Journal on Education
Volume 04, No. 04, Mei-Agustus 2022, pp. 1470-1476
E-ISSN: 2654-5497, P-ISSN: 2655-1365
Website: http://jonedu.org/index.php/joe

Analisa Infrastruktur Jaringan *Wireless* dan *Local Area Network* (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux

Tri Yusnanto[1], Muhammad Abdul Muin[2], Sugeng Wahyudiono[3]

[1,2,3]STMIK Bina Patria, Jl. Raden Saleh No.7, Potrobangsan, Kec. Magelang Utara, Kota Magelang, Jawa Tengah
yusnanto@gmail.com

Abstract

Computer networks and the internet play an important role for the smooth running of various fields of work. One example of information and communication technology is the Wireless Local Area Network (WLAN) or also called wireless local network technology. The method used in this research is the Penetration Testing method, with the intention of analyzing the Wireless Network computer security system in the STMIK Bina Patria Laboratory. Testing is carried out with several activities, including identifying and exploiting vulnerabilities in computer network security. In analyzing the security of the WLAN network, it is carried out using the Penetration Testing method where a form of attack on the network is simulated, one of the operating systems that has the right specifications in this regard is Kali Linux. Wireless network is a network that is widely used in institutions and public places. Even though it has a security system, wireless networks can still be attacked by attackers.
Keywords: Information Technology, Penetration Testing, Kali Linux, wireless

Abstrak

Jaringan komputer dan internet sangatlah berperan penting untuk kelancaran berbagai bidang pekerjaan. Salah satu contoh teknologi informasi dan komunikasi tersebut adalah Wireless Local Area Network (WLAN) atau disebut juga teknologi jaringan lokal nirkabel. Metode yang digunakan pada penelitian yaitu dengan metode Penetration Testing, dengan maksud melakukan analisis kepada sistem keamanan komputer Wireless Network yang ada pada Laboratorium STMIK Bina Patria. Pengujian dilakukan dengan beberapa kegiatan yang diantaranya dengan cara mengidentifikasi serta mengeksploitasi kerentanan pada keamanan jaringan komputer. Dalam menganalisa keamanan jaringan WLAN dilakukan dengan metode Penetration Testing dimana bentuk serangan terhadap jaringan disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux. Jaringan wireless merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum. Walaupun memiliki sitem keamanan, jaringan wireless masih dapat di diserang oleh para attacker.
Kata kunci Teknologi Informasi, Penetration Testing, Kali Linux, wireless

✉ Corresponding author: Tri Yusnanto
Email Address: yusnanto@gmail.com (Jl. Raden Saleh No.7, Potrobangsan, Kec. Magelang Utara, Kota Magelang, Jawa Tengah)
Received 22 August 2022, Accepted 29 August 2022, Published 30 August 2022

PENDAHULUAN

Pada masa sekarang diera 4.0 penggunaan jaringan komputer dan internet sangatlah berperan penting untuk kelancaran berbagai bidang pekerjaan. Teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi yang selalu *uptodate*. Teknologi jaringan komputer wireless merupakan salah satu teknologi yang dikembangkan pada saat ini untuk kelancaran berinternet(Supriadi et al., 2018). Mudahnya pengguna umum terhubung dengan jaringan wireless tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data(Adiguna & Widagdo, 2022). Jaringan wireless merupakan sebuah jaringan computer dengan gelombang radio yang menjadi media transmisinya, oleh karena itu jaringan

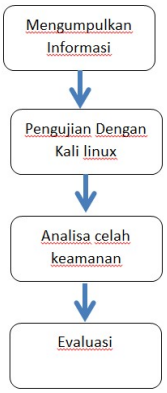
komputer sangatlah rentan terhadap penyusupan serta serangan yang berasal dari semua arah karena menggunakan pancaran gelombang radio (Wibowo et al., 2017).

Jaringan komputer yang sering diakses secara masal seperti halnya jaringan wifi hotspot rentan terhadap gangguan sistem oleh karenanya diperluan bermacam-macam aturan terhadap pengunaan sistem jaringan tersebut. Ada berbagi macam aturan yang diterpkan untuk mengontrol kinerja maupun kondisi jaringan sehingga sistem berjalan sesuai dengan yang diharapkan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan analisa terhadap sistem keamanan yang ada dalam jaringan tersebut (Yunus, 2019). Kali linux adalah salah satu sistem operasi yang sering digunakan dalam melakukan penetration testing serta untuk audit keamanan jaringan computer dari keluarga Linux tingkat lanjut yang kembangkan oleh offensive Security. Kali Linux merupakan pembaharuan dari Back Track Linux secara sempurna dan stabil, sesuai dengan standar pengembangan Debian dan rilis sekitar tahun 2014 (Muhammad Addy, 2017).

Maka jaringan wireless sangat berperan penting dalam kelancaran proses kegiatan akademik STMIK Bina Patria pada saat. STMIK Bina Patria menggunakan sistem operasi MikrotikOS untuk pengelolan dan manajemen jaringan yang berjalan. Sistem keamanan jaringan wireless yang digunakan STMIK Bina Patria yaitu WPA2. Tingkat keamanan yang baik akan menentukan mudah atau sulitnya masuk dalam jaringan wireless tersebut (Muhammad Addy, 2017). Sehingga dengan keamann yang terenkripsi diharapkan akan meningkatkan keamanan jaringan dari ganguan pembobolan dan pengintaian dari pihak lain(Rusdi & Prasti, 2019). *American Psychological Association 6th Edition (APA style*) (Erwin, 2015).

METODE

Tahapan dalam penelitian ditunjukan Oleh Gambar 1 dibawah ini



Gambar 1. Tahapan Penelitian yang dilakukan.

Semua tahapan diatas sudah mencakup langkah awal yaitu pengumpulan data, implementasi dan evaluasi sistem. Penelitian ini menggunakan metode penelitian tindakan atau *action research*. Penelitian

tindakan merupakan kegiatan dengan mengujicobakan sebuah gagasan ke dalam praktek atau situasi nyata berskala mikro sehingga diharapkan kegiatan tersebut dapat memperbaiki, meningkatkan kualitas, dan melakukan perbaikan(Zuriah, 2003).Adapun tahapan penelitian yang merupakan siklus dari *action research* adalah:

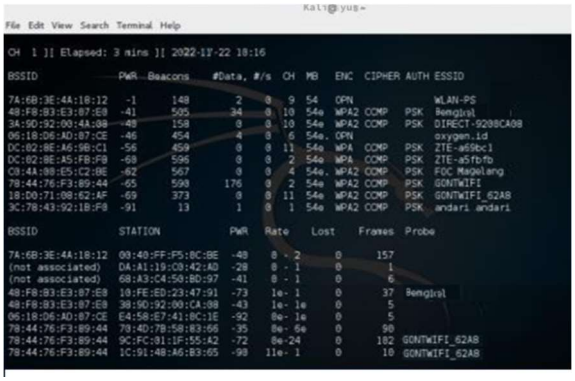
1. *Diagnosing*, dengan melakukan identifikasi masalah-masalah pokok yang ada.
2. *Action Planning*, memahami pokok masalah yang ada kemudian dilanjutkan dengan melakukan rencana tindakkan yang tepat ketika akan menyelesaikan masalah yang ada.
3. *Action Taking*, dengan melakukan implementasi dan tindakkan dari rencana yang telah dibuat dengan harapan dapat menyelesaikan masalah.
4. E*valuating*, melaksanakan evaluasi terhadap hasil implementasi yang telah dilakukan.

HASIL DAN DISKUSI

Pada penelitian ini, pengujian dilakukan di dalam Laboratorium Kampus STMIK Bina Patria. Pengujian dilakukan dengan 4 tahapan berbeda yaitu :

Cracking The Ecryption

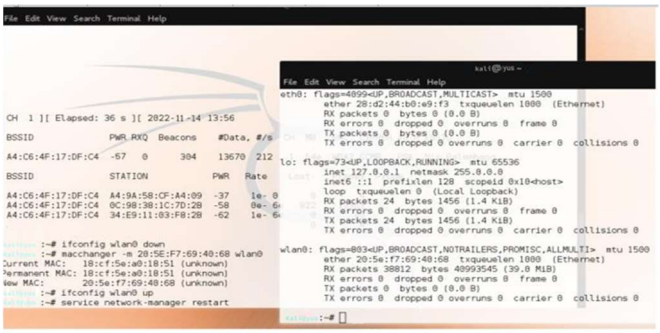
Melakukan Scanning tujuan dari serangan cara ini dilakukan untuk mengetahui apakah semua access point dilindungi dengan sistem keamanan terenkripsi seperti halnya WEP, WPA ataupun WPA2. Dengan uji scanning terhadap access point tersebut selanjutnya menentukan target untuk mencoba cracking terhadap key yang digunakan sebagai pengamanan yang ditunjukkan pada Gambar 2.



Gambar 2. Ilustrasi Scanning

Bypassing MAC Authentication

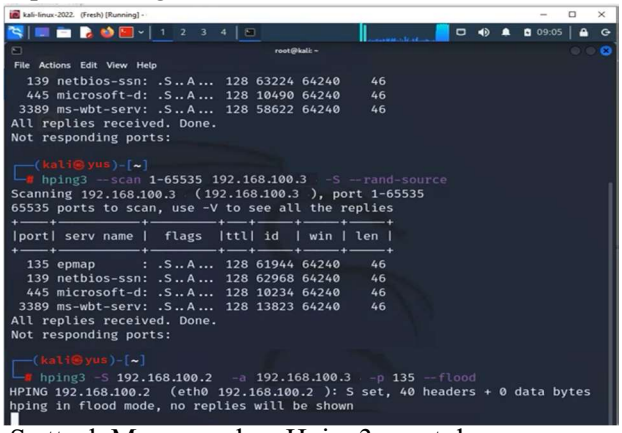
Selanjutnya melakukan Bypassing MAC Authentication, tujuan dari percobaan ini adalah untuk mengetahui apakah sistem keamanan menggunakan metode pembatasan hak akses dengan MAC filtering atau tidak. Setelah melakukan percobaan dengan cara menghubungkan antara perangkat pengujian serta access point dapat ditemukan bahwa system keamanan dari jaringan wireless tersebut menggunakan MAC filtering.



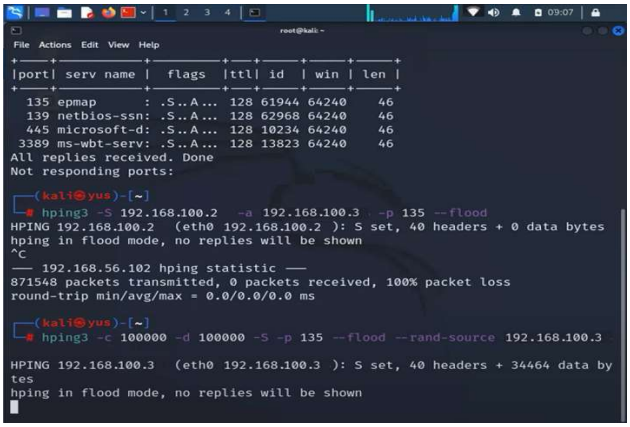
Gambar 3. Bypassing MAC Authentication

Attacking The Infrastructure

Tahap selanjutnya serangan pada layanan mesin dan wireless untuk client sehingga dapat mempengaruhi kinerja jaringan dan juga mesin pc tersebut. Bentuk serangan ini melakukan serangan ke infrastruktur jaringan DoS attack menggunakan Hping yang bertujuan melumpuhkan koneksi user lain di dalam jaringan. Informasi yang penting adalah password dari jaringan wireless yang diuji, agar komputer tester dapat terhubung dengan layanan wireless. Gambar 4 dan 5 menunjukkan DoS attack menggunakan Hping3 saat melakukan tahap Attacking the Infrastructure.



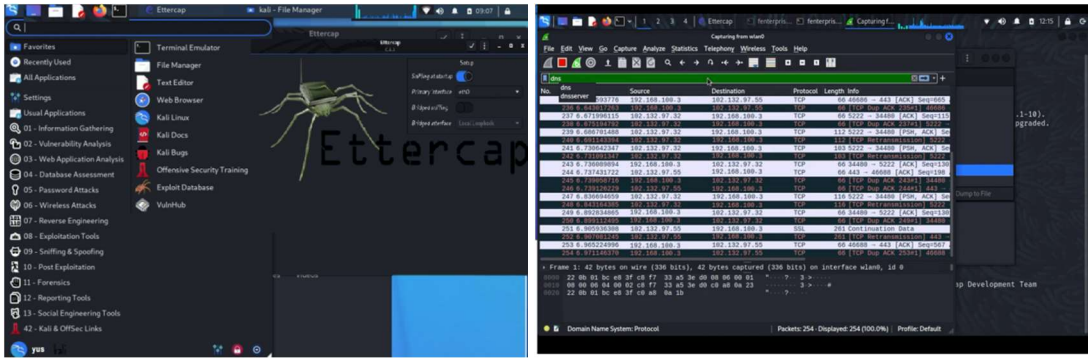
Gambar 4 DoS attack Menggunakan Hping3 ~ untuk menyerang resource mesin



Gambar 5. DoS attack Menggunakan Hping3 ~c pada resource jaringanya

Man In The Middle (MITM) Attack

Tahap selanjutnya melakukan serangan terhadap user pada jaringan WLAN yang sama dengan melakukan penyadapan paket data. Pengujian ini menggunakan aplikasi ettercap sebagai alat uji dan juga wireshark. Tampilan Ettercap ditunjukkan pada Gambar 6.



Gambar 6. Tampilan Ettercap dan Wireshark

Ditahapan ini yaitu Man In The Middle Attack, pertama-tama yang diperlukan adalah komputer tester serta komputer target yang perlu terhubung di jaringan wireless tersebut „Hotspot STMIK BIPA". Pada tahapan ini komputer tester akan mempunyai peran sebagai pihak ketiga disamping target serta access point yang menjadi perantara target serta layanan internet yang ada pada jaringan tersebut. Pada tahapan ini, konfigurasi ettercap yang menjadi target pertama adalah gateway dari Access Point yaitu 192.168.100.3 dan yang menjadi target kedua adalah IP dari komputer target yaitu 102.132.97.32.

Kemudian melakukan Address Resolution Protocol (ARP) ke dalam TCP/IP Protocol Suite yang bertanggung jawab dalam melakukan resolusi alamat IP Media Access Control (MAC Address). ARP Poisoning merupakan suatu teknik menyerang pada jaringan komputer local baik dengan media kabel maupun wireless, yang memungkinka penyerang bisa mengetahui frames data pada jaringan local atau melakukan modifikasi traffic atau bahkan menghentikan traffic. Pada prinsipnya ARP poisoning ini memanfaatkan kelemahan pada teknologi jaringan komputer sendiri yang menggunakan ARP broadcastEvaluasi dilakukan supaya dapat mengetahui tingkat kerentanan dalam jaringan *wireless local area network*, dengan melakukan 4 tahapan penyerangan maka terbukti kerentanan jaringan *wireless local area network* yang di miliki Laboratorium STMIK Bina Patria bisa di katakan kurang baik. Secara keseluruhan, implementasi dari pengujian keamanan jaringan *wireless local area network* dengan metode penetration testing dapat dilihat pada Tabel 1

Tabel 1. Hasil Dari Penetrasi Testing dengan Kali Linux

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

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama Analisa Keamanan Jaringan Wireless dengan Metode Penetration Testing (Cracking The Encryption, Bypassing MAC Authentication, Attacking The Infrastructure dan MITM) menggunakan Kali Linux, maka dapat di ambil kesimpulan bahwa: (1) Dalam menerapkan penetration testing pada sebuah institusi dibutuhkan jaminan hukum terhadap pelaku dan objek penetration testing. (2) Keamanan jaringan menggunakan metode Penetration Testing dapat memberikan gambaran tentang kelemahan sistem jaringan WLAN di Laboratorium STMIK Bina Patria yang masih memiliki banyak celah untuk dieksploitasi. Hal tersebut ditunjukan dengan bukti hasil penelitian dengan melakukan empat jenis serangan, hanya satu yang berstatus gagal yaitu pada jenis serangan Bypassing WLAN Authentication. (3) Gagalnya tahapan Bypassing WLAN Authentication di karenakan pada proses ini dibutuhkan penyamaan MAC Address dalam 1 jaringan wireless, sedangkan Laboratorium STMIK Bina sudah memakai Router MikrotikOS yang dengan fitur firewall mampu menolak MAC Address yang sama, jadi jika ada MAC Address yang sama tidak akan bisa masuk ke dalam jaringan WLAN tersebut.

REFERENSI

Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan)*, *5*(2), 1–8. https://doi.org/10.47970/siskom-kb.v5i2.268

Erwin, gunadhi H. arranuri. (2015). Pengamanan Basis Data Pengelolaan Hak Akses Dengan Metode Role—Based Access Control. *Algoritma*, *12*(1).

Kurniadi, A. (2021). *Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)*. *1*(1).

Muhammad Addy, R. (2017). *IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER*. Universitas Telkom.

Rusdi, M. I., & Prasti, D. (2019). *Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux*.

Sahren, S., Dalimuthe, R. A., & Amin, M. (2019). Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus. *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, *1*, 994. https://doi.org/10.30645/senaris.v1i0.109

Supriadi, D., Fahmi, H., & Imtihan, K. (2018). ANALISA DAN PERANCANGAN INFRASTRUKTUR JARINGAN WIRELESS LOCAL AREA NETWORK (WLAN) PADA DINAS PERINDUSTRIAN DAN PERDAGANGAN KABUPATEN LOMBOK TENGAH. *Jurnal Informatika dan Rekayasa Elektronik*, *1*(2), 1. https://doi.org/10.36595/jire.v1i2.53

Wibowo, M. G. H., Triyono, J., & Sutanta, E. (2017). *KEAMANAN JARINGAN WLAN TERHADAP SERANGAN WIRELESS HACKING PADA DINAS KOMUNIKASI & INFORMATIKA DIY*. *1*(1).

Yunus, M. (2019). ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY TOOLS PROJECT BERDASARKAN FRAMEWORK OWASP VERSI 4. *Jurnal Ilmiah Informatika Komputer*, *24*, 37–48. https://doi.org/10.35760/ik.2019.v24i1.1988

Zuriah. (2003). *Penelitian Tindakan Dalam Bidang Pendidikan dan Sosial*. Banyu Publishing.