BAB 1
USULAN GAGASAN

1.1 Latar Belakang Masalah

Perangkat seluler dan komputer pribadi (PC) adalah alat kerja yang umum dan telah menjadi bagian dari kehidupan sehari-hari. Perangkat-perangkat ini dilengkapi dengan fitur-fitur menarik, seperti kamera, perekam suara, dan kemampuan untuk menghubungkan perangkat seluler ke PC untuk memudahkan produktivitas. Namun, adaptabilitas yang tinggi dari perangkat-perangkat ini juga menimbulkan potensi ancaman keamanan bagi perusahaan dan pemerintah yang menyimpan informasi rahasia.

Salah satu keprihatinan utama dalam teknologi nirkabel adalah masalah keamanan. Dalam upaya untuk mengatasi masalah ini, metode enkripsi terus dikembangkan. Namun, kehadiran Wireless Intrusion Detection System (WIDS) telah menjadi solusi lain yang efektif. Sistem ini telah menjadi bagian penting dalam bidang keamanan dan teknologi nirkabel, membantu perusahaan/lembaga untuk mendeteksi dan melindungi diri dari ancaman potensial[1].

Perusahaan/lembaga ini menerapkan kebijakan "no signal policy" untuk mengatasi masalah tersebut. Kebijakan ini melarang penggunaan perangkat nirkabel pada waktu dan lokasi tertentu sesuai dengan aturan yang telah ditetapkan. Namun, untuk memastikan penerapan kebijakan ini lebih efektif, WIDS diperlukan. WIDS bertujuan untuk melacak perangkat-perangkat penyusup yang mencoba melakukan spionase, merekam tanpa izin, atau melakukan berbagai bentuk serangan lain, seperti pembobolan data untuk mencari, mendapatkan, mengubah, atau menghapus informasi yang ada. Walaupun kebijakan ini diterapkan, beberapa penyusup masih dapat menggunakan perangkat dengan access point pribadi. Oleh karena itu, WIDS menjadi penting untuk mengidentifikasi dan mencegah akses ilegal atau aktivitas tidak sah yang terjadi di dalam jaringan.

Dengan munculnya fitur-fitur serangan jaringan nirkabel yang baru, metode deteksi penyusupan dengan kemampuan beradaptasi yang tinggi, stabilitas dan efektivitas sangat dibutuhkan. Saat ini, mekanisme otentikasi jaringan nirkabel umum dan teknologi firewall pada dasarnya dapat memenuhi keamanan dasar persyaratan perlindungan pengguna, tetapi kemampuan perlindungan relatif lemah[2]. WIDS dapat mengidentifikasi berbagai macam potensi serangan. Berikut ini adalah daftar serangan dan kejadian penting yang dapat dikenali dengan bantuan WIDS[1].

Serangan dalam bentuk intersepsi melibatkan pihak ketiga yang berwenang yang memiliki akses ke sistem informasi, sedangkan interupsi melibatkan penyerang yang mengganggu sistem tanpa memperoleh hak akses. Dalam jaringan seluler, salah satu ancaman yang muncul adalah spionase, di mana pihak yang tidak berwenang berupaya mengumpulkan informasi rahasia tentang perusahaan atau organisasi tanpa izin. Metode spionase yang umum digunakan adalah menyelipkan ponsel ke dalam saku atau saku tanpa sepengetahuan pemiliknya.

Pada Wi-Fi rerangan berupa pencurian data yang mencakup penyadapan data pribadi pengguna dapat terjadi. Peretas dan penyusup dapat dengan mudah menipu target mereka dengan menggunakan Wi-Fi palsu atau penyedia hotspot. Disarankan untuk tidak menggunakan Wi-Fi publik saat menggunakan perangkat nirkabel karena titik akses dapat dengan mudah disusupi oleh peretas, dan memberi mereka akses ke data sensitif. Untuk melindungi tempat-tempat ini dari beberapa hal yang tidak menyenangkan ini, *Wireless Intrution Detection System* menjadi sangat penting.

1.2 Informasi Pendukung Masalah

Teknologi saat ini sangat cepat mengalami perkembangan, oleh sebab itu negara kita pun terkena dampak positif maupun negatif dari hal tersebut. Salah satu teknologi yang seringkali digunakan adalah *mobile devices* berupa *handphone* dan laptop. Dapat dilihat pada saat ini manusia tidak dapat dilepaskan dari *handphone* dan laptop karena sudah menjadi kebutuhan sehari-hari yang praktis dipakai untuk memudahkan mendapatkan informasi, berkomunikasi dan lainnya.

Oleh karena itu, ada beberapa hal yang menyebakan terjadinya masalah karena pada saat ini ada beberapa area ada yang mengharuskan tidak adanya penggunaan jaringan *Wi-Fi,* dan data seluler. Tetapi, terkadang ada beberapa pihak yang tidak mematuhi peraturan tersebut sehingga pada area yang menerapkan kebijakan *no signal policy* harus dilakukan pengecekan secara berkala dan bergantian. Hal tersebut sayangnya tidak praktis dan memakan banyak waktu sehingga dibutuhkan suatu alat untuk mendeteksi keberadaan sinyal dan jaringan *wireless* secara cepat dan akurat.

Salah satu teknologi yang dapat melakukan hal tersebut adalah *Wireless Instrusion Detection System* yang dapat melacak secara cepat keberadaan keberadaan sinyal dan jaringan *wireless* pada bidang keamanan sistem informasi yang saat ini dikenal dengan *cyber security*.

1.3 Analisis Umum

Selama ponsel, laptop, dan perangkat nirkabel lainnya terhubung ke jaringan yang direkam oleh adaptor nirkabel, penggunaan perangkat seluler dengan sinyal tidak dibatasi. Oleh karena itu, dilarang menggunakan perangkat nirkabel di lokasi di mana kebijakan tanpa sinyal berlaku. Hal ini dilakukan untuk memastikan keamanan dan kenyamanan serta menghindari gangguan sinyal. Hal ini dapat digunakan di lokasi dengan keamanan tinggi termasuk pesawat terbang, rumah sakit, pangkalan militer, lembaga keuangan, ruang ujian, dan bangunan lainnya. Pembatasan ini bertujuan untuk mengurangi kemungkinan gangguan sinyal yang dapat mengganggu alat penting dan operasi penting serta untuk mencegah risiko keamanan dan pelanggaran privasi. Berikut adalah beberapa aspek yang terhubung dan berdampak pada Wireless Intrution Detection System:

1.3.1 Aspek Ekonomi

Penggunaan gadget jarak jauh yang melanggar hukum di wilayah tanpa tanda dapat berakibat serius. Pelanggaran semacam itu mungkin dapat mengganggu tugas, meningkatkan pertaruhan keamanan dan perlindungan, dan pada dasarnya membahayakan kedudukan organisasi. Tidak hanya itu, pelanggaran semacam itu mungkin dapat mengurangi efisiensi, mengganggu koherensi bisnis, dan menyebabkan kemalangan moneter yang signifikan.

Bagaimanapun, strategi yang tepat terhadap pemanfaatan gadget jarak jauh dapat membawa keuntungan finansial yang penting. Langsung saja, mereka mengambil peran penting dalam menjaga keamanan dan kehormatan informasi bisnis. Dengan membatasi penggunaan gadget jarak jauh yang tidak disetujui, pertaruhan tumpahan informasi, serangan digital, dan perampokan data yang sensitif dapat dibatasi, yang dengan demikian melindungi organisasi dari kemalangan moneter karena pelanggaran keamanan.

Selain itu, WIDS juga dapat menambah keefektifan fungsional dengan mengamati gadget jarak jauh, misalnya, ponsel dan lorong-lorong di wilayah terbatas. Dengan pengamatan dinamis melalui kerangka kerja ini, bahaya keamanan dapat diawasi dan gangguan yang terorganisir dapat dikenali dengan cepat, sehingga dapat menghasilkan dana cadangan jangka panjang.

Secara umum, pelaksanaan strategi permusuhan yang ditegakkan oleh inovasi WIDS jelas mempengaruhi area keuangan. Hal ini melindungi keamanan informasi, meningkatkan efektivitas fungsional, dan mengurangi kemungkinan gangguan organisasi. Di tengah

persaingan pasar yang ketat, kegiatan semacam ini memberdayakan asosiasi untuk mengerjakan pameran mereka, melindungi spekulasi mereka, dan memperkuat posisi mereka.

1.3.2 Aspek Manufakturabilitas

Dalam aspek manufakturabilitas alat untuk mendeteksi *Wi-Fi* dan data seluler dalam area dengan kebijakan *no signal policy* adalah sebagai berikut:

1. Desain yang efisien: Alat dirancang dengan mempertimbangkan efisiensi produksi. Desain yang sederhana dengan jumlah komponen yang minimal akan memudahkan proses produksi perakitan ataupun penggunaan.
2. Kompatibilitas teknologi: Alat harus mampu mendeteksi dan membedakan sinyal *Wi-Fi dan* data seluler. Desain alat memperhitungkan kecocokan dengan berbagai standar teknologi nirkabel yang ada dan memastikan ketersediaan komponen yang sesuai.
3. Toleransi dan keandalan: Karena alat akan digunakan dalam lingkungan dengan kebijakan *no signal policy*, maka toleransi terhadap sinyal yang lemah atau tidak ada harus diperhitungkan. Alat tersebut harus dirancang untuk dapat mendeteksi sinyal dengan sensitivitas yang tinggi dan memberikan hasil yang akurat dalam kondisi yang sulit.
4. Efisiensi daya: Alat ini harus dirancang dengan mempertimbangkan efisiensi daya yang baik agar dapat digunakan dalam waktu yang lama tanpa perlu pengisian daya yang terlalu sering. Pemilihan komponen yang hemat daya dan penggunaan teknik manajemen daya yang cerdas akan membantu meningkatkan manufakturabilitas alat.
5. Pengujian dan verifikasi: Proses manufakturabilitas alat ini harus mencakup pengujian dan verifikasi yang ketat untuk memastikan bahwa alat tersebut berfungsi dengan baik dan dapat mendeteksi sinyal. Alat yang dirancang dapat mendeteksi jaringan *Wi-Fi* dan seluler pada *layer* ke 2 dalam model referensi *Opens Systems Interconnection* (OSI).

1.3.3 Aspek Efektivitas dan Efisiensi

Sejauh efektivitas dan efiensi, penggunaan WIDS dapat menggantikan penggunaan pelacak logam oleh petugas keamanan untuk memeriksa apakah seseorang membawa gadget yang mengomunikasikan organisasi Wi-Fi dan informasi serbaguna. Dengan WIDS, siklus identifikasi dapat dilakukan dengan lebih tepat dan efektif, sehingga mengurangi waktu dan tenaga yang dibutuhkan dalam pemeriksaan manual. Demikian juga, WIDS juga dapat diperiksa di luar zona strategi tanpa transmisi menggunakan layar web, yang memungkinkan tenaga kerja keamanan untuk menyaring pergerakan organisasi jarak jauh dengan lebih efektif dan mudah.

1.3.4 Aspek Keamanan

WIDS berfungsi untuk mendeteksi dan melindungi jaringan dari serangan yang dapat dilakukan oleh perangkat *wireless* yang tidak sah atau mencurigakan. WIDS dapat mengidentifikasi serangan seperti *Brute Force*, *Denial of Service* (DoS), *Man-in-the-Middle* (MITM), dan serangan protokol lainnya yang dapat membahayakan keamanan jaringan. Dengan adanya WIDS, petugas atau admin jaringan dapat mengambil langkah-langkah untuk mengatasi serangan tersebut dan mencegah ancaman yang lebih lanjut.

Selain itu, WIDS juga memiliki kemampuan untuk mengidentifikasi perangkat wireless yang tidak diizinkan, termasuk *mobile phone* dan *access point* yang beroperasi dalam area dengan kebijakan *no signal policy*. Hal ini penting untuk menjaga keamanan dan integritas jaringan, terutama dalam konteks kebijakan yang melarang penggunaan perangkat wireless di area tersebut. Dengan mendeteksi perangkat *wireless* yang tidak diizinkan, dengan demikian hal ini membantu memitigasi risiko keamanan yang terkait dengan pelanggaran dan menjaga keamanan jaringan secara keseluruhan.

1.4 Kebutuhan yang Harus Dipenuhi

Dalam penyelesaian masalah, kebutuhan yang harus dipenuhi peneliti dalam implementasi solusi yang akan dibuat yaitu:

1. Diperlukan penggunaan sistem integrasi WIDS untuk menjaga keamanan dalam ruangan yang menerapkan kebijakan *no signal policy.*
2. Alat yang dibuat harus memiliki ukuran sekecil mungkin agar memudahkan mobilitas dan penggunaan yang fleksibel.
3. Alat yang dibuat harus mampu mendeteksi jaringan *Wi-Fi* dan seluler secara *real-time.* Informasi tentang jaringan wireless yang terdeteksi harus dapat dikirimkan ke *web monitor.*
4. Pengguna harus dapat memantau data yang terdeteksi melalui *web monitoring*. *Web monitoring* tersebut akan menampilkan informasi dari d*atabase* jaringan yang terdeteksi.

Tujuan dari penyusunan dan penelitian terkait masalah keamanan dalam ruangan yang menerapkan kebijakan *no signal policy* adalah:

1. Menciptakan alat atau produk yang berbasis WIDS untuk sektor keamanan dan pengawasan jaringan *wireless.*

2. Alat yang dibuat akan membantu mempermudah pengawasan suatu perusahaan atau institusi terhadap para pelanggar yang tidak mematuhi kebijakan area *no signal policy.*
3. Tujuan lainnya adalah mencegah terjadinya hal-hal yang tidak diinginkan, termasuk pencurian data penting yang dapat merugikan perusahaan atau institusi.

1.5 Solusi Sistem Yang Diusulkan

Sebagai bagian dari implementasi sistem deteksi intrusi nirkabel, dua sistem diusulkan. Yang pertama adalah *Wireless Intrusion Detection System* dengan sensor pendeteksi *Spectrum Analyzer*, yang berfokus pada analisis spektrum sinyal untuk mengidentifikasi aktivitas yang mencurigakan. Usulan yang kedua adalah *Wireless Intrusion Detection System* dengan Sensor Pendeteksi TP-Link WN725N dan Nooelec NESDR SMArTee XTR. Sistem ini mengandalkan beragam sensor pendeteksi untuk memantau jaringan nirkabel, dengan memperhatikan perangkat khusus seperti TP-Link WN725N dan Nooelec NESDR SMArTee XTR guna mengamankan lingkungan jaringan dari potensi ancaman.

Kedua usulan sistem ini memiliki pendekatan yang berbeda namun memiliki tujuan yang sama, yaitu meningkatkan keamanan jaringan nirkabel dengan deteksi dan pencegahan terhadap intrusi yang berpotensi merugikan.

1.5.1 Karakteristik Produk

1.5.1.1 Wireless Intrusion Detection System Dengan Sensor Pendeteksi Spectrum Analyzer

Solusi pertama yang ditawarkan untuk produk WIDS dengan sensor pendeteksi berupa *spectrum analyzer* yang diintegrasikan dengan *web monitor*. Berikut rincian fitur-fitur pada *spectrum analyzer:*

1. Fitur Utama

   Penggunaan satu sensor yang memiliki kemampuan langsung untuk mendeteksi jaringan Wi-Fi dan seluler secara simultan. Dengan menggunakan sensor ini, pengguna dapat dengan mudah dan efisien mengidentifikasi keberadaan dan mengamati aktivitas jaringan nirkabel di sekitar mereka. Pendeteksi atau pengukur sinyal dalam domain frekuensi pada jaringan Wi-Fi dan seluler. Hal ini memungkinkan pemantauan dan analisis sinyal yang ada di sekitar.
2. Fitur Dasar

   Fitur dasar produk ini mencakup deteksi jaringan Wi-Fi dan seluler yang diintegrasikan ke *web monitor*.

3. Fitur Tambahan

   Fitur tambahan *spectrum analyzer* mencakup analisis spektrum lebar, deteksi interferensi, analisis modulasi, pengukuran kekuatan sinyal, analisis harmonik, pemantauan panjang gelombang, dan pemantauan lalu lintas jaringan.

4. Hasil solusi yang diharapkan

   Dengan adanya *Wireless* IDS dengan sensor pendeteksi *spectrum analyzer* diharapkan pengguna dapat mendeteksi jaringan *wireless* dengan akurat.

1.5.1.2 Wireless Intrusion Detection System Dengan Sensor Pendeteksi TP-Link WN725N dan Nooelec NESDR SMArTee XTR

Solusi kedua yang ditawarkan adalah menggunakan *Wireless IDS* dengan tiga sensor pendeteksi terpisah yang terintegrasi melalui *web monitor*. Ketiga sensor tersebut meliputi TP-Link WN725N untuk mendeteksi jaringan Wi-Fi dan Noolec NESDR XTR untuk mendeteksi jaringan seluler.

1. Fitur Utama

   Fitur utama solusi ini adalah integrasi *web monitor* yang menggabungkan tiga sensor pendeteksi terpisah, yaitu TP-Link WN725N untuk jaringan Wi-Fi dan Noolec SMArTee NESDR XTR untuk jaringan seluler, sehingga sensor-sensor ini mampu secara akurat mendeteksi dan memantau keberadaan jaringan nirkabel yang berbeda secara terpisah.

2. Fitur Dasar

   Fitur dasar ini adalah menyediakan analisis dan visualisasi data yang membantu pengguna dalam memantau dan menganalisis karakteristik jaringan nirkabel yang terdeteksi. Dengan *interface* yang intuitif dan integrasi dengan *web monitor*, solusi ini memberikan pengalaman pemantauan yang efisien dan pengambilan keputusan yang tepat terkait keamanan dan kinerja jaringan nirkabel.

3. Fitur Tambahan

   Dengan menggunakan sensor yang memiliki ukuran yang relatif kecil agar dapat dengan mudah memindahkan perangkat tersebut.

4. Hasil solusi yang diharapkan

   Dengan menggunakan sensor-sensor terpisah, diharapkan dapat memperoleh informasi yang akurat dan terperinci tentang jaringan Wi-Fi dan seluler yang terintegrasi melalui *web monitor.*

1.6 Kesimpulan dan Ringkasan CD-1

Penggunaan perangkat seperti *handphone* dan laptop yang menggunakan jaringan nirkabel telah membuka potensi ancaman terhadap keamanan informasi. Meskipun langkah-langkah kebijakan tanpa sinyal telah diambil, tantangan masih muncul melalui pelanggaran yang terjadi melalui perangkat terhubung melalui akses pribadi seperti *Wi-Fi* dan seluler. Oleh karena itu, keberadaan *Wireless Intrusion Detection System* (WIDS) menjadi hal yang penting dalam mendeteksi dan mencegah perangkat nirkabel yang melanggar kebijakan tersebut.

WIDS berperan sebagai pertahanan tambahan dengan tujuan melindungi data sensitif, meningkatkan efisiensi operasional, dan mengurangi risiko gangguan jaringan. Keunggulan WIDS terletak pada kemampuannya dalam mendeteksi ancaman yang tidak terdeteksi sebelumnya dan meresponsnya secara cepat, memastikan integritas lingkungan jaringan. Dengan penerapan pemantauan khusus untuk perangkat yang teridentifikasi, alat WIDS mampu beroperasi secara optimal, memberikan perlindungan yang lebih kuat terhadap serangan potensial.

Dalam era yang semakin terhubung, perlunya solusi seperti WIDS sangat penting untuk menjaga keamanan dan stabilitas lingkungan kerja. Dengan demikian, integrasi sistem ini dapat memberikan dampak positif, mengurangi risiko potensial, dan memberikan jaminan bagi kelangsungan operasional dalam menghadapi tantangan keamanan yang terus berkembang.