ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) DENGAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) (STUDI KASUS : PT. WIN PRIMA LOGISTIK)

Abdul Kholiq[1] , Diyah Khoirunnisa[2]
Program Studi Teknik Informatika Fakultas Teknik
Dosen Prodi Teknik Informatika[1] , Mahasiswa Prodi Teknik Informatika[2]
Universitas Satya Negara Indonesia
Email: *kholiq05@gmail.com, diyahkhoirunnisa@gmail.com*

ABSTRAK

Wireless memiliki beberapa keunggulan dibandingkan dengan media kabel dalam hal kemudahan mengakses data dan mengakses internet, yaitu bisa lebih mudah dan fleksibel selama masih dalam jangkauan wirelesss tersebut.PT. Win Prima Logistik menggunakan jaringan Wireless Local Area Network (WLAN) sebagai media komunikasi, baik komunikasi pada jaringan local dan internet. Jaringan wireless menggunakan gelombang sebagai penghantar datanya, maka resiko keamanan menjadi lebih besar, hal ini disebabkan oleh medium gelombang lebih bebas dan tidak dapat dikontrol, sehingga memungkinkan para penyusup untuk melakukan tindakan ilegal, maka dari itu dibutuhkan sebuah tools standar dalam analisis dengan menggunakan Penetration Testing Execution Standard (PTES) yang merupakan salah satu tools yang dikembangkan oleh pentest organitation untuk menjadi standar dalam menganalisis atau mengaudit sistem keamanan jaringan pada sebuah perusahaan dalam kasus ini yaitu menganalsis keamanan jaringan wireless pada PT. Win Prima Logistik. Pengujian yang telah dilakukan diantaranya,serangan WPS Aktif, Bypassing MAC Address, ARP Spoofing dan cracking the encryption.Dari analisis pengujian penetration testing yang telah dilakuakan maka dapat disimpulkan bahwa sistem keamanan jaringan wireless PT. Win Prima Logistik sudah cukup aman tetapi masih bisa diserang oleh serangan bypassing MAC Address dan ARP Spoofing.

Kata Kunci : *Penetration Testing Execution Standard, WLAN,* keamanan jaringan, *WPS Aktif, Bypassing MAC Address, ARP Spoofing, cracking the encryption.*

Abstract

Wireless has several advantages compared to cable media in terms of the ease of accessing data and accessing the internet, which can be easier and more flexible as long as it is still within reach of these wirelesss. PT. Win Prima Logistik uses a Wireless Local Area Network (WLAN) network as a communication medium, both communication on local and internet networks. Wireless networks use waves as a conduit of data, so security risks are greater, this is caused by the wave medium is freer and cannot be controlled, allowing intruders to carry out illegal actions, therefore we need a standard tool in analysis using Penetration Testing Execution Standard (PTES) is one of the tools developed by the pentest organitation to become a standard in analyzing or auditing network security systems in a company in this case, namely analyzing wireless network security at PT. Win Prima Logistik. Tests that have been done include, Active WPS attacks, MAC Address Bypassing, ARP Spoofing and cracking the encryption. From the analysis of penetration testing testing that has been done, it can be concluded that the wireless network security system of PT. Win Prima Logistik is safe enough but can still be attacked by bypassing MAC Address and ARP Spoofing attacks.

Keywords : *Penetration Testing Execution Standard, WLAN, network security, Active WPS, MAC Address Bypassing, ARP Spoofing, cracking the encryption.*

PENDAHULUAN

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun *network security* biasanya bertentangan dengan *network access*, dimana bila *network access* semakin mudah, maka *network security* semakin rawan, begitu pula sebaliknya. (Ariyus, 2007:3).

Penetration Testing (disingkat pentest) adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi / perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Menurut *Chow* (2011) dalam penelitiannya menyimpulkan bahwa *ethical hacking* dan *penetration testing* dianggap sebagai cara yang efisien dan efektif dalam mengatasi celah keamanan. PT. Win Prima Logistik menggunakan jaringan *Wireless Local Area Network* (WLAN) sebagai media komunikasi, baik komunikasi pada jaringan local dan internet. Sedangkan untuk sistem keamanan yang digunakan saat ini menggunakan WPA (*Wifi Protected Access*). Akan tetapi, sistem keamanan ini masih memiliki kelemahan yaitu *password* yang masih mudah untuk ditembus sehingga memungkinkan untuk penyusup mengambil data-data penting pada perusahaan melalui celah keamanan pada jaringan tersebut, misalnya melakukan serangan terhadap *wireless access point*, dengan cara melakukan pengujian serangan *WPS* Aktif, *Bypassing MAC Address*, *ARP Spoofing* dan *cracking* the *encryption*. Untuk mengatasi permasalahan tersebut, maka perlu dilakukan suatu pengujian untuk mengetahui kelayakan sistem keamananWireless Local Area Network (WLAN), sehingga diharapkan dapat menggali dan menemukan celah-celah keamanan yang ada untuk kemudian dilakukan perbaikan dari sistem keamanan jaringan saat ini.

TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah untuk menganalisis tingkat keamanan fasilitas jaringan *Wireless Local Area Network* (WLAN) pada PT. Win Prima Logistik.

DASAR TEORI

Keamanan Jaringan

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun network security biasanya bertentangan dengan network access, dimana bila network access semakin mudah, maka network security semakin rawan, begitu pula sebaliknya. (Ariyus, 2007:3). Menurut Garfinkel dan Spafford pada tahun 1999, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu :

a. *Confidentiality*, mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
b. *Integrity*, mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
c. *Availability*, mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
d. *Authentication*, mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
e. *Nonrepudiation*, mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan. (Garfinkel dan Spafford).

Serangan (gangguan) terhadap keamanan dapat dikategorikan dalam empat kategori utama, yaitu :

a. *Interruption*, suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang.
b. *Interception*, suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain.
c. *Modification*, Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset.
d. *Fabrication*, Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem.

Menurut Nugroho (2016:16) "Kehandalan jaringan menjadi tujuan utama dari proses awal sebuah perencanaan jaringan. Pengguna jaringan akan merasa lebih "nyaman" jika menggunakan jaringan handal (reliable)". Jaringan dapat dikatakan handal apabila sudah memenuhi parameter berikut :

a. *Fault Tolerance*
   Adalah istilah yang mengijinkan jalur utama yang digunakan untuk mengalirkan data dari sumber ke tujuan menjadi tidak berfungsi, namun harus disediakan jalur cadangan agar ketika jalur utama putus, data masih bisa dialirkan ke perangkat tujuan.
b. Skalabilitas

Adalah untuk menjaga performasi dari sebuah jaringan. Skalabilitas dari sebuah jaringan mempunyai definisi bahwa keberadaan jaringan yang baru harus tidak mempengaruhi performasi jaringan yang lama.

c. QoS (*Quality of Service*)
   Qos akan menjamin data yang penting mendapatkan prioritas utama untuk diteruskan keperangkat tujuan. Data yang penting identik dengan data yang sifatnya real time, misalnya data suara atau video. Kedua jenis antrian perangkat sebuah jaringan dibandingkan data yang sifatnya unreal time seperti data teks dan gambar.
d. Keamanan
   Keamanan jaringan menjadi bagian yang sangat penting dalam proses komunikasi data dalam sebuah jaringan. Data yang dikirim oleh penerima yang sah. Sehingga hal terpenting dalam keamanan jaringan adalah bagaimana menjamin data tidak diambil dan dibaca oleh pengguna lain yang tidak sah.

***Penetration Testing Execution Standard* (PTES)**

Penetration Testing (disingkat pentest) adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi / perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut.

Metode penetration testing dilakukan dengan cara mensimulasikan bentuk-bentuk serangan terhadap jaringan komputer. Menurut Chow (2011) dalam penelitiannya yang berjudul "Ethical Hacking & Penetration Testing" menyimpulkan bahwa ethical hacking dan penetration testing dianggap sebagai cara yang efisien dan efektif dalam mengatasi celah keamanan. Berikut adalah tahapan-tahapan yang harus dilakukan jika ingin melakukan penetraton testing pada sebuah jaringan Wireless Local Area Network (WLAN).

Gambar 1. Tahapan Penetration Testing

a. *Pre-Engagement*, adalah tahap dimana seorang pentester menjelaskan kegiatan pentest yang akan dilakukan kepada client (perusahaan).
b. *Intelligence Gathering*, adalah tahap dimana seorang pentester berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media.
c. *Threat Modelling*, adalah tahap dimana seorang pentester mencari celah keamanan (vulnerabilities) berdasarkan informasi yang berhasil dikumpulkan pada tahap sebelumnya.
d. *Vulnerability Analysis*, adalah tahap dimana seorang pentester mengkombinasikan informasi mengenai celah keamanan yang ada dengan metode serangan yang bisa dilakukan untuk melakukan serangan yang paling efektif.
e. *Exploitation*, adalah tahap dimana seorang pentester melakukan serangan pada target.
f. *Post-Exploitation*, adalah tahap dimana seorang pentester berhasil masuk ke dalam sistem jaringan target dan kemudian melakukan analisis infrastruktur yang ada.
g. *Reporting*, adalah bagian paling penting dalam kegiatan pentest. Seorang pentester menggunakan report (laporan) untuk menjelaskan pada perusahaan mengenai pentesting yang dilakukan.

Wireless Local Area Network

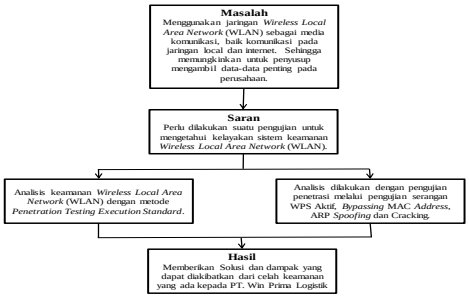
Wireless (nirkabel) adalah teknologi yang menghubungkan dua piranti untuk bertukar data tanpa media kabel. Adapun *Wireless Fidelity* (WiFi), yaitu perangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (*Wireless Local Area Network* / WLAN) yang didasari pada spesifikasi IEEE 802.11 (Sofana, 2013).

Wireless Local Area Network (WLAN)adalah sistem komunikasi yang fleksibel dimana pengirim dan penerimaan datanya melalui media udara dengan menggunakan teknologi frekuensi radio. *Wireless Local Area Network* (WLAN) dapat digolongkan menjadi dua kategori utama yakni :

a. WLAN berbasis *Ad-Hoc*
   Pada model jaringan yang berbasis ad-hoc, jaringan antara satu perangkat dengan perangkat yang lain dilakukan secara spontan/langsung tanpa melalui konfigurasi tertentu selama signal dari pemancar yakni transmitter dapat diterima dengan baik oleh perangkat-perangkat penerima yakni receiver.
b. WLAN berbasis Infrasturkur
   Pada model jaringan yang berbasis infrastruktur, model ini, untuk memberikan koneksi antara perangkat yang terhubung kedalam jaringan *Wireless Local Area Network* (WLAN), diperlukan suatu

intermediary device berupa *wireless access point* yang terhubung dalam jaringan komputer nirkabel, sebelum melakukan transmisi kepada perangkat-perangkat penerima signal.(Pratama, 2015, S'to, 2015).

METODOLOGI PENELITIAN



Gambar 2. Metodologi Penelitian

Sesuai dengan diagram alir penelitian diatas, penelitian ini dilakukan dalam beberapa tahapan, yaitu sebagai berikut :

a. Menyiapkan buku-buku, ebook, dan jurnal untuk menunjang penelitian.
b. Memenuhi persyaratan/prosedur perizinan penelitian yang diberikan oleh PT. Win Prima Logistik.
c. Mencari informasi data-data yang ada, konfigurasi jaringan Wireless Local Area Network (WLAN) yang terpasang pada PT. Win Prima Logistik.
d. Menyiapkan hardware dan software yang dibutuhkkan untuk menunjang pelaksanaan penelitian.
e. Melakukan sebuah percobaan penyerangan kepada jaringan Wireless Local Area Network (WLAN) dengan metode penetration testing untuk mendapatkan informasi tentang keamanannya.
f. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan jaringan Wireless Local Area Network (WLAN) melihat dari sisi pengguna.

ANALISIS KEAMANAN JARINGAN

Sistem keamanan jaringan Wireless Local Area Network (WLAN) saat ini pada PT. Win Prima Logistik adalah WLAN berbasis Infrastruktur. Dalam merancang model keamanan, aset jaringan yang beresiko perlu diperhatikan seperti titik kelemahan dalam sistem keamanannya, atau gangguan yang datang dari si penyerang, serta motivasi serangan tersebut untuk masing-masing potensi kelemahan yang ada. Berikut adalah bagan WLAN Infrastruktur yang terdapat pada PT. Win Prima Logistik saat ini.

Gambar 3. Arsitektur Jaringan Saat Ini

Sistem yang berjalan saat ini pada PT. Win Prima Logistik belum cukup kuat dalam hal keamanan jaringan, hal ini dikarenakan semua device pengguna (user) dapat melakukan layanan berbagi berkas, layanan berbagi alat pencetak (printer), DNS Service, http service, dan lain sebagainya yang terhubung dalam jaringan Wireless Local Area Network (WLAN) yang sama. Hal ini memungkinkan untuk siapa saja dapat melakukan tindakan diluar tanggung jawab nya dan mengambil data untuk keperluan diluar jobdesk pekerjaan nya.

Dalam hal ini perlu ditingkatkan sistem keamanan jaringan agar lebih safety. Maka dalam penelitian ini penulis melakukan analisis keamanan jaringan Wireless Local Area Network (WLAN) pada PT. Win Prima Logistik dengan metodePenetration Testing

Berikut adalah tabel serangan yang akan di analisis pada jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik.

Tabel 1. Jenis Serangan Keamanan

Pengujian	Batasan Serangan	Alat Bantu
Serangan pada WPS aktif	Serangan dilakukan pada jaringan WLAN yang aktif WPSnya. Jaringan WLAN yang akan diserang bertipe WPA2 PSK dan bertipe enkripsi TKIP+AES.	Dumper, Jumpstart
Bypassing MAC *Address*	Serangan dilakukan pada jaringan WLAN.	T-MAC
ARP *Spoofing*	Serangan attacker berada di tengah-tengah user yang menggunakan jaringan WLAN. Attacker menyerang user yang sedang terkoneksi.	Netcut
Cracking the encryption	Proses scanning dan capture data	Aircrack-ng

Analisis Penetration Testing

Adapun metode penelitian yang dilakukan untuk melakukan analisis sistem keamanan jaringan wireless menggunkan penetration testing. Penjelasan dari tahap-tahap metode penetration testing adalah sebagai berikut :

a. Pre-engagement Interactions

Tahap dimana seorang pentester menjelaskan kegiatan pentest yang akan dilakukan kepada client (perusahaan). Disini seorang pentester harus bisa menjelaskan kegiatan-kegiatan yang akan dilakukan dan tujuan akhir yang akan dicapai. Adapun yang dibahas pada tahap ini adalah pertanyaan – pertanyaan :

1) Pertanyaan Network Penetration Test

Pertanyaan network penetration test merupakan salah satu bagian dari pre-engagement. Pertanyaan network penetration test dibuat untuk membantu dalam proses wawancara agar lebih mudah dalam memberikan pertanyaan. Pertanyaan network penetration test dapat dilihat pada tabel dibawah ini.

Tabel 2. Pertanyaan *network penetration test*

No	Pertanyaan
1	Mengapa harus diadakan tes penetrasi pada jaringan di PT. Win Prima Logistik ?
2	Kapan waktu yang diberikan perusahaan untuk uji penetrasi ? (saat jam kantor, setelah jam kantor, saat akhir pekan)
3	Berapa banyak alamat IP yang diujikan ?
4	Apakah ada perangkat yang terkena dampak hasil uji penetrasi, seperti (firewall, sistem deteksi, aplikasi firewall)?

2) Pertanyaan Wireless Network Penetration Test

Pertanyaan wireless network penetration test merupakan sebuah pertanyaan yang di siapkan untuk mencari informasi mengenai jaringan wireless target (perusahaan). Pertanyaan network penetration test dapat dilihat pada tabel dibawah ini.

Tabel 3. Pertanyaan *wireless network penetration test*

No.	Pertanyaan
1	Seberapa banyak perangkat *wireless* yang aktif di PT. Win Prima Logistik ?
2	Apakah *wireless* dapat diakses oleh orang luar, tanpa harus menggunakan hak akses ?
3	Apa jenis keamanan yang digunakan perangkat *wireless* PT. Win Prima Logistik ?
4	Apakah ada yang pernah mencoba menyerang melalui jaringan *wireless* PT. Win Prima Logistik ?
5	Berapa banyak user yang menggunakan jaringan *wireless* di PT. Win Prima Logistik ?

3) Pertanyaan Physical Penetration Test

Pertanyaan physical penetration test memiliki kegunaan yang sama dengan pertanyaan-pertanyaan yang lainnya untuk membantu dalam pengumpulan informasi. Pertanyaan physical penetration test berisikan mengenai cangkupan penelitian. Pertanyaan physical penetration test dapat dilihat pada tabel dibawah ini.

Tabel 4. Pertanyaan *physical penetration test*

No.	Pertanyaan
1	Apakah PT. Win Prima Logistik memiliki Standard Operating Procedure (S.O.P) dalam akses, perawatan dan penanganan jaringan ?
2	Apakah ada berita acara atau dokumentasi tentang keamanan jaringan ?
3	Apakah terdapat kamera *cctv* di PT. Win Prima Logistik ?

4) Pertanyaan Administrator Sistem

Pertanyaan administrator sistem merupakan pertanyaan yang berisikan mengenai pertanyaan yang ditujukan untuk mengetahui tentang administrator sistem yang ada pada target. Pertanyaan administrator sistem dapat dilihat pada tabel dibawah ini.

Tabel 5. Pertanyaan administrator sistem

No.	Pertanyaan
1	Apakah sistem operasi selalu *update* ?
2	Apakah ada perangkat lunak pemantauan sistem ?
3	Apakah *backup* data *server* dilakukan secara teratur ?
4	Kapan terakhir *restore backup* data *server* ?

b. Intelligence Gathering

Tahap dimana seorang pentester berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media. Intelligence gathering pada penelitian ini berfokus pada jaringan wireless. Berikut adalah sub pembahasan dari intelligence gathering :

1) Karakteristik Sistem Jaringan Wireless

Setelah dilakukan analisis terhadap sistem jaringan wireless yang digunakan, baik dari segi hardware dan sistemnya, maka didapatkanlah hasil dari karakteristik sistem jaringan wireless yang ada saat ini adalah sebagai berikut :

Tabel 6. Spesifikasi Wi-Fi

Spesifikasi	Kecepatan	Frekuensi Band	Sesuai spesifikasi
802.11b	11 Mbps	2.4 GHz	b
802.11a	54 Mbps	5 GHz	a
802.11g	54 Mbps	2.4 GHz	b,g
802.11n	100 Mbps	2.4 GHz	b,g,n

Tabel 7. Tabel Frequensi WiFi

Channel	Frequency (Ghz)	Range	Channel Range
1	2.412	2.401 - 2.423	1 - 3
2	2.417	2.406 - 2.428	1 - 4
3	2.422	2.411 - 2.433	1 - 5
4	2.427	2.416 - 2.438	2 - 6
5	2.432	2.421 - 2.443	3 -7
6	2.437	2.426 - 2.448	4 - 8
7	2.442	2.431 - 2.453	5 - 9
8	2.447	2.436 - 2.458	6 - 10
9	2.452	2.441 - 2.463	7 - 11
10	2.457	2.446 - 2.468	8 - 11
11	2.462	2.451 - 2.473	9 - 11
12	2.467	2.456 - 2.478	Not US
13	2.472	2.461 - 2.483	Not US
14	2.484	2.473 - 2.495	Not US

2) Cara Kerja Sistem Jaringan Wireless
   Dari analisis yang telah dilakukan oleh penulis, informasi yang didapatkan mengenai cara kerja sistem jaringan wireless pada PT. Win Prima Logistik adalah :
   (a) Setiap PC (Personal Computer) menggunakan adapter wireless untuk menangkap sinyal dari access point.
   (b) Adaptor wireless komputer menerjemahkan data menjadi sinyal radio dan mengirimkan (memancarkan) menggunakan antena.
   (c) Router access point wireless menerima sinyal dan melakukan decode data. Router access point mengirimkan informasi ke Internet koneksi kabel Ethernet dan terhubung ke komputer penerima.
3) Metode Serangan Yang Bisa Digunakan
   Dari hasil analisis yang dilakukan oleh penulis, maka dengan ini serangan yang dapat dilakukan pada jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik untuk menguji keamanan jaringannya dengan serangan pada *WPS* aktif, *Bypassing MAC Address*, *ARP Spoofing*, *Cracking the Encryption*.

c. Threat Modeling

Tahap dimana seorang pentester mencari celah keamanan (vulnerabilities) berdasarkan informasi yang berhasil dikumpulkan pada tahap sebelumnya. Pada tahap ini seorang pentester tidak hanya mencari celah keamanan, tetapi juga menentukan celah yang paling efektif untuk digunakan.

d. Vulnerability Analysis

Tahap dimana seorang pentester mengkombinasikan informasi mengenai celah keamanan yang ada dengan metode serangan yang bisa dilakukan untuk melakukan serangan yang paling efektif. Vulnerability analisis bertujuan untuk menemukan kekurangan didalam sistem jaringan yang dapat dimanfaatkan oleh penyerang. Berikut adalah kelemahan atau kekurangan yang terdapat dalam sistem jaringan Wireless Local Area Network (WLAN) pada PT. Win Prima Logistik :

Tabel 8. Kelemahan jaringan Wireless PT. Win Prima Logistik

No.	Kelemahan Jaringan *Wireless*
1	Jaringan Wi-Fi masih bisa di akses oleh siapa pun, tidak adanya hak akses khusus.
2	Tidak ada situs atau web yang di blokir dalam jaringan *wireless*.
3	Tidak ada batasan dalam penggunaan bandwith bagi seluruh karyawan PT. Win Prima Logistik

e. Exploitation

Tahap dimana seorang pentester melakukan serangan pada target. Walaupun demikian tahap ini kebanyakan dilakukan dengan metode brute force tanpa memiliki unsur presisi. Seorang pentester profesional hanya akan melakukan exploitation ketika dia sudah mengetahui secara pasti apakah serangan yang dilakukan akan berhasil atau tidak. Namun tentu saja ada kemungkinan tidak terduga dalam sistem keamanan target. Walaupun begitu, sebelum melakukan serangan, pentester harus mengetahui kalau target mempunyai celah keamanan yang bisa digunakan. Melakukan serangan secara terus-menerus dan berharap sukses bukanlah metode yang produktif. Seorang pentester profesional

selalu menyempurnakan analisisnya terlebih dahulu sebelum melakukan serangan yang efektif. Dengan kata lain exploitation adalah penyerangan terhadap target setelah mendapatkan informasi dari target.

f. Post Exploitation

Tahap dimana seorang pentester berhasil masuk ke dalam sistem jaringan target dan kemudian melakukan analisis infrastruktur yang ada. Pada tahap ini seorang pentester mempelajari bagian-bagian di dalam sistem dan menentukan bagian yang paling critical bagi target (perusahaan). Disini seorang pentester harus bisa menghubungkan semua bagian-bagian sistem yang ada untuk menjelaskan dampak serangan / kerugian yang paling besar yang bisa terjadi pada target (perusahaan).

g. Reporting

Bagian paling penting untuk menjelaskan pada perusahaan mengenai pentesting yang dilakukan seperti: apa yang dilakukan, bagaimana cara melakukannya, resiko yang bisa terjadi dan yang paling utama adalah cara untuk memperbaiki sistemnya.

Pengujian Kemananan

Untuk mengimplementasikan kerangka berfikir yang sudah disusun, maka penulis melakukan simulasiuntuk mengetahui keamanan jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik dengan menggunakan metode Penetration Testing, yaitu dengan menggunakan tools Dumper, JumpStart, NetCut, T-MAC dan juga Aircrack-ng for windows. Penetration Testing yang dilakukan yaitu tipe Overt pentest dimana penulis melakukan pengujian keamanan jaringan dengan sepengetahuan perusahaan.

Pengujian keamanan jaringan WLAN menggunakan metode penetration testing execution standard (PTES) adalah sebagai berikut :

a. *Information Gathering*

Proses ini dilakukan untuk mengetahui informasi tentang jaringan WLAN yang ingin diuji. Pada bab sebelumnya sudah diajukan pertanyaan-pertanyaan dengan metode wawancara kepada sumber terkait.

1) Pertanyaan *network penetration test*
   Dari hasil wawancara kepada sumber terkait maka didapatkan informasi mengenai tes pentrasi harus dilakukan pada jaringan PT. Win Prima Logistik karena dengan adanya tes penetrasi ini maka akan diketahui sejauh mana keamanan jaringan yang terdapat pada perusahaan. Penulis diberikan waktu untuk melakukan simulasi tes penetrasi ini pada saat jam kantor telah berakhir agar tidak menggangu aktifitas karyawan lainnya. Untuk tes penetrasi ini menguji kurang lebih sebanyak 20 alamat IP (*Internet Protocol*) dan tidak ada dampak untuk perangkat lain karena tes pentrasi ini bersifat simulasi.
2) Pertanyaan *wireless network penetration test*
   Untuk pertanyaan seputar *wireless network penetration test*, penulis mengetahui bahwa perangkat *wireless* yang aktif pada PT. Win Prima Logistik pada saat jam kerja berlangsung mencapai 20 device. Dan untuk koneksi *wireless* pada perusahaan ini dapat diakses oleh pihak luar (dala hal ini tamu) dengan memasukkan password *wireless.* Jenis keamanan yang digunakan adalah WPA2-PSK. Sejauh ini belum ada yang mencoba untuk menyerang melalui jaringan wireless PT. Win Prima Logistik.
3) Pertanyaan *physical penetration test*
   Untuk pertanyaan seputar *physical penetration test*, penulis mendapatkan informasi bahwa pada PT. Win Prima Logistik belum ada *Standard Operating Procedure* (S.O.P) dalam akses jaringan, dikarenakan tidak ada divisi IT untuk bagian tersebut. Dan untuk keamanan sekitar perusahaan, telah dipasang kamera *cctv* di berbagai sudut ruangan kantor.
4) Pertanyaan *administrator* sistem
   Dari hasil wawancara kepada sumber terkait, maka penulis mendapatkan informasi bahwa operating system tidak selalu di update, dan tidak ada perangkat lunak untuk pemantauan sistem atau pemantauan penggunaan jaringan wireless pada perusahaan. Karena pada perusahaan ini tidak terdapat komputer server, maka *back up* data dilakukan secara pribadi dengan *hardisk external.*

b. Analisis Awal

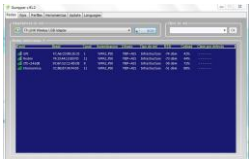
Proses ini dilakukan untuk menentukan jenis tindakan dan kebutuhan pengujian dengan penetrasi. Setelah analisis awal dilakukan, maka penulis dapat langsung menjalankan proses *penetration testing executin standard* (PTES) pada jaringan WLAN di PT. Win Prima Logistik. Tindakan yang akan dilakukan dalam pengujian antara lain adalah :

1) Pengujian serangan WPS aktif dengan menggunakan tools Dumper dan Jumpstart.
2) *Bypassing* MAC *address* dengan menggunakan tools T-MAC.
3) ARP *spoofing* dengan menggunakan tools Netcut.
4) *Cracking the encryption* dengan menggunakan tools aircrak-ng.

c. *Attacking*

Proses ini dilakukan untuk melakukan penetrasi jaringan dengan berbagai macam serangan. Tindakan attacking untuk penetrasi ke jaringan WLAN. Pengujian dilakukan dengan menggunakan pengujian serangan WPS aktif, bypassing MAC address, ARP spoofing, dan cracking the encryption.

1) Pengujian Serangan WPS Aktif dengan menggunakan *tools Dumper* dan *Jumpstart*
Pada pengujian ini dilakukan scanning WPS untuk mengetahui jaringan wireless WPS yang aktif. Jaringan wireless yang terdeteksi WPS aktif dapat dilakukan proses jumpstart untuk menyerang jaringan wireless. Berikut adalah tampilan scanning WPS yang aktif dengan menggunakan tools Dumper.



Gambar 4. Scanning WPS Aktif

Setelah proses scanning WPS telah dilaksanakan, maka langkah selanjutnya untuk pengujian serangan WPS aktif adalah dengan melakukan proses Jumpstart. Keberhasilan proses jumpstart ke jaringan wireless tersebut antara lain dipengaruhi oleh tingkat enkripsi pada access point dan stabilitas jaringan pada saat dilakukan penyerangan. Jaringan wireless akan bisa diserang menggunakan dumper dan jumpstart jika hanya memiliki tipe auntentifikasi WPA_PSK dan WPS_PSK dan tipe enkripsi TKIP. Tipe-tipe tersebut dijumpai pada access point atau router model lama, Sedangkan model baru memiliki tipe auntentifikasi minimal WPA2_PSK dan tipe enkripsi AES, sehingga sangat sulit diserang menggunakan dumper dan jumpstart. Kegagalan proses penyerangan tersebut dapat dilihat pada gambar dibawah ini.

Gambar 5. Uji Keamanan Jumpstart

Setelah dilakukan proses Jumpstart pada jaringan Wireless Local Area Network (WLAN) dan hasilnya adalah gagal, dikarenakan security jaringan sudah cukup aman sehingga tidak bisa tembus oleh jumpstart.

2) ARP *Spoofing* dengan menggunakan *tools Netcut*.
Pengujian ini dilakukan untuk mengetahui apakah pengguna yang sedang terhubung pada jaringan Wireless Local Area Network (WLAN) aman atau tidak. Aplikasi netcut digunakan untuk melihat pengguna yang terhubung pada jaringan Wireless Local Area Network (WLAN), selanjutnya dilakukan proses scanning, dan serangan ke salah satu pengguna dengan cara mematikannya (OFF). Setelah proses scanning dilakukan dengan menggunakan Netcut, maka penulis akan mengetahui berapa jumlah device yang terhubung dengan jaringan WLAN, setelah itu penulis bisa memutuskan koneksi jaringan dengan cara drag and drop data device tersebut ke kolom jail. Berikut adalah salah satu simulasi jaringan yang dibuat terputus koneksi WLAN.

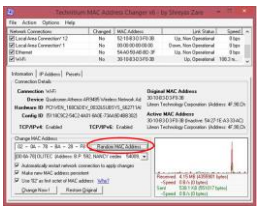
Gambar 6. Hasil Scanning & Proses Shutdown Koneksi

Apabila salah satu device sudah di off jaringan nya, maka user tersebut tetap terhubung dalam jaringan tersebut akan tetapi tidak dapat akses internet.

Gambar 7. Hasil Shutdown Koneksi Client

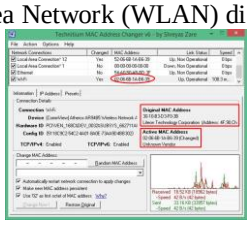
Gambar diatas adalah pembuktian bahwa jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik dapat diserang dengan ARP Spoofing. Sehingga salah satu user tetap terhubung kedalam jaringan akan tetapi tidak bisa melakukan akses internet pada jaringan tersebut.

3) *Bypassing MAC Address* dengan menggunakan *tools T-MAC*
Pada pengujian ini dilakukan perubahan nilai network address pada wireless adapter menggunakan MAC address tujuan yang akan digunakan untuk mengakses jaringan Wireless Local Area Network (WLAN). Pada pengujian ini penggunaan MAC address dapat dirubah dengan T-MAC.



Gambar 8. Hasil Scanning & Change Mac Address

Penulis telah memilih Network Connetion yang akan dirubah MAC Address nya. Setelah dipilih Wi-Fi sebagai Network Connection nya maka akan terlihat informasi Original MAC Address. Random MAC Address akan bekerja dengan mengacak pada MAC Address original. Kemudian penulis mencoba mengganti Mac Address yang sekarang dengan Mac Address Palsu dan berhasil masuk ke jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik.



Gambar 7. Mac Address Original dan Palsu

4) *Cracking the encryption* dengan menggunakan *tools aircrack-ng*
WPA dan WPA2 mempunyai *initial vector* yang berubah-ubah sehingga tidak ada gunanya mengumpulkan paket data sebanyak-banyaknya seperti pada *WEP* untuk melakukan mendapatkan keys yang digunakan. Hacking dengan cara ini membutuhkan waktu yang sangat lama sehingga metode yang paling memungkinkan adalah brute force berdasarkan dictionary file. Brute force membutuhkan sebuah file yang berisi passphrase yang akan dicoba satu persatu dengan paket handshake untuk mencari *keys* yang digunakan. Penetrasi yang dilakukan pada pengujian ini menggunakan *tools aircrack-ng* dan setelah proses penetrasi dilakukan berulangkali didapatkan hasil keamanannya telah aman dan tidak bisa ditembus dengan teknik ini.

I. Hasil Pengujian

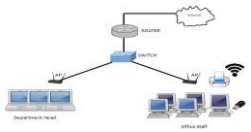
Dari seluruh tahap pengujian yang telah dilakukan, maka penulis dapat menyampaikan hasil dari Penetration Testing Execution Standard pada jaringan Wireless Local Area Network (WLAN) yang dilakukan pada PT. Win Prima Logistik. Berikut adalah laporan dari hasil pengujian keamanan :

Tabel 9. Hasil dari pengujian *Penetration Testing Execution Standard*

Jenis Serangan	Informasi yang dibutuhkan	Tools	Status Serangan
Serangan WPS Aktif	Tipe autentifikasi *access point*	Dumper, Jumpstart	Gagal
Bypassing MAC *Address*	*List* MAC *User* lain yang terhubung di jaringan	T-MAC	Berhasil
ARP *Spoofing*	IP *user*, MAC *address*	Netcut	Berhasil
Cracking the encryition	*Dictionary Word*, *handshake user* lain, *Channel* yang digunakan dan BSSID dari *access point*	Aircrack-ng	Gagal

Analisisis Keamanan Yang Diusulkan

Setelah dilakukan pengujian celah keamanan jaringan degan metode Penetration TestingExecution Standardpada jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik, maka penulis memberikan usulan untuk infrastruktur keamanan jaringan yang lebih baik. Berikut adalah bagan dari keamanan WLAN infrastruktur yang diusulkan oleh penulis kepada PT. Win Prima Logistik.



Gambar 5. WLAN Infrastruktur yang diusulkan

Pada Gambar diatas terlihat bahwa penulis mengusulkan untuk perancangan keamanan jaringan yang diusulkan kepada PT. Win Prima Logistik adalah dengan menambahkan 1 buah router, 1 buah switch dan 1 buah access point dari infrastruktur sebelumnya.

Penulis mengusulkan router dalam perancangan infrastruktur yang baru, agar dapat membuat access list dengan cara mendaftarkan IP address dan MAC address setiap user kedalam jaringan Wireless Local Area Network (WLAN) di PT. Win Prima Logistik, hal ini bertujuan agar tidak sembarangan orang bisa mengakses jaringan tersebut dan juga mencegah terjadinya bypassing MAC address.

Serta menambahkan 1 buah switch agar bisa menghubungkan 2 access point ke dalam 1 router. Access point pertama khusus untuk department head dan access point kedua khusus untuk office staff. Hal ini dibuat agar komunikasi data dapat dibatasi antara staff karyawan dan setingkat manager sampai direktur.

Hal lain yang dapat dilakukan untuk meningkatkan keamanan jaringan Wireless Local Area Network (WLAN) pada PT. Win Prima Logistik perlu diaktifkan fitur ARP atau binding pada access point atau router agar terhindar dari serangan spoofing seperti nmap, netcut, dan lain-lain, sehingga pengguna menjadi aman dalam menggunakan jaringan WLAN tanpa diganggu oleh pengguna lainnya.

II. Kesimpulan

a. Berdasarkan hasil pengujian yang telah dilakukan menunjukkan bahwa keamanan jaringan Wireless Local Area Network (WLAN) pada PT. Win Prima Logistik sudah cukup aman, karena access point atau router jaringan Wireless Local Area Network (WLAN) yang tersedia sudah menerapkan sistem keamanan setingkat WPA/WPA2-PSK.
b. Celah keamanan yang ditemukan adalah ada pada pengguna yang sedang menggunakan jaringan Wireless Local Area Network (WLAN) masih bisa diserang menggunakan teknik serangan bypassing MAC Address dan ARP Spoofing.

Daftar Pustaka

Bayu, Imam Kreshna, dkk. 2017. Analisa Keamanan Jaringan WLAN dengan Metode Penetration Testing. ISSN 2502-8928 Vol.3 No.2.

Hidayat, Sidiq Syamsul, dkk. 2013. Wireless Hacking Tools & Tricks. Yogyakarta: Graha ilmu.

Manuaba Ida Bagus Verry Hendrawan, dkk. 2012. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel. ISSN 2301 – 415613. JNTETI, Vol. 1, No. 1.

Mentang, Randy, dkk. 2015. Perancangan dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. E-journal Teknik Elektro dan Komputer, Volume 5, No.7: ISSN:2301-8402.

Pujiarto, Bambang, dkk. 2013. Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing. ISSN 1411-3201, Vol. 14 No.2.

Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan. 2015. Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra.