PROSIDING

ISSN : 2654 - 5438

Palembang, 19 September 2018

Seminar Hasil Penelitian Vokasi

SEMHAVOK

PERAN STRATEGIS PENDIDIKAN VOKASI DALAM MENGHADAPI REVOLUSI INDUSTRI 4.0

Universitas Bina Darma

UNIVERSITAS BINADARMA
Jln. Jendral A. Yani No. 03 Palembang
Sumatera Selatan
Telp. 0711-515582, www.binadarma.ac.id

ANALISIS KEAMANAN JARINGAN *WIRELESS* MENGGUNAKAN METODE *PENETRATION TESTING* PADA KANTOR PT. MORA TELEMATIKA INDONESIA REGIONAL PALEMBANG

[1]Harry Dwi Sabdho, [2]Maria Ulfa
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, harrydwi79@gmail.com
[2]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, mariakurniawan2009@gmail.com

Abstract **-** *Information and communication technology is something that is difficult to separate from human life in the present era. One example of information and communication technology is Wireless Local Area Network (WLAN) or also called wireless local network technology. This study uses Penetration Testing method, which aims to analyze the security system of WLAN technology that has been applied in PT. Mora Telamatika Indonesia. Penetration testing is a series of activities carried out to identify and exploit security vulnerabilities. In analyzing the security of WLAN networks is done by the Penetration Testing method where the form of attacks on the network is simulated, one operating system that has the right specifications in that case is Kali Linux. Wireless networks are networks that are widely used in institutions and public places. Despite having a security system, the wireless network can still be attacked by attackers.*

Keywords: *Penetration Testing, Wireless LAN, Kali Linux*

Abstrak - Teknologi informasi dan komunikasi merupakan hal yang sulit terpisahkan dari kehidupan manusia di era sekarang ini. Salah satu contoh teknologi informasi dan komunikasi tersebut adalah *Wireless Local Area Network* (WLAN) atau disebut juga teknologi jaringan lokal nirkabel. Penelitian ini menggunakan metode *Penetration Testing*, yang bertujuan melakukan analisis terhadap sistem keamanan teknologi WLAN yang sudah diterapkan di PT. Mora Telamatika Indonesia. Uji penetrasi adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan. Dalam menganalisa keamanan jaringan WLAN dilakukan dengan metode *Penetration Testing* dimana bentuk serangan terhadap jaringan disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux. Jaringan *wireless* merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum. Walaupun memiliki sitem keamanan, jaringan *wireless* masih dapat di diserang oleh para *attacker*.

Kata kunci: *Penetration Testing, Wireless LAN,* Kali Linux

1. Pendahuluan

Perkembangan teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi media transmisi nirkabel atau *wireless*. Mudahnya pengguna umum terhubung dengan jaringan *wireless* tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data. Jaringan *wireless* menggunakan gelombang radio sebagai media transmisi sehingga jaringan akan lebih mudah dimasuki oleh penyusup dan serangan yang berasal dari semua arah [1].

Pada jaringan yang diakses secara bersama seperti jaringan *hotspot* memiliki gangguan terhadap sistem sehingga perlu dilakukan aturan terhadap sistem jaringan. Beberapa aturan diberlakukan untuk mengontrol kinerja maupun kondisi jaringan sehingga sistem berjalan sesuai

dengan yang diharapkan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan analisa terhadap sistem keamanan yang ada dalam jaringan tersebut.

PT. Mora Telematika Indonesia Regional Palembang, merupakan penyedia jasa jaringan interkoneksi domestik maupun internasional, penyedia Jasa *Internet* (*internet Services)* serta penyedia Pusat Data *(Data Center)*. Maka jaringan *wireless* sangat berperan penting dalam PT Mora Telematika Indoesia ini. PT. Mora Telematika Indonesia menerapkan sistem operasi yang canggih yaitu *MikrotikOS*. Sitem keamanan jaringan *wireless* yang digunakan PT. Mora Telematika Indonesia yaitu WPA2. Tingkat keamanan menentukan kesulitan untuk masuk dalam jaringan *wireless* tersebut.

2. Tinjauan Pustaka

2.2 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut peladen (*server*). Desain ini disebut dengan sistem *client-server,* dan digunakan pada hampir seluruh aplikasi jaringan komputer [2].

2.2 Analisis

Analisa adalah suatu cara membagi-bagi suatu objek kedalam komponen-komponen yang berarti melepaskan, menanggalkan, menguraikan sesuatu yang terikat padu, sesuai dengan sifat komponen analisa dibagi menjadi analisa bagian, analisa fungsional, analisa proses. (*Rahayu, 2001*). Salah satu metode analisa yang dijadikan acuan peneliti yaitu "Domain informasi suatu masalah harus dipahami dan proses analisa harus bergerak dari informasi dasar ke detail implementasi"[3].

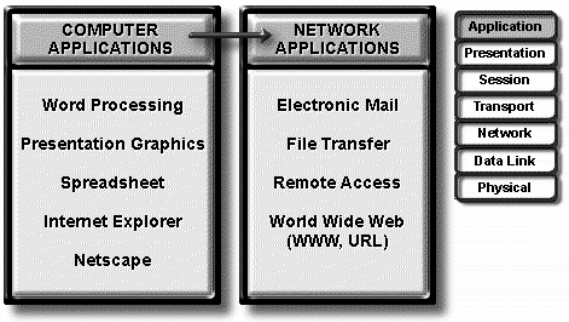
2.3 OSI Layer

OSI Layer adalah salah satu dari arsitektur jaringan. OSI layer sendiri sering digunakan untuk menjelaskan cara kerja jaringan komputer secara logika. Secara umum model OSI membagi berbagai fungsi *network* menjadi 7 lapisan sedangkan lembaga yang mempublikasikan model OSI adalah International Organization for Standardization (ISO). Model OSI diperkenalkan pada tahun 1984. Model OSI terdiri atas layer-layer atau lapisan-lapisan berjumlah 7 buah. Ketujuh layer tersebut yaitu :

1. Layer Aplikasi (*Application Layer)*

Pada layer ini berurusan dengan program komputer yang digunakan oleh *user*. Program komputer yang berhubungan hanya program yang melakukan akses jaringan, tetapi bila yang tidak berarti tidak berhubungan dengan OSI.

Contoh: *Aplikasi Word Processing*, aplikasi ini digunakan untuk pengolahan teks sehingga program ini tidak berhubungan dengan OSI. Tetapi bila program tersebut ditambahkan fungsi jaringan misal pengiriman *email,* maka aplikasi *layer* baru berhubungan disini. Sehingga bila digambar dapat digambar seperti Gambar 1

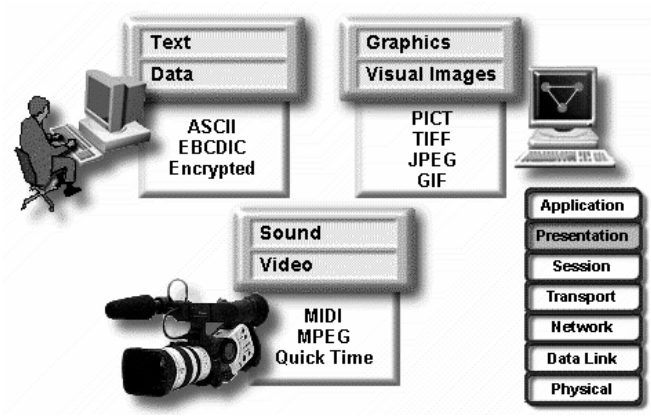


Gambar 1. Layer Aplikasi

2. Layer Presentasi (*Presentation Layer)*

Pada *layer* ini bertugas untuk mengurusi format data yang dapat dipahami oleh berbagai macam media. Selain itu layer ini juga dapat mengkonversi format data, sehingga *layer* berikutnya dapat memafami format yang diperlukan untuk komunikasi.

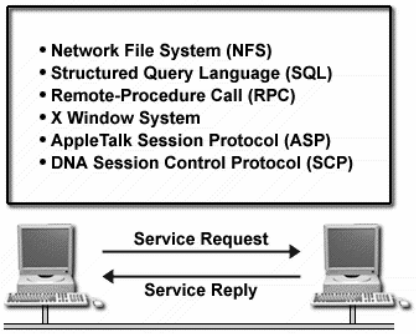
Contoh format data yang didukung oleh *layer* presentasi antara lain: *Text, Data, Graphic, Visual Image, Sound, Video*. Bisa digambarkan seperti pada Gambar 2



Gambar 2. Format Data Pada Layer Presentasi

3. Layer Sesi (*Session Layer)*

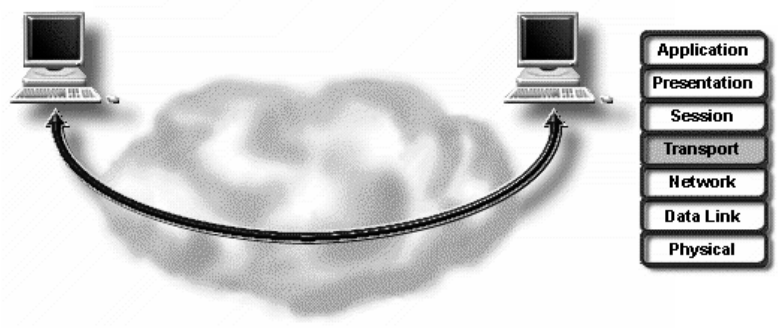
Sesi *layer* mendefinisikan bagaimana memulai, mengontrol dan mengakhiri suatu percakapan (biasa disebut session). Contoh *layer session* : NFS, SQL, RPC, ASP, SCP seperti yang ditunjukkan pada Gambar 3



Gambar 3. Mengkoordinasi Berbagai Aplikasi Pada Saat Berinteraksi Antar Komputer

4. *Transport Layer*

Pada layer 4 ini bisa dipilih apakah menggunakan protokol yang mendukung *error-recovery* atau tidak. Melakukan *multiplexing* terhadap data yang datang, mengurutkan data yang datang apabila datangnya tidak berurutan. Pada layer ini juga komunikasi dari ujung ke ujung (*end-to-end*) diatur dengan beberapa cara, sehingga urusan data banyak dipengaruhi oleh *layer* 4 ini. *Layer* 4 ditunjukkan pada Gambar 4



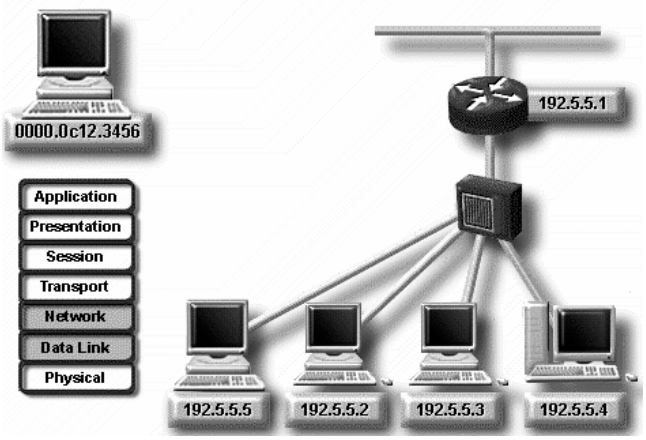
Gambar 4. Fungsi *Transport Layer*

Fungsi yang diberikan oleh *Transport Layer :*

a. Melakukan segmentasi pada *layer* atasnya
b. Melakukan koneksi *end-to-end*
c. Mengirimkan segmen dari satu *host* ke *host* yang lainnya
d. Memastikan reliabilitas data

5. *Network Layer*

Fungsi utama dari *layer network* adalah pengalamatan dan *routing*. Pengalamatan pada *layer network* merupakan pengalamatan secara *logical,* Contoh penggunaan alamat IP seperti pada Gambar 5



Gambar 5. Pengalamatan Pada *Layer Network*

6. *Data Link Layer*

Fungsi yang diberikan pada *layer data link* antara lain :

a. *Arbitration,* pemilihan media fisik
b. *Addressing,* pengalamatan fisik
c. *Error Detection,* menentukan apakah data telah berhasil terkirim
d. *Identify Data Encapsulation,* menentukan pola header pada suatu data

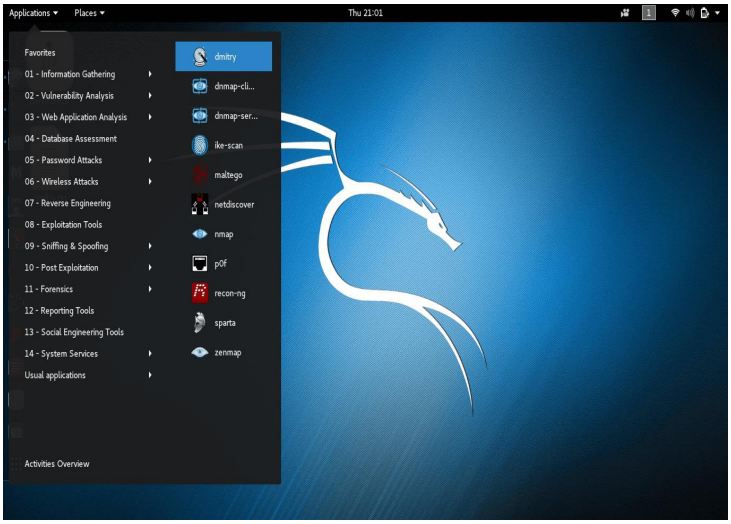
7. *Physical Layer*

Layer ini mengatur tentang bentuk *interface* yang berbeda-beda dari sebuah media transmisi. Spesifikasi yang berbeda misal konektor, pin, penggunaan pin, arus listrik yang lewat, *encoding*, dan sumber cahaya.

2.4 Kali Linux

Kali Linux (Kali) adalah sistem distribusi Linux yang di kembangan dengan fokus pada tugas *penetration testing.* Sebelumnya, Kali Linux dikenal sebagai *BackTrack*, yang mana merupakan penggabungan antara tiga distro *penetration testing* Linux yang berbeda: IWHAX, WHOPPIX, dan *Auditor*. *BackTrack* adalah salah satu sistem distribusi yang paling terkenal Linux, seperti dapat dibuktikan dengan jumlah *download* yang mencapai lebih dari empat juta pada *BackTrack* Linux 4.0 pra final [4].

Kali Linux Versi 1.0 dirilis pada 12 Maret 2013. Lima hari kemudian, Versi 1.0.1 dirilis, yang telah memperbaiki masalah *keyboard* USB. Dalam lima hari, Kali telah diunduh lebih dari 90.000 kali.



Gambar 6. Tampilan Kali Linux

Beberapa fitur yang dimiliki oleh Kali Linux, yaitu :

1. Lebih dari 300 *tools penetration testing.*
2. Gratis.
3. *Open SourceGit Tree.*
4. Mengikuti FHS *compliant.*
5. Dukungan perangkat *wireless* yang luas.
6. Modifikasi *kernel* yang sudah di *patch* untuk *injection.*
7. Lingkungan pengembangan yang aman.
8. GPG menandai beberapa paket dan repositori.
9. Banyak bahasa.
10. Dapat dirubah sepenuhnya.
11. Mendukung ARMEL dan ARMHF.

2.5 *Wireless* LAN

Wireless (nirkabel) merupakan jaringan nirkabel yang terkoneksi dengan menggunakan gelombang udara atau nirkabel (*wireless*). Teknologi ini terkoneksi tanpa menggunakan kabel atau perangkat elektronika lainnya sebagai media transmisi [5].

2.6 Keamanan *Wireless LAN*

Sebuah sistem yang aman (*secure system*) diasumsikan sebagai sebuah sistem dimana seorang intruder harus mengorbankan banyak waktu, tenaga, dan biaya besar yang tidak di kehendakinya dalam rangka penyerangan tersebut, atau resiko yang harus dikeluarkansangat tidak sebanding dengan keuntungan yang akan diperoleh. [6] Ia mengatakan, sebuah jaringan dikatakan aman apabila memenuhi 6 prinsip, yaitu :

1. Kerahasiaan (*Secrecy)*

   Secrecy berhubungan dengan hak akses untuk membaca data atau informasi dari suatu sistem komputer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal.
2. Integritas (*Integrity)*

   Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem komputer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat diubah oleh pihak yang telah diberi hak.
3. Ketersediaan (*Availability)*

   Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak.
4. *Authentication*

   Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.
5. Akses Kontrol

   Akses kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana user dan sistem berkomunikasi dan berinteraksi dengan sistem dan sumberdaya yang lainnya. Akses kontrol melindungi sistem dan sumberdaya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi.
6. *Non-Repudiation*

   Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuahtransaksi. Penggunaan digital *signature*, *certificates*, dan teknologi kriptografi secara umum dapat menjaga aspek ini.Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital *signature* itu jelas legal.

   Wireless LAN menggunakan teknologi *Radio Frequency* (RF) untuk mentransmisikan data. Jauh lebih sulit untuk menjamin keamanan dalam jaringan *wireless* daripada jaringan kabel, karena media yang digunakan adalah udara. Dalam jaringan kabel, pengguna harus terhubung langsung melalui kabel ke dalam jaringan LAN. Sedangkan *Wireless* LAN bisa diakses dimanapun perangkat *wireless* diletakkan selama masih dalam jangkauan wireless. Akses ke dalam suatu jaringan WLAN oleh pengguna yang tidak mempunyai hak dapat mengakibatkan modifikasi data, *denial of service*, penggunaan data informasi yang ada di dalam *Wireless* LAN.

   Perangkat yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada host yang tidak terhubung kemana-mana. Dengan mengendalikan *network security*, resiko tersebut dapat dikurangi. Namun *network security* biasanya bertentangan dengan *network access*, karena bila *network access* semakin mudah, *network security* makin rawan. Bila *network security* makin baik, *network access* semakin tidak nyaman. Suatu jaringan didesain sebagai komunikasi data *highway* dengan tujuan meningkatkan akses ke sistem komputer, sementara keamanan didesain untuk mengontrol akses. Penyediaan *network security* adalah sebagai aksi penyeimbang antara *open access* dengan *security.*

3. Metodologi Penelitian

3.1 Waktu dan Tempat Penelitian

Penelitian ini dilakukan pada bulan Mei 2018 sampai Juni 2018 dengan melakukan penelitian pada PT Mora Telematika Indonesia Regional Palembang yang berlokasi di Jalan Puntikayu I, Srijaya, Alang Alang Lebar, Kota Palembang, Sumatera Selatan.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah :

1. Pengumpulan Data Primer
   Observasi atau pengamatan yaitu dengan cara mengamati dan mencatat secara sistematik gejala-gejala yang sedang diselidiki.
2. Pengumpulan Data Sekunder
   Studi Pustaka (literatur), data diperoleh melalui studi kepustakaan yaitu dengan mencari bahan dari internet, jurnal, dan perpustakaan serta buku referensi pada penelitian-penelitian terdahulu yang sejenis.

3.3 Metode Penelitian

Adapun metode penelitian yang digunakan yaitu metode *Penetration Testing*. [7] *Mengatakan bahwa Penetration Testing (Pentest)* adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa di lakukan terhadap yang ada pada sistem jaringan tersebut. Orang yang melakukan kegiatan ini disebut *Penetration Tester* disingkat *Pentester*.

4. Hasil dan Pembahasan

4.1 Hasil

Penelitian dalam kegiatan evaluasi ini dilakukan agar mengetahui tingkat kerentanan dalam jaringan *wireless local area network*, dengan melakukan 4 tahapan penyerangan maka terbukti kerentanan jaringan *wireless local area network* yang di miliki PT. Mora Telematika Indonesia bisa di katakan lemah. Secara keseluruhan, implementasi dari pengujian keamanan jaringan *wireless local area network* dengan metode *penetration testing* dapat dilihat pada Tabel 1

Tabel 1. Hasil *Penetration Testing*

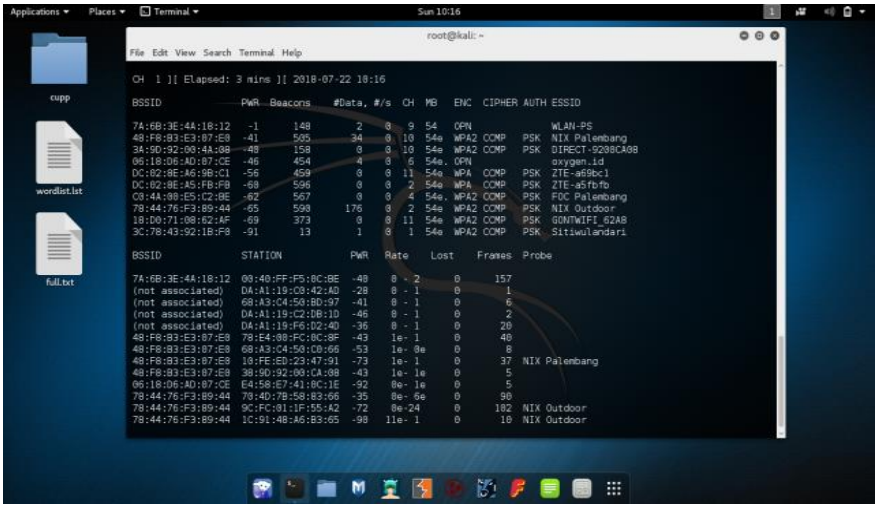
Jenis Serangan	Informasi yang dibutuhkan	Status Serangan
Cracking The Ecryption	*Dictionary Word, handshake user* lain, Channel yang digunakan dan BSSID dari *access point*.	Berhasil
Bypassing MAC Authentication	*List* MAC *User* lain yang terhubung di jaringan	Gagal
Attacking The Infrastructure	*Attacker* harus bedara dalam jaringan WLAN, MAC *Address* dari perangkat *tester*	Berhasil
MITM	*Attacker* harus berada dalam jaringan WLAN, IP *address* dari *user* yang terkoneksi	Berhasil

4.2 Pembahasan

Pada penelitian ini, pengujian dilakukan di dalam kantor PT. Mora Telematika Indonesia. Pengujian dilakukan dengan 4 tahapan berbeda [8], yaitu :

1. *Cracking The Ecryption*

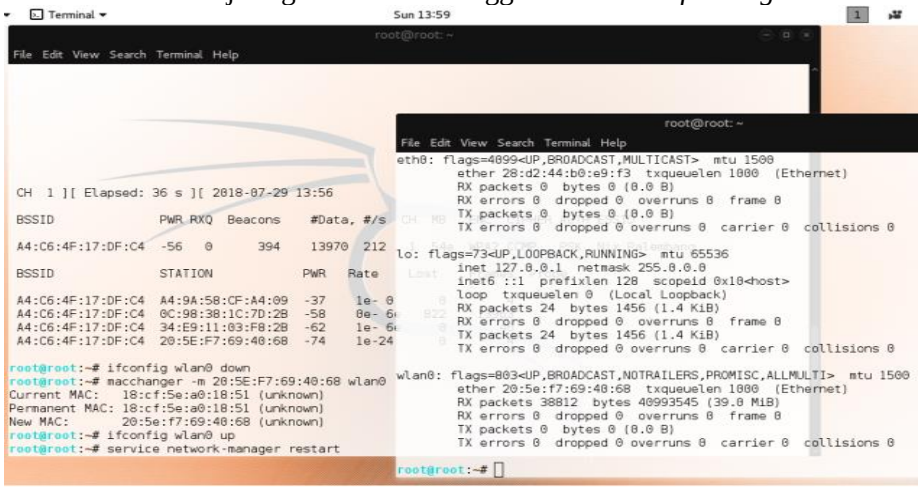
Tahapan yang pertama, dimana tujuan dari serangan ini adalah untuk mengetahui apakah semua access point dilindungi dengan sistem keamanan enkripsi seperti WEP, WPA ataupun WPA2. Penguji melakukan *scanning* terhadap *access point* kemudian menentukan target untuk dilakukan *cracking* terhadap *key* yang digunakan sebagai pengamanan yang ditunjukkan pada Gambar 7.



Gambar 7. *Scanning*

2. *Bypassing MAC Authentication*

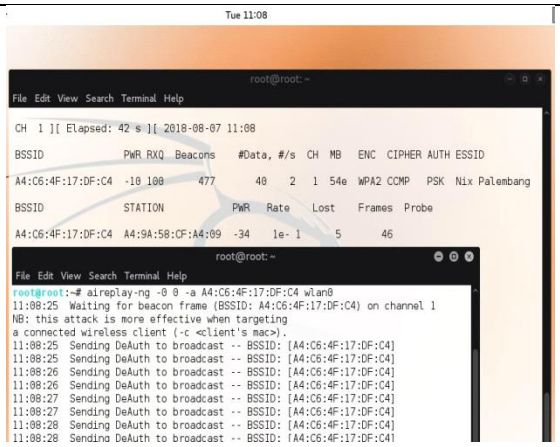
Tahapan yang kedua, tujuan dari percobaan ini adalah untuk mengetahui apakah sistem keamanan menggunakan metode pembatasan hak akses dengan MAC *filtering* atau tidak. Setelah dilakukan percobaan menghubungkan antara perangkat pengujian dan *access point* ditemukan bahwa system keamanan dari jaringan *wireless* menggunakan MAC *filtering.*



Gambar 8. MAC *Changer*

3. *Attacking The Infrastructure*

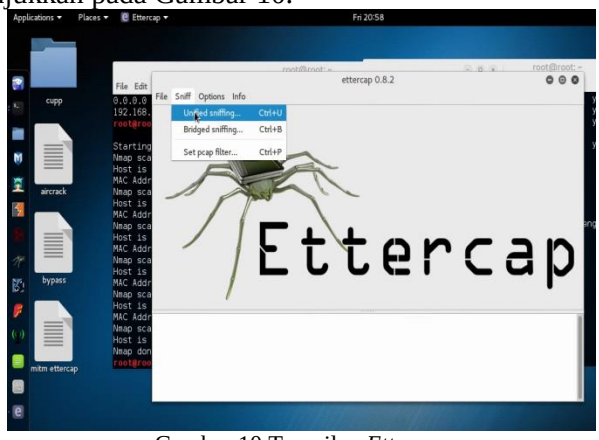
Dalam tahap ini dilakukan serangan pada layanan *wireless* untuk client sehingga dapat mempengaruhi kinerja jaringan. Bentuk serangan ini adalah DoS *attack* yang bertujuan melumpuhkan koneksi *user* lain di dalam jaringan. Informasi awal yang dibutuhkan adalah *password* dari jaringan *wireless* yang diuji, agar komputer *tester* dapat terhubung dengan layanan *wireless*. Gambar 9 menunjukkan DoS attack saat melakukan tahap *Attacking the Infrastructure*.



Gambar 9 DoS *attack*

4. *Man In The Middle* (MITM) *Attack*

Dalam tahap ini dilakukan serangan terhadap *user* lain jaringan WLAN yang sama dengan melakukan penyadapan paket data. Pengujian ini menggunakan aplikasi *ettercap* sebagai alat uji. Tampilan *Ettercap* ditunjukkan pada Gambar 10.



Gambar 10 Tampilan *Ettercap*

Pada tahapan *Man In The Middle Attack*, kondisi awal yang dibutuhkan adalah komputer *tester* dan komputer target harus terhubung di jaringan *wireless* 'Nix Palembang'. Disini komputer *tester* berperan sebagai pihak ketiga diantara target dan *access point* yang menghubungkan antara target dan layanan internet. Dalam hal ini, pada konfigurasi ettercap yang menjadi target pertama adalah *gateway* dari *Access Point* yaitu 192.168.100.1 dan yang menjadi target kedua adalah IP dari komputer target yaitu 192.168.100.6.

Tahap selanjutnya adalah melakukan ARP *Poisoning*. Address Resolution Protocol (ARP) adalah sebuah protocol dalam TCP/IP Protocol Suite yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (*MAC Address*). ARP Poisoning adalah suatu teknik menyerang pada jaringan komputer local baik dengan media kabel maupun wireless, yang memungkinka penyerang bisa mengetahui frames data pada jaringan local atau melakukan modifikasi *traffic* atau bahkan menghentikan traffic. Pada prinsipnya ARP poisoning ini memanfaatkan kelemahan pada teknologi jaringan komputer sendiri yang menggunakan ARP *broadcast*

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan selama Analisa Keamanan Jaringan *Wireless* dengan Metode *Penetration Testing (Cracking The Encryption, Bypassing* MAC *Authentication,*

Attacking The Infrastructure dan MITM*)* menggunakan Kali Linux pada PT. Mora Telematika Indonesia, maka dapat di ambil kesimpulan bahwa :

1. Dalam menerapkan *penetration testing* pada sebuah institusi dibutuhkan jaminan hukum terhadap pelaku dan objek *penetration testing.*
2. Keamanan jaringan menggunakan metode *Penetration Testing* dapat memberikan gambaran tentang kelemahan sistem jaringan WLAN di PT. Mora Telematika Indonesia yang masih memiliki banyak celah untuk dieksploitasi. Hal ini dibuktikan dengan hasil penelitian yang dilakukan bahwa dari empat jenis serangan yang dilakukan, hanya satu yang berstatus gagal yaitu pada jenis serangan *Bypassing* WLAN *Authentication.*
3. Gagalnya tahapan *Bypassing* WLAN *Authentication* di karenakan pada proses ini dibutuhkan penyamaan MAC *Address* dalam 1 jaringan *wireless*, sedangkan PT. Mora Telematika Indonesia sudah memakai *Router MikrotikOS* yang dengan fitur *firewall* mampu menolak MAC *Address* yang sama, jadi jika ada MAC *Address* yang sama tidak akan bisa masuk ke dalam jaringan WLAN tersebut.

5.2 Saran

Adapun saran dalam penelitian ini yaitu :

1. *Penetration Testing* merupakan tindakan yang membahayakan bagi sistem, maka perlu dipertimbangkan resiko dari tindakan ini.
2. Nilai yang di hasilkan dari pengujian dapat dijadikan acuan dalam meningkatkan kualitas sistem keamanan jaringan WLAN.
3. Pengembangan teknik serang *Penetration Testing* menggunakan aplikasi / *tools* lain seperti *cewl*, *johnny*, *ncrack*, *ophcrack* dan lain-lain yang tersedia pada Kali Linux untuk menjadi bahan evaluasi bagi pengembangan keamanan jaringan WLAN.

Referensi

[1] B. P. Nuryanto, *Model Pengujian Keamanan Jaringan WLAN Melalui Penetration Testing Methods Guna Peningkatan Pengamanan Sistem Jaringan Dari Tindakan Hacking*, Magelang: Universitas Muhammadiyah Magelang, 2013.
[2] A. Kristanto, *Jaringan Komputer*, Yogyakarta: Penerbit Graha Ilmu, 2003.
[3] K. Sutarti dan K. Khairunnisa, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan DDOS (Distributed Denial of Service) berbasis Honeypot", *Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 4, no. 2, 2017.
[4] I. Faishal, "Analisis Kinerja TCP pada Jaringan Mobile Ad-Hoc Menggunakan Protokol Routing DSR dan AODV", *Doctoral dissertation, Universitas Widyatama*, 2013.
[5] I. K. Bayu, M. Yamin dan L. F. Aksara, "Analisis Keamanan Jaringan WLAN Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO), *semanTIK*, vol. 3, no, 2, 2018.
[6] D. M. Sari, M. Yamin dan L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) MAC Address, Menggunakan Metode Penetration Testing", s*emanTIK*, vol. 3, no. 2, 2018.
[7] R. J. Al-Haroh, *Wardriving Dan Testing Penetrasi Wi-Fi Lanjut Di Wilayah Kota Yogyakarta*, Yogyakarta : Universitas AMIKOM Yogyakarta, 2012.
[8] S'to, *Wireless Kung Fu Networking & Hacking*, Jasakom, 2015.