Analisis Keamanan Jaringan *Wireless* menggunakan Metode *Penetration Testing* di SMK Xyz Tana Toraja

Gidion Aryo Nugraha Pongdatu[1*], Aryo Michael[2], Enohk Eightry Patalo[3]

[1*, 2, 3] Program Studi Teknik Informatika, Universitas Kristen Indonesia Toraja, Tana Toraja, Sulawesi Selatan
Email: [1*]dionpongdatu@ukitoraja.ac.id, [2] aryomichael@ukitoraja.ac.id, [3]enohkeightry@gmail.com

Abstrak

Perkembangan teknologi informasi pada era modern seperti sekarang ini memudahkan masyarakat untuk mengakses informasi dengan mudah melalui media internet. Salah satu teknologi yang digunakan untuk mengakses informasi adalah teknologi media transmisi nirkabel atau wireless. Teknologi wireless berkembang sangat pesat saat ini karena akses dan perawatannya lebih mudah dan fleksibel. Namun, akses mudah terhadap jaringan wireless memerlukan perhatian khusus pada segi keamanan data, terutama di dalam instansi atau lembaga. SMK Xyz Tana Toraja adalah salah satu instansi pendidikan yang menggunakan jaringan wireless sebagai fasilitas penunjang proses pembelajaran dan administrasi. Jaringan *wireless* yang digunakan oleh SMK Xyz Tana Toraja terhubung langsung ke server yang berisi data siswa, data guru dan pegawai, serta data keuangan. Oleh karena itu, keamanan pada jaringan wireless sangat penting untuk melindungi data dari ancaman dari luar. Metode yang digunakan untuk pengujian sistem keamanan jaringan Wireless LAN (WLAN) adalah dengan metode *penetration testing* yang dilakukan pada jaringan instansi terkait untuk menemukan kelemahan yang ada pada jaringan tersebut. Hasil dari pengujian penetration testing menunjukkan bahwa kualitas keamanan jaringan pada SMK Xyz Tana Toraja masih lemah. Hal ini tampak dari hasil pengujian jaringan wireless menggunakan metode *penetration testing*, seperti *sniffing* pada komputer target yang berhasil jika website yang diakses menggunakan protokol http, enkripsi yang digunakan pada *access point* yang masih dapat ditembus menggunakan *dictionary attack*. Oleh karena itu, perlu dilakukan peningkatan pada sistem keamanan jaringan wireless di SMK Xyz Tana Toraja untuk mengamankan data yang disimpan di dalamnya.
.

Kata Kunci: keamanan jaringan, *penetration test*, jaringan *wireless*.

Analysis of Wireless Network Security Using Penetration Testing Method at Vocational School of Xyz Tana Toraja

Abstract

The development of information technology in the modern era, such as today, has made it easier for people to access information through the internet. One of the technologies used to access information is wireless transmission media technology or wireless. Wireless technology is developing rapidly today because access and maintenance are easier and more flexible. However, easy access to wireless networks requires special attention to data security, especially in institutions. SMK Xyz Tana Toraja is one of the educational institutions that uses wireless networks as a supporting facility for learning and administration processes. The wireless network used by SMK Xyz Tana Toraja is directly connected to the server containing student data, teacher and staff data, as well as financial data. Therefore, security on wireless networks is very important to protect data from external threats. The method used to test the security system of Wireless LAN (WLAN) network is by penetration testing method, which is conducted on related institution networks to find weaknesses in the network. The results of the penetration testing show that the network security quality at SMK Xyz Tana Toraja is still weak. This is evident from the results of wireless network testing using penetration testing methods, such as sniffing on the target computer that was successful if the website accessed using the HTTP protocol, and encryption used on the access point that can still be penetrated using a dictionary attack. Therefore, an improvement is needed in the wireless network security system at SMK Xyz Tana Toraja to secure the data stored in it..

Keywords: *network security, penetration test, wireless network.*

I. PENDAHULUAN

Perkembangan teknologi informasi di era modern seperti sekarang ini semakin memudahkan masyarakat untuk mengakses informasi. Sehingga, semua jenis informasi dapat diakses dengan mudah melalui media internet. Salah satu teknologi yang digunakan untuk mengakses informasi adalah teknologi media transmisi nirkabel atau *wireless*.

Akses yang mudah terhadap jaringan *wireless* memerlukan perhatian yang lebih khususnya pada segi keamanan, mengingat keamanan data adalah sesuatu yang penting apalagi di dalam suatu instansi atau lembaga. Sebab pada jaringan *wireless Service Set Identifier* (SSID) akan di *broadcast* sehingga koneksi akan mudah diretas oleh orang-orang yang tidak bertanggung jawab. Sebagai contoh peristiwa Estonia pada tahun 2007 dan Georgia pada tahun 2008

SMK Xyz Tana Toraja merupakan salah satu instansi yang bergerak di bidang pendidikan yang menjadikan *Wireless* LAN (WLAN) sebagai salah satu fasilitas penunjang dalam proses pembelajaran dan administrasi. Jaringan *wireless* yang berada di SMK Xyz Tana Toraja tergabung dalam satu jaringan *Local Area Network* yang terhubung langsung ke *server* yang di dalamnya terdapat data siswa, data guru dan pegawai, serta data keuangan. Sehingga keamanan pada jaringan *wireless* perlu diperhatikan agar dapat mengantisipasi ancaman dari luar yang dapat merusak seperti serangan *malware* ataupun dari orang-orang yang ingin mencuri data-data penting yang dimiliki oleh sekolah.

SMK Xyz Tana Toraja menerapkan sistem keamanan menggunakan aplikasi yang terdapat pada perangkat jaringan seperti *access point* dan *modem.* Akan tetapi sistem keamanan yang ada pada perangkat tersebut masih memiliki kelemahan, seperti pada konfigurasi *access point* masih ada yang menggunakan konfigurasi bawaan dari *vendor* dan kelemahan pada enkripsi yang digunakan dapat dipecahkan dengan serangan *cracking the encryption* menggunakan metode *dictionary attack* sehingga rentan terhadap serangan dari luar yang dapat bersifat merusak atau merugikan.

Untuk mengetahui bagaimana kualitas keamanan jaringan di SMK Xyz Tana Toraja maka perlu dilakukan pengujian terhadap sistem keamanan yang ada pada jaringan tersebut. Metode yang dapat digunakan untuk pengujian sistem keamanan jaringan *Wireless LAN* (WLAN) yaitu dengan metode *penetration testing* yang dilakukan pada jaringan instansi terkait untuk menemukan kelemahan yang ada pada jaringan tersebut.

II. METODOLOGI PENELITIAN

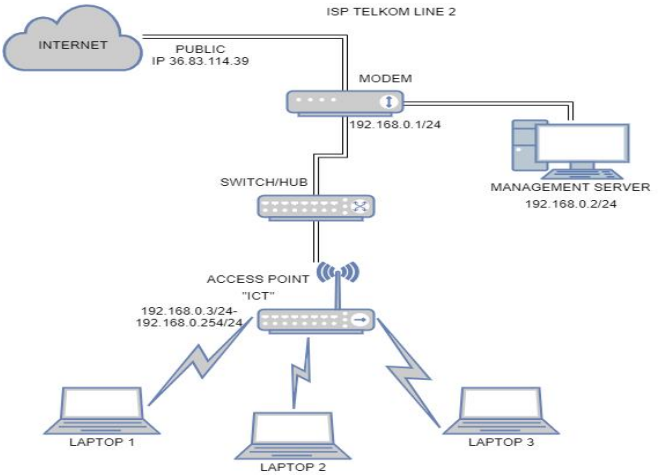
Dalam penelitian ini, jenis penelitian yang digunakan yaitu penelitian deskriptif. Penelitian deskriptif dilakukan untuk mengetahui nilai variabel mandiri, baik satu variabel atau lebih (independent) tanpa membuat perbandingan antara variabel satu dengan yang lain. Tahapan prosedur yang dilakukan pada penelitian ini yaitu: 1. Pengumpulan data yaitu melakukan pengkajian teori untuk mengetahui prosedur pengujian keamanan jaringan dan melakukan pengamatan langsung terhadap objek penelitian serta melakukan wawancara terhadap pihak IT untuk memperoleh data-data yang diperlukan untuk penelitian. 2. Tahap selanjutnya yaitu persiapan hardware dan software yang akan menunjang pelaksanaan penelitian, mulai dari persiapan hardware yang meliputi laptop dan wireless adapter serta persiapan software yang meliputi penginstallan dan konfigurasi tools yang akan digunakan pada penelitian. 3. Langkah berikutnya yaitu melakukan pengujian sistem keamanan menggunakan empat jenis serangan pada jaringan wireless : *a. MiTM Attack: ARP Poisoning; b. Attacking the Infrastructure; c. MAC Address Spoofing; d. Cracking the WPA2-PSK Key.* 4. Tahap selanjutnya yaitu melakukan analisis data yang telah diperoleh dari pengujian sistem keamanan yang telah dilakukan, kemudian menarik kesimpulan dan saran yang berguna untuk mengamankan jaringan wireless untuk mengantisipasi serangan di kemudian hari..

III. PEMBAHASAN

A. Topologi Jaringan.

Berdasarkan pemetaan topologi jaringan secara fisik yang telah dilakukan pada SMK Xyz Tana

Toraja didapatkan hasil topologi infrastruktur seperti yang terdapat pada Gambar 1

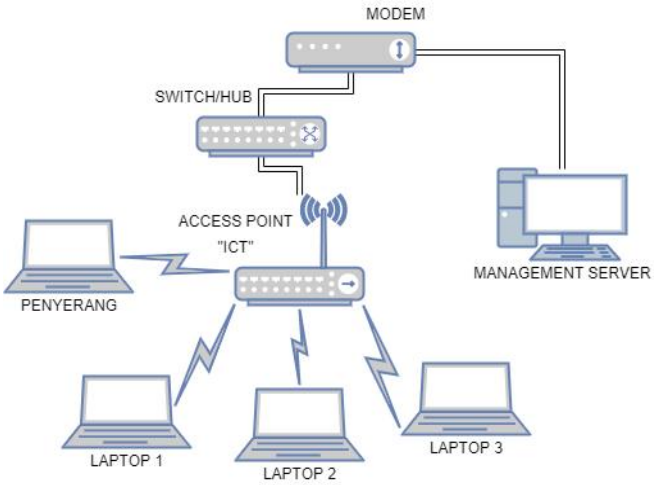


Gambar 1. Topologi jaringan SMK Xyz

Pada Gambar 1 akses internet dari ISP (*Internet Service Provider*) memiliki *ip public* yaitu xx.xx.114.39, kemudian koneksi jaringan tersebut terhubung ke *modem* melalui kabel *fiber optic* dan mendapatkan *ip private* yang memiliki *gateway* 192.168.0.1/24, selanjutnya dari *modem* akses internet terhubung langsung ke *Management Server* menggunakan kabel UTP yang memiliki *ip address* 192.168.0.2/24 serta terhubung ke *switch*. Kemudian dari *switch* dihubungkan ke *access point* yang memiliki *range ip* 192.168.0.3/24-192.168.0.254/24 dan akses internet dapat disebarkan melalui sinyal *wifi* dapat digunakan oleh *client* atau melalui kabel UTP untuk dapat terhubung ke internet.

B. Skenario Pengujian

Penelitian ini dilakukan dengan menggunakan metode *penetration testing* pada jaringan *wireless* yang ada di laboratorium TKJ SMK Xyz Tana Toraja. Pengujian yang dilakukan antara lain yaitu MiTM *Attack*: ARP *Poisoning* yang bertujuan untuk menyadap paket data dari *client* yang terhubung ke jaringan *wireless*, *Attacking the Infrastructure* yang bertujuan untuk melumpuhkan koneksi pengguna yang terhubung ke suatu jaringan *wireless*, MAC *Address Spoofing* bertujuan untuk mendapatkan akses ke jaringan *wireless* yang menggunakan MAC *filltering* dan juga untuk menyembunyikan identitas dari penyerang, dan *Cracking* WPA *Key* yang bertujuan untuk mengetahui *password* yang digunakan untuk mengamankan *access point*. Setiap serangan dilakukan sebanyak tiga kali percobaan dan skenario pengujian yang ditunjukkan pada Gambar 2.



Gambar 2. Skenario Pengujian

1) MiTM (Man in the Middle) Attack: ARP Poisoning

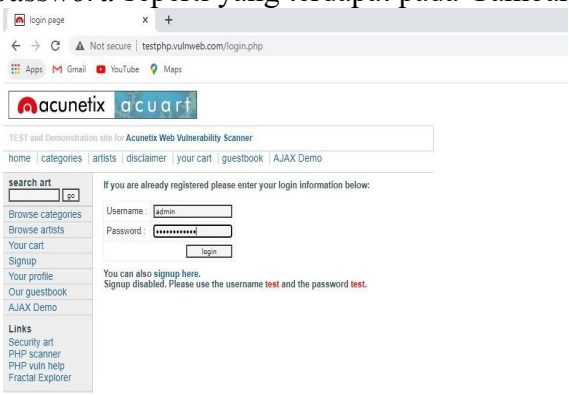
Pada pengujian ini dilakukan *sniffing* atau penyadapan paket data terhadap *user* lain yang berada dalam suatu jaringan WLAN. Untuk melakukan *Man in The Middle* dibutuhkan komputer *tester* dan komputer target yang terhubung ke jaringan *wireless* yang sama dalam hal ini yaitu jaringan *wireless* "ICT" dengan *range ip* yaitu 192.168.0.3/24-192.168.0.254/24 yang ada di laboratorium komputer SMK Xyz Tana Toraja, komputer *tester* berperan sebagai pihak ketiga antara komputer target dan *access point* yang terhubung ke layanan internet. Aplikasi yang digunakan pada pengujian ini yaitu Ettercap

Langkah pertama yang dilakukan yaitu mengaktifkan *ip_forward*. Tujuan diaktifkannya *ip_forward* agar *sniffing* yang dilakukan terhadap paket data antara komputer target dan *access point* dapat terekam oleh komputer *tester*.

Pada tahap selanjutnya yaitu melakukan *scanning host* yang bertujuan untuk melihat daftar *user* lain yang terkoneksi pada jaringan *wireless* dan menentukan target mana yang akan disadap. Pada konfigurasi ettercap target pertama yang dimasukkan yaitu *ip* dari komputer target yaitu

192.168.0.19 dan kemudian terget kedua yaitu *ip gateway* dari *access point* yaitu 192.168.0.1

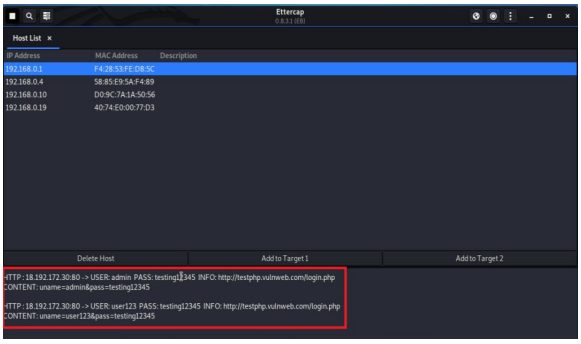
Tahap selanjutnya yaitu ARP *Poisoning* dengan parameter *Sniff remote connections* terhadap jaringan *wireless*. Kemudian proses *sniffing* dijalankan untuk merekam aktifitas jaringan pada komputer target saat mengakses internet. Pada percobaan *sniffing* diperoleh bahwa komputer target mengakses *website* http://testphp.vulnweb.com/login.php dan melakukan *login* dengan memasukkan *username* dan *password* seperti yang terdapat pada Gambar 3



Gambar 3. Halaman login vulnweb

Tabel diletakkan rata tengah pada paragraf. Setiap tabel harus diberikan penomoran dan keterangan yang diletakkan tepat pada atas dari tabel yang bersesuaian. Tabel haruslah dibuat dan diketik dengan menggunakan fitur tabel pada Microsoft Word. Dilarang untuk menampilkan tabel yang berasal dari *screen capture* Excel atau gambar dari referensi lain. Tabel yang mengambil referensi dari pustaka lain wajib untuk mencantumkan sumbernya dengan cara pengutipan yang sama dengan paragraf dan menuliskan sumber referensinya pada bagian daftar referensi.

Hasil *sniffing* menunjukkan *username*: *admin* dan *password*: *testing12345* yang dimasukkan oleh *user* saat mengakses *website* dan melakukan *login* seperti yang terdapat pada Gambar 4.



2) Attacking the Infrastructure

Pengujian ini dilakukan serangan *deauthentication attack* menggunakan aplikasi *aireplay-ng*. Serangan ini bertujuan untuk melumpuhkan koneksi *user* yang terhubung pada jaringan serta mempengaruhi kinerja jaringan *wireless*. Langkah pertama yang dilakukan adalah mengubah mode *wireless interface* pada komputer *tester* ke mode monitor, selanjutnya yaitu melakukan *scanning* terhadap jaringan *wireless* untuk mendapatkan MAC *address* dari *access point*

Hasil *scanning* pada langkah sebelumnya didapatkan MAC *address* dari jaringan "LAB TKJ" yaitu "xx:xx:xx:0B:16:C8" dan jaringan "ICT" yaitu "xx:xx:xx:FE:D8:5C". Langkah selanjutnya yaitu melakukan *scanning host* pada jaringan "LAB TKJ". Langkah selanjutnya yaitu melakukan serangan *deauthentication attack*, jika serangan *deauthentication attack* berhasil maka hasil koneksi jaringan pada komputer target akan terputus dan hasil *test ping Request timed out.*

3) MAC Address Spoofing

Pada pengujian ini bertujuan untuk mengetahui apakah jaringan *wireless* menggunakan MAC *address filtering*. Dalam serangan ini menggunakan aplikasi *macchanger* untuk menduplikasikan MAC *address* dari *client* yang sebelumnya telah terkoneksi ke jaringan *wireless*

4) Cracking WPA2/PSK Key

Pada pengujian ini langkah pertama yaitu untuk mengetahui jenis enkripsi dari sistem keamanan yang digunakan pada jaringan *wireless* dengan melakukan *scanning, kemudian* menentukan target untuk melakukan *cracking* WPA2 *key.* Tahap selanjutnya yaitu melakukan *capture.* Setelah proses *handshake* terjadi maka *file handshake* akan

tersimpan pada *folder* yang telah ditentukan. Langkah selanjutnya yaitu melakukan *cracking* WPA *key* pada jaringan "ICT"

Untuk proses cracking dapat memakan waktu beberapa menit, beberapa jam atau beberapa bulan tergantung seberapa kuat kombinasi password yang digunakan pada access point yang ditarget. Hasil cracking WPA key pada jaringan ICT dapat dilihat pada Gambar 5.

5) Hasil Pengujian

Seluruh hasil dari tahap pengujian keamanan jaringan *wireless* menggunakan metode *penetration testing* dapat dilihat pada Tabel 1.

No	Jenis Serangan	Software yang digunakan	Data yang dibutuhkan	Jml Percobaan	Status
1	MiTM *Attack*: *Arp Poisoning*	Ettercap, Arp *poisoning*	Penyerang harus berada dalam jaringan WLAN, *ip address* target	1 2 3	Berhasil
2	*Deauth Attack*	Airodump-ng, Aireplay-ng	MAC *address* dari *access point*, *client* yang terkoneksi pada jaringan	1 2 3	Berhasil
3	MAC *Spoofing*	Airodump-ng, Macchanger	Daftar MAC *address user* yang terkoneksi ke jaringan	1 2 3	Berhasil
4	*Cracking* WPA2 Key *Encryption*	Aireplay-ng, Airodump-ng, Aircrack-ng	*File* WPA *handshake, password wordlist*, BSSID *access point*, *channel access point*	1 2 3	Berhasil

a) Analisis hasil pengujian serangan MiTM Attack: ARP Poisoning

Berdasarkan hasil pengujian yang telah dilakukan, proses sniffing menggunakan serangan ARP Poisoning berhasil dilakukan terhadap komputer target dengan ip address 192.168.0.19 yang terkoneksi ke access point yang sama dimana komputer tester juga terkoneksi. Dari proses sniffing diperoleh informasi mengenai website http://testphp.vulnweb.com/login.php yang diakses oleh komputer target dan login dengan menggunakan username dan password. Namun ada suatu kendala dimana aplikasi ettercap tidak dapat melakukan sniffing serta komputer target juga tidak dapat mengakses website yang dituju, hal ini dikarenakan saat proses sniffing sedang berjalan dan disaat yang bersamaan komputer target mengakses website yang mana dalam hal ini adalah https://www.facebook.com maka otomatis protokol keamanan yang diterapkan pada website yang diakses mendeteksi aktivitas yang mencurigakan dan langsung memblokir koneksi antara komputer target dan website yang akan dikunjungi, dan penyebab ettercap tidak dapat melakukan sniffing yaitu karena protokol keamanan yang digunakan pada website yang diakses merupakan https bukan http. HTTPS (Hypertext Transfer Protocol Secure) merupakan protokol komunikasi internet yang menggunakan sistem keamanan yaitu SSL (Secure Socket Layer) berbeda dengan HTTP, HTTPS mengenkripsi pertukaran informasi antara client dan server sehingga semua data yang terlibat dalam proses pertukaran tidak dapat diakses oleh pihak lain.

b) Analisis hasil pengujian serangan Attacking The Infrastructure

Pada pengujian ini serangan dilakukan pada jaringan *wireless* dengan mempengaruhi kinerja jaringan serta melumpuhkan koneksi *user/signal jamming* yang sedang terhubung dalam jaringan. Hal yang dibutuhkan untuk melakukan serangan ini yaitu MAC *address* dari *access point* yang akan diserang. Untuk mendapatkan MAC *address* dari *access point* dapat dilakukan dengan *scanning* menggunakan *airodump-ng*. Dari hasil *scanning* didapatkan MAC *address* dari jaringan yang menjadi target serangan yaitu "LAB TKJ" dengan MAC *address* "14:4D:67:0B:16:C8" dan jaringan "ICT" dengan MAC *address* "F4:28:53:FE:D8:5C", setelah MAC *address*

didapatkan langkah selanjutnya yaitu melakukan *deauthentication attack*. Jumlah *user* dalam jaringan juga berpengaruh pada lamanya waktu yang dibutuhkan untuk melakukan serangan ini. Penyebab lainnya yang cukup berpengaruh yaitu jarak antara penyerang dan *access point*, semakin jauh jaraknya maka semakin lama juga waktu yang dibutuhkan untuk *user* terkena serangan *deauthentication attack*. Saat serangan *deauthentication* berjalan maka koneksi *user* yang terhubung ke jaringan yang diserang akan terputus.

c) Analisis hasil pengujian serangan MAC Address Spoofing

Pengujian ini bertujuan untuk mengetahui apakah jaringan *wireless* menggunakan MAC *address filtering*. Tetapi setelah dilakukan pengujian didapatkan hasil bahwa jaringan *wireless* tidak menggunakan MAC *address filltering*, maka dari itu siapa saja dapat terkoneksi ke jaringan asalkan mengetahui *password* yang digunakan pada jaringan *wireless* tersebut. Untuk serangan ini yang pertama dilakukan adalah *scanning* terhadap jaringan menggunakan *airodump-ng* untuk mendapatkan MAC *address* dari *client* yang terhubung ke suatu jaringan *wireless*. Setelah MAC *address* dari *client* didapatkan selanjutnya dapat dilakukan MAC *address spoofing* menggunakan aplikasi *macchanger.* Setelah dilakukan proses duplikasi MAC *address* menggunakan aplikasi *macchanger* komputer *tester* dapat terkoneksi ke jaringan *wireless* tetapi membutuhkan alamat *ip* yang berbeda dari *client* yang MAC *addressnya* telah diduplikasi. Untuk membatasi agar dalam suatu jaringan *wireless* tidak terdapat MAC *address* yang sama maka dapat digunakan *Mikrotik Router* sebagai keamanan tambahan dimana pada *Mikrotik Router* terdapat fitur yang dapat membatasi agar tidak ada MAC *address* yang sama pada suatu jaringan.

d) Analisis hasil pengujian serangan Cracking WPA2/PSK Key

Pada pengujian ini langkah pertama yang dilakukan yaitu mengetahui jenis enkripsi yang digunakan pada *access point*. Pada proses *scanning* didapatkan hasil bahwa jaringan *wireless* ICT menggunakan enkripsi WPA2/PSK. Setelah mengetahui jenis enkripsi yang digunakan pada jaringan *wireless* langkah selanjutnya yaitu melakukan proses WPA *handshake* untuk mendapatkan data yang akan digunakan pada proses *cracking*. Untuk mendapatkan WPA *handshake* dapat dilakukan dengan *scanning airodump-ng* terhadap jaringan ICT dan pada saat yang sama dilakukan *deauthentication attack* terhadap jaringan ICT. Setelah *file handshake* didapatkan langkah selanjutnya yaitu melakukan proses *cracking* menggunakan aplikasi *aircrack-ng*, lama waktu yang diperlukan untuk melakukan proses *cracking* tergantung dari seberapa kuat kombinasi *password* yang digunakan pada keamanan *wireless* tersebut, serta kemampuan dan spesifikasi dari *hardware* yang digunakan, jika spesifikasi *hardware* dapat diandalkan maka proses *cracking* juga akan cepat selesai. Jika *password* yang menggunakan kombinasi angka, huruf, dan simbol maka hal ini dapat memakan waktu yang sangat lama bisa sampai berhari-hari bahkan berbulan-bulan, hal ini juga dapat menyulitkan bagi serangan *brute force* dan *dictionary attack*. Pada pengujian ini waktu yang diperlukan untuk melakukan proses *cracking password* pada *access point* memakan waktu kurang lebih sepuluh menit dan didapatkan hasil berupa *password* yang terdapat di dalam *wordlist*. Untuk dapat terhindar dari serangan ini langkah yang dapat dilakukan adalah menggunakan *password* yang panjang dengan kombinasi angka, huruf dan simbol serta rutin mengganti *password* minimal seminggu sekali.

REFERENSI

[1] I. Rahmawati, “Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense,” p. 16, 2017.

[2] Sri Hidayati, Rudi A.G. Gultom, “Analisis Kebutuhan Senjata Siber Dalam Meningkatan Pertahanan Indonesia Di Era Peperangan Siber,” p.18, 2020.

[3] H. Pangaribuan, “Analisis Penggunaan Mikrotik Router OS Sebagai Router Pada Jaringan Komputer Terhadap Keamanan Data di PT JMS BATAM,” p. 18, 2015.

[4] A. Putri and I. Solikin, "Analisa Kinerja Koneksi Jaringan Komputer pada SMK Teknologi Bistek Palembang," BISTEK Palembang, no. 12,p. 11, 2017

[5] S. Halawa, "Perancangan Aplikasi Pembelajaran Topologi Jaringan Komputer Untuk Sekolah Menengah Kejuruan (SMK) Teknik Komputer Dan Jaringan," JURIKOM (Jurnal Ris. Komputer), vol. 3, pp. 66–71, 2016.

[6] Feri N.W, "Analisa Sistem Keamanan Jaringan (Network Security) Firewall Asa Dan Firewall Cyberoam Pada Kantor Pusat Badan Sar Nasional (BASARNAS)," p. 95, 2017.

[7] G. K. Dewi, "Analisa Keamanan Jaringan Wireless Di Sekolah Menengah Al Firdaus," Univ. Muhammadiyah Surakarta, p. 16, 2016.

[8] W. Pipit, "*Studi Analisa Quality of Service Pada Jaringan Akses Wireless Fidelity di Gedung KPA Politeknik Negeri Sriwijaya,"*Politeknik Negeri Sriwijaya, 2017.

[9] S. Amri, "Analisis Jenis-Jenis Sistem Keamanan Jaringan Wireless Hotspot," Univ. Sumatera Utara, 2015.

[10] A. Adrian and A. Setiyadi, "Analisis Keamanan Jaringan dengan Metode Penetration Testing Execution Standard (PTES) di Dinas Kesehatan Provinsi Jawa Barat," J. Unikom Repisitory, no. 1, pp. 1–8, 2018.

[11] R. Mentang, A. A. E. Sinsuw, and X. B. N. Najoan, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," E-Journal Tek. Elektro Dan Komput., vol. 4, no. 7, pp. 35–44, 2015.

[12] D. M. Sari, M. Yamin dan L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) MAC Address, Menggunakan Metode Penetration Testing", semanTIK, vol. 3, no. 2, 2018.

[13] K. M. Asteroid and Y. Hendrian, "Analisis Wireless Local Area Network (WLAN) dan Perancangan MAC Address Filtering Menggunakan Mikrotik (Studi Kasus Pada PT. Graha Prima Swara Jakarta)," J. Tek. Komput. amik bsi, vol. II, no. 2, pp. 77–82, 2016.

[14] Yunanri W, Imam Riadi, Anton Yudhana, "Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (Pentest)", Annu. Res. Semin., vol. 2, no. 1, pp. 300–304, 2016.

[15] C. Nickerson, D. Kennedy, and C. J. Reil, "The Penetration Testing Execution Standard," 2014, 2017.

[16] A. R. Fauzi, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan IDS," J. Manaj. Inform., vol. 8, no. 2, p. 7, 2018.

[17] M. I. Susanto, A. Hasad, and M. A. Bakri, "Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking," vol. 7, no. 1, pp. 25-34, 2019.

[18] I. K. Bayu, M. Yamin, and L. F. Aksara, "Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus : Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO)," SemanTIK, vol. 3, no. 2, pp. 69–78, 2018.

[19] S. Maulana, T. Y. Arif, and R. Munadi, "Pengujian dan Analisis Keamanan WPA2 dan Signal Strength pada Router Berbasis OpenWrt," J. Karya Ilm. Tek. Elektro, vol. 2, no. 3, pp. 105–111, 2017.