Prosiding Seminar Nasional
Hasil Penelitian dan Pengabdian Kepada Masyarakat
Universitas Islam Kuantan Singingi, 17-18 Desember 2021 **Halaman: 37-41 | E-ISSN 2809-882X**
DOI: https://doi.org/10.36378/prosidinguniks.v0i0.1961

Analisa Dan Implementasi Penetration Testing Pada Jaringan Wi-Fi Fakultas Teknik Universitas Islam Kuantan Singingi

Eval Agustin Martin[1], Jasri[2]
[1,2]Teknik Informatika, Fakultas Teknik, Universitas Islam Kuantan Singingi
[1]evalagustinmartin@gmail.com, [2]jasri.skom@gmail.com

Abstrak

Teknologi informasi dan komunikasi merupakan dua hal yang sulit terpisahkan dari kehidupan manusia di zaman yang serba teknologi. Salah satu contoh teknologi informasi dan komunikasi adalah jaringan. Penelitian ini menggunakan metode penetration testing, yang bertujuan agar dapat diterapkan untuk menganalisa terhadap keamanan jaringan Wireles yang telah sudah diterapkan di Fakultas Teknik Universitas Islam Kuantan Singingi. Penetration testing adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan jaringan. Dalam penerapan metode penetration testing ini 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, perguruan tinggi maupun tempat umum. Walalupun memiliki sistem keamanan, jaringan Wirelessmasih dapat di serang oleh para attacker.

Kata kunci : Penetration Testing, Jaringan Wireless, Kali Linux

1. Pendahuluan

Pesatnya perkembangan teknologi jaringan komputer dapat memudahkan masyarakat umum untuk mengakses dan memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi jaringan nirkabel atau wireless. Mudahnya cara akses bagi pengguna umum mengakses jaringan wireless tentunya menimbulkan masalah di aspek keamanan yang sangat perlu untuk di perhatikan, terlebih lagi apabila suatu instansi atau lembaga sangat peduli dengan keamanan data, jaringan wireless yang menggunakan gelombang radio sebagai media transmisinya memungkinkan penyusup atau serangan dengan mudah masuk ke dalam sistem dari semua arah.

Fakultas Teknik Universitas Islam Kuantan Singingi merupakan sebuah bagian yang menyediakan akses jaringan wireless, jaringan wireless memiliki peran yang sangat penting di Fakultas Teknik. Sistem keamanan yang digunakan di Fakultas Teknik WPA2 yaitu adalah singkatan dari WiFi Protected Access 2 sebuah teknologi yang digunakan untuk mengamangan koneksi WiFi. WPA2 merupakan generasi lanjutan dari WPA.

Umumnya perangkat Wi-Fi saat ini mendukung WPA dan WPA2. WPA dan WPA2 bekerja dengan cara meng-eknripsi transfer data pada sebuah jaringan Wi-Fi. Keduanya juga membutuhkan password dengan panjang minimum 8 karakter., maka kualitas kemanan menentukan kesulitan untuk akses masuk ke dalam jaringan wireless tersebut. Banyaknya penggunaan secara umum pada jaringan wireless di Fakultas Teknik membuat sistem jaringan dipaksa bekerja dengan maksimal yang membuat sistem keamanan menjadi melemah, akibat dari akses jaringan wireless yang begitu padat dapat mempermudah pengguna yang tidak sah untuk mengakses kedalam sistem jaringan, oleh karena itu perlu dilakukannya pengujian terhadap keamanan sistem jaringan yang mana hasil dari pengujian tersebut di analisa dan mencari celah dari kelemahan sistem jaringan tersebut lalu memperbaiki agar terciptanya kemanan sistem jaringan yang kuat.

Salah satu metode yang dapat di gunakan untuk mengevaluasi jaringan adalah dengan cara melakukan pengujian terhadap sistem dengan mensimulasikan bentuk-bentuk serangan terhadap jaringan atau biasa disebut dengan metode penetration testing. Teori tentang penetration testing sudah lama di dikembangkan oleh beberapa peneliti dalam bidang keamanan sistem informasi dan jaringan. Metode penetration testing adalah sebagai bukti uji untuk memperkuat sistem keamanan jaringan agar dapat mengevaluasi setiap celah kemanan dari sebuah sistem jaringan, dengan metode penetration testing ini dapat menghasilkan sebuah analisa bagaimana penyusup/attacker dapat memperoleh akses kedalam sistem jaringan tersebut, penerapan metode ini diperlukan untuk mencegah berbagai macam gangguan di masa yang akan datang.

2. Metode Penelitian

Metode penelitian yang benar semakin dirasakan urgensinya terhadap keberhasilan suatu penelitian. Satu hal yang penting dalam setiap penelitian adalah perumusan metodologi penelitian. Melalui metodologi harus dengan jelas tergambar bagaimana penelitian tersebut dilaksanakan yang disusun dan tertata secara sistematis.

Sedangkan penelitian merupakan suatu proses mencar sesuatu secara sistematis dalam waktu yang relatiflama dengan menggunakan metode ilmiah dengan prosedur

maupun aturan yang berlaku. Penelitian itu sendiri terjadi Karenaadanya dorongan rasa ingin tahumengenai sesuatu hal yang sedang terrjadi dilingkungan sekitar. Seseorang melakukan penelitian untuk mencari jawaban dari permasalahan yang sedang terjadi.

3. Hasil dan Pembahasan

3.1 Analisa

Analisa dilakukan untuk mengetahui masalah atau kelemahan dari sistem keamanan yang ada, pada penerapan metode penetration testing analisa penting dilakukan karena merupakan dasar dalam merencanakan dan bagaimana serangan dilakukan untuk mengetahui celah dari sistem keamanan jaringan yang ada, dan mengetahui cara untuk mengantisipasi serangan yang ada.

3.2 Implementasi Penetration Test

Implementasi metode penetration testing ini menggunakan tools serangan yang sudah ada, namun akan di sesuaikan dengan kebutuhan dari penelitian ini sendiri

3.3 Proses Pengujian

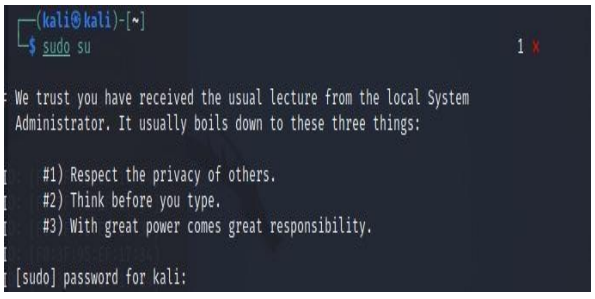
Proses pengjian menggunakan metode penetration test berfungsi untuk melakukan pengujian terhadap sistem keamanan jaringan WiFi Fakultas Teknik agar dapat mengetahui kelemahan dan celah dari sistem keamanan jaringan WiFi yang dituju. Tools-tools yang digunakan dalam kali linux

1. aircrack-ng
2. airmon-ng
3. airodump-ng
4. aireplay-ng

3.4 Penjelasan Mengenai Teknik Serangan

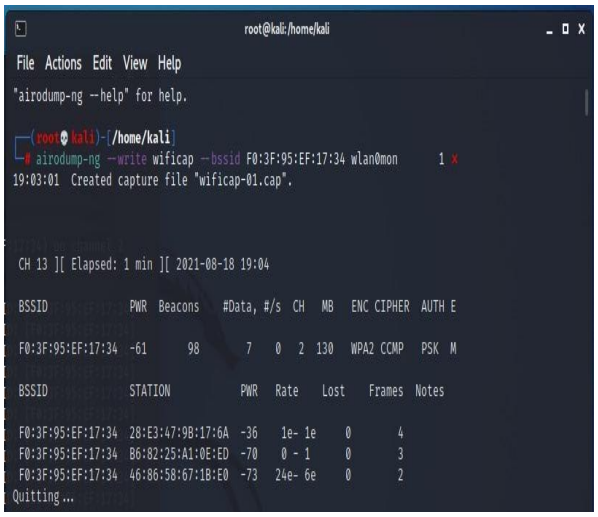
1. Cracking The Encryption

    a) Pertama kita akan masuk ke terminal yang ada di kali linux lalu akan sebagai root untuk dapat menggunakan tools yang ada di kali linux dengan perintas “sudo su” maka selanjutnya akan muncul perintah untuk memasukkan password dari kali linux.



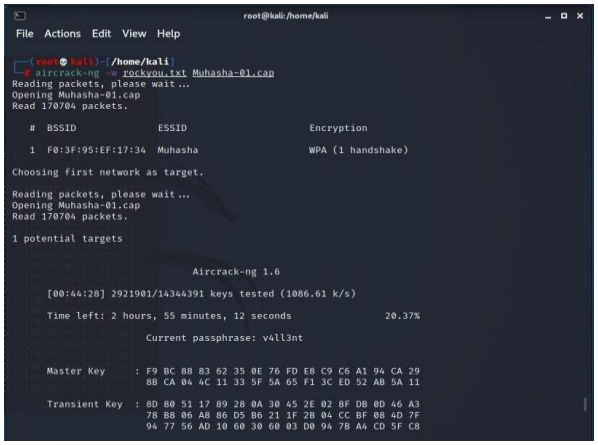
Gambar 1. Masuk Sebagai Root

    b) Selanjutnya untuk melihat perangkat yang aktif pada target dengan perintah “airodump-ng –write wificap –bssid F0:3F:95:EF:17:34 wlan0mon” yang mana perintah ini untuk melakukan capture terhadap Wi-Fi target.



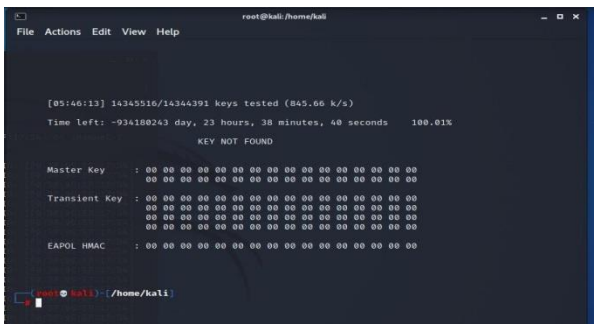
Gambar 2. Perangkat yang aktif di target

    c) Langkah terakhir yaitu melakukan scanning serangan dengan perintah “aircrack-ng –w rokyou.txt muhasha-01.cap”



Gambar 3. Melakukan scanning

    d) Untuk pengujian cracking the encryption tidak di temukan dikarenakan sistem keamanan password sudah baik.

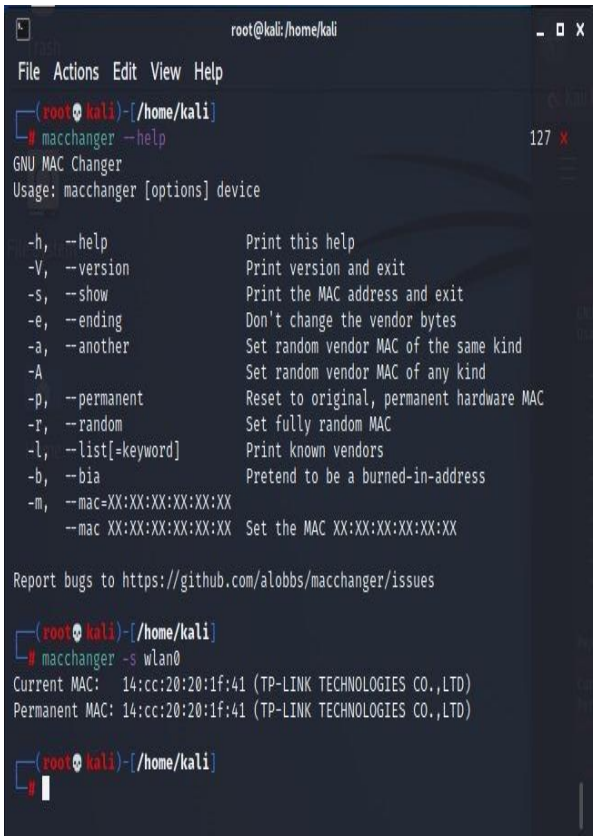


Gambar 4. Hasil scanning

2. Bypassing MAC Authentication

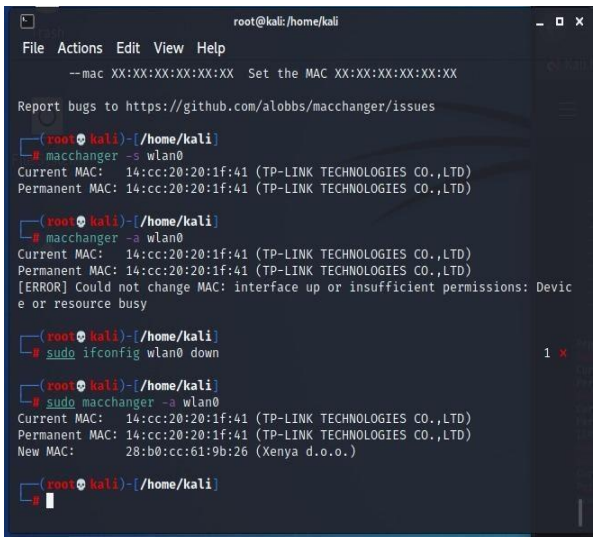
Teknik serangan ini bertujuan untuk mengetahui apakah sistem keamanan jaringan target sudah menggunakan MAC Filtering atau belum, serangan ini nantinya akan melakukan pemalsuan MAC address komputer penguji yang dan menggunakan MAC address dari client yang terdapat di dalam jaringan agar tidak dapat dicurigai.

a) pertama kita akan masuk keterminal seperti langkah pada serangan sebelumnya, lalu mengaktifkan mode monitor selanjutnya ketikan perintah “maccharger –help” perintah ini merupakan langkah awal untuk melakukan serangan bypassing MAC authentication bertujuan untuk melakukan perubahan MAC address.



Gambar 5. Perintah bypass MAC authentication

b) langkah selanjutnya yaitu ketikan perintah “macchanger –s wlan0” maka akan tampil alamat MAC address dari komputer penguji yaitu 14:cc:20:20:1f:41, setelah itu selanjutnya ketikan perintah “ sudo ifconfig wlan0 down” untuk mematikan jaringan kemudian ketikan kembali “sudo macchanger –a wlan0” maka akan mucul MAC address yang asli atau pertama dan Mac address yang baru dengan MAC address “28:b0:cc:61:9b:26” yang akan digunakan untuk mengelabui client.



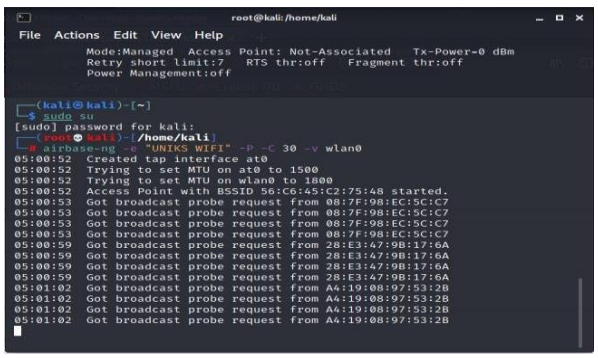
Gambar 6. MAC Address berhasil dirubah

3. Man In The Middle (MITM) Attack

Man In The Middle Attack merupakan salah satu serangan dimana serangan ini bertujuan untuk membuat koneksi independen dengan korban dan menyampaikan pesan atau memberikan informasi untuk membuat korban percaya bahwa sedang berkomunikasi secara pribadi.

Penjelasan :

a) Pertama serangan Man in the middle yang di terapkan kali ini yaitu membuat jaringan palsu/SSID dengan tujuan agar dapat mengelabui client dan penguji dapat mendapatkan mac address dari client.
b) Untuk membuat alamat jaringan/SSID yang palsu pertama kita harus masuk ke mode super user dengan mengetikkan “ Sudo Su” kemudian mengetikkan password login kali linux di terminal kali linux.
c) Selanjutnya masuk ke directory home/kali setelah itu ketikkan “airbase-ng –e “UNIKS WIFI” –p –c 30 –v wlan0”, maka pada gambar terlihat alamat jaringan atau SSID yang kita buat menggunakan nama “UNIKS WIFI” setelah itu tekan enter, maka tunggu proses selanjutnya.



Gambar 7. Membuat SSID fake UNIKS WIFI

Tabel 1. Hasil Pengujian

Jenis Serangan	Informasi Yang dibutuhkan Untuk Serangan	Status Serangan
Cracking The Encryption	*handshake user* lain, *Channel* yang digunakan dan BSSID dari *access point.*	Gagal
Bypassing MAC Authentication	*List MAC User* lain yang terhubung di jaringan	Berhasil
Attacking The Infrastrutur	*Attacker* harus berada dalam jaringan WLAN, *MAC Address* dari perangkat *tester*	Berhasil
Man In The Midle(MITM) Attack	*Attacker* harus berada dalam jaringan WLAN, *IP address* dari *user* yang terkoneksi	Berhasil

3.5 Solusi Dari Serangan

1. Craking 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.

2. Bypass MAC Authentication

Solusi pencegahan dari serangan bypass MAC authentication bisa dilakukan yaitu:

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.

3. Attacking The Infrastructur

Solusi pencegahan dari serangan ini adalah dengan cara :

a) pengguna komputer bisa melakukan sendiri dengan menggunakan script untuk memfilter DDoS traffic mengandalkan firewall untuk mem-block traffic.
b) Memperbarui sistem operasi ke versi terbaru. Hal ini bertujuan untuk mengatasi menutupi bagian-bagian rentan yang bisa saja dijadi kan pintu masuk akses ilegal.
c) Membatasi akses dari dan ke sistem sehingga bisa menyaring trafik data yang masuk dan keluar pada komputer atau server yang digunakan.
d) Menggunakan perangkat lunak keamanan tambahan untuk sistem

4. Man In The Midle (MITM) Attcak

Solusi pencegahan dari serangan ini adalah dengan cara :

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.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan dan pembahasan pada bab-bab sebelumnya maka penulis dapat mengambil beberapa kesimpulan.

1. Pada jaringan Fakultas Teknik Masih banyak celah yang bisa di exploitasi oleh dikarenakan sistem keamanan masih belum maksimal.
2. Setelah melakukan pengujian pada jaringan Fakultas Teknik dengan empat macam serangan yaitu Cracking The Encryption, Bypassing MAC Authentication, Attacking The Infrastruktur, Man In The Midle(MITM) Attack dapat diambil kesimpulan hanya pengujian pertama yang gagal dikarenakan sistem keamanan yang di terapkan sudah baik.
3. Perlunya evaluasi lebih lanjut terhadap jaringan Fakultas Teknik agar bisa memberikan keamanan kepada user lain apabila sewaktu-waktu terjadi serangan keamanan jaringan di Fakultas Teknik Universitas Islam Kuantan Singingi.

Daftar Rujukan

Aminanto, Alja, and Wiwi Sulistyo. "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery." Jurnal Teknologi Informasi, Agustus 2019.

Arif Hidayat, Ismail Puji Saputra. "Analisa Dan Poblem Solving Keamanan Router Mikrotik Rb750ra Dan Rb750gr3 Dengan Metode Penetration Testing." Jurnal Resistor, 2018.

Bambang Pujiarto, Ema Utami, Sudarmawan. "Evaluasi Wireless Local Area Network." Jurnal Dasi, Juni 2013.

Daulay, Muhammad Iqbal. "analisa perbandingan keamanan WEP, WPA, WPA2 pada access point." 2019.

Dermawati, Rosi, and M. Hasim Siregar. "Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik Uniks Menggunakan Dionae Sebagai Keamanan Jaringan." Jurnal Ilmiah Edutic, n.d.

Gilvan Januar Sirait, and Indrastanti R. Widiasari, M.T. "Analisis Keamanan Jaringan Wireless Local Area Network dengan Metode." 2018.

Haerudin, and Arif Kurniadi. "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)." 2021.

Imam Kreshna Bayu, Muh. Yamin, LM Fid Aksara. "Analisa Keamanan Jaringan Dengan." Juli-Desember 2017: 69-78.

Michael, Ikhwan Ruslianto, and Rahmi Hidayati. "Analisis Perbandingan Sistem Keamanan Jaringan Wi-Fi." jurnal komputer dan aplikasi, 2021.

Muhammad Addy Rahmadani, Mochammad Fahru Rizal , Tedi Gunamawan. "Implementasi Hacking Wireless Dengan Kali Linux Menggunakan." e-Proceeding of Applied Science, Desember 2017: 17-67.

Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan. "Penetration Testing Server Sistem Informasi Manajemen." 2015.

Stefanus Eko Prasetyo, Ricky Chandra Lee. "Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing." 2021.