access point* sehingga koneksi pengguna terputus. Pada gambar 5 terlihat proses serangan *denial ofservice* dengan teknik *deauthentication* menggunakan *tools* aireplay-ng. Serangan ini membuat pengguna terputus dengan jaringan *access point.* Pada gambar 6 terlihat salah satu pengguna terputus dari jaringan *access point*.

C. Serangan ARP Poisoning

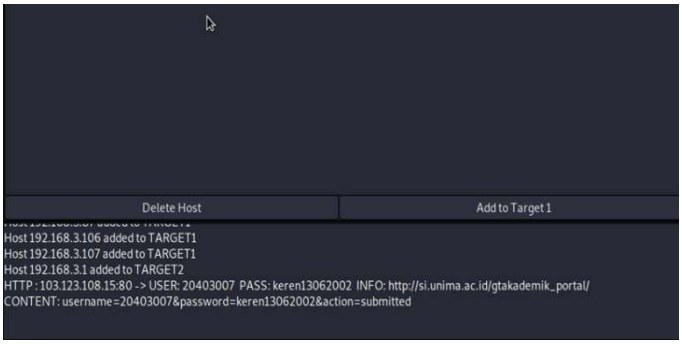
Serangan ARP *poisoning* bertujuan untuk mendapatkan informasi – informasi secara illegal dari pengguna yang sedang berada pada jaringan yang sedang di sadap. Cara kerja dari serangan ini menggunakan teknik serangan *man in the middle*.

Gambar 7. Hasil *scanning*

TABEL 4
ARP *POISONING*

Nama Serangan	*Tools*	Informasi yang dibutuhkan
ARP *Poisoning*	Ettercap, Wireshark	IP *address user,* IP *address access point*.

Penggunaan *tools* dan informasi yang dibutuhkan pada serangan *poisoning* dapat dilihat pada tabel 4. Serangan ARP *poisoning* menggunakan jaringan *access point* dengan ESSID Keuangans, memiliki MAC *address* 10:32:7E:7C:BE:F4 dan IP *address* 192.168.3.1. Untuk melakukan serangan ini penyerang perlu berada di dalam jaringan *access point.* Ketika telah berada di dalam jaringan *access point,* akan dilanjutkan ke tahap *scanning*. Pada tahap ini serangan akan dilakukan dengan menggunakan *tools* ettercap. Hasil dari *scanning* ditemukan ada 5 pengguna dengan IP address beserta MAC address yang terlihat yang sedang sementara terhubung ke jaringan *access point* tersebut, bisa dilihat pada gambar 7. Pengguna yang ditemukan antara lain MAC *address* adalah 10.32.7E.7C.BE.EB, 3C.6A.A7.SE.77.E8, F4.60.E2.36.44.B4, CO.E4.34.8A.33.1D, 3C.B6.B7.22.51.8D. 5 pengguna yang ditemukan bisa menyimpulkan bahwa *access point* tidak mengaktifkan fitur *access point isolation.* Fitur ini membuat pembatasan antara semua *user* yang berada di jaringan tersebut sehingga semua *user* tidak akan bisa berkomunikasi secara bebas antara *user* yang satu dengan *user* lainnya. Maka sebaliknya dengan tidak mengaktifkan fitur *access point isolation* membuat semua *user* yang berada dalam satu jaringan yang sama bisa berkomunikasi secara bebas tanpa dibatasi. Kemudian akan dilanjutkan dengan mensimulasikan serangan ARP *Poisoning* pada jaringan *access point* yang dijadikan target yaitu jaringan dengan ESSID Keuangans dengan menggunakan *tools* ettercap. ARP *Poisoning* bekerja dengan memanipulasi tabel ARP, dimana penyerang akan mengirimkan paket ARP palsu ke jaringan sehingga membuat isi tabel ARP akan tertimpa dengan ARP palsu yang dikirimkan oleh penyerang. Sehingga membuat semua paket akan mengarah ke perangkat penyerang. Ketika serangan ini berhasil informasi – informasi dari pengguna bisa dicuri oleh penyerang. Pada gambar 8 terlihat salah satu pengguna yang sedang megakses jaringan *access point* telah melakukan aksi login dengan menggunakan *username* dan *password*.



Gambar 8. Hasil Serangan ARP *Poisoning*

D. Result

Ketiga serangan yang di implementasikan terhadap jaringan berstatus berhasil. Hal ini dikarenakan masih begitu banyak kelemahan – kelemahan yang terdapat pada penggunaan jaringan nirkabel dan penerapan yang diterapkan pada jaringan belum efisien. Hasil dari analisa jaringan *wireless* pada Kantor Dinas Pendidikan Kabupaten Minahasa menggunakan metode *penetration test* ditampilkan dalam tabel 5.

TABEL 5
RESULT UJI PENETRASI

Jenis Serangan	Informasi Yang Dibutuhkan	Status	Keterangan
Cracking the Encryption	MAC *Address* dan Channel *access point*, WPA *Handshake*, *wordlist* dictionary	Berhasil	Berhasil mendapatkan katasandi *access point*
Denial of service	MAC *Address* dan Channel *access point*	Berhasil	Berhasil memutuskan koneksi
ARP *Poisoning*	IP *address user* dan IP *address access point*. Penyerang harus berada didalam jaringan	Berhasil	Berhasil mendapatkan datapengguna

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian analisa keamanan jaringan yang telah dilakukan pada Kantor Dinas Pendidikan Kabupaten Minahasa dengan menggunakan metode *penetration testing* dengan mensimulasikan serangan *cracking the encryption*, *denial of service* dan ARP *Poisoning* terhadap jaringan dapat ditarik kesimpulan bahwa penerapan sistem keamanan jaringan yang diterapkan oleh Kantor Dinas Pendidikan Kabupaten Minahasa masih belum sepenuhnya dikatakan aman karena serangan *cracking the encryption* yang di simulasikan berstatus berhasil. Serangan *cracking the encryption* yang dilakukan menghasilkan kata sandi yang ada pada *access point* bisa ditemukan atau dipecahkan dengan teknik *brute force* dengan menggunakan *tools* crunch, airmon-ng, airodump-ng, aireplay-ng, aircrack-ng dan wireshark. Serangan *denial of service* yang di simulasikan berstatus berhasil. Serangan *denial of service* yang dilakukan menghasilkan pengguna dan *access point* terputus sehingga pengguna tidak bisa terkoneksi dengan *access point* dengan menggunakan *tools* airmon-ng, airodump-ng dan aireplay-ng. Serangan ARP *Poisoning* berstatus berhasil. serangan ARP *poisoning* yang dilakukan menghasilkan informasi - informasi penting pengguna bisa diketahui dengan menggunakan *tools* ettercap dan wireshark.

Pada pengujian yang dilakukan terhadap jaringan berstatus berhasil di setiap serangan. Sehingga penerapan sistem keamanan jaringan pada Kantor Dinas Pendidikan Kabupaten masih perlu untuk di evaluasi dan ditingkatkan agar bisa meminimalisir terhadap upaya serangan – serangan yang bisa merugikan.

B. Saran

Adapun saran yang bisa diberikan yaitu, pada Kantor Dinas Pendidikan Kabupaten Minahasa dengansistem keamanan enkripsi pada *access point* sudah menggunakan WPA2 namun penggunaan kata sandi masih bisa di pecahkan oleh serangan *cracking the encryption* sehingga memerlukan mengganti kata sandi dengan kata yang sulit ditebak, kata yang panjang dan menggunakan kombinasi – kombinasi seperti angka dan simbol untuk lebih mempersulit pemecahan kata sandi. Perlunya mengaktifkan fitur *access point isolation* pada *access point* yang dipasang oleh Kantor Dinas Pendidikan untuk membatasi komunikasi antara para *host* di dalam satu jaringan yang sama. Mengaktifkan mode WIPS/WIDS yang ada pada *access point*. Melakukan pemantauan atau pengecekan rutin terhadap jaringan serta melakukan evaluasi atau perbaikan secara berkala pada sistem keamanan jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa.

V. KUTIPAN

[1] B. Adhi Prakosa, “Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method,” *J. Mantik*, vol. 4, no. 3, pp. 1658–1662, 2020, [Online]. Available: https://iocscience.org/ejournal/index.php/mantik.

[2] D. F. Sengkey, Widyawan, and I. W. Mustika, “Vehicle Classification in Traffic Density Estimation Using Vehicular Ad hoc Network,” *Proc. 10th Int. Forum Strateg. Technol. 2015*, pp. 387–392, 2015.

[3] A. M. Sambul, S. R. U. A. Sompie, D. F. Sengkey, A. Jacobus, and A. A. E. Sinsuw, “Ship-to-Shore Wireless Communication for Asynchronous Data Delivery to the Remote Islands,” *J. Sustain. Eng. Proc. Ser.*, vol. 1, no. 1, pp. 103–107, 2019, doi: 10.35793/joseps.v1i1.13.

[4] L. D. Samsumar, K. Gunawan, D. Program, S. Manajemen, D. Program, and S. Komputerisasi, “Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi,” *Ilm. Teknol. Inf. Terap.*, vol. IV, no. 1, pp. 73–82, 2017.

[5] Pusat Operasi Keamanan Siber Nasional, “Laporan

Tahunan Hasil Monitoring Keamanan Siber 2020," *Bul. Jendela Data dan Inf. Kesehat.*, pp. 29–33, 2020.

[6] PUSOPSKAMSINAS BSSN, "Indonesia Cyber Security Monitoring Report 2019," *Indones. Secur. Incid. Response Team Internet Infrastruct.*, p. 42, 2020, [Online]. Available: https://cloud.bssn.go.id/s/nM3mDzCkgycRx4S/download

[7] X. B. N. N. Abraham Yano Suharmanto, Arie S.M Lumenta, "Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 13, no. 3, 2018, doi: 10.35793/jti.13.3.2018.28074.

[8] S. D. S. K. Virgiawan A. Manoppo, Arie S. M. Lumenta, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[9] P. Daerah and K. Ibukota, "Dinas pendidikan," no. 3, pp. 1–7, 2016.

[10] D. M. Sari, M. Yamin, and L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing," *SemanTIK*, vol. 3, no. 2, pp. 203–208, 2017, doi: 10.1016/j.neuropharm.2007.08.010.

[11] H. J. Lu and Y. Yu, "Research on WiFi Penetration Testing with Kali Linux," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5570001.

[12] R. R. Asaad, "Penetration Testing: Wireless Network Attacks Method on Kali Linux OS," *Acad. J. Nawroz Univ.*, vol. 10, no. 1, p. 7, 2021, doi: 10.25007/ajnu.v10n1a998.

[13] L. Allen, *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide*, vol. 1. 2015.

[14] B. A. Forouzan, *Data Communications and Networking (McGraw-Hill Forouzan Networking)*. 2007.

[15] Sonny Rumalutur, "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong Sonny Rumalutur," *Tek. Elektro*, vol. 19, no. 100, pp. 48–60, 2014.

[16] 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.

[17] A. Arora, "Preventing wireless deauthentication attacks over 802.11 Networks," 2018, [Online]. Available: http://arxiv.org/abs/1901.07301.

[18] B. Prabadevi, N. Jeyanthi, and A. Abraham, "An analysis of security solutions for ARP poisoning attacks and its effects on medical computing," *Int. J. Syst. Assur. Eng. Manag.*, vol. 11, no. 1, 2020, doi: 10.1007/s13198-019-00919-1.

[19] H. D. Sabdho and M. Ulfa, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang," *Semhavok*, vol. 1, no. 1, 2018.

Astri Saraun, lahir di Tonom pada tanggal20 Juli 1999 dari pasangan Bapak Herman Frans Saraun dan Ibu Magrita Solang. Penulis merupakan anak kedua dari 3 bersaudara, yakni Diamond Saraun sebagai kakak dan Aril Saraun sebegai adik.Penulis sekarang bertempat tinggal di Kelurahan Rinegetan Kecamatan Tondano Barat Kabupaten Minahasa.

Penulis menyelesaikan Pendidikan Sekolah Dasar di SD Negeri2 Tondano pada tahun 2012, kemudian dilanjutkan pendidikandi SMP Negeri 2 Tondano lulus pada tahun 2014, dan dilanjutkan pendidikan di SMA Negeri 1 Tondano dan lulus pada tahun 2017. Setelah lulus SMA, penulis melanjutkan pendidikan di salah satu perguruan tinggi di Manado yaitu Universitas Sam Ratulangi dengan mengambil Program Studi Teknik Informatika Jurusan Teknik Elektro. Selama kuliah penulis juga tergabung dalam organisasi mahasiswa yaitu UnitPelayanan Kerohanian Kristen Fakultas Teknik (UPK Kr-FT UNSRAT), Himpunan Mahasiswa Elektro (HME), tergabung dalam anggota Unsrat IT Community (UNITY).