e-ISSN 2962-6129
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 Agustus 2022

Pengujian Celah Keamanan Untuk Mengetahui Kerentanan Keamanan Jaringan *Wireless* Dengan *Metode Penetration Testing Execution Standard* (PTES) Pada PT. QWE

Rulli Azani Akbar [1], Henki Bayu Seta [2], Jayanta[3]
Program Studi Informatika, Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya No.1, Pd. Labu, Kec. Cilandak, Jakarta Selatan 12450
rulliaa@upnvj.ac.id, henkiseta@upnvj.ac.id

Abstrak. Keamanan jaringan *wireless* diperlukan demi untuk perlindungan serta pencegahan dari tindakan kejahatan pencurian informasi. Aspek tersebut sering diabaikan pada setiap instansi karena menganggap bahwa jaringan *wireless* selalu dianggap aman karena bagi setiap instansi akan merasa aman jika permasalahan tersebut belum mengganggu aktivitas pekerjaan dengan memasang *antivirus* maupun *firewall*. Masih banyak instansi yang meremehkan soal ini. Sehingga, perlu dilakukan *penetration testing* untuk mengetahui kerentanan pada jaringan *wireless* dengan metode yang digunakan PTES (*Penetration Testing Execution Standard*) untuk dijadikan standar dalam melakukan analisis sistem keamanan jaringan *wireless* dalam mencari celah keamanan pada sebuah instansi dalam kasus ini yaitu jaringan *wireless local area network* (WLAN) pada PT. Sehat Tentrem dimana pada penelitian ini ditemukan kerentanan berupa *bypassing,, arp spoofing, certificate cannot be trusted,* dan adanya kegiatan *sniffing* yang dapat dilakukan pada jaringan *wireless* untuk *dieksploitasi*.

Kata Kunci: Keamanan Jaringan, *Vulnerability Analysis*, *Penetration Testing*, *Penetration Testing Execution Standard*, *sniffing*, *arp spoofing.*

1. PENDAHULUAN

Dengan adanya perkembangan teknologi pada saat ini, internet sudah menjadi suatu kebutuhan untuk saat ini. Dapat kita lihat dengan aktivitas sehari-hari yang kita lakukan selalu menggunakan internet sebagai alat penunjang kebutuhan. Seperti hal yang kita lakukan layaknya komunikasi, mencari sebuah informasi, transaksi digital, dan bahkan untuk mencari sebuah hiburan untuk saat ini selalu menggunakan internet sebagai alat bantu. Oleh karena itu, adanya perlindungan informasi melalui pendekatan yang baik dan terstruktur yang dilakukan untuk menghindari risiko yang timbul. alasan pemilihan pengujian celah keamanan jaringan wireless dengan metode PNTS karena banyaknya sebuah PT yang tidak memperdulikan soal keamanan jaringan itu sendiri yang dimana hanya mengandalkan sebuah aplikasi atau antivirus yang dianggap sudah cukup aman dari serangan para siber. Akan tetapi kenyataan yang ada jauh berbeda, yang dimana banyak data yang sangat penting dan perlu untuk di rahasiakan yang juga melibatkan tiga alasan pentingnya keamanan sistem informasi yang dikenal sebagai *CIS Triad yaitu Confidentiality* (Kerahasiaan), *Integrity* (Integritas), *Availability* (Ketersediaan).

.

Pada penelitian sebelumnya [1] juga telah melakukan analisis keamanan system informasi untuk mengetahui kerentanan keamanan *Server* dengan metode *penetration testing execution standard* (PTES) pada Universitas VWX dengan berbagaimacam *tools* yang digunakan seperti *nmap*, *wohis*, dan *metropolitan framework*. Yang di mana kerentanan yang ditemukan terdapat pada keamanan *server* yang kurang baik dengan melakukan serangan *sniffing*, dan *post guesting*.

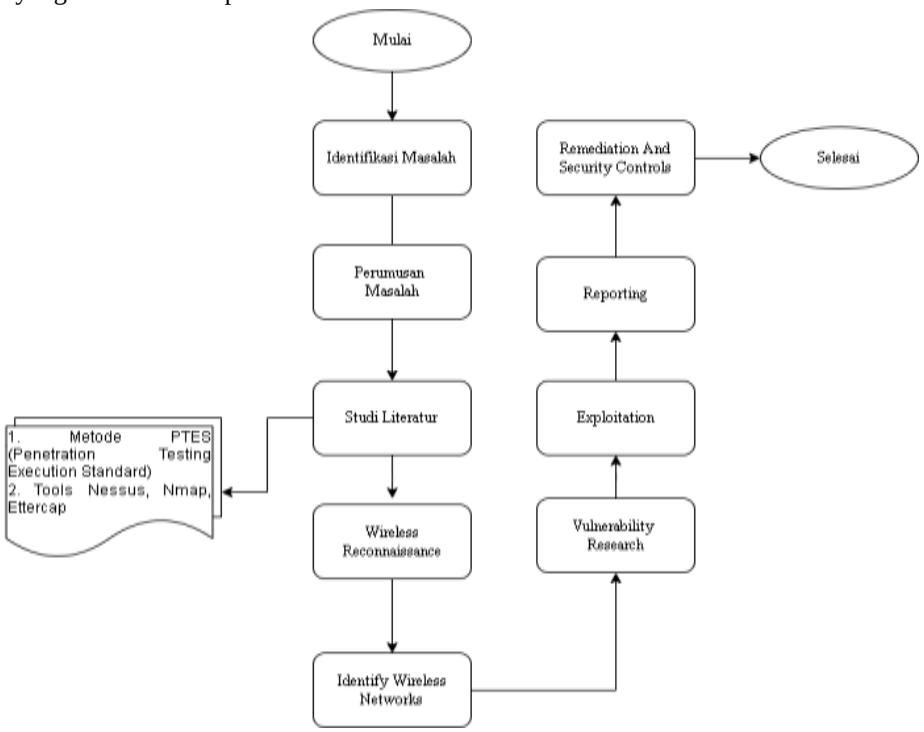
Kemudian penelitian terkait menemukan celah keamanan juga pernah dilakukan sebelumnya [2] pada jaringan *wireless* dengan menggunakan metode *penetration testing* yang dimana mendapatkan hasil yaitu Berdasarkan pengujian kerentanan yang dilakukan yaitu pengujian keamanan jaringan *wireless wardriving* menggunakan metode Penetration Testing pada PT. Puma Makmur Aneka *Engineering*, maka dapat diambil kesimpulan bahwa pengujian keamanan jaringan internal dan publik telah dilakukan dengan menggunakan metode *Penetration Testing* dan mendapatkan kerentanan seperti WPA2 Cracking, Dos,Paswword Router Wireless Cracking, dan AP Isolation Testing sehingga diketahui kerentanan pada jaringan internal dan publik.

Lalu penelitian berlanjut dengan menganalisis celah keamanan pada jaringan *wireless* yang dimana focus dalam penelitian ini hanya dari serangan *packet sniffing* yang dimana *tools* yang digunakan pada penelitian ini adalah *Ettercap*. Dan medapatkan kerentanan yang dimana berhasil menyadap percakap dua arah atau dapat disebut dengan MITM (*man in the midel*) dan mendapatkan informasi berupa *username* dan *password* [3].

Oleh karena itu, pada penelitian kali ini akan melakukan pengecekan celah keamanan jaringan *wireless* untuk mengetahui kerentanan jaringan *wireless* dengan melakukan *Penetration Testing ExecutionStandard* (PTES) dengan studi kasus pada PT.QWE yang merupakan salah satu perusahaan yang akan dijadikan target pengujian celah keamanan. Pengujian dilakukan dengan menggunakan jaringan yang ada pada PT. QWE untuk mengetahui kerentanan apa saja yang ada.

2. TINJAUAN PUSTAKA

Dalam mencapai tujuan penelitian, terdapat tahapan-tahapan PTES (*Penetration Testing ExecutionStandard*) yang perlu dilakukan yang diilustrasikan pada Gambar 1.



Gambar. 1. Tahapan Penelitian

2.1 Identifikasi Masalah

Pada tahapan pertama ini yang pertama kali dilakukan adalah mencari permasalahan yang berhubungan dengan topik yang akan diteliti. Dilakukan pencarian beragam ide yang baru untuk memetakan dan memecahkan masalah yang ditemukan pada tahap ini. Pada penelitian ini, ternyata ditemukan berbagai masalah yang cukup banyak dan membahayakan pada PT. QWE yang berada pada satu jaringan. Dapat dilihat dari banyaknya pencurian data yang dapat di akses oleh pata siber yang marak pada saat ini. Dan juga kurangnya SDM yang memadai untuk melakukan evaluasi keamanan secara berkala pada jaringan wireless

.

2.2 Perumusan Masalah

Tahapan perumusan masalah adalah tahapan dimana penelitian telah disusun tahapan masalahnya pada bagian tahapan identifikasi masalah. Rumusan masalah pada penelitian kali ini adalah pengujian celah keamanan pada jaringan wireless untuk membantu sebuah dalam meningkatkan dan memperbarui sistem jaringan wirelessStudi Literatur

2.3 Studi Literatur

Dalam penelitian ini, literatur digunakan sebagai sumber pustaka, dengan jurnal, e-book, dan buku-buku yang berkaitan dengan isu-isu seperti jaringan, serangan, *sniffing*, *kali linux*, dan metode *ManinTheMiddle* dibahas selama penelitian. Pembahasan ini dikarenakan dengan pengumpulan berbagai macam literatur, jurnal, website, dan e-book untuk penelitian. Setelah menyelesaikan langkah-langkah ini, studi pustaka ditetapkan sebagai referensi untuk menyelesaikan masalah yang dihadapi.

2.4 *Wireless Reconnaissance*

Tahapan ini dilakukan untuk mengumpulkan informasi yang akan menjadi acuan dalam melakukan penetrasi, dengan melakukan komunikasi dengan kepala PT. QWE mengenai tujuan dari penelitian, menentukan scope dan pertanyaan mengenai gambaran umum jaringan. Penelitian ini juga dikonsultasikan kepada PT. QWE agar nanti penelitian ini tidak merugikan pihak manapun dan tidak dianggap sebagai kegiatan yang melanggar hukum[4].

2.5 *Identify Wireless Networks*

Pada tahapan ini pentester akan mengumpulkan informasi sebanyak mungkin mengenai perusahaan target yang dapat dengan berbagai macam metode dan berbagai media. Identify wireless networks pada penelitian ini bertujuan pada jaringan wireless[4].

2.6 Vulnerability Analysis

Tahapan dimana penelitian ini mencampurkan informasi mengenai celah keamanan yang telah ditemukan dengan metode serangan yang biasa dilakukan untuk melakukan serangan yang paling efektif. Tujuan melakukan vulnerability analysis untuk menemukan sebuah kekurangan yang ada di dalam jaringan wireless yang dapat dimanfaatkan oleh penyerang[4].

2.7 *Exploitation*

Tahap ini melakukan serangan kepada kerentanan yang telah ditemukan sekaligus mengetes apakah kerentanan tersebut dapat di exploitation. Peneliti (pentester) akan melakukan eksploitasi berdasarkan pada ancaman yang dapat terjadi dan kerentanan yang didapat dalam melakukan analisis sehingga model serangan yang akan dilakukan dapat memenuhi tujuan dalam penelitian ini. Peneliti juga ingin membuktikan apakah kerentanan yang didapatkan dapat berpotensi sebagai serangan, akan tetapi ada kemungkinan tidak terduga yang membuat hasil eksploitasi tidak sesuai dengan apa yang diharapkan. Serangan oleh peneliti juga dibantu oleh tools Ettercap, Nmap, Nesus [4].

2.8 *Reporting*

Pada tahapan ini peneliti membuat laporan tertulis yang berisi hasil dari seluruh penelitian yang telah dilakukan mulai dari awal sampai akhir dimana penelitian ini menggunakan metode Penetration Testing Execution Standard (PNTS) sehingga diharapkan untuk mudah dan dapat dipahami. Passtester juga akan memberitahu pada target PT. QWE mengenai proses pengujian yang dilakukan seperti: bagaimana cara melakukannya, apa yang sudah dilakukan, resiko yang didapat, Dan cara mengatasi [4].

2.9 *Nessus*

Nessus merupakan alat pemindai keamanan yang dimana jika menemukan kerentanan yang dapat digunakan oleh penyerang untuk mendapatkan akses computer manapun yang telah terhubung kedalam sebuah jaringan akan menimbulkan sebuah peringatan. Nessus juga berfungsi untuk security scanner yang akan mengaudit jaringan-jaringan yang dituju lalu akan mendapatkan kelemahan – kelemahannya Nmap[5].

2.10 *Ettercap*

Ettercap adalah untuk menganalisis protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk mencegat lalu lintas pada jaringan, menangkap sandi, dan melakukan tindakan aktif terhadap protokol umum. Dalam putaran penelitian ini, saya menggunakan ARP Spoofing untuk mencari tahu apa yang terjadi dengan pengguna saat mereka mengumpulkan informasi[6].

2.11 *Nmap*

Network Mapper atau yang sering kita kenal dengan istilah NMAP adalah sebuah tool yang bersifat open source. Yang dimana alat ini digunakan untuk eksplorasi jaringan serta melakukan audit terhadap keamanan jaringan. Untuk menemukan sebuah host yang aktif dalam suatu jaringan, Nmap membutuhkan IP dalam menjalankan prosesnya. Hal penting di antara informasi itu adalah table port yang berisi daftar angka port beserta protokolnya, nama, layanan, dan status[7].

2.11 *Metasploit framework*

Metasploit Framework adalah tools untuk keperluan penetration testing yang dikembangkan untuk memberikan informasi tentang suatu kerentanan terhadap suatu sistem. Metasploit bersifat open source yang bertujuan untuk menyediakan sumber daya pengembangan dan riset kode exploit. Dalam awal pengembangannya Metasploit dikembangkan menggunakan dalam bahasa Perl namun pada akhir tahun 2007 semua source codenya ditulis ulang menggunakan bahasa Ruby[5]

3. HASIL DAN PEMBAHASAN

3.1 *Wireless Reconnaissance*

Pada tahap pertama ini, kegiatan penetration testing dilakukan dengan mempersiapkan peralatan atau tools dan Teknik yang akan digunakan, dari pertanyaan yang telah diajukan sebelumnya mengenai pertanyaan serta interaksi dan

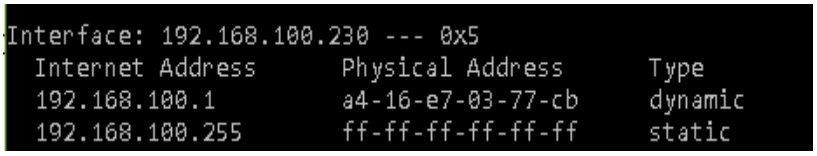
wawancara pada PT. QWE dengan system terkait mengenai Jaringan Wireless. Tools yang digunakan antara lain yaitu Nmap, Whois, Nessus, Dan Ettercap. Untuk Teknik yang dimana akan melakukan split yaitu sniffing, Arp Spoofing, dan Scanning Service yang akan peneliti uji menggunakan jaringan wireless internal yang artinya penguji akan menggunakan jaringan secara langsung pada PT. QWE.

3.2 *Identify Wireless Network*

Pencarian informasi dilakukan mulai dari jaringan wireless yang nantinya akan dideteksi oleh target dan target akan mengartikannya sebagai kegiatan yang mencurigakan atau berbahaya. Dalam melakukan identify untuk mengetahui port mana yang terbuka pada jaringan, dan service yang berjalan pada port, serta sistem operasi yang digunakan. Ada beberapa tahapan yang dilakukan sebagai berikut:

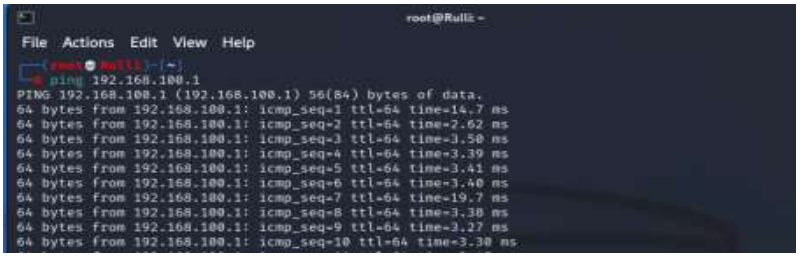
3.2.1 Internal Footprinting

Pertama kali akan melakukan perintah untuk mencari tahu tentang Ip address jaringan wireless yang ada pada perusahaan.



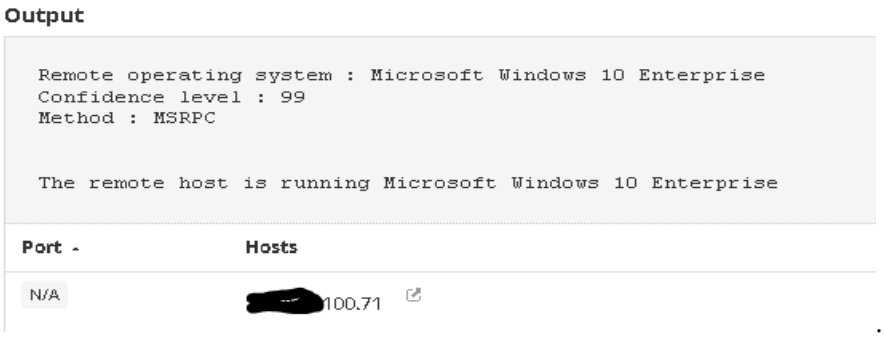
Gambar. 2. Mencari Ip *addres*

Setelah mengetahui gambar yang ada diatas lalu akan melakukan perintah ping (packet Internet Groper) di Kali Linux ke target terhadap 192.168.100.1 yang bermaksud untuk mengetahui ICMP (Internet Control Message Protocol) dan mendeteksi host target online atau up pada jaringan atau tidak



Gambar. 3. Ping Target

Pada informasi gambar 4.2 menunjukan perangkat pentester sudah terhubung dengan jaringan Ip target. Ip pentest mengirim banyak pesan ICMP atau pesan echo request ke target dan menunggu pesan echo respon dari host ke perangkat pentester



Gambar. 4. *Nessus Scanning Port*

dapat kita lihat hasil dari scan os yang digunakan ip xxx.xxx.100.1 yaitu Microsoft windows 10 enterprise dengean metohod MSRPC.

3.3 *Vulnerability Analysis*

Nessus dibuat untuk memeriksa celah keamanan jaringan dari kecil sampai besar dengan cepat serta dapat digunakan untuk host tunggal, host tunggal adalah host yang hanya berisi 1 alamat IP.

Gambar 5. *Nessus Scanning Vulnerability*

Gambar 5 merupakan jenis kerentanan yang ada saat melakukan pencarian melalui *nessus*

3.4 *Exploitation*

Exploitation disini melakukan pengecekan kerentanan yang telah didapat setelah melakukan vulnerability berdasarkan ancaman yang mungkin terjadi pada jaringan wireless pada PT. QWE menggunakan berbagai macam tools yang akan digunakan. Berikut merupakan proses eksploitasi yang akan dilakukan berdasarkan kerentanan yang sudah ditemukan melalui vulnerability yang telah ditemukan dimana terdapat 5 kerentanan yang ditemukan dan akan dilakukan menggunakan Teknik yang berbeda-beda.

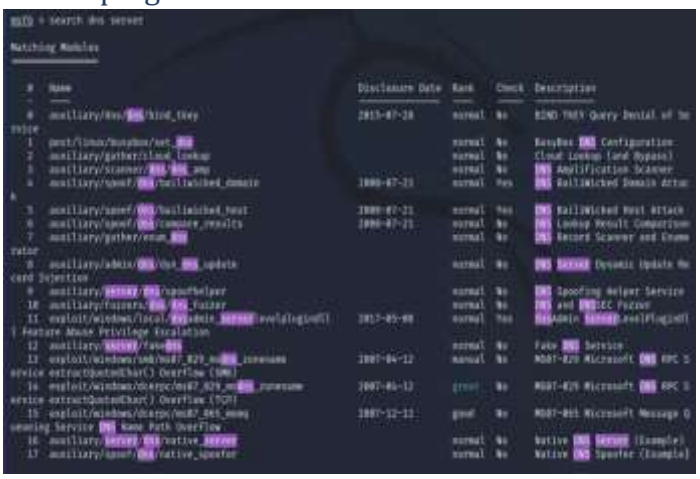
3.4.1 SSL Certificate Cannot Be Trusted

Kerentanan ini didapatkan dari scanning vulnerability yang dilakukan dengan bantuan aplikasi Nessus dimana terdapat kerentanan pada sertifikat SSL. Sertifikat SSL yang tidak dapat dipercaya tersebut dapat dimanfaatkan oleh attacker untuk melakukan penyerangan dikarenakan sudah sertifikat yang sudah tidak lagi aman.

Gambar 6. Indormasi Dari *Cert*

Dalam informasi yang terdapat pada gambar 6 yang menjelaskan tentang sebuah kondisi sertifikat yang ada pada kerentanan tersebut. Gambar 6 juga mendeskripsikan bahwa sertifikat yang ditentukan untuk memastikan subjek dan penerbit cocok dengan pola yang diberikan dan sertifikat dapat dipercaya

3.4.2 DNS Server Cache Snooping Remote Information Disclosure



Gambar 7. Daftar Modul DNS

Setelah melihat deskripsi yang ada pada gambar 4.13 tidak ada kerentanan dengan nama *DNS Server Cache Snooping Remote Information Disclosure* yang artinya kerentanan tersebut tidak menyebabkan adanya serangan

4.4.3 TLS Version 1.1 Protocol Detection

Gambar 8. *SSL Scanning*

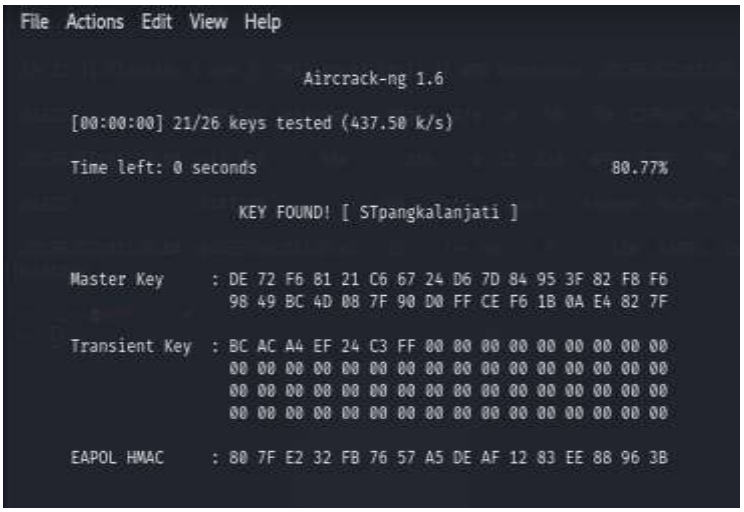
Perintah sslscan tersebut akan memproses audit pada SSL untuk mengetahui adanya kesalahan konfigurasi yang dapat mempengaruhi SSL. Hasil dari gambar 8 dibawah menyatakan bahwa tidak ada kerentanan yang dapat dimanfaatkan oleh para attacker

4.4.4 SSL/TLS Certificate Know Hard Coded Private Key

Jenis kerentanan yang ditemukan dalam pencarian *Vulnerability* yang dilakukan menggunakan *tools nessus* ini memungkinkan terjadinya serangan berupa *Cracking the encryption*, ARP Spoofing, *Sniffing*, dan *Bypassing MAC Addres*

1. *Cracking The Encrypsyion*

Serangan ini bertujuan untuk mengetahui seberapa aman jaringan WLAN yang ada pada PT. QWE dengan menggunakan jenis keamanan WPA2-PSK dengan menggunakan *tools aircrack-ng* dan metode *Brute force* yang berdasarkan dictionary fileThreat Modelling



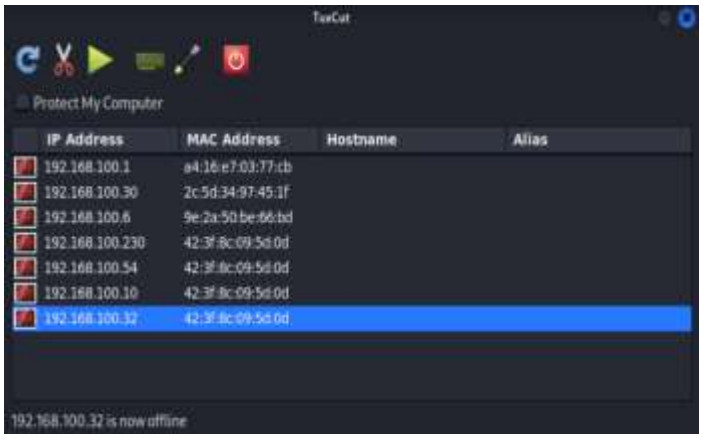
Gambar 9. Hasil Dari *Cracking The Encrypsyion*

Dan setelah melakukan percobaan maka penulis memperoleh *password access point* yang terdapat pada PT. QWE

yaitu “STpangkalanjati”. Yang artinya keamanan pada PT. QWE masih belum aman karena memiliki celah di keamanan access point yang dapat di hack dengan menggunakan tools *aircrack-ng*

2. ARP Spoofing

kerentanan ini memungkinkan penyerang bias mengetahui frame data pada jaringan lokal dan memungkinkan melakukan modifikasi lalu lintas atau bahkan melarangnya. Prinsip serangan ARP spoofing adalah memanfaatkan kelemahan pada teknologi jaringan komputer yang menggunakan ARP broadcast.

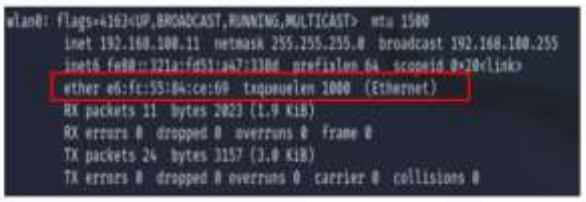


Gambar 10. Proses *ARP Spoofing*

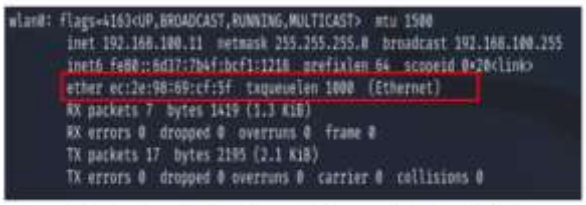
Pada gambar 10 dapat dilihat gambar yang dulunya berwarna biru menjadi warna merah dan memiliki keterangan *offline* yang artinya *user* seolah-olah tetap terhubung ke dalam jaringan tetapi tidak dapat mengakses semua koneksi yang ada dan tidak dapat *online* atau berkomunikasi dengan internet**.**

3. Bypassing Mac Address

Disini peneliti akan menggunakan *Bypassing Mac addres* untuk mengubah identitas MAC untuk melihat kerentanan MAC *address filtering*. Pengujian kali ini melakukan pengubahan nilai network address pada wireless adapter menggunakan MAC address tujuan yang akan digunakan untuk mengakses jaringan Wireless Local Area Network (WLAN). Dalam hal ini, alamat MAC dapat diubah dengan bantuan Macchanger



Gambar 4.33 Mac *address* sebelum diubah



Gambar 4. 34 Mac Address setelah diubah

Gambar 11. Hasil *Bypassing Mac Address*

Pada gambar 11 dapat dilihat perubahan yang ada pada *Mac Address* yang dimana pada gambar yang pertama memiliki *Mac Address ether* e6:fc:55:84:ce:69 dan gambar yang bawahnya memiliki *Mac address* baru yang telah peneliti lakukan perubahan untuk mengecek kerentanan yang ada menjadi *Mac Address ether* ec:2e:98:69:cf:5f

4. Sniffing

Sniffing pada penelitian ini hanya ingin mengetes keamanan pada jaringan *wireless* tanpa mengubah paket data yang sudah ada

Gambar 12. Hasil *Sniffing* Dengan *tools Ettercap*

Hasil yang didapat setelah melakukan proses *sniffing* dengan Ettercap adalah dimana hanya dapat mencapture *username* saja

Gambar 13. Hasil *Sniffing* dengan *tools KeyLoger*

Hasil dari *sniffing* menggunakan *tools keyloger* dapat mengcaptuer semua percakapan yang di akses melalui *keyboard*

4.5 Reporting

Pada bagian *Reporting* ini akan menjelaskan hasil dari percobaan *Penetration Testing* yang telah dilakukan dari mulai tahap *Wireless Reconnaissance* sampai tahap *Exploitation*. Di temukan serangan yang dapat membahayakan jaringan *Wireless Area Network* (WLAN) yang dapat dimanfaatkan untuk mencuri informasi yang penting diantar serangan tersebut berupa *Sniffing* atau yang dapat dikenal dengan *Man In The Middle* (MITM), *Cracking The Encryption* yang dapat menyebabkan kebobolan pada password wifi dengan jenis keamanan WPA2-PSK, dan ARP Spoofing yang dapat mematikan semua jaringan *wireless* yang sedang *online* menjadi *offline*. untuk memperjelasnya berikut adalah laporan dari hasil pengujian keamanan:

Tabel 1. Laporan Hasil *Penetration Testing*

No	Jenis Kerentanan	Port	Severity	CVSS	Hasil Eksploitasi	Tools
1	*SSL/TLS Certificate Known Hard Coded Private Key*	3744	*High*	7.5	*False Positive*	Aircrack-ng
2	*SSL Certificate Cannot Be Trusted*	80	*Medium*	6.5	*False Positive*	*Metasploit Framework*
3	*TLS Version 1.1 Protocol Deprecated*	80	*Medium*	6.5	*False Positive*	*Scan SSL*

4	*DNS Server Cache Snooping Remote Information Disclosure*	53	*Mediu m*	5.3	*False Negative*	*Metasploit Framework*
5	*Cracking the encryption*	67	*High*	8.2	*True Negative*	*Aircrack-ng*
6	*ARP Spoofing*	53	*High*	7.1	*True Negative*	*TuxCut*
7	*Sniffing*	3344	*High*	8.2	*True Negative*	*Keyloger Ettercap*
8	*Bypassing MAC Address*	3744	*High*	9.3	*True Negative*	*Macchanger*

4.6 Remediation And Security Controls

Dari hasil eksploitasi tersebut yang dapat dilihat pada tabel 1 dapat kita buat kesimpulan bahwa masih terdapat beberapa kerentanan yang dapat menimbulkan serangan pada jaringan *Wireless Area Network* (WLAN) dengan demikian ada usulan yang akan penulis buat diantaranya adalah:

4.6.1 Ususlan Sistem

Menurut Mahendro (2016) ada beberapa tips yang mungkin berguna untuk mengamankan jaringan *Wireless Local Area Network* (WLAN), berdasarkan penelitian yang telah dilakukan dan terbukti dapat mengamankan keamanan jaringan diantarnya yaitu :

1. *IP Spoofing*
    a. Mencegah web *spoofing*
        - Tidak mengaktifkan Javascrip pada browser sehingga penyerang tidak dapat menyembunyikan petunjuk atau bukti dari adanya penyerangan
        - Memastikan bahwa *location line* dari browser selalu tampak

    b. Pencegahan DNS *Spoofing*
        - DNS spoofing dapat diatasi dengan mendisable recursive query ke name server dengan membuat split DNS yaitu membuat dua name server. Name server utama digunakan untuk menangani domain name dari public domain, sedangkan name server kedua di yang berada di internal network bertugas sebagai cache name server yang bertugas menjawab query dari user yang merequest domain tersebut.

    c. ARP *Spoofing*
        - Melakukan pengecekan MAC Address dengan menggunakan tools Colasoft MAC Scanner.
        - Scan network ,jika terdapat 2 buah IP Address yang sama dengan Gateway putus client tersebut dari jaringan kemudian scan Virus denggn menggunakan antivirus yang Up-to-date virus databasenya.
        - Setelah dilakukan virus scanning, dilakukan langkah penutup ini,buka Command prom kemudian ketik : arp –s ip_address_gateway mac_address_gateway lalu tekan tombol Enter

2. *Sniffing*
    Solusi pencegahan dari serangan ini adalah dengan cara (Martin & Jasri 2021). :
    a. Menghindari koneksi WiFi yang tidak dilindungi oleh kata sandi.
    b. Tidak mengakses informasi sensitif ketika menggunakan WiFi publik.
    c. Hanya mengakses website dengan protokol HTTPS.
    d. Menggunakan VPN (Virtual Private Network). VPN akan mengenkripsi lalu lintas website untuk membatasi kemampuan penyerang untuk membaca atau memodifikasi komunikasi yang sedang Anda lakukan.
    e. Pastikan server DNS (cache DNS) yang Anda gunakan aman
3. *Cracking The Encryption*

Dari percobaan Cracking the Encryption dapat ditarik kesimpulan bahwa untuk meningkatkan ketahanan dari password terhadap upaya cracking, maka ada beberapa hal yang harus dilakukan, diantaranya :

a. Menggunakan jenis keamanan enkripsi WPA, WPA2, WPA-PSK, atau WPA2-PSK yang memiliki tingkat keamanan di atas WEP.
b. Menggunakan kombinasi dari huruf besar, huruf kecil, angka dan simbol dalam membuat password, untuk mempersulit serangan baik dengan jenis brute-force attack maupun dictionary.
c. Membuat password dengan panjang di atas 15 karakter, untuk mempersulit serangan baik dengan metode brute-force attack maupun dictionary.

4. *Baypass MAC Authentication*
   a. Mengaktifkan fasiltas sistem keamanan MAC filtering yang ada di wireless access point ataupun router, dengan memanfaatkan ”ingress dan engress filtering” pada router merupakan langkah pertama dalam mempertahankan diri dari spoofing. Kita dapat memanfaatkan ACL (acces control list) untuk memblok alamat IP privat di dalam jaringan untuk downstream. Dilakukan dengan cara mengkonfigurasi router agar menahan paket-paket yang datang dengan alamat sumber paket yang tidak legal (illegitimate).
   b. Enkripsi dan Authentifikasi, kita juga dapat mengatasi IP spoofing dengan mengimplementasi kan authentifikasi dan enkripsi data. Kedua fitur ini sudah digunakan pada Ipv6. Selanjutnya kita harus mengeliminasi semua authentikasi berdasarkan host, yang di gunakan pada komputer dengan subnet yang sama.

4. PENUTUP

4.1 KESIMPULAN

Berdasarkan hasil pengujian penetrasi yang dilakukan dengan menggunakan metode PTES (Penetration Testing Execution Standard), antara lain teknik exploiting, scanning, nmap, sniffing, arp spoofing, dan cracking enkripsi. Sebagai hasil dari ini, dapat disimpulkan bahwa:

1. Kerentanan yang harus diwaspada yang dapat diserang oleh *attacker* merupakan kerentanan *Cracking the encryption, Arp Spoofing, Sniffing, dan Bypassing Mac Address* yang memiliki tingkat kerentanan *sensitive data exposure High*
2. Dalam melakukan analisisi keamanan jaringan wireless pada PT. QWE dengan metode *Penetration Testing Execution Standard* (PTES). Dalam tahapan awal yang dimana melakukan beberapa tahapan yang pertama adalah *Wireless Reconnaissance*, *Identify Wireless Networks*, *Vulnerability Research*, *Exploitation*, *Reporting*, dan *Remediation And Security Controls*. Yang dimana disetiap tahap tersebut sudah dilakukan dalam penelitian ini seperti melakukan persiapan dalam melakukan penyerangan dengan menidetifikasi ada berapa jaringan dan jenis keamanan dari jaringan wireless tersebut, mengecek kerentanan yang ada pada jaringan wireless dengan tools *nessus*, melakukan serangan setelah menentukan jenis kerentanan dan menghasilkan apasaja jenis kerentanan yang ada pada jaringan tersebut yang mungkin dapat membahayakan sebuah PT.QWE
3. Hasil dari pengujian penetrasi yang dilakukan dengan serangan *Sniffing* terhadap jaringan *Wireless* PT. QWE yang dimana menghasilkan sebuah kerentanan yang dapat membahayakan PT. QWE tersebut. Yang dimana peneliti mendapatkan sebuah akses MITM (*Man In The Middel*) yang memiliki arti dimana kita dapat mendengarkan komunikasi dua arah yang dilakukan oleh korban dengan jenis serangan *Sniffing.*

4.2 SARAN

Berdasarkan uraian dari kesimpulan, maka kelebihan dan kekurangan diatas dapat menjadi pelajaran serta referensi untuk kedepannya. Saran-saran yang dapat dipertimbangkan untuk kedepannya antara lain :

1. Diperlukan pembagian jaringan agar dapat membedakan jaringan. yang nantinya apabila ada serangan tidak semua data dapat dicuri oleh *attacker*
2. Sebaiknya dilakukan penggantian *password* secara berkala untuk login untuk menghindari terjadinya penyusupan oleh pihak-pihak yang tidak bertanggung jawab.
3. Pengecekan jaringan secara berkala diperlukan untuk menghindari terjadinya permasalahan pada jaringan yang dapat menyebabkan kinerja jaringan menjadi lambat

5. REFERENSI

[1] Kusumarini, A. I. (2021). *Analisis Keamanan Sistem Informasi Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Penetration Testing Execution Standard (PTES) Pada Universitas VWX* (Doctoral dissertation, Universitas Pembangunan Nasional Veteran Jakarta).

[2] Suharmanto, A. Y., Lumenta, A. S., & Najoan, X. B. (2018). Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *13*(3).

[3] Kurniawan, T. A. (2020). ANALISA KEAMANAN JARINGAN WIFI TERHADAP SERANGAN PACKET SNIFFING. *Jurnal Ilmiah Fakultas Teknik LIMIT'S Vol*, *16*(2), 11.

[4] Purplesec.us. (2022, 18 Maret). How To Perform A Wireless Penetration Test. Diakses pada 10 juni 2022, dari https://purplesec.us/perform-wireless-penetration-test/

[5] Raj, S., & Walia, N. K. (2020, July). A study on metasploit framework: a pen-testing tool. In *2020 International Conference on Computational Performance Evaluation (ComPE)* (pp. 296-302). IEEE

[6] Fauzi, A. R. F., & Suartana, I. M. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. *Jurnal Manajemen Informatika*, *8*(2).

[7] Stiawan, D. (2005). *Sistem Keamanan Komputer*. Elex Media Komputin