BAB I

PENDAHULUAN

1.1 Latar Belakang

Sekarang ini penggunaan perangkat teknologi jaringan WiFi sudah berkembang luas di seluruh dunia, baik digunakan untuk komunikasi suara maupun data. Jaringan WiFi memanfaatkan frekuensi tinggi untuk menghantarkan dan menghubungkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh *user* maupun oleh operator yang memberikan layanan komunikasi. Namun, dengan adanya *user* yang memanfaatkan teknologi jaringan WiFi, maka dapat memberikan sedikit celah keamanan yang dapat dimanfaatkan oleh *attacker*. Kemudian *attacker* dapat mengetahui password keamanan WPA2-PSK pada saat *user* terhubung ke jaringan WiFi tersebut. Sehingga dihasilkan password melalui beberapa teknik dan pengujian yang digunakan. Diantaranya dengan memanfaatkan *user* yang terhubung ke jaringan WiFi, pengujian SSID palsu dan pengujian WPS PIN. Namun pada penelitian ini hanya dilakukan pengujian melalui *user* yang terhubung ke jaringan WiFi. Teknik dan pengujian ini semata-mata dilakukan untuk penetrasi terhadap keamanan jaringan WiFi, yang bertujuan untuk mengetahui password WPA2-PSK pada jaringan WiFi (Baihaqi & Yanti, 2018)

Keamanan jaringan WLAN merupakan hal penting yang perlu diketahui oleh pengelola jaringan, agar dapat diketahui tingkat keamanan jaringan yang

disediakan. Dan jaringan komputer kabel dan WLAN biasanya dipakai sebagai media pertukaran data/informasi untuk pelayanan umum atau komersial, kepegawaian, dan lainnya. Penggunaan media WLAN tersebut rentan terhadap ancaman serangan karena menggunakan gelombang radio. Penelitian ini dilakukan untuk memperoleh hasil pengujian keamanan jaringan *wireless*, sehingga bisa digunakan sebagai masukan bagi pengelola dalam rangka menjaga dan/atau meningkatkan kualitas layanan koneksi jaringan WLAN yang disediakan. (Mochamad Gilang Hari Wibowo, 2017).

Karena munculnya teknik baru dan teknologi intrusi inilah yang membuat protokol jaringan nirkabel telah menjadi usang (Acosta-López, Melo-Monroy, & Linares-Murcia, 2018). Dan sekarang kebanyakan tempat menggunakan jaringan *wireless.*

Protokol keamanan pada jaringan *wireless* sekarang menggunakan "Wi-Fi Protected Access" (WPA) dan yang lebih spesifik adalah versi pertama WPA. Namun karena hash algoritma kriptografi yang lemah, terbukti bahwa WPA bukanlah keputusan yang ideal untuk jaringan infrastruktur terbuka seperti jaringan radio untuk akses Internet. (Proff. Assistant Linko G. Nikolov, 2018)

Akan tetapi WPA, WEP dan WPA2 ternyata ada yang mengklaim masih bisa di bobol. WPA, WEP dan WPA2 pernah di bobol oleh *attacker*, sebelum melakukan pengamanan terlebih dahulu mengetahui bagaimana cara *attacker* melakukan *attacker* kejaringan wifi menggunakan tools yang sering digunakan para *attacker* atau cracker khususnya dalam jaringan wifi tool tersebut adalah Reaver, aircrack, macchanger, Crunch, Wash, Fern Wifi Cracker, oclHashcat, Wireshark,Wifite, dan terahir Pixiewps. Dari beberapa tool tersebut ada dua tool

yang akan di pakai dan di perbandingkan. (Purwanto & Wijaya, 2017)

Sifat transmisi jaringan nirkabel dan serangan yang muncul terus menerus membuat atau mengeksploitasi lebih banyak kerentanan, dan umumnya mengadopsi IEEE 802.11 Wi-Fi-Protected-Access-2IPre-Shared-Key (WPA2-PSK) masih terkena beberapa kategori serangan seperti serangan *deauthentication* yang bertujuan untuk mendorong klien nirkabel untuk mengautentikasi ulang ke Access Point (AP) dan mencoba untuk menangkap kunci yang dipertukarkan selama *handshake* untuk membahayakan keamanan jaringan. (GHANEM & RATNAYAKE, 2020)

Serangan hacker yang kerap sekali mencari kesempatan untuk mengetahui aktivitas suatu jaringan, dan mencari celah kelemahan yang ada. Teknik dengan kemampuan dalam merecord semua kegiatan paket masuk dan keluar pada suatu data dan mencari intersep yang memungkinkan merecord username dan password ketika host login pada suatu ur, dalam hal ini pada segmen jaringan antara host dan hacker disebut Teknik Sniffing (Kurnia, 2019)

Dalam mencegah ancaman terhadap kriminalitas yang di lakukan di dalam jaringan internet (dunia maya) banyak tool yang dapat digunakan untuk melindungi sistem yang dibangun. Terdapat banyak tool dan IDS (*Intrusion Detection System*) yang dapat di download karena bersifat *free*, prabayar serta *open source*. (Zonggonau & Sajati, 2015)

Pada penelitian kali ini, penulis ingin mengimplementasikan kemanan jaringan berdasarkan pada Wireless Local Area Network yang terdapat pada Scomptec Surabaya terhadap serangan jenis *Brute Force* dan juga serangan jenis *Sniffing* yang biasanya dilakukan oleh *Attacker* agar data yang ada tidak dapat

dicuri oleh pihak yang tidak bertanggung jawab.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah di jelaskan di atas maka didapatkan rumusan masalah sebagai berikut :

1. Bagaimana tahapan serangan dan pertahanan terhadap *Brute Force* dan *Sniffing* pada *Wireless Local Area Network.*
2. Bagaimana cara mendeteksi serangan *Sniffing* yang dilakukan oleh *Attacker*.
3. Bagaimana cara mencegah dan melawan serangan *Brute Force* dan *Sniffing* yang dilakukan oleh *Attacker.*

1.3 Batasan Masalah

Adapun yang menjadi batasan-batasan dalam penelitian ini adalah sebagai berikut :

1. Implementasi pencegahan yang dilakukan adalah dengan cara *detection* dan *blocking system*
2. Sistem Operasi dari *Attacker* menggunakan *Kali Linux*
3. *Router* yang digunakan adalah *Router Nokia* dengan ISP Indihome 20mbps.
4. Sistem operasi target yang diuji adalah *Windows 7* dan *Linux Centos 7*
5. Pendeteksian dan pencegahan serangan menggunakan metode *IDPS* dengan menggunakan *arpwatch*, dan juga *filtering MAC Address* dengan menggunakan *router* yang akan digunakan.

1.4 Tujuan Penelitian

Adapun Tujuan dari penelitian yang dilakukan oleh penulis dengan judul

"Implementasi Sistem Keamanan Jaringan Terhadap Paket *Sniffing* Pada *Wireless Local Area Network*" antara lain :

1. Memahami celah yang terdapat pada jaringan *WLAN* yang tersedia.
2. Memahami bagaimana cara mendeteksi serangan *Sniffing* yang dilakukan oleh *Attacker.*
3. Memahami bagaimana cara mencegah dan melawan serangan *Brute Force* dan *sniffing* yang dilakukan oleh *attacker*.
4. Meningkatkan kemanan pada topologi jaringan setelah implementasi dilakukan.

1.5 Manfaat Penelitian

Adapun manfaat dari deteksi dan pencegahan terhadap serangan *Sniffing* menggunakan *arpwatch,* dan *MAC address Filtering* adalah sebagai berikut :

1. Bagi penulis adalah sebagai sarana untuk mengimplementasikan pengetahuan yang telah didapatkan dalam mata kuliah "Keamanan Jaringan" selama perkuliahan berlangsung, dan dapat memahami beberapa jenis serangan dan pertahanan yang paling efektif diimplementasikan pada jaringan *Wireless Local Area Network* serta pada sistem operasi yang terdapat pada komputer yang digunakan.
2. Bagi mahasiswa maupun pembaca sebagai sarana untuk penelitian lebih lanjut tentang keamanan jaringan dalam ruang lingkup *WLAN* dan juga penjelasan akan bahaya serta pencegahan terhadap serangan *brute force* dan *sniffing.*