ANALISIS KEAMANAN JARINGAN WLAN MENGGUNAKAN METODE PENETRATION TESTING DI SMK KRISTEN GETSEMANI MANADO

Wasti[1], Peggy Veronica Togas[2], Johan Reimon Batmetan[3], Arje Cerullo Djamen[4]
[1,2,3,4]Jurusan Pendidikan Teknologi Informasi dan Komunikasi, Fakultas Teknik, Universitas Negeri Manado
e-mail: [1]19208053@gmail.com,[2]peggytogas@unima.ac.id, [3]john.reimon@unima.ac.id, [4]arjedjamen@unima.ac.id

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan jaringan WLAN yang telah diterapkan di SMK Kristen Getsemani Manado dengan menggunakan metode Penetration Testing. Dalam Analisa keamanan jaringan WLAN dilakukan dengan menggunakan metode Penetration Testing dengan mensimulasikan bentuk serangan terhadap jaringan menggunakan sistem operasi yang biasa digunakan dalam penetration yaitu Kali Linux. Berdasarkan hasil pengujian ditemukan bahwa jaringan WLAN di SMK Kristen Getsemani Manado masih memiliki kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.Dua jenis serangan yang berhasil dilakukan dalam penelitian ini adalah Analisis Lalu lintas Jaringan(Traffic Network) dan Man In The Middle Attack. Dari temuan tersebut disimpulkan bahwa Jaringan WLAN di SMK Kristen Getsemani Manado belum memberikan perilndungan yang optimal bagi pengguna yang terhubung, sehingga masih memungkinkan terjadinya gangguan saat mengakses layanan internet.

Kata kunci: *penetration testing, WLAN, Kali Linux.*

ABSTRACT

This study aims to broadcast the level of WLAN network security that has been implemented at SMK Kristen Getsemani Manado using the Penetration Testing method. In the WLAN network security analysis is carried out using the Penetration Testing method with a copy of the form of attack on the network using the operating system commonly used in penetration, namely Kali Linux. Based on the test results, it was found that the WLAN network at SMK Kristen Getsemani Manado still has vulnerabilities that can be exploited by irresponsible parties. Two types of attacks that were successfully carried out in this study were Network Traffic Analysis and Man In The Middle Attack. From these findings, it is concluded that the WLAN Network at SMK Kristen Getsemani Manado has not provided optimal protection for connected users, so it is still possible for disruptions to occur when accessing internet services.

Kata kunci: *penetration testing, WLAN, Kali Linux.*

PENDAHULUAN

Teknologi informasi dan komunikasi adalah hal yang tidak terpisahkan dari kehidupan manusia diera yang semakin berkembang seperti sekarang ini. Salah satu contoh dari kemajuan teknologi informasi dan komunikasi yaitu adanya *Wireless Local Area Network* (WLAN) yang disebut juga teknologi jaringan lokal nirkabel (Bayu dkk, 2017). Sebuah jaringan tidak akan lepas dari ancaman berupa serangan yang berbahaya, yang dapat merugikan pemilik sistem,untuk itu keamanan jaringan perlu diperhatikan. Keamanan jaringan adalah salah satu hal terpenting dalam implementasi jaringan komputer. Banyak jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Dikarenakan kelalaian tersebut, dapat memberi peluang bagi para hacker untuk meretas dan merusak jaringan yang dibangun tersebut (Amarudin & Faruk, 2018). WLAN(*Wireless Lokal Area Network*) adalah teknologi jaringan yang tidak menggunakan kabel sebagai media pengantar (*transmisi)* data yang umum dijumpai di dalam sebuah jaringan komputer , teknologi ini sesuai dengan namanya *wireless* yang artinya jaringan tanpa kabel,memanfaatkan gelombang radio untuk melakukan komunikasi antar unit komputer (Supriadi dkk, 2018). Keamanan jaringan nirkabel lebih rentan ketimbang jaringan yang menggunakan kabel.Salah satu penyebabnya adalah karena pengguna umum dapat terhubung dengan jaringan WLAN sehingga tentunya masalah keamanan jaringan perlu diperhatikan, apalagi disebuah lembaga yang peduli dengan keamanan data.Keamanan jaringan harus di tingkatkan agar meminimalisir ancaman yang bisa saja terjadi.

SMK Kristen Getsemani Manado adalah salah satu sekolah yang terletak di kota Manado yang menggunakan Jaringan WLAN sebagai fasilitas dalam proses belajar mengajar.Dari hasil observasi dan wawancara yang dilakukan, sebagian perangkat jaringan belum memadai yang dapat menyebabkan bottleneck, memperlambat kinerja jaringan dan mengganggu layanan. Selain itu, tanpa perangkat yang tepat, akan sangat sulit untuk memantau atau mendeteksi aktivitas mencurigakan dalam jaringan. Selain perangkat jaringan yang tidak lengkap, jaringan di SMK Kristen Getsemani Manado juga tidak ada firewall yang digunakan sehingga sangat rentan terhadap serangan dari luar, termasuk malware dan peretas..Serta pengguna luar dapat mengakses jaringan WLAN dengan meminta password wifi kepada siswa yang ada di sekolah,yang bisa saja mengakibatkan pengguna yang tidak berwenang dapat mencuri data sensitif dan menggunakan data tersebut untuk hal-hal yang tidak baik, seperti informasi pribadi atau kredensial. Serta kemungkinan pengguna luar dapat meluncurkan serangan yang dapat mengganggu layanan jaringan,serta dapat menyebarkan malware ke perangkat yang terhubung di jaringan, dan akibat fatal yang bisa terjadi adalah kerusakan sistem. Untuk itu, peneliti akan melakukan pengujian terhadap jaringan WLAN di SMK Kristen Getsemani Manado untuk mengetahui seberapa kuat keamanan jaringan yang diterapkan untuk bisa mencegah terjadinya kemungkinan serangan siber yang tidak di inginkan, dengan menggunakan metode Penetration Testing. Penelitian ini bertujuan untuk mengevaluasi tingkat kerentanan keamanan jaringan WLAN terhadap potensi serangan dengan memakai metode *penetration testing* agar bisa dimanfaatkan sebagai referensi

ISSN 2798-141X

untuk meningkatkan sistem keamanan jaringan WLAN di SMK Kristen Getsemani Manado agar tidak terjadi hal-hal yang dapat merugikan.

KAJIAN TEORI

Jaringan Komputer

Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi adalah mencakup semua jenis perangkat komputer (komputer desktop, komputer jinjing, *smartphone*, PC tablet dan perangkat penghubung (*router, switch, modem, hub*) (Hafiz & Iin, 2021).

Jaringan WLAN

Jaringan tanpa kabel (*wireless*) atau jaringan nirkabel merupakan suatu jalan keluar terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Pada saat ini jaringan nirkabel atau *wireless* sudah banyak digunakan dengan memanfaatkan jasa satelit dan bahkan mampu memberi kecepatan dan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel (Parenreg, 2022).

Keamanan Jaringan WLAN

Wireless LAN menggunakan teknologi *Radio Frequency* (RF) untuk mentransmisikan data. Jauh lebih sulit untuk menjamin keamanan dalam sistem jaringan *wireless* daripada jaringan kabel, karena media yang digunakan adalah udara. Dalam jaringan kabel, pengguna harus terhubung langsung melalui kabel kedalam jaringan LAN. Sedangkan *Wireless LAN* bisa diakses diamanapun perangkat wireless diletakkan selama masih dalam jangkauan *wireless.*Kelemahan pada jaringan *wireless* secara umum dapat dibagi menjadi dua jenis, yaitu kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Contoh penyebab kelemahan pada konfgurasi adalah banyak yang membangun jaringan *wireless* menggunakan konfigurasi *wireless default* bawaan vendor (Darmadi, 2018).

Protocol Wireless Protected Access (WPA)

Wi-fi Protected Access (WPA) yang juga dikenal sebagai WEP versi 2 (WEPv2), yang diperkenalkan pada bulan April 2003. WPA dikembangkan sebagai peningkatan dari WEP, jadi bukan sebagai sistem keamanan yang baru.Oleh karena, kelemahan yang ada pada WEP masih tetap ditemukan pada WPA, karena metode enkripsi yang digunakan tetap menggunakan RC4.Konfigurasi keamanan pada WPA tergoong sederhana karena hanya perlu memilih opsi WPA pada perangkat klien maupun pada *Access point* (Putra, 2021).

Router

Router merupakan perangkat keras jaringan komputer yang dapat digunakan untuk menghubungkan beberapa jaringan yang sama atau berbeda. Router ialah sebuah alat untuk jaringan atau internet untuk dapat menuju tujuannya, proses tersebut

ISSN 2798-141X

dinamakan *routing*. Fungsi utama router yaitu untuk membagi atau mendistribusikan *IP Address*, baik itu secara Statis ataupun DHCP kepada semua komputer yang terhubung ke router tersebut (Gunawan & Deny, 2020).

Penetration Testing

Penetration Testing merupakan sub kategori dalam *Ethical Hacking* yang merupakan salah satu langkah yang berfungsi dalam memeriksa atau menaungi keamanan informasi. *Penetration testing* adalah kegiatan menilai *security system* yang telah dibuat dengan menggunakan tiruan serangan yang seringkali dimanfaatkan bagi peretas (Prasetyo & Try, 2022).

Web Proxy

Proxy merupakan aplikasi perantara antara *client* dan *server*, sehingga *client* tidak akan berhubungan langsung dengan server. *Web proxy* akan membuat *HTTP reques*t ke *web server* di internet atas permintaan dari komputer *user*. Sehingga *web server* akan mengetahui bahwa yang melakukan *request* adalah *proxy server* dan bukan komputer *use*r (Irawan dkk, 2018).

Virtual Private Network

VPN adalah sebuah teknologi komunikasi yang memungkinkan dapat dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan local. Koneksi VPN dalam bentuk *virtual* (maya) dan bersifat *private* (rahasia), sehingga hanya *user* tertentu saja yang bisa mengaksesnya (Musril, 2019). Prinsip kerja VPN:

1. Komponen utamanya adalah *VPN server*.
2. *VPN client* akan mengirim pesan ke *server VPN*.
3. Untuk proses login, *VPN server* memeriksa akun *client*.
4. Komputer *clien*t dapat digunakan mengakses berbagai *resourc*e di *VPN server*.

Wireshark

Wireshark adalah program penganalisa jaringan yang sangat populer, walaupun program ini kebanyakan dikenal bukan karena fungsi utamanya,melainkan karena sering digunakan untuk keperluan *hacking* pemula. Dengan kata lain bahwa *Wireshark* adalah program *Network Protocol Analyzer* atau penganalisa protokol jaringan yang lengkap. Program ini dapat merekam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar di blog bahkan *username* dan *password* (Amarudin & Sampurna, 2019).

Kali Linux

Kali Linux merupakan *operating system* berbasis linux debian yang dikembangkan oleh *offensive Security*. *User interface* dari Kali Linux memiliki tampilan *graphical user interface (GUI)* yang sederhana dan tidak terlalu mencolok. Kali Linux adalah salah satu distribusi Linux tingkat lanjut untuk melakukan *penetration testing* dan audit keamanan (Adiguna & Bambang 2022).

ISSN 2798-141X

METODE PENELITIAN

Penelitian ini dilaksanakan di SMK Kristen Getsemani Manado yang meliputi beberapa tahapan, dari tahap perencanaan sampai selesai. Dalam analisis keamanan jaringan WLAN menggunakan metode penetration testing di SMK Kristen Getsemani Manado ini, memerlukan kebutuhan perangkat keras dan perangkat lunak. Kebutuhan perangkat keras yaitu laptop dengan spesifikasi tertentu, yaitu: *Procecor intel Celeron* N4000, 2.6Ghz, RAM 4GB, HDD 250GB. Sedangkan perangkat lunak menggunakan system operasi Windows untuk mengelolah fungsi dasar komputer, Aplikasi wireshark yang digunakan untuk menganalisis dan mengidentifikasi gangguan jaringan, dan Kali linux yang digunakan untuk melakukan pengujian keamanan dengan metode penetrasi pada jaringan.

Metode Penetration Testing

Penelitian ini dilakukan dengan menggunakan metode Penetration Testing, dimana akan melakukan pengujian terhadap keamanan jaringan WLAN untuk mengetahui celah atau kerentanan jaringan tersebut. Dalam proses pengujian, penetration testing dilakukan melalui empat tahapan yaitu: Tahap perencanaan (*Planning),* Penemuan *(Discovery),* Serangan (*Attack*) dan Pelaporan (*Reporting).*

1. *Planning* (Perencanaan)

   Pada fase ini tim pentester harus memahami tujuan pengujian,lingkup sistem yang akan di uji dan mencakup koordinasi dengan pemilik sistem untuk memastikan bahwa pengujian tidak mengganggu operasional sehari-hari.

   Jelaskan langkah penelitian secara singkat tetapi jelas sehingga memungkinkan penelitian lain untuk melakukan kembali dengan hasil yang sama
2. *Discovery* (Penemuan)

   Pada fase ini tim pentester akan mengumpulkan informasi tentang target yang akan diuji, ini mencakup informasi tentang sistem,jaringan,alamat IP,dan domain yang terkait.
3. *Attack* (Serangan)

   Pada fase ini pentester melakukan Vulnerability Detection untuk mencari celah keamanan jaringan dan melakukan serangan terhadap sistem dengan memanfaatkan celah keamanan untuk mendapatkan akses kedalam sistem atau jaringan tersebut. Jenis serangan yang akan digunakan daam pengujian ini meiputi: Analisis lalulintas jaringan(*Traffic Network*), dan serangan *Man in the Middle* (MitM).
4. *Reporting* (Pelaporan)

   Pada fase ini pentester akan mengumpulkan semua temuan dan bukti dari pengujian dan menyusun laporan yang merinci kerentanan yang ditemukan,tingkat resiko,dan rekomendasi untuk perbaikan. Dan kemudian laporan ini disampaikan kepada pemilik sistem untuk tindakan lebih lanjut.

ISSN 2798-141X

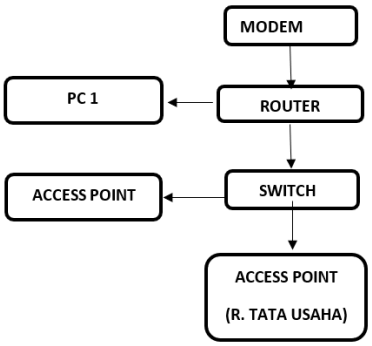
HASIL DAN PEMBAHASAN

Planning

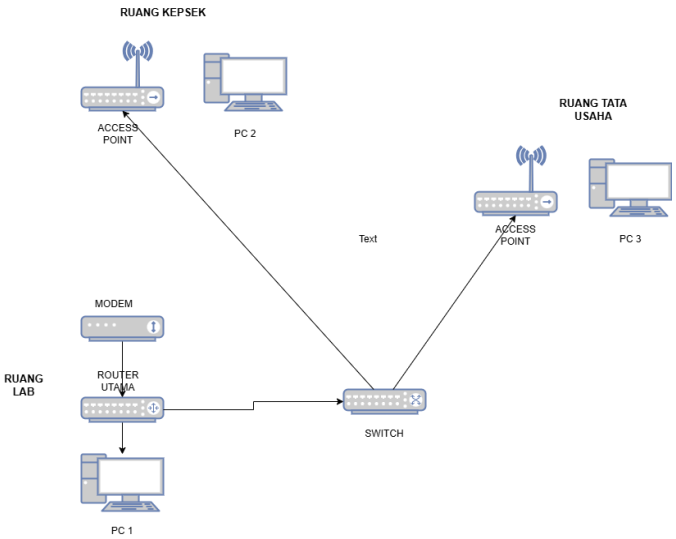
Tahap pertama dalam penelitian ini adalah melakukan Planning(perencanaan) dari metode Penetration Testing yang di terapkan dalam penelitian ini. Tujuan melakukan Planning yaitu untuk memahami lingkup sistem jaringan di SMK Kristen Getsemani Manado dan mencakup koordinasi dengan kepala sekolah dan pihak administrator jaringan untuk melakukan pengujian terhadap jaringan WLAN dan memastikan tidak mengganggu operasional sehari-hari.

Discovery

Pada tahap ini pentester akan mengumpulkan informasi tentang target yang akan di uji yang mencakup sistem jaringan, alamat IP dan domain yang terkait yang ada di SMK Kristen Getsemani Manado. Hasil dari tahapan ini yaitu Anaisa bog diagram jaringan seperti pada gambar 1 dan topoogi jaringan yang digunakan yang terihat pada gambar 2.



Gambar 1. Blok Diagram Jaringan



Gambar 2. Topologi Jaringan SMK Kristen Getsemani Manado

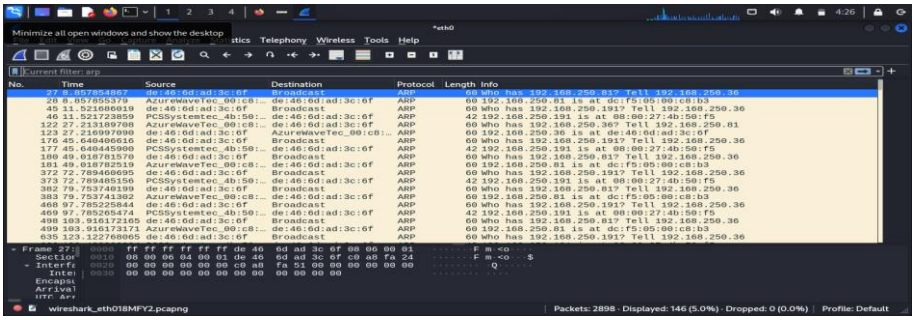
ISSN 2798-141X

Attack (Serangan)

Pada tahap ini yang dilakukan adalah melakukan serangan terhadap jaringan WLAN dengan menggunakan tools yang ada di Kali Linux. Jenis serangan yang akan di lakukan pada jaringan meliputi analisis lalu lintas jaringan menggunakan aplikasi *Wireshark* serta serangan *Man in the Middle Attack* menggunakan Ettercap.

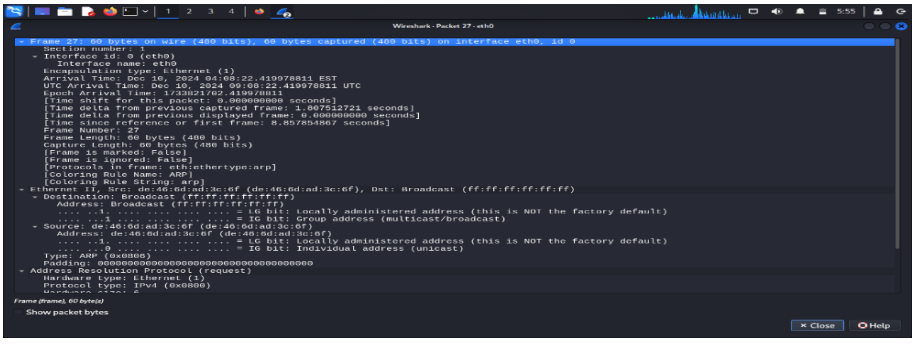
1. Analisis Lalulintas Jaringan

Pada tahap ini pentester akan melakukan pemantauan daftar paket *(packet list)*, yang mencakup alamat IP sumber (*source IP*) dan IP tujuan (*IP destination*) dengan merekam serta mengamati aktivitas jaringan melaui antarmuka nirkabel (*Wireless Interface)* pada modem diruang lab dengan menggunakan apikasi *Wireshark.* Melalui proses penangkapan paket (*capture packet)* ini, dapat diperoleh berbagai informasi seperti *time,source, destination, protocol, length dan info*. Hasil tangkapan paket dapat dilihat pada gambar 3.



Gambar 3. Hasi Pengambilan Paket

Seperti yang ditunjukkan pada gambar 3, peneliti melakukan pengambilan sampe paket data untuk di analisis. Tujuannya adalah untuk mengetahui waktu pengiriman (*time),*alamat IP sumber (*source),* alamat IP tujuan (*destination),* jenis protocol yang digunakan (*protocol),*ukuran data *(length),* serta detail informasi pada masing-masing alamat IP. Analisis yang pertama adalah tentang informasi lalu lintas jaringan yang mnggunakan protokol ARP seperti yang terlihat pada gambar 4.

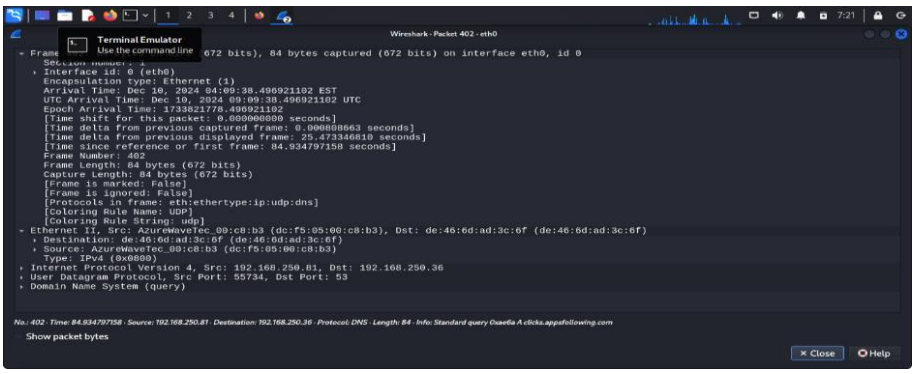


Gambar 4. Detail Paket Protokol ARP

Dari gambar 4, dapat ditemukan bahwa jenis protokol ARP yang diterapkan adalah menggunakan tipe enkapsuasi *Ethernet* 1 dan dijalankan melalui interface bernama eth0.

ISSN 2798-141X

Paket data diterima pada tanggal 10 Desember 2024 pada jam 09:08.22, yang menunjukkan waktu pengiriman informasi. Identitas pengirim dan penerima permintaan ARP dapat diketahui melalui alamat *IP Address* serta *Mac Address* yang tercantum dalam protokol tersebut.Ketika dilakukan pengujian untuk menganalisis protocol ARP, pentester ternyata bisa mengakses dan menganalisis protocol ARP. Jika orang yang tidak bertanggung jawab dapat mengaskses jaringan dan memindainya secara menyeluruh, maka informasi mengenai alamat IP dapat di ekstraksi dan mereka dapat melakukan serangan ARP Spoofing yang dapat membahayakan jaringan. Analisis kedua adalah untuk mengetahui informasi lalu lintas jaringan pada protokol DNS yang dapat dilihat pada gambar 5.



Gambar 5. Detail Protokol DNS

Berdasarkan gambar 5, dapat ditemukan bahwa protokol DNS yang dianalisa menggunakan tipe enkapulasi *Ethernet* 1 dan nama antarmuka adalah eth0. 10 Desember 2024 jam 09:09.38, menunjukkan waktu saat data dikirimkan. Melaui protokol DNS (*Domain Name System*) ini, dapat diketahui bahwa situs web yang diakses adalah *clicks.appsfollowing.com*. Dengan adanya informasi yang menyangkut IP dari pengirim dan tujuan,pihak ketiga dapat memanfaatkan untuk memperoeh informasi lebih detail yang memiliki alamat IP tersebut.

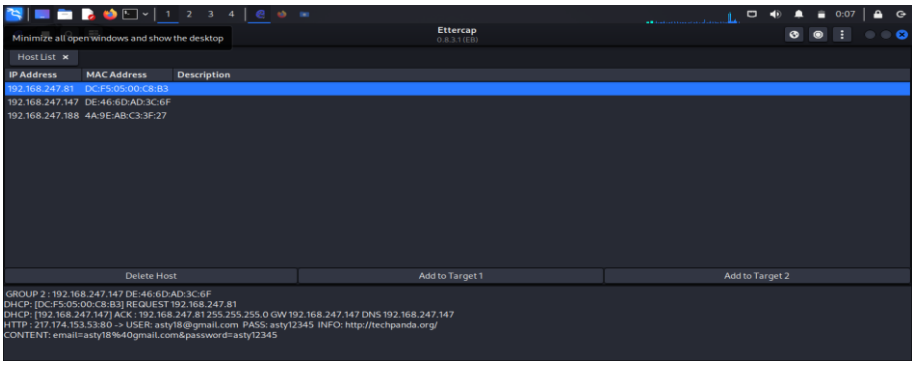
Jika orang yang tidak bertanggung jawab dapat mengaskses jaringan dan memindainya secara menyeluruh, maka informasi mengenai alamat IP dapat di ekstraksi dan mereka dapat melakukan serangan ARP Spoofing yang dapat membahayakan jaringan. ARP Spoofing adalah serangan yang diakukann untuk memecahkan kode pertukaran informasi yang terjadi di seuruh jaringan dan diantara perangkat. ARP Spoofing dapat membantu penyerang menyebabkan kerusakan parah pada jaringan.Untuk mengurangi resiko serangan tersebut, maka hal yang perlu dilakukan adalah menggunakan VPN karena teknologi ini dapat membuat alamat IP tersembunyi dari semua orang, menggunakan ARP statis, mengaktifkan keamanan port pada switch dan lain-lain.

2. Man In The Middle Attack

Pada tahap ini dilakukan serangan terhadap pengguna lain yang berada dalam jaringan *Wireless LAN* yang sama dengan cara menyadap paket data. Pengujian ini memanfaatkan

ISSN 2798-141X

aplikasi *Ettercap* sebagai alat bantu.Untuk menjalankan serangan *Man In The Middle Attack* (MITM), kondisi awal yang diperlukan adalah komputer penyerang dan komputer target harus berada dijaringan *Wireless Access Point* yang sama diruang Lab komputer. Daam kondisi ini, komputer penyerang bertindak sebagai perantara atau pihak ketiga yang berada diantara perangkat target dan *Access point* yang terhubung dalam jaringan internet. Tahap yang dilakukan selanjutnya adalah melakukan *ARP Poisoning* untuk menyadap komunikasi antara target 1 dan target 2. ARP Poisoning adalah metode serangan dalam jaringan komputer lokal baik melalui media kabel maupun nirkabe (*Wireless)*, yang memungkinkan penyerang untuk mengintip (sniffing),memodifikasi, atau bahkan menghentikan lalu lintas data dalam jaringan tersebut. Serangan *ARP Poisoning* ini memanfaatkan kelemahan pada sistem jaringan yang menggunakan *ARP Broadcast* sebagai bagian dari proses komunikasi antar perangkat. Setelah serangan ARP Poisoning berhasil dilakukan, proses *sniffing* akan dijalankan, untuk merekam seluruh aktivitas komputer target saat mengakses layanan internet. Berdasarkan gambar 6, hasil percobaan proses *snifiing* menunjukkan bahwa komputer target mengunjungi situs http://techpanda.org/ dan meakukan login menggunakan user asty18@gmail.com serta *password* asty12345.



Gambar 6. Hasil Sniffing

Reporting (Pelaporan)

Berikut adalah hasil pengujian terhadap jaringan *Wireless Local Area Network* di SMK Kristen Getsemani Manado menggunakan metode Penetration testing dengan dua jenis serangan, yaitu analisis lalu lintas jaringan (*Traffic Network)* dan serangan *Man In The Middle Attack* seperti yang dapat dilihat di tabel 1.

Tabel 1. Hasil Pengujian

No	Jenis serangan	Informasi yang dibutuhkan	Status serangan
1	Analisis lalu lintas jaringan (*Traffic Network*) menggunakan Wireshark	Ip source dan IP Destination	Berhasil
2	*Man In The Middle Attack*	Attacker harus terhubung ke jaringan WLAN, IP Address dari user yang terkoneksi	Berhasil

ISSN 2798-141X

KESIMPULAN

Setelah dilakukan pengujian Analisis keamanan pada Jaringan *Wireless Local Area Network* (WLAN) menggunakan Metode *Penetration Testing* dengan sistem operasi Kali Linux di SMK Kristen Getsemani Manado dapat disimpulkan bahwa keamanan jaringan WLAN di SMK Kristen Getsemani manado tergolong sangat rentan dan sangat perlu untuk ditingkatkan. Kerentanan tersebut dapat di lihat dari hasil pengujian yang di lakukan pada tahap attack yaitu pada proses Analisis Lalu lintas Jaringan (*Traffic Network*) dengan aplikasi *Wireshark*, ditemukan adanya aktivitas komunikasi data melalui *protocol* ARP dan DNS. Dari analisis ini diperoleh informasi penting seperti lamat IP,waktu,sumber, tujuan, protocol,panjang data dan Informasi lainnya. Dengan adanya informasi yang menyangkut IP dari pengirim dan tujuan,bisa berpotensi dimanfaatkan oleh pihak ketiga untuk mengakses atau menggali informasi lebih dalam dari perangkat pemilik IP tersebut. Dan pengujian *Man In The Middle Attack* ditemukan bahwa tingkat keamanan jaringan masih rentan, dimana *user* yang terkoneksi bisa mendapatkan gangguan berupa penyadapan dari *use*r lain saat mengakses layanan internet yang sama. Untuk itu,pihak sekolah dapat memanfaatkan hasil penelitian sebagai referensi untuk meningkatkan sistem keamanan jaringan WLAN di SMK Kristen Getsemani Manado.

DAFTAR PUSTAKA

Adiguna, M. A., & Bambang,W.W. (2022). Analisis Keamanan Jaringan Wpa2 Psk Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r). *Jurnal Sistem Komputer dan Kecerdasan Buatan*, 5 (2), 1-8.

Amarudin & Faruk U. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal TEKNOINFO*, 12(2):72-75.

Amarudin & Sampurna D.R. (2019). Analisis Dan Desain Jalur Transimisi Jaringan Alternatif Menggunakan Virtual Private Network (VPN). *Jurnal TEKNOINFO*, 13(2),100-106.

Bayu, I. K., M. Yamin, & LM F. A. (2017). Analisa Keamanan Jaringan WLAN Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi Dan Programing Teknik Informatika UHO). *SemanTIK*, 3(2),69-78.

Darmadi, E.A.2018. Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless Untuk Meningkatkan Keamanan Jaringan Komputer.*Jurnal IKRA-ITH Informatika*,2 (3), 9-16.

Gunawan, T., & D. F. Kurniawan, 2020. Rancang Bangun Jaringan Wireless Local Area Network (WLAN) Menggunakan Metode Penetration Routing Statik Pada SMPN 7 Pesawaran. *Jurnal Informatika software dan Network*,1(1),41-47.

Hafiz, A., & Iin, K. (2021). Mengembangkan Jaringan Wireless Local Area Network (WLAN) Dan Hotspot Pada Amik Dian Cipta Cendekia (DCC) Pringsewu Menggunakan Router Mikrotik. *Jurnal Informatika software dan Network*,2(1),15-22.

ISSN 2798-141X

Irawan, H. T., M. Djaohar, & M. Ficky, D. (2018). Perancangan Dan Implementasi Sistem Kemanan Jaringan Menggunakan Firewall Dan Web Proxy Berbasis Mikrotik Di SMA Negeri 1 Kota Sukabumi. *Jurnal PINTER*, 2(1), 27-32.

Musril, H. A. (2019). Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF). *Jurnal Nasional dan Teknologi Jaringan*, 3 (2),83-88.

Parenreng, J. M., Wahid, A., Sanatang, S. P., & Yusmalasari, A. (2022). *Pengantar Jaringan Komunikasi Nirkabel*. Zahira Media Publisher.

Prasetyo, S.E., & Try, W. (2022). Perbandingan Sistem Autentikasi WPA2 EAP-PSK Pada Jaringan Wireless Dengan Metode Penetration Testing Menggunakan Fluxion Tools. *Jurnal Teknologi dan Sistem Informasi Univrab*,7(1),43-51.

Putra, A. A. (2021, July). Analisis Dan Evaluasi Keamanan Wireless Lan Pada Pt. Bumi Jage Dalam. In *Seminar Nasional Ilmu Komputer (SNASIKOM)* (Vol. 1, No. 1, pp. 138-150).

Supriadi, D., Hairul F., & Khairul I. (2018). Analisis Dan Perancangan Infrastruktur Jaringan Wireless Local Arean Network (WLAN) Pada Dinas Perindustrian Dan Perdagangan Kabupaten Lombok Tengah. *Jurnal Informatika &Rekayasa Elektronika*,1(2), 1-6.

ISSN 2798-141X