BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan nirkabel atau yang sering disebut dengan wifi, yang ditetapkan sebagai teknologi untuk menghubungkan perangkat digital seperti; ponsel pintar, tablet, laptop, dan perangkat IoT. telah menimbulkan ancaman dalam keamanan Data. Tidak adanya langkah-langkah keamanan yang tidak fleksibel telah membuat banyak organisasi menyumbang jutaan untuk memverifikasi sistem mereka. pengembangan konvensi keamanan yang berbeda untuk LAN Nirkabel, kerentanan WEP/WPA/WPA2/WPA3 bagaimana jaringan nirkabel diserang menggunakan kelemahan desain yang ada dalam Protokol Keamanan Nirkabel.[1]

Router sebagai perangkat yang sangat penting untuk mengatur keluar dan masuknya data pada suatu jaringan, router berada pada lapisan terluar yang terhubung langsung ke jaringan publik. Router mempunyai berbagai fitur, antara lain; manajemen user hotspot, manajemen bandwith, manajemen akses jalur kebutuhan komunikasi data pelanggan semakin meningkat setiap tahun, sehingga membuat pengamanan pada router perlu diperhatikan. [2].

Deauther merupakan serangan yang menghalangi semua perangkat untuk terhubung ke jaringan. memutuskan sambungan dari jaringan, dan mencegahnya menyambung kembali. Deauther Esp8266 menggunakan *hardware Microcontroller* Esp8266 yang akan di konfigurasi untuk melakukan serangan Deauther dan melakukan phishing SSID. Bekerja di *Data Link* dan *Network*. Dengan memanfaatkan struktur data dengan cara membuat paket-paket palsu terhadap perangkat router, ketika paket dikirimkan dari deauther membuat

terganggunya proses koneksi antara client dan router yang mengakibatkan terputusnya jaringan antara client dan router. penyerang akan melakukan phising SSID dengan membanjiri frekuensi Wifi 802.11 (2400 - 2483.5 MHz, 5180 – 5825 MHz). Dengan SSID phising.

Serangan ini mengeksploitasi kemampuan rentan dari *The 4-way handshake* di WPA2 yang mengamankan Wi-Fi modern. Penyerang dapat mengelabui korban agar menginstal ulang kunci yang sudah digunakan. Hal ini dilakukan dengan memanipulasi dan memutar ulang pesan *handshake* kriptografis untuk mengatur ulang parameter terkait kunci ke nilai awalnya. Ini akan memungkinkan paket untuk di putar ulang, didekripsi dan atau di palsukan. [3]. Serangan Deauther Esp8266 Wi-Fi berhasil diterapkan pada arsitektur smart farm yang terhubung ke jaringan 2.4 GHz. Serangan ini termasuk dalam serangan Denial of Service (DoS) dan mengeksploitasi kerentanan 802.11. [4]

Penyerang akan membangkitkan satu frekuensi yang sama dengan frekuensi pada wireless LAN dengan menggunakan daya yang lebih besar daripada wireless LAN eksisting. Hal ini mengakibatkan sistem pada wireless LAN seolah-olah mendapatkan noise yang besar dari luar sehingga membuat komunikasi antara Router dan client terputus. [5] Di sisi pengguna, akan terputus dari titik akses aslinya dan akan memaksa pengguna untuk terhubung ke titik akses palsu. Sertifikat SSL akan muncul di layar pengguna yang meminta untuk masuk ke jaringan karena beberapa masalah keamanan. [6]

Handshake muncul ketika pengguna memasukkan kata sandi dan kata sandi itu cocok dengannya. kata sandi cocok, pengguna akan terputus dari AP palsu dan kata sandi ditampilkan di terminal Informasi WiFi. [7] Pada penelitian ini

penulis akan melakukan analisis dengan melakukan pengujian serangan terhadap perangkat router, Uji coba menggunakan topologi jaringan Personal area network, dengan frekuensi rentan router 2.4 ghz, standar IEEE 802.11 b/g/n. penulis menggunakan metode VAPT (*Vulnerability Assessment & Penetration Testing*) sebagai penilaian serta pengujian terhadap kerentanan keamanan yang ada.

Pokok permasalahan tersebut yang akan dibahas pada penelitian ini dengan melakukan analisis serangan deauther menguji coba serangan terhadap router dengan frekuensi 2.4 ghz dan untuk pengujian protokol menggunakan router yang menggunakan standar IEEE 802.11 b/g/n dengan melakukan serangan deauther terhadap router. pada tahap pengujian simulasi serangan untuk mengetahui dampak yang terjadi dan digunakan sebagai laporan analisis untuk dilakukan proses evaluasi kelemahan dan ancaman serangan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah sebagai berikut :

1. Bagaimana melakukan serangan wi-fi deauther ESP8266 ?
2. Bagaimana hasil evaluasi kelemahan dan ancaman dari serangan wi-fi deauther ESP8266 ?

1.3 Tujuan Penelitian

Tujuan analisis perancangan yang akan dicapai dari penelitian ini adalah:

1. Untuk mencari kelemahan serangan Deauther Esp8266.
2. Mengamankan perangkat wifi.
3. Menguji dan menganalisa keamanan perangkat.
4. Memberikan beberapa strategi pertahanan terhadap serangan Deauther Esp8266.
5. Menguji kerentanan jaringan 2.4 GHz.
6. Menguji kerentanan 802.11
7. Untuk membangun kesadaran yang lebih besar tentang masalah yang terkait dengan keamanan nirkabel.
8. Menganalisa serangan Deauther Esp8266.
9. Penetration Test perangkat.
10. Studi tentang protokol untuk menguji mekanisme keamanan router.

1.4 Batasan Masalah

Pada pembahasan ini penulis menyimpulkan beberapa batasan masalah dalam penelitian adalah sebagai berikut:

1. Perancangan serangan menggunakan Deauther Esp8266.
2. Topologi PAN (Personal Area Network).
3. Konfigurasi Nodemcu firmware programmer.
4. Konfigurasi IP port COM.
5. Tenda N300 f6 IEEE 802.11 b/g/n
6. Pengiriman paket palsu deauthentication
7. Phissing ssid evil twin

1.5 Manfaat Penelitian

Manfaat dari penelitian ini :

1. Melakukan pencegahan terhadap serangan Deauther Esp8266.
2. Mengedukasi para Administrator jaringan terhadap keamanan.
3. Melakukan pencegahan ancaman penyusup ke dalam jaringan.
4. Memberikan Informasi tentang enkripsi.
5. Mengevaluasi keamanan sistem perangkat.
6. Untuk memperbaiki kerentanan.

1.6 Metode Penelitian

Penulis menggunakan beberapa metode dalam penulisan ini. Metode yang digunakan antara lain :

1.6.1 Metode Pengumpulan Data

Pada tahapan ini penulis mencari informasi yang berkaitan tentang teknologi keamanan dan jaringan komputer. Referensi didapat dan diperoleh melalui Internet situs-situs jurnal serta studi pendahulu yang dapat dipercaya dan akurat. Serta menyesuaikan keadaan dalam pengambilan informasi di lapangan sebagai bahan teori dari penelitian. Dengan Tujuan dari tahapan ini dapat memperoleh informasi yang dapat membantu menyelesaikan permasalahan terkait.

1.6.2 Metode VAPT (Vulnerability Assessment & Penetration Testing)

Dalam mendukung penelitian tersebut, penulis menggunakan metode VAPT (*Vulnerability Assessment & Penetration Testing*) merupakan metode yang dapat digunakan untuk melakukan penilaian serta pengujian terhadap kerentanan keamanan yang ada. Hasil dari penelitian ini adalah kerentanan keamanan yang akan digunakan pada tahap pengujian simulasi serangan untuk mengetahui dampak yang terjadi dan digunakan sebagai laporan kepada pihak terkait untuk dilakukan proses evaluasi. metode VAPT yang meliputi.[8]

a. Scope adalah tahapan peneliti dengan menentukan ruang lingkup penelitian, dan pada Penelitian ini berfokus pada menemukan dan mengeksploitasi kerentanan Wifi Router.

b. Reconnaisance adalah proses mengumpulkan informasi awal tentang sistem baik target dengan cara aktif atau pasif. Informasi itu dapat berupa sistem protokol jaringan yang dipakai Wifi Router, Frekuensi, Enkripsi yang digunakan dan Perangkat yang digunakan pada target yang akan diuji. informasi ini diperoleh dengan menggunakan tools wifi scanner dalam memata-matai target.

c. Vulnerability Detection ini merupakan hasil dari pencarian celah keamanan pada target. Hasil dari temuan celah berupa informasi ini terbatas pada proses sniffing traffic tools whireshark seperti yang digunakan standar protokol IEEE 802.11 b/g/n pada router. digunakan sebagai bahan evaluasi dan pengujian serangan deauther esp8266. Yang akan digunakan sebagai dasar perencanaan pada tahap berikutnya.

d. Information Analysis & Planning Pada tahap ini akan melakukan perencanaan pengujian yang didasarkan pada celah dan melakukan perencanaan pengujian yang didasarkan pada celah yang didapatkan. Hasil analisis kemudian akan dilanjutkan dengan perencanaan simulasi penyerangan.

e. Penetration testing Pada tahap ini peneliti melakukan serangan terhadap target berdasarkan analisis dan perencanaan yang dirancang pada fase sebelumnya.

f. Privilege Escalation adalah memanfaatkan celah keamanan yang berhasil dilakukan pada proses penetration testing. Pemanfaatan celah yang dimaksud adalah manajemen data dan pemanfaatan hak akses.

g. Reporting adalah tahap penulisan laporan hasil penelitian yang nantinya akan diserahkan sebagai bahan laporan analisis kerentanan celah yang sudah didapatkan.