BAB 1
USULAN GAGASAN

1.1 Latar Belakang Masalah

Dalam era konektivitas yang semakin meningkat, jaringan nirkabel menjadi infrastruktur kunci dari rumah tangga hingga perusahaan. Namun, meskipun terdapat keuntungan, terdapat juga resiko serangan, seperti *wireless router impersonation* yang dapat merugikan pengguna dengan mengakses data pribadi yang sangat sensitif.

Serangan seperti itu dapat dilakukan oleh penyerang yang dapat melakukan sejumlah besar serangan terhadap orang yang tidak bersalah. Salah satu contohnya adalah penyerang memiliki kemampuan untuk melakukan serangan aktif dengan menulis ulang permintaan *Domain Name System* (DNS) dan menghasilkan tanggapan yang mengarahkan pengguna ke situs *web phishing*. Penyerang bahkan dapat menginfeksi perangkat pengguna dengan *software* berbahaya (*malware*) dengan mengirimkan konten berbahaya sebagai tanggapan terhadap permintaan penjelajahan pengguna[1].

Mengakses jaringan Wi-Fi publik menghadirkan berbagai resiko, salah satunya adalah serangannya *Evil Twin Attack* (ETA). Dalam serangan ETA, penyerang membuat *Rogue Access Point* (RAP) dengan *Service Set IDentifie* (SSID) yang sama dengan *Access Point* (AP) asli untuk membajak koneksi nirkabel pengguna. Selain itu, dalam beberapa kasus yang telah terjadi, penyerang biasanya menyediakan koneksi internet kepada pengguna untuk menunjukkan bahwa RAP bukanlah AP palsu [2].

Kepolisian Federal Australia baru-baru ini menangkap seorang pria yang diduga mengoperasikan *hotspot* Wi-Fi palsu di beberapa bandara besar, termasuk Perth, Melbourne, dan Adelaide. Jaringan Wi-Fi ETA ini meniru jaringan yang sah untuk menarik pengguna agar memberikan data pribadi mereka, seperti akun email dan media sosial. Insiden ini menunjukkan resiko keamanan yang serius di lingkungan bandara karena konsentrasi orang yang tinggi dan kebutuhan untuk berkomunikasi menjadikannya target empuk bagi para penjahat siber. Kasus ini menunjukkan pentingnya upaya proaktif dalam mendeteksi dan mencegah kejahatan siber di lokasi-lokasi strategis, seperti bandara[3], [4].

Pakar digital forensik, Ruby Alamsyah, mengingatkan akan resiko penggunaan Wi-Fi gratis dan Wi-Fi publik ini. Serangan RAP dapat menggunakan Wi-Fi palsu untuk mengancam pengguna yang tidak dapat membedakan Wi-Fi yang asli dengan yang palsu. Pemerhati

keamanan siber, Yerry Niko Borang, menambahkan bahwa serangan seperti ini dapat terjadi tanpa diketahui oleh pengguna dan penyerang dapat mencuri data penting, terutama terkait dengan nama pengguna dan kata sandi[4]. Selain itu, pakar keamanan siber, Alfons Tanuwijaya, menekankan resiko penggunaan Wi-Fi palsu. Dalam jaringan Wi-Fi palsu, data dapat disadap dan dicuri. Selain itu, pemilik Wi-Fi palsu dapat memasukkan *malware* atau iklan berbahaya yang dapat meningkatkan resiko pencurian data pribadi dan aset digital[5].

Dalam menghadapi permasalahan *wireless router impersonation* ini, solusi menggunakan *Machine Learning* (ML) menjadi semakin penting. ML dapat memberikan solusi yang fleksibel dan cerdas untuk mengidentifikasi *wireless router impersonation*, mengidentifikasi pola yang sulit terlihat secara langsung, dan menanggapi serangan yang disesuaikan dengan pola lalu lintas yang kompleks.

Dengan meningkatnya ancaman terhadap keamanan jaringan nirkabel, *Detection of Wireless Router Impersonation* menjadi sangat penting. Implementasi solusi yang menggabungkan pendekatan ML dan teknik deteksi konvensional dapat memberikan perlindungan yang lebih baik terhadap serangan seperti ini, melindungi data sensitif, dan menjaga keamanan pengguna dalam mengakses jaringan nirkabel.

1.2 Analisa Masalah

1.2.1 Aspek Ekonomi

RAP dapat menyebabkan kerugian finansial bagi organisasi dan individu, misalnya melalui pencurian data sensitif atau penurunan kinerja jaringan nirkabel. Kasus RAP dapat memiliki dampak ekonomi yang signifikan. Berikut adalah beberapa aspek ekonomi yang dapat muncul sebagai akibat dari kasus ini :

1. Kerugian keuangan : RAP dapat membuka jalan bagi serangan terhadap jaringan pribadi yang dapat mengakibatkan pencurian data, kehilangan informasi rahasia, dan kerusakan sistem. Semua ini dapat berdampak negatif pada perusahaan dan individu, baik dalam bentuk biaya langsung maupun tidak langsung. Biaya yang terkait dengan pemulihan, perbaikan, dan peningkatan keamanan jaringan dapat menjadi beban yang signifikan bagi perusahaan dan individu[6].
2. Kehilangan reputasi : Jika sebuah perusahaan mengalami pelanggaran keamanan yang melibatkan RAP. Hal ini dapat merusak reputasi perusahaan di mata pelanggan, mitra bisnis, dan pemegang saham. Kehilangan kepercayaan ini dapat berdampak negatif pada pendapatan jangka panjang perusahaan.

3. Gangguan operasional : Serangan yang melibatkan RAP dapat mengganggu operasional perusahaan, seperti layanan pelanggan yang terganggu, penurunan produktivitas karyawan, atau bahkan penundaan dalam peluncuran produk baru. Semua ini dapat berdampak negatif pada pendapatan perusahaan.
4. Kerugian pelanggan : Jika pelanggan merasa tidak aman atau tidak puas dengan tingkat keamanan perusahaan. Mereka akan beralih ke pesaing yang menawarkan jaminan keamanan yang lebih baik. Hal ini dapat mengakibatkan kerugian pendapatan jangka panjang bagi perusahaan.

1.2.2 Aspek Keberlanjutan (*Sustainability*)

Pada penerapan yang sudah ada terdapat dua model yang dapat diterapkan, antara lain penggunaan model perangkat keras dan perangkat lunak dalam mengidentifikasi RAP. Kedua pendekatan tersebut mempunyai kelebihan dan kekurangannya masing-masing. Beberapa klasifikasi tersebut direkomendasikan untuk penelitian lebih lanjut untuk mengidentifikasi RAP.

Beberapa penelitian telah dipublikasikan mengenai cara mengidentifikasi RAP. Dengan menggunakan tinjauan pustaka yang sistematis, penelitian ini bertujuan untuk menganalisis berbagai metode tentang cara membedakan AP sebagai RAP atau AP yang sah, berdasarkan model pendekatan perangkat keras dan perangkat lunak. Solusi alternatif yang dapat ditawarkan, antara lain dengan menggunakan airodump-ng di OS Linux untuk mengumpulkan dataset, pengolahan dataset menggunakan ML, dan solusi-solusi lainnya. Masih banyak solusi alternatif untuk memecahkan masalah tersebut. Oleh karena itu, diperlukan penelitian lebih lanjut untuk mengidentifikasi RAP dan menemukan solusi alternatif lainnya.

1.2.3 Aspek Etis

Terdapat beberapa aspek etis yang terkait dengan impersonasi *router* nirkabel. Salah satu kekhawatiran utama adalah potensi akses tidak sah ke jaringan yang dapat menyebabkan pencurian data atau aktivitas jahat lainnya. Impersonasi *router* nirkabel juga dapat digunakan untuk melakukan serangan *man-in-the-middle*, di mana penyerang menangkap dan mengubah komunikasi antara dua pihak. Hal ini dapat mengakibatkan terungkapnya informasi sensitif, seperti nama pengguna, kata sandi, dan nomor kartu kredit.

Kekhawatiran etis lainnya adalah potensi penggunaan impersonasi untuk aktivitas ilegal, seperti memblokir akses ke situs *website* atau layanan tertentu. Penting untuk dicatat bahwa impersonasi adalah bentuk penipuan dan dapat dianggap sebagai perilaku tidak etis. Oleh

karena itu, penting untuk mengambil tindakan untuk mencegah impersonasi dan melindungi jaringan dari serangan potensial menganalisa keberlanjutan masalah.

1.2.4 Aspek Teknis

"Detection of Wireless Router Impersonation with Machine Learning" merujuk pada penggunaan teknologi *Machine Learning* untuk mendeteksi serangan terhadap jaringan Wi-Fi yang bertujuan meniru *router* yang sah dan mengelabui pengguna jaringan untuk terhubung dengannya. Dalam kasus ini, terdapat solusi identifikasi keamanan berdasarkan pengidentifikasian digital, seperti *Channel, Speed, Privacy, Cipher, Authentication, Power, beacons,* dan *ID-length.*

Salah satu contoh penggunaan ML untuk mendeteksi RAP adalah menggunakan *Feedforward Neural Network* (FNN) dengan dataset yang telah dikumpulkan oleh airodump-ng. Dalam contoh ini, FNN didesain untuk mengidentifikasi RAP dengan membandingkan dataset *Channel, Speed, Privacy, Cipher, Authentication, Power, beacons,* dan *ID-length* untuk mendeteksi RAP.

1.3 Tujuan Capstone

Beberapa tujuan dan maksud dari dokumen ini diantaranya adalah:

1. Dokumen ini dibuat untuk melakukan identifikasi terhadap masalah terkait keamanan jaringan nirkabel yang berkaitan dengan serangan *Wireless Router Impersonation*.
2. Dokumen ini menjelaskan solusi terbaru yang digunakan untuk mendeteksi serangan *Wireless Router Impersonation* menggunakan *Machine Learning.*
3. Dokumen ini ditujukan kepada para profesional, peneliti, dan praktisi di bidang keamanan jaringan nirkabel, serta mereka yang tertarik dalam pengembangan sistem keamanan berbasis *Machine Learning.*
4. Tujuan dari dokumen ini adalah untuk memberikan pengetahuan yang kuat tentang serangan yang terjadi pada *router* nirkabel dan solusi yang dapat diterapkan.

1.4 Analisis Solusi yang ada

1.4.1 Solusi WIDS Menggunakan Cara *Delay Fluctuation* di Jaringan *Backbone*

Dalam makalah ini, penelitian fokus pada ancaman keamanan pada jaringan LAN nirkabel, terutama serangan ETA yang dapat membahayakan keamanan data pengguna. ETA menciptakan RAP dengan SSID yang sama dengan AP yang sah, mengelabui klien untuk terhubung ke sana. Metode yang diusulkan untuk mendeteksi RAP melibatkan perbandingan fluktuasi penundaan jaringan *backbone* yang didefinisikan sebagai perbedaan antara perjalanan

Internet Control Message Protocol (ICMP) dari klien ke *gateway* pertama dan ke server internet[2].

Dalam eksperimen yang melibatkan lima jaringan nirkabel berbeda dengan *backbone* yang berbeda, penelitian ini menggunakan histogram penundaan untuk membedakan jaringan. Pengukuran penundaan *backbone* dilakukan dengan mengirimkan ICMP *echo request* dari klien ke *gateway* pertama dan ke server internet, kemudian menghitung perbedaan antara keduanya. Histogram dari 100 sampel penundaan dibuat dan dihitung jarak kosinusnya untuk mengevaluasi persamaan antarjaringan.

Hasil eksperimen menunjukkan bahwa metode ini dapat membedakan AP palsu dari AP yang sah dengan memanfaatkan fluktuasi penundaan *backbone*. Histogram penundaan dari berbagai jaringan nirkabel memberikan gambaran yang berbeda, memungkinkan identifikasi AP palsu. Dengan menggunakan pendekatan ini, penelitian ini memberikan kontribusi dalam meningkatkan keamanan jaringan nirkabel terhadap serangan ETA.

1.4.2 Solusi WIDS Mengidentifikasi *Radio Frequency* (RF) *Fingerprinting*

Pada cara ini dijelaskan tentang perancangan *neural network* menggunakan data simulasi untuk mendeteksi serangan impersonasi *router* WLAN. Pada Simulasi ini dilakukan dengan menghasilkan *frame beacon* WLAN dari *router* yang dikenal dan tidak dikenal untuk melakukan identifikasi berdasarkan RF *fingerprinting*. RF *fingerprinting* ini memanfaatkan sinyal *Legacy-Long Training Field* (L-LTF) pada *frame* WLAN untuk membedakan *router* dan mendeteksi potensi serangan impersonasi[7].

RF *fingerprinting* dapat menjadi solusi yang lebih aman dalam mendeteksi *router* impersonasi dibandingkan dengan metode identifikasi sederhana, seperti MAC *address*, IP *address*, dan SSID yang rentan terhadap *spoofing*. *Frame beacon* WLAN dari *router* yang dikenal digunakan untuk melatih *neural network* dan jaringan ini diuji terhadap sinyal dari *router* yang tidak dikenal untuk mendeteksi potensi serangan.

Kesimpulan yang dapat diambil adalah bahwa pendekatan RF *fingerprinting* dengan menggunakan *neural networks* dapat menjadi solusi yang efektif dalam mendeteksi *router impersonation* pada jaringan WLAN. Metode ini memanfaatkan karakteristik unik dari RF *fingerprinting* untuk membedakan *router* yang sah dan mendeteksi upaya serangan yang berusaha meniru *router* yang sah. Pendekatan ini dapat meningkatkan keamanan jaringan WLAN terhadap serangan yang menggunakan metode *spoofing*.

1.4.3 Solusi WIDS Menggunakan Airodump-ng pada *Platform* Linux dan *Machine Learning*

Wireless Intrusion Detection System (WIDS) adalah sebuah mekanisme keamanan yang digunakan untuk mendeteksi akses tidak sah dan aktivitas mencurigakan pada jaringan nirkabel. Salah satu solusi WIDS yang efektif adalah dengan memanfaatkan perangkat lunak airodump-ng pada *platform* Linux, dikombinasikan dengan teknologi *Machine Learning* untuk meningkatkan akurasi dan efisiensi deteksi[8].

WIDS merupakan komponen penting dalam infrastruktur keamanan jaringan, khususnya pada jaringan nirkabel yang rentan terhadap berbagai ancaman seperti akses tidak sah, *sniffing*, dan serangan DoS. Solusi tradisional seringkali tidak cukup efektif dalam menghadapi ancaman yang semakin kompleks. Oleh karena itu, implementasi WIDS dengan kombinasi airodump-ng dan ML diharapkan mampu memberikan solusi yang lebih adaptif dan cerdas.

Airodump-ng adalah bagian dari *suite* aircrack-ng yang merupakan perangkat lunak *open source* untuk keamanan jaringan nirkabel. Airodump-ng berfungsi untuk memonitor dan mengumpulkan paket data dari jaringan nirkabel, termasuk informasi tentang AP dan klien yang terhubung[9].

Machine learning digunakan untuk menganalisis data yang dikumpulkan oleh airodump-ng. Model ML dapat dilatih untuk mengenali pola-pola yang mencurigakan dan mendeteksi aktivitas yang tidak biasa berdasarkan data historis dan fitur-fitur tertentu seperti frekuensi percobaan autentikasi, intensitas sinyal, dan pola perpindahan klien.

Pengumpulan data dilakukan dengan airodump-ng secara terus-menerus. Data yang dikumpulkan kemudian diproses untuk menghilangkan *noise* dan menyusun fitur-fitur yang relevan. Model ML dilatih menggunakan data yang telah diproses dengan algoritma yang digunakan adalah *Feedforward Neural Network* (FNN). FNN adalah jenis *Artificial Neural Network* (ANN) yang strukturnya memungkinkan untuk memecahkan berbagai masalah kompleks, seperti pengenalan pola, klasifikasi, dan prediksi[10].

Solusi WIDS menggunakan airodump-ng pada *platform* Linux dan ML memberikan pendekatan yang lebih cerdas dan efisien dalam mendeteksi ancaman pada jaringan nirkabel. Dengan kemampuannya untuk belajar dan beradaptasi, solusi ini diharapkan dapat meningkatkan keamanan jaringan nirkabel secara signifikan.