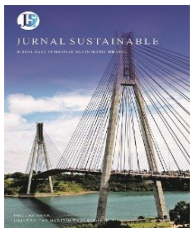


Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan
Vol. 12 , No. 01, hal. 23-29, Mei 2023
Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan
ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

ANALISIS PENERAPAN METODE *PENETRATION TESTING* PADA KEAMANAN JARINGAN WLAN (Studi Kasus: Universitas Maritim Raja Ali Haji)

Afrio Triputra Sitompul[1], Ferdi Chahyadi[2,*], Nurfalinda[3]
[1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Maritim Raja Ali Haji
[1,2,3]Jl. Politeknik Senggarang, Tanjungpinang 29100
[*]Corresponding Author: ferdi.chahyadi@umrah.ac.id

Abstract—This test is carried out to find security holes in the *Wireless* Local Area Network (WLAN) network. In this paper, author simulates attacks on a WLAN network using four attack parameters: Bypassing MAC Authentication, Attacking The Infrastructure and Man In The Middle Attacks. There were four attacks carried out, and two of them were successful. Thus, it can be concluded that the Raja Ali Haji Maritime University (UMRAH) WLAN network is quite secure. Nonetheless, other offensive actions, such as infrastructure attacks or Man In the Middle Attacks, In order to ensure more security, it is necessary to add a DNS Security Extensions protocol to prevent fake DNS redirects, add a firewall to the security system and use TLS on captive portals
Keywords— WLAN, *Penetration testing*, Network security

Intisari— Pengujian ini dilakukan dengan mencari celah keamanan pada jaringan *Wireless* Local Area Network (WLAN). Penulis melakukan simulasi serangan dengan Metode *Penetration testing* menggunakan tiga parameter serangan yaitu, Bypassing MAC Authentication, Attacking The Infrastructure dan Man In The Middle Attack pada jaringan WLAN dua dari empat serangan yang dilakukan berhasil dijalankan, maka dapat disimpulkan jaringan WLAN Universitas Maritim Raja Ali Haji (UMRAH) sudah cukup aman, namun tidak menutup kemungkinan terhadap serangan lain seperti Attacking the infrastructure dan Man in the middle Attack, agar keamanan lebih terjamin perlunya penambahan protokol DNS Security Extensions untuk menghalangi pengarahan DNS palsu, penambahan firewall pada sistem keamanan dan penggunaan TLS pada captive portal
Kata kunci— WLAN, *Penetration testing*, Keamanan jaringan.

I. PENDAHULUAN

Perkembangan teknologi informasi sangat pesat, dimana komunikasi terus berkembang dan sulit terpisahkan dari kehidupan manusia, dengan kemajuan teknologi berbagi informasi kepada orang lain lebih cepat dan mudah salah satu contoh dari kemajuan teknologi tersebut adalah *Wireless Local Area Network* (WLAN) atau disebut juga jaringan lokal nirkabel. Penggunaan teknologi ini sudah diterapkan di

berbagai kampus salah satunya yaitu Universitas Maritim Raja Ali Haji (UMRAH) dimana mahasiswa dapat dengan mudah mengakses *wifi* sebagai media internet di area kampus yang dapat dipergunakan untuk mencari atau mengumpulkan tugas yang diberikan dosen. Keamanan jaringan merupakan salah satu aspek penting dari sebuah sistem informasi [1]. Dalam menganalisa keamanan jaringan dengan metode *Penetration testing* bentuk serangan terhadap jaringan dapat disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux. Berbeda dengan distro-distro linux yang lain, semisal Ubuntu yang lebih mengutamakan aspek *user* friendly dan balancing, Kali Linux dirancang khusus untuk pengujian keamanan jaringan, dengan dilengkapi aplikasi pendukung yang digunakan dalam aktivitas hacking dan memanfaatkannya sebagai alat pengujian keamanan jaringan [2]. Keamanan jaringan merupakan sebuah entitas dimana befungsi untuk menjaga keamanan sebuah informasi maupun data yang ditransfer melalui internet sehingga file yang dikirimkan maupun yang ditransfer dapat sampai ke tujuan tanpa distorsi gangguan [4].

Perancangan sistem keamanan jaringan *wireless* yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para hacker [3]. Dikarenakan kurangnya kesadaran administrator atau orang yang berperan sebagai admin dalam menjalankan sistem aplikasi tersebut, sedangkan faktor eksternal bisa terjadi dikarenakan lemahnya sistem yang dibuat (*configuration)* dan besarnya tingkat kejahatan cyber [6]. Keamanan jaringan komputer sebagai bagian dari sebuah system yang penting untuk menjaga validitas dan integritas data. Jaringan komputer sangat berkaitan erat dengan jaringan nirkabel. Seperti komputer, notebook, handphone dan periperalnya mendominasi pemakaian teknologi *wireless.* Penggunaan teknologi *wireless* dalam suatu jaringan lokal sering dinamakan dengan WLAN (*Wireless Local Area Network*) [5].

Dari permasalahan tersebut maka perlu dilakukan dilakukan analisis keamanan jaringan WLAN dengan menerapkan metode *penetration testing* dengan menggunakan empat jenis serangan yaitu *Bypassing MAC Authentication, Attacking The Infrastructure* dan *Man In The Middle Attack* dimana serangan ini bertujuan untuk mengatasi permasalahan keamanan jaringan WLAN dan hasil dari analisis ini di harapkan dapat menjadi rekomendasi kepada PTIK untuk pengembangan sistem yang lebih baik.

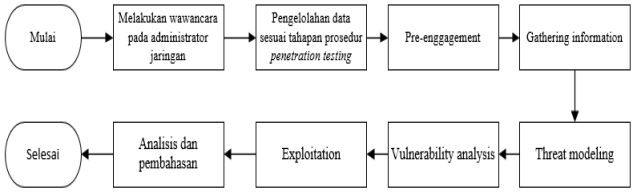
II. METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian experimen karena penelitian ini bertujuan untuk mengetahui kerentanan WLAN saat diberi beberapa serangan dengan mengikuti prosedur *penetration testing,* serangan dilakukan dengan tiga jenis yaitu *Bypassing MAC Authentication, Attacking the Infrastructure* dan *Man in the middle attack*

Pada penelitian ini dilakukan dengan mengumpulkan data dengan melakukan wawancara terlebih dahulu kepada administrator jaringan di PTIK untuk menetukan celah yang akan digunakan dalam proses *penetration testing* nantinya, tahapan pertama yang akan dilakukan penulis adalah mengidentifikasi masalah dimana sebelum penulis melakukan kegiatan pentest pada jaringan *Wireless* Local Area Network (WLAN) Pada penelitian ini penulis melakukan simulasi serangan pada jaringan WLAN untuk mengetahui tingkat keamanan yang sudah ada. Kemudian penulis melakukan pengumpulan data

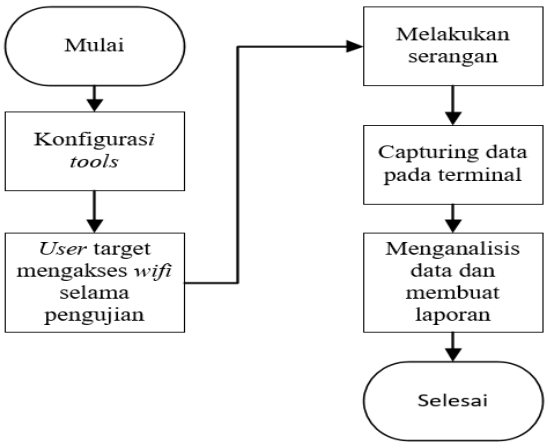
ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

dengan melakukan studi literatur mengumpulkan referensi dari jurnal, buku-buku yang berisi bagaimana melakukan pengujian jaringan *Wireless Local Area Network* (WLAN) pada sistem operasi kali linux. Pada tahap selanjutnya penulis melakukan analisis dari permasalahan serta pengumpulan data untuk dijadikan pembahasan sehingga penulis dapat menyimpulkan hasil dari penelitian ini



Gambar 1. Flowchart Analisis Pengelolahan Data

Penelitian ini Penelitian ini dimulai dengan melakukan wawancara pada administrator jaringan kemudian penulis melakukan analisis mengikuti ketentuan *penetration testing* dari data yang didapatkan, pada tahap *Pre-enggagement* yaitu penjelasan kegiatan yang akan dilakukan, selanjutnya mengelolah informasi yang didapatkan pada *Gathering information,* mengidentifikasi ancaman pada *Threat modeling*, mencari celah yang akan dianalisis pada *Vulnerability Analysis* dan melakukan uji serangan pada tahapan *Exploitation*



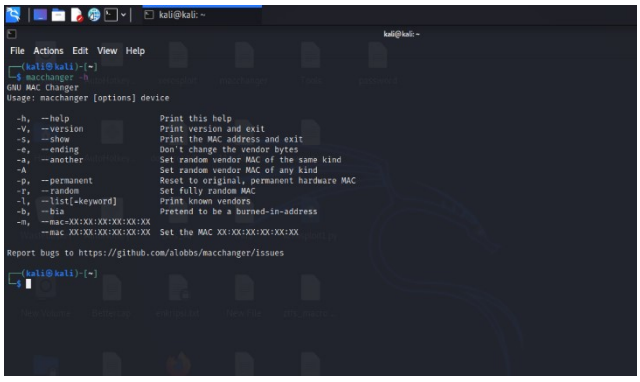
Gambar 2. Skema Teknik Pengujian

Tahapaan ini penulis melakukan implementasi sesuai dengan tahapan-tahapan dari metode *Penetration testing*. Selanjutnya penulis melakukan simulasi serangan untuk mengetahui tingkat kerentanan dari jaringan WLAN Universitas Maritim Raja Ali Haji dengan melakukan serangan *Bypassing MAC Authentication, Attacking the Infrastructure* dan *Man in the middle attack*. Tipe *pentes* yang digunakan yaitu *Overt penetration testing* dimana pengujian jaringan dilakukan dengan sepengetahuan pihak PTIK.

III. HASIL DAN PEMBAHASAN

A. Bypassing Mac Authentication

Seluruh Bypassing MAC authentication yaitu proses mengubah identitas MAC untuk mengatasi MAC *address filtering*. Mengganti MAC *address* bisa dilakukan pada sistem operasi kali linux karena MAC *address* akan tersimpan pada NIC (Network Interface Card) dan tersimpan pada basis data linux. Pengujian ini dilakukan pada *wifi* UMRAH di lab 3 Teknik dimana tujuan dari serangan ini yaitu perubahan MAC *address* dengan tujuan untuk mengakses jaringan *Wireless Local Area Network* (WLAN). Pada pengujian ini MAC *address* dirubah dengan *tools macchang*



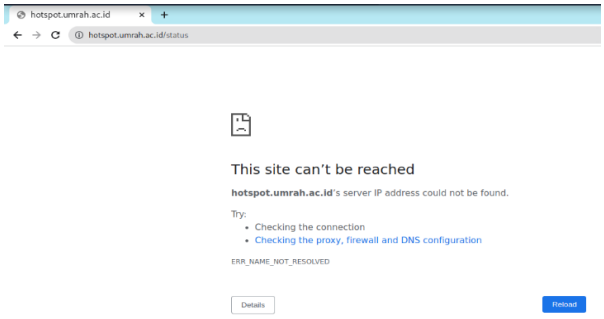
Gambar 3. Tampilan dari tools Macchanger

Penulis mengetik *macchanger-h* pada terminal perintah ini bertujuan untuk membuka *tools* macchanger dan disertai informasi seperti -

v (untuk menampilkan version dan keluar) dan -m (untuk set-up MAC *address* yang akan digunakan). Merupakan langkah-langkah yang dilakukan penulis untuk merubah MAC *address* pada terminal kali linux, Perubahan MAC *address* berhasil dilakukan telihat pada lampiran 3 dimana MAC *address* tersebut akan menggantikan permanen MAC *address* untuk sementara waktu.

Tabel 1 konfigurasi serangan pada tools macchanger

Konfigurasi serangan pada tools macchanger
1 Masuk sebagai root dengan menggunakan perintah ***"sudo su"***
2 Cek ip konfigurasi ***" ifconfig"***
3 Mengaktifkan mode monitor dan memutus interface jaringan ***"airmon-ng start wlan0"***
4 Menampilkan traffic *wireless* sekitar ***"airodump-ng wlan0mon"***
5 Pengembalian interface pada jaringan ***"ifconfig wlan0 down"***
6 Mengubah MAC *address* dengan perintah ***"macchanger -m 5c:93:a2:8b:2e:85 wlan0"***
7 Cek ip konfigurasi setelah MAC *address* dirubah ***" ifconfig"***



Gambar 4. Tampilan laptop attacker saat mengakses *wifi* UMRAH

Tampilan laptop attacker saat mencoba login pada *wifi* UMRAH dan hasilnya gagal dimana landing page login *wifi* UMRAH tidak muncul hingga MAC *address* dirubah kembali

B. Attack The Infrastructure

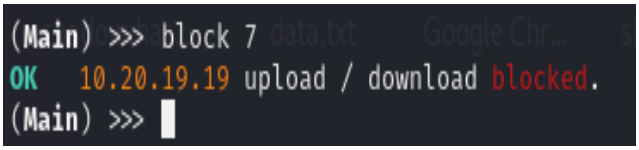
Attack the infrastructure yaitu jenis serangan yang dilakukan pada layanan *wireless* untuk *user* sehingga dapat mempengaruhi kinerja dari jaringan, bentuk dari serangan ini yaitu DoS dimana tujuan dari serangan ini untuk memutus koneksi *user* yang terhubung pada jaringan *Wireless* Local Area Network (WLAN) UMRAH. Adapun serangan dilakukan sebanyak dua kali serangan pertama menggunakan tools Evil Limiter dengan tujuan untuk memutus salah satu *user* yang terkoneksi ke jaringan *wifi* dan yang kedua yaitu serangan menggunakan tools aireplay-ng dengan tujuan memutus koneksi pada *user* yang terhubung dalam satu gateway.

1. Percobaan pertama

Tabel 2. Konfigurasi serangan pada tools Evil Limiter

Konfigurasi serangan pada tools Evil Limiter
1 Masuk sebagai root dengan menggunakan perintah ***"sudo su"***
2 Ketik ***"cd evillimiter"***
3 Menjalankan tools Evil Limiter ***"evillimiter"***
4 Menampilkan seluruh ip yang terhubung pada jaringan ***"scan"***
5 Melakukan pemutusan koneksi pada jaringan ***"block7"***

merupakan langkah-langkah untuk melakukan serangan terhadap jaringan pada *tools* Evil Limiter. Setelah melakukan scaning terlihat seluruh ip yang terhubung pada ip *gateway* 10.20.19.1



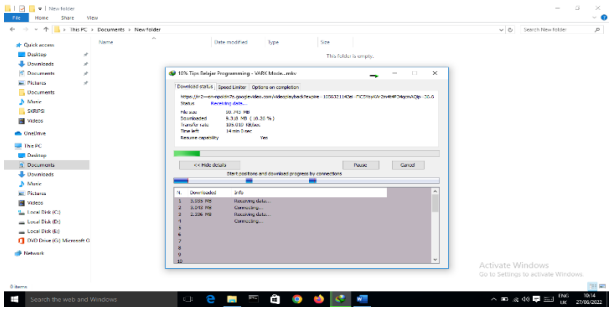
Gambar 5. Tampilan perintah block koneksi pada ip 10.20.19.19

Setelah setelah melakukan perintah block 7 yang merupakan ID hosts ip target yang akan dilakukan pemblokiran saat menggunakan jaringan *wifi* UMRAH

Tampilan laptop target yang masih bisa menggunakan jaringan *wifi* UMRAH dengan

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

lancar dan hasil dari serangan pada *wifi* UMRAH menggunakan tools Evil Limiter yaitu gagal



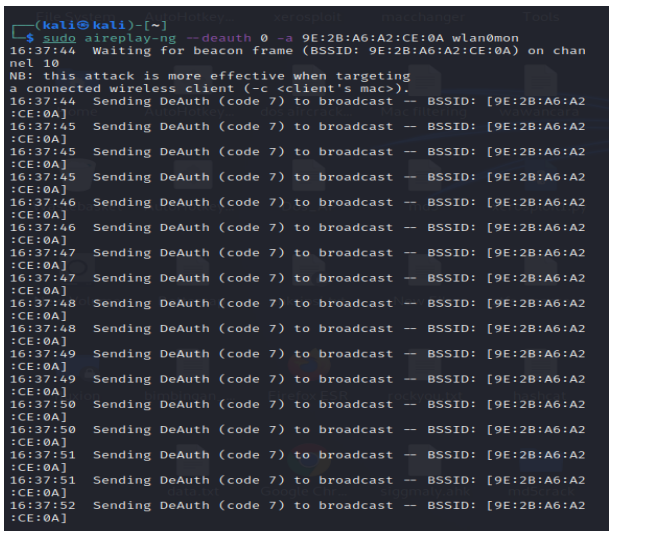
Gambar 6. Tampilan downlod pada IDM

2. *Percobaan kedua*

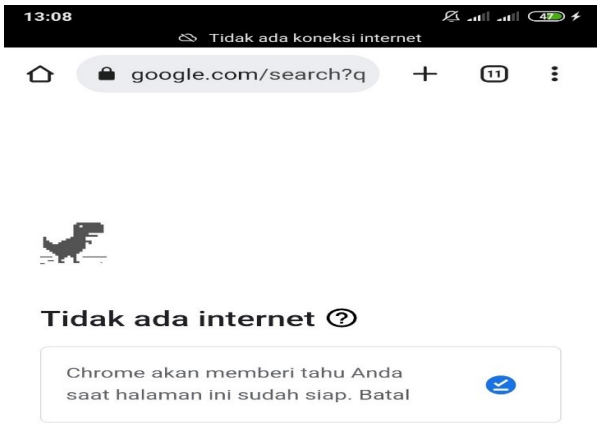
Tabel 3. konfigurasi serangan pada tools Aireplay-ng

Konfigurasi serangan pada tools Aireplay-ng	
1	Mengaktifkan mode monitor dan memutus interface jaringan ***"airmon-ng start wlan0"***
2	Menampilkan traffic *wireless* sekitar ***"airodump-ng wlan0mon"***
3	Target serangan ***"sudo airodump-ng wlan0mon -d 93:2b:a6:a2:ce:0a "***
4	Memulai serangan ***"sudo aireplay-ng –deauth 0 -a 93:2b:a6:a2:ce:0a wlan0mon"***

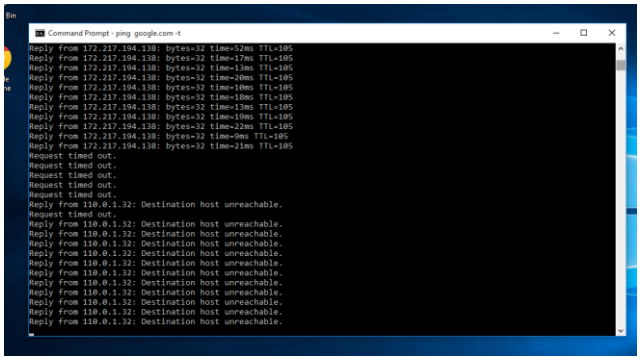
Merupakan langkah-langkah yang dilakukan penulis untuk melakukan serangan pemutusan koneksi pada jaringan UMRAH di lab 3 teknik.



Gambar 7. Tampilan serangan DeAuth pada *wifi* UMRAH di Lab Teknik



Gambar 8. Print screen halaman pengguna offline

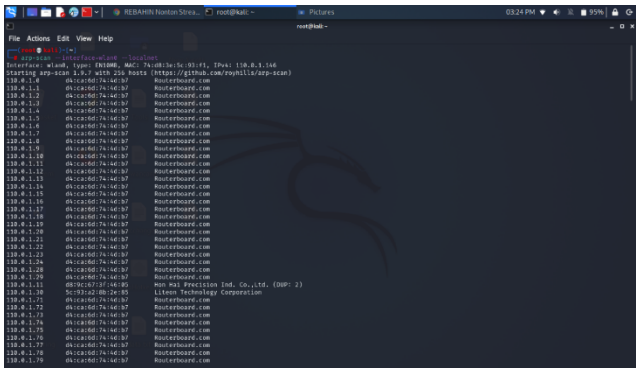


Gambar 9. Print screen tampilan CMD pengguna offline

Pada Gambar 8 dan Gambar 8 diatas merupakan pembuktian bahwa jaringan *Wireless* Local Area Network (WLAN) di Universitas Maritim Raja Ali Haji (UMRAH) masih dapat diserang dengan mengirim paket deauth kepada pengguna sehingga pengguna tidak dapat mengakses *wifi* tersebut hingga serangan dihentikan dan serangan juga berhasil pada tiga tempat yang berbeda.

C. *Man In The Middle Attack*

Man In The Middle (MITM) Attack adalah salah satu teknik penyerangan dengan kondisi dimana penyerang harus berada dalam satu jaringan *Wireless* Local Area Network (WLAN) dengan tujuan melakukan penyadapan atau perekaman pengetikan keyboard pada target yang akan login pada *wifi* UMRAH serangan dilakukan pada empat tempat yang berbeda. Berikut hasil dari percobaan yang sudah dilakukan penulis pada komputer target pada jaringan *wifi* UMRAH di lab 3 Teknik



Gambar 10. Tampilan hasil scanning interface wlan0

Penulis melakukan scanning pada terminal kali linux dengan perintah arp-scan –interface=WLAN0 –localnet dimana perintah ini bertujuan untuk menampilkan.

Tabel 4. konfigurasi serangan pada tools bettercap

Konfigurasi serangan pada tools bettercap	
1	Masuk sebagai root dengan menggunakan perintah ***"sudo su"***
2	Memulai penyadapan ***"bettercap -X -G 110.0.1.1 -S --proxy –proxy-https"***

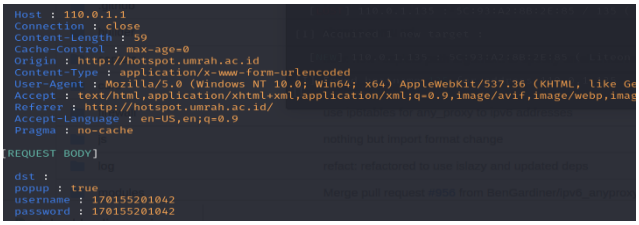
Merupakan langkah-langkah yang dilakukan penulis untuk melakukan penyadapan pada jaringan UMRAH di lab 3 teknik. setelah perintah dijalankan bettercap akan melakukan upaya pemutusan koneksi pada seluruh penggun yang terhubung kedalam jaringan

Gambar 11. Tampilan *user* yang terputus pada jaringan internet

Menampilkan kondisi *user* yang terhubung pada ip gateway 110.0.1.1 dimana bettercap akan mencoba untuk melakukan pemutusan koneksi pada *user* yang sedang menggunakan *wifi* UMRAH. Pada saat *user* login kembali pada landing page yang sudah berubah perekaman pengetikan terjadi

Gambar 12. Tampilan landing page *wifi* UMRAH saat MITM berlangsung

merupakan tampilan landing page umrah yang sudah berganti, tampilan ini hanya terjadi pada ip address yang terhubung pada gateway 110.0.1.1.



Gambar 13 Hasil perekaman dari tools bettercap

tampilan dari hasil perekaman pengetikan dari keyboard komputer target, dengan hasil diatas menunjukkan masih terdapat celah pada keamanan captive portal *wifi* UMRAH yang masih bisa disusupi dimana ini dapat membahayakan data pribadi pengguna jaringan tersebut dan serangan juga berhasil dilakukan di tiga tempat yang berbeda.

D. Report dari Metode Penetration testing

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

Tabel 5 Hasil dari pengujian *Penetration testing*

Jenis serangan	Informasi yang dibutuhkan	Status
Bypassing MAC Authentication	List MAC *user* lain yang terhubung di jaringan	Gagal
Attacking The Infrastructure	Attacker harus berada dalam jaringan WLAN, ip adress tester	Gagal
	Bssid dan MAC adress dari perangkat tester	Berhasil
Man In The Middle Attack	Attacker harus berada dalam jaringan WLAN, ip adress dari *user* dan ip router	Berhasil

IV. KESIMPULAN

Pengujian keamanan jaringan *Wireless* Local Area Network dengan metode *penetration testing* di Universitas Maritim Raja Ali Haji dengan jenis serangan, *Bypassing MAC Authentication, Attacking the Infrastructure* dan *Man in the middle attack* dari hasil pengujian tersebut menunjukan bahwa jaringan *Wireless* Local Area Network (WLAN) UMRAH sudah cukup bagus dari empat serangan hanya dua yang berhasil. Hal ini dikarenakan *wireless* tersebut sudah menggunakan halaman login (captive portal), Filtering di setiap MAC addres *user* yang akan login kedalam jaringan, Celah keamanan masih terdapat pada jaringan *Wireless* Local Area Network (WLAN) Universitas Maritim Raja Ali Haji yaitu pada landing page *wifi* yang masih bisa disusupi oleh penyusup dan pemutusan koneksi pada *user* yang terhubung pada jaringan internet. Serangan DeAuthentication dapat dicegah dengan penambahan firewall, dimana firewall akan melakukan validasi DeAuthentication frame terhadap seluruh serangan yang dilakukan terhadap jaringan dan perlunya penambahan protokol DNS Security Extensions (DNSSEC) dimana protokol ini mampu menghalangi pengarahan pada DNS palsu seluruh user yang akan terhubung kedalam jaringan wifi dan penambahan TLS pada halaman login wifi UMRAH.

REFERENSI

[1] Amarudin, A. 2018, Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking. Prosiding Semnastek.

[2] Bayu, M., K., Yamin., L. F. Aksara, 2018, Analisis Keamanan Jaringan WLAN Dengan Metode Penetration testing (Studi Kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO), semanTIK, Vol. 3, No, 2.

[3] Fauzi, A. R. F., & Suartana, I. M. 2018. Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. Jurnal Manajemen Informatika, Vol. 8

[4] Prasetyo, S. E., & Lee, R. C. 2021, Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing. In CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences. Vol. 1, No. 1, pp. 710-718.

[5] Santoso, J. D. 2019. Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. INFOS Journal-Information System Journal, Vol. 1, No 44-50.

[6] Sirait, F., & Putra, K. 2018, Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan. Jurnal Teknologi Elektro, Universitas Mercu Buana, 9.