SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

JUDUL

ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI

TUGAS AKHIR

Farhan Thariq Huzaini

0110220006

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

JULI 2024

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

JUDUL

ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom)

Farhan Thariq Huzaini

0110220006

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

JULI 2024

HALAMAN PERNYATAAN ORISINALITAS

Skripsi/Tugas Akhir ini adalah hasil karya penulis, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Farhan Thariq Huzaini

NIM : 0110220006

Depok, 27 Juli 2024

Tanda Tangan

Farhan Thariq Huzaini

HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh:

Nama : Farhan Thariq Huzaini

NIM : 0110220006

Program Studi : Teknik Informatika

Judul Skripsi : ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar SarjanaKomputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri

DEWAN PENGUJI

Pembimbing	Penguji
(Efrizal Zaida, S.Kom, M.M, M.Kom.)	(April Rustianto, S.Komp., M.T.)

Ditetapkan di : Jakarta

Tanggal : 27 Juli 2024

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmatNya, penulis dapat menyelesaikan skripsi/Tugas Akhir ini. Penulisan skripsi/Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi/tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT.
2. Orang tua dan semua anggota keluarga yang telah memberikan dorongan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Dr. Lukman Rosyidi, S.T., M.M., M.T. selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu Tifanny Nabarian, S.Kom., M.T.I. selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Ibu Nurul Janah, S.IIP., M.Hum. selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Efrizal Zaida, S.Kom, M.M, M.Kom. selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Bapak April Rustianto, S.Komp., M.T. selaku Dosen Penguji Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
8. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
9. PT Mitra Bhakti Informasi Manajer Om Claudius, Mas Hengky dan beserta karyawan yang telah meluangkan waktunya untuk memberikan data yang diperlukan bagi penulisan ilmiah ini.
10. Semua teman – teman yang telah membantu dan memberi arahan terhadap penelitian ini,

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan-kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang penulis miliki. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

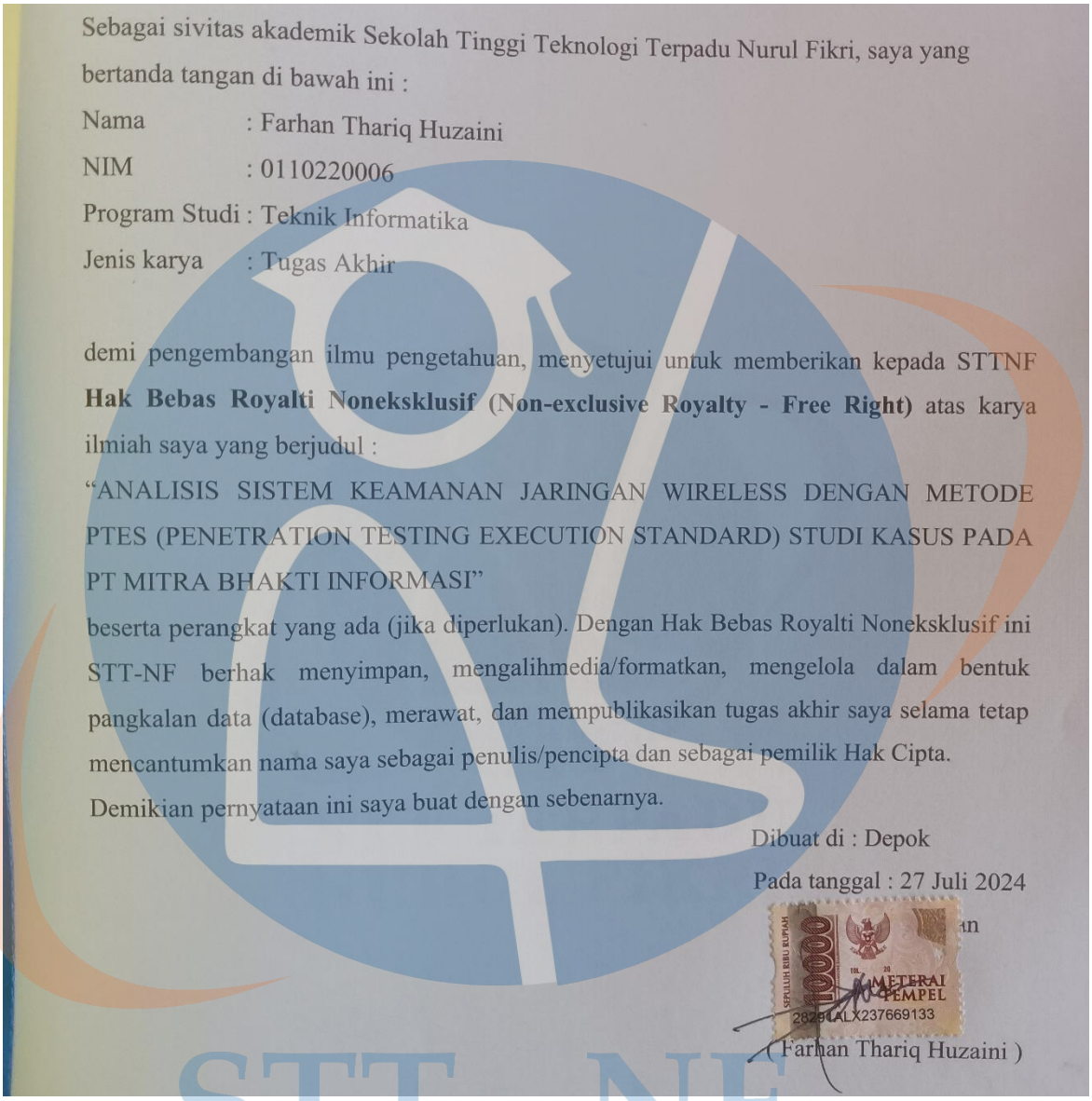
Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 27 Juli 2024

Penulis

Farhan Thariq Huzaini

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS



Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini :

Nama : Farhan Thariq Huzaini

NIM : 0110220006

Program Studi : Teknik Informatika

Jenis karya : Tugas Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STTNF **Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty - Free Right)** atas karya ilmiah saya yang berjudul :

"ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI"

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : 27 Juli 2024

an

(Farhan Thariq Huzaini)

ABSTRAK

Nama : Farhan Thariq Huzaini

NIM : 0110220006

Program Studi : Teknik Informatika

Judul : ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI

Dalam era teknologi yang terus berkembang, jaringan wireless menjadi bagian integral dari operasional banyak perusahaan, termasuk PT Mitra Bhakti Informasi. Meskipun memberikan banyak kemudahan, jaringan wireless juga rentan terhadap berbagai ancaman keamanan, seperti serangan *Man-in-the-Middle (MitM), cracking password*, dan *deauthentication attack*. PT Mitra Bhakti Informasi telah mengalami tantangan keamanan ini, yang mengancam integritas dan kerahasiaan data perusahaan. Untuk mengatasi masalah ini, pihak management IT pada perusahaan memutuskan untuk menerapkan metode *PTES (Penetration Testing Execution Standard)* sebagai langkah proaktif dalam menilai dan memperkuat keamanan jaringan *wireless* mereka. Penelitian ini bertujuan untuk mengidentifikasi kerentanan yang ada dalam jaringan *wireless* perusahaan, mengevaluasi efektivitas langkah - langkah keamanan yang ada, dan memberikan rekomendasi perbaikan yang konkret. Metode *PTES* digunakan untuk melakukan penilaian keamanan secara menyeluruh melalui tahapan perencanaan, pengumpulan informasi, pemindaian kerentanan, eksploitasi, dan pelaporan. Hasil dari penelitian ini diharapkan dapat membantu PT Mitra Bhakti Informasi dan pembaca dalam memperkuat pertahanan perangkat jaringan *wireless* terhadap ancaman siber, melindungi data sensitif, dan memastikan kelangsungan operasional yang aman dan andal. Selain itu, hasil penelitian ini juga dapat berfungsi sebagai panduan dan referensi bagi perusahaan / organisasi dan pembaca dalam mengadopsi langkah-langkah serupa untuk mengamankan jaringan wireless mereka dari ancaman yang terus berkembang. Dengan demikian, semoga hasil penelitian ini menjadi kontribusi yang berguna untuk meningkatkan keamanan dan mengelola risiko keamanan jaringan nirkabel di lingkungan organisasi perusahaan.

Kata Kunci : Penteration Testing, Wireless, Hacking, Hack Wifi, Wifi, PTES, Wireshark, Alfa Network, Analisis Keamana Jaringan Wireless

ABSTRACT

Nama : Farhan Thariq Huzaini

NIM : 0110220006

Study Program : Informatics Engineering

Title : WIRELESS NETWORK SECURITY SYSTEM ANALYSIS USING THE PTES (PENETRATION TESTING EXECUTION STANDARD) METHOD CASE STUDY AT PT MITRA BHAKTI INFORMASI

In an era of ever-developing technology, wireless networks have become an integral part of the operations of many companies, including PT Mitra Bhakti Information. Even though it provides many conveniences, wireless networks are also vulnerable to various security threats, such as Man-in-the-Middle (MitM) attacks, password cracking, and deauthentication attacks. PT Mitra Bhakti Information has experienced this security challenge, which threatens the integrity and confidentiality of company data. To overcome this problem, the company's IT management decided to implement the PTES (Penetration Testing Execution Standard) method as a proactive step in assessing and strengthening the security of their wireless network. This research aims to identify existing vulnerabilities in corporate wireless networks, evaluate the effectiveness of existing security measures, and provide concrete recommendations for improvements. The PTES method is used to carry out a comprehensive security assessment through the planning, information gathering, vulnerability scanning, exploitation and reporting stages. It is hoped that the results of this research can help PT Mitra Bhakti Information and readers in strengthening the defense of wireless network devices against cyber threats, protecting sensitive data, and ensuring safe and reliable operational continuity. In addition, the results of this research can also serve as a guide and reference for companies/organizations and readers in adopting similar steps to secure their wireless networks from growing threats. Thus, we hope that the results of this research will be a useful contribution to improving security and managing wireless network security risks in corporate organizational environments.

Keywords : Penetration Testing, Wireless, Hacking, Hack Wifi, Wifi, PTES, Wireshark, Alfa Network, Wireless Network Security Analysis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

BAB I
PENDAHULUAN

1.1 Latar belakang

Pada era modern, teknologi semakin kesini semakin maju dengan perkembangan yang sangat pesat bagi manusia untuk mendorong menciptakan teknologi baru yang dapat mempermudah pekerjaan manusia. Organisasi atau perusahaan menginginkan informasi yang cepat dan detail. Organisasi yang telah berkembang saat ini telah banyak menggunakan perkembangan teknologi dari jaringan nirkabel yang menggunakan standar protokol *Wireless Fidelity (WiFi)* berbasiskan *standar IEEE 802.11.* [1] Pada awal mula teknologi ini belum sepenuh nya aman karena masih ada sering laporan bahwa masih ada pihak yang tidak bertanggung jawab alias *hacker* meretas berbagai data informasi mereka, terutama bagi mereka yang menggunakan jaringan *Wireless LAN*. [2] Saat melakukan proses pengiriman data sampai tujuan harus melewati berbagai terminal, pada saat itu ada kesempatan pengguna lain yang tak bertanggung jawab dapat mengubah dan menyadap data tersebut. Banyak manfaat pada penggunaan internet, dan juga memliki berbagai banyak nya sebuah ancaman yang sangat *high risk* untuk mengintai target nya. Contohnya seperti *Phising Email & Messagess, Hacking, Cracking, DdoS* dan lain – lain, [3] yang digunakan untuk tindakan yang tidak izinkan dan dilarang secara hukum yang akan digunakan sebagai penyalahaan data, pencurian data, penyalahgunaan hak akses, ancaman dan lain – lain.

PT Mitra Bhakti Informasi adalah Perusahaan industri teknologi jaringan dan *server* di dirikan pada 2019 oleh Johan Widjaja dengan Legalisasi Kode. AHU-0005480.AH.01.02.Tahun 2019. Berdasarkan wawancara dengan bapak Johan Widjaja PT Mitra Bhakti Informasi merupakan perusahaan swasta yang bergerak sebagai vendor yang menjualkan produk – produk software layanan teknologi dan mengelola produk jaringan dan server pada jaringan lokal organisasi Perusahaan. Salah satu nya adalah produk *Access Point* sebagai alat transmisi penyeberan sinyal. Dengan tim profesional yang berpengalaman dan fokus pada kepuasan pelanggan, perusahaan ini telah membangun reputasi yang kuat dan bermitra dengan berbagai perusahaan ternama. Maka dari itu penulis yang sebagai salah satu karyawan di PT Mitra Bhakti Informasi ingin meneliti dan melakukan *testing* keamaanan jaringan pada perangkat *wireless*. Meskipun jaringan

wireless memberikan banyak keuntungan, PT Mitra Bhakti Informasi menghadapi berbagai tantangan keamanan. Beberapa serangan kemungkinan akan terjadi pada perangkat wireless untuk mengeksploitasi celah keamanan atau mengakses data tanpa izin ialah *Man-in-the-Middle (MitM), Cracking password* dan *Deauthentication Attack* tantangan-tantangan ini menuntut PT Mitra Bhakti Informasi untuk mengambil langkah proaktif guna melindungi jaringan wireless dan data sensitif perusahaan dari ancaman yang terus berkembang.

Untuk melindungi dan mencegah terjadinya dari serangan pada perangkat *wireless*, pihak *management IT* pada PT Mitra Bhakti Informasi memutuskan untuk menggunakan metode *PTES (Penetration Testing Execution Standard)* dalam melakukan penilaian keamanan pada jaringan *wireless* mereka. Metode *PTES* merupakan kerangka kerja yang sistematis dan komprehensif untuk melakukan *penetration testing*, yang melibatkan berbagai tahapan mulai dari perencanaan, pengumpulan informasi, pemindaian kerentanan, eksploitasi, hingga pelaporan dan rekomendasi. Penilaian keamanan ini diharapkan dapat mengidentifikasi berbagai jenis kerentanan yang ada pada jaringan *wireless* perusahaan dan memberikan rekomendasi yang tepat untuk memperkuat keamanan. Selain itu, penggunaan metode *PTES* juga akan membantu dalam mengedukasi tim *IT* perusahaan mengenai potensi ancaman dan langkah-langkah *mitigasi* yang perlu diambil. Dengan demikian, PT Mitra Bhakti Informasi dapat meningkatkan keamanan jaringan *wireless* mereka dan mengurangi risiko terhadap ancaman siber di masa mendatang.

Salah satu pendekatan yang dipilih adalah menggunakan metode *PTES (Penetration Testing Execution Standard)* dalam melakukan penilaian keamanan pada jaringan *wireless* perusahaan. *PTES* menyediakan kerangka kerja yang komprehensif untuk mengidentifikasi kerentanan dalam jaringan *wireless*, mengevaluasi efektivitas kebijakan dan prosedur keamanan, serta memberikan rekomendasi perbaikan yang konkret. Dengan menggunakan metode *PTES (Penetration Testing Execution Standard)* adalah kerangka kerja standar yang digunakan untuk melakukan pengujian penetrasi terhadap sistem dan jaringan, termasuk jaringan wireless. *PTES* menyediakan pedoman yang komprehensif dan

terstruktur untuk mengidentifikasi, menganalisis, dan mengatasi kerentanan keamanan dalam sebuah sistem [4].

Penetration testing pada jaringan *wireless* merupakan proses penting untuk memastikan keamanan data pada suatu jaringan. Dengan mengidentifikasi dan mengatasi kerentanan secara proaktif, organisasi dapat melindungi diri dari ancaman yang terus berkembang dan memastikan bahwa jaringan mereka aman dan andal. *Penetration testing* pada perangkat WiFi di PT Mitra Bhakti Informasi sangat penting untuk memastikan keamanan jaringan dari ancaman dan serangan yang semakin kompleks. Dengan mengidentifikasi kerentanan, mengevaluasi kebijakan keamanan, menguji respons terhadap serangan, dan memberikan rekomendasi perbaikan, *penetration testing* membantu perusahaan untuk meningkatkan keamanan jaringan secara keseluruhan, memenuhi persyaratan regulasi, dan melindungi aset informasi dari potensi ancaman.

Penelitian ini bertujuan untuk mengidentifikasi dan mengatasi kerentanan keamanan pada jaringan wireless PT Mitra Bhakti Informasi menggunakan metode PTES. Dengan mengikuti langkah-langkah yang terstruktur, penelitian ini diharapkan dapat memberikan evaluasi yang akurat, simulasi serangan nyata untuk menguji respons tim keamanan, serta menghasilkan laporan yang merinci temuan dan rekomendasi perbaikan. Melalui penelitian ini, PT Mitra Bhakti Informasi berharap dapat memperkuat keamanan jaringan *wireless* mereka, melindungi data sensitif, dan memastikan kelangsungan operasional yang aman dan andal. Hasil penelitian ini juga diharapkan dapat menjadi referensi bagi perusahaan lain dalam mengadopsi langkah – langkah proaktif untuk mengamankan jaringan *wireless* mereka.

Dengan menerapkan metode *PTES*, organisasi dapat memastikan bahwa jaringan *wireless* mereka diperiksa secara menyeluruh dan dilindungi dari berbagai ancaman keamanan, meningkatkan integritas dan kerahasiaan data serta kelangsungan operasional jaringan. Mengapa menggunakan metode *PTES* pada perangkat *wireless* di PT Mitra Bhakti Informasi merupakan langkah strategis dan efisien untuk mengidentifikasi, menilai, dan mengatasi kerentanan keamanan secara menyeluruh. *PTES* menyediakan kerangka kerja yang komprehensif, relevan, dan efektif yang memungkinkan perusahaan untuk memahami risiko, meningkatkan kesadaran keamanan, dan mengambil tindakan korektif yang tepat. Dengan demikian, penerapan Metode *PTES* dapat membantu PT Mitra Bhakti

Informasi untuk memperkuat keamanan jaringan wireless mereka dan melindungi aset informasi dari ancaman yang potensial.

1.2 Rumusan Masalah

Berdasarkan dari penjelesan judul dan latar belakang sebelumnya penulis merangkum inti pokok dari permasalahan yang di tulis "Analisis sistem keamanan jaringan wireless dengan metode *PTES (penetration testing execution standard)* di PT mitra bhakti informasi"

a. Bagaimana mengidentifikasi, menganalisis dan mengevaluasi kerentanan keamanan yang ada dalam jaringan nirkabel pada PT Mitra Bhakti Informasi?
b. Bagaimana metode PTES ini dapat di fungsikan pada PT Mitra Bhakti Informasi?

1.3 Tujuan dan Manfaat Penelitian

- Tujuan dari kegiatan penelitian ini adalah untuk meningkatkan keamanan dan mengurangi kerentanan serangan jaringan WLAN terhadapa serangan luar / dalam dengan metode penetration testing.
- Manfaat dari penelitain ini adalah untuk memberikan wawasan dalam memonitoring data pada suatu jaringan dan cara untuk menganalisis tingkat kemanaan data pada suatu jaringan

1.4 Batasan Masalah

Pada batasan masalah dalam kegiatan penelitian ini memliki keterbatasan yang dimiliki dari dalam waktu, pemikiran, biaya. Maka dari itu batasan masalah pada penelitian ini yaitu adalah :

a. Dalam kegiatan penelitian ini menggunakan perangkat dan *tools* yaitu *Alfa Network, Access Point, Tools* berbayar dan *Restirected* yang dirahasiakan oleh perusahaan.
b. Kegiatan ini hanya akan menganalisa salah satu jaringan *wireless* dengan menggunakan metode *PTES (penetration testing execution standard)*
c. Metode Teknik *PTES (penetration testing execution standard)*
d. Penelitian dilakukan pada saat jam tertentu (*Ex Office Hour*)

1.5 Sistematika Penulisan

Pada penelitian ini Sistematika Penulisan mencakup 5 BAB untuk mempermudah pemahaman keseluruhan penelitian. Maka dari itu, sistematika penulisan tugas akhir ini sebagai berikut:

1. BAB I PENDAHULUAN. Pada bab ini mencakup untuk memberikan gambaran dan informasi secara penjelasan latar belakang penelitian, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, serta sistematika penulisan. Pada bab ini merangkum dari penggambaran peniliti dari Analisis sistem keamanan jaringan wireless, mencakup rumusan masalah sampai kesimpulan serta rekomendasi yang akan dijadikan langkah selanjutnya.
2. BAB II KAJIAN LITERATUR. Pada BAB kali ini menguraikan landasan teori yang relevan yang akan diterapkan dalam penelitian ini. Landasan teori ini mencakup konsep-konsep penting, teori-teori yang mendukung, dan kerangka pemikiran yang menjadi dasar penelitian. Selain itu, juga akan dibahas penelitian terkait yang telah dilakukan sebelumnya untuk memberikan konteks yang lebih luas dan pemahaman yang mendalam tentang analisis sistem keamanan jaringan wireless dengan metode PTES (Penetration Testing Execution Standard) studi kasus pada PT Mitra Bhakti Informasi. Akan disampaikan rangkuman dari bab ini yang meliputi inti-inti yang telah dijelaskan sebelumnya. Dalam rangkuman ini, akan mencakup dasar-dasar teori yang relevan yang digunakan dalam penelitian, serta penelitian terkait yang telah dilakukan sebelumnya. Tujuannya adalah untuk membantu pembaca memahami landasan teoritis dari penelitian ini dan konteksnya dalam bidang yang relevan. Dalam bab ini, telah diuraikan konsep-konsep penting dan teori-teori yang mendukung penelitian mengenai analisis sistem keamanan jaringan wireless dengan metode PTES. Telah dibahas juga beberapa penelitian terkait yang memberikan konteks dan pemahaman lebih mendalam tentang topik ini. Penelitian-penelitian tersebut menunjukkan pentingnya metode PTES dalam mengidentifikasi kerentanan, serta pentingnya pembaruan protokol keamanan, pelatihan staf, dan implementasi kebijakan keamanan yang ketat untuk melindungi jaringan wireless dari ancaman

potensial. Rangkuman ini bertujuan untuk membantu pembaca memahami landasan teoritis dari penelitian ini dan konteksnya dalam bidang yang relevan.

3. BAB III METODOLOGI PENELITIAN. Pada bab ini menguraikan tahapan-tahapan proses penelitian yang digunakan oleh penulis untuk menghasilkan tampilan sebagai hasil dari penelitian analisis sistem keamanan jaringan wireless dengan metode PTES (Penetration Testing Execution Standard) studi kasus pada PT Mitra Bhakti Informasi. Proses ini melibatkan langkah-langkah seperti merencanakan penelitian, mengumpulkan dan menganalisis data, menafsirkan temuan, dan mengembangkan tampilan yang sesuai dengan tujuan penelitian. Dan telah dijelaskan secara teruarai dalam tahapan atau langkah-langkah yang diperlukan oleh peneliti dalam menyusun penelitian dari analisa keamanan jaringan, meliputi pendahuluan, landasan teori, jenis metodologi penelitian, prosedur penelitian, tahapan penelitian, lingkungan penelitian, dan timeline penelitian. Melalui tahapan-tahapan yang telah dijelaskan, penelitian ini menemukan beberapa kerentanan utama yang perlu ditangani segera untuk mengurangi risiko keamanan. Implikasi dari temuan ini adalah perlunya pembaruan protokol keamanan, peningkatan pelatihan staf, dan penerapan kebijakan keamanan yang lebih ketat. Akan diberikan ringkasan singkat yang mencerminkan inti dari penelitian ini. Ringkasan tersebut akan memuat temuan utama yang dihasilkan melalui proses penelitian, serta implikasi dan kontribusi penelitian ini dalam bidang terkait. Selain itu, akan diberikan juga pemikiran mengenai arah penelitian masa depan yang dapat dilakukan untuk mengembangkan dan memperluas pemahaman dalam topik ini. Dengan mengikuti tahapan-tahapan yang telah dijelaskan di atas, penelitian ini bertujuan untuk memberikan pemahaman yang mendalam tentang kondisi keamanan jaringan wireless di PT Mitra Bhakti Informasi dan memberikan rekomendasi yang dapat diimplementasikan untuk memperkuat keamanan jaringan tersebut.
4. BAB IV IMPLEMENTASI DAN EVALUASI. Pada bab ini peneliti menjelaskan tentang pelaksanaan implementasi dari solusi yang diusulkan dalam penelitian analisis sistem keamanan jaringan wireless dengan metode *PTES (Penetration Testing Execution Standard)* studi kasus pada PT Mitra Bhakti Informasi serta evaluasi terhadap hasil yang telah dicapai. Dalam bab ini, akan menguraikan secara terperinci mengenai penerapan konsep, metode, atau sistem yang telah dirancang, serta melibatkan evaluasi terhadap hasil implementasi

tersebut. Akan diberikan rangkuman yang mencerminkan inti dari bab ini. Rangkuman ini akan meliputi penjelasan mengenai pelaksanaan implementasi solusi yang diusulkan dalam penelitian ini, beserta evaluasi terhadap hasil yang telah dicapai. Dengan adanya rangkuman ini, pembaca akan mendapatkan gambaran ringkas tentang langkah-langkah pelaksanaan dan dampak dari solusi yang diusulkan tersebut.

5. BAB V KESIMPULAN DAN SARAN. Pada bab ini berisi ringkasan hasil dari penelitian analisis sistem keamanan jaringan wireless dengan metode *PTES (Penetration Testing Execution Standard)* studi kasus pada PT Mitra Bhakti Informasi serta saran-saran yang akan diberikan berdasarkan hasil penelitian tersebut. Akan disajikan sebuah rangkuman yang mencerminkan inti dari bab ini. Rangkuman ini akan meliputi penjelasan singkat mengenai hasil dari penelitian yang telah dilakukan, serta saran-saran yang diberikan berdasarkan temuan-temuan tersebut. Melalui rangkuman ini, pembaca akan memperoleh gambaran singkat mengenai hasil penelitian dan rekomendasi yang disampaikan guna membimbing langkah-langkah selanjutnya.

BAB II
KAJIAN LITERATUR

Pada bab ini, akan dibahas berbagai literatur yang relevan dengan judul "Analisis Sistem Keamanan Jaringan Wireless Dengan Metode *PTES (Penetration Testing Execution Standard)"* yang mencakup konsep - konsep dasar, metode *PTES*, serta penelitian-penelitian terdahulu yang berhubungan dengan topik ini. Kajian literatur ini bertujuan untuk memberikan landasan teoritis yang kuat bagi penelitian ini. Selain itu, pada kegiatan penelitian analisa ini penulis menjelaskan beberapa teori pada penelitian yang telah dilakukan pada bab berikut.

2.1 TINJAUAN PUSTAKA

Teknologi wireless yang digunakan pada teknologi komunikasi data sekrang menggunakan suatu jaringan komputer yang terhubung tanpa menggunakan kabel LAN (Local Area Network) dari perangkat komputer ke router dan dari perangkat jaringan komputer lainnya. [4] Teknologi wireless atau nirkabel ini memanfaatkan sinyal radio atau gelombang cahaya sebagai pengiriman dan penerima data tanpa harus menggunakan kabel LAN untuk menghubungkan perangkat komputer ke perangkat lain, sehingga tidak tergantung pada suatu port dan kabel yang penggunaannya terbatas dan tidak fleksibel eligeble pada suatu kondisi. Wireless Local Area Network atau WLAN adalah teknologi dengan sistem komunikasi pertukaran data yang fleksibel dan menjadi sebagai alternatif untuk penggunaan jaringan lokal yang masih menggunkan kabel. Teknologi wireless ini menggunakan frekuensi gelombang radio untuk mengirim dan menerima data melalui gelombang udara [5]. Agar dengan menggunakan nya teknologi wireless ini kebutuhan teknologi persambungan kabel dapat diminimalisir. Maka dari itu, Wireless Local Area Network adalah teknologi terbaik yang digunakan untuk jaringan lokal tanpa harus memerlukan kabel yang sulit atau bangunan yang membutuhkan banyak perangkat tanpa kabel.

Teknologi Wireless atau yang biasa orang – orang menyebut nya *Wireless Fidelity (Wi-Fi),* sebuah teknologi yang di gunakan sebagai alat bantu transmisi data yang dipakai pada jaringan lokal tanpa harus menggunakan kabel *UTP* atau *LAN* dengan memakai

infrastruktur yang menggunakan gelombang radio. Agar berbagai perangkat Wireless lain yang dimiliki perusahaan lain atau merek dapat kompatibel dan terhubung dengan satu dari berbagai jaringan dibuatlah standar disebut dengan *IEEE (Institute for Electrical and Electronic Engineers) 802.11*. [6]

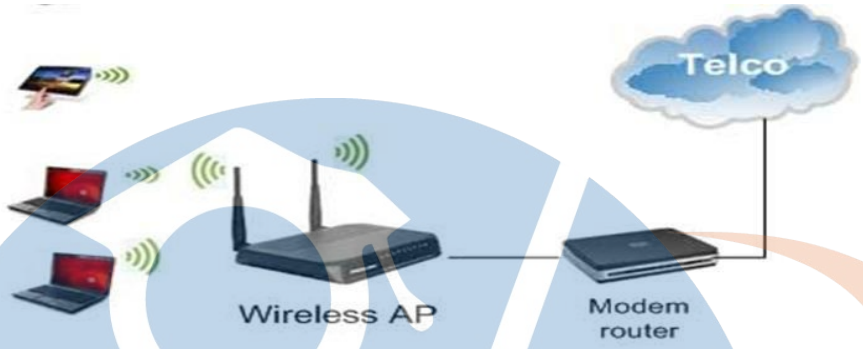
Model teknologi wireless atau jaringan nirkabel ini hampir sama dengan jaringan LAN, akan tetapi wireless LAN ini pada suatu jaringan lokal perlu menggunakan Wireless Device untuk dapat terhubung [1, 1]dengan jaringan lokal nirkabel. Untuk terhubung dengan jaringan nirkabel perlu memerlukan channel frekuensi yang sama dengan perangkat WLAN atau access point dan nama SSID yang sama dengan access point atau perangkat wireless nya. Tidak hal nya sama seperti jaringan kabel, jaringan nirkabel ini mempunyai dua mode pita gelombang radio yang yaitu 2,4 GHz dan 5 GHz [6]. Penggunaan mode pita gelombang wireless ini tergantung dari kebutuhan untuk berbagi data dan kegunaan nya dengan aktiftas manusia. Pada topologi infrastruktur dari jaringan nirkabel ini untuk membuat perangkat komputer ber komunikasi ke antara semua perangkat komputer lainnya melalui sebuah perangkat Access Point. Komunikasi *wireless* ini secara langsung akan bertukar informasi dari perangkat masing – masing melalu piranti *wireless*. Jaringan nirkabel atau WLAN terdiri dari perangkat komputer pengguna dan Access Point. Yang dimana akan digunakan user tanpa harus mengukur panjang dan colok port kabel [7].

2.1.1 TOPOLOGI JARINGAN

Topologi jaringan ini terdiri dari beberapa suatu kumpulan perangkat komputer dari dua atau lebih perangkat komputer yang saling terhubung dan terkoneksi dengan interaktif komunikasi data yang dapat di koneksikan dengan media alat komunikasi dengan media nirkabel maupun kabel dan membentuk suatu kumpulan dengan tujuan dan target tecapai untuk saling menukar berbagai sumber data dan informasi dari hardware atau perangkat keras komputer ataupun perangkat jaringan maupun software atau perangkat lunak yang terkoneksi pada suatu jaringan komputer. [4]

Pada teknologi perangkat *wireless* memiliki suatu *SSID* atau *Service Set Identifier* yang berfungsi untuk penamaan pada suatu jaringan nirkabel. Pada sistem SSID ini dapat

diberikan nama, angka, spesial karakter yang penulisan karakter nya sebanyak 32 karakter. Pada penulisan karakter atau penamaan *SSID* ini juga dapat dibuat *case sensitive* sehingga SSID dapat dibeda – beda kan. Dan nama SSID ini dapat di sembunyikan dengan mencentang bagian “Hide my SSID” pada konfigurasi *Access Point.* [4]



Gambar 2. 1 Topologi jaringan

Dan dengan itu penamaan SSID sebuah jaringan *wireless* in dapat diketahui oleh sang administrator dan pengguna yang akan menggunakan jaringan nirkabel ini. Di saat perangkat komputer sudah terhubung dengan SSID yang ingin di koneksikan, maka terbuatlah suatu jaringan infrastruktur [8]. Dari terbentuknya infrastruktur ini akan menjadi sebuah jaringan komunikasi untuk saling bertukar data informasi dari perangkat komputer satu ke perangkat komputer lain.

2.1.2 Keamanan Jaringan Komputer

Pada suatu sistem keamanan jaringan komputer ini sebagai jaminan agar data informasi yang harus nya di dapatkan original tidak digunakan atau dimodifikasi oleh pihak atau pengguna yang tidak dikenal [9]. Pengamanan ini juga sebagai masalah teknis bagi setiap perangkat dan suatu jaringan baik secara nirkabel dan kabel. Sistem keamanan jaringan komputer terbagi menjadi dua bagian yaitu:

1. Sistem jaringan keamanan eksternal, ancaman dan bahaya dari eksternal itu ada 2 macam, yaitu bencana alam dan serangan oleh seorang yang bukan dari dalam organisasi perusahaan atau karyawan perusahaan. Untuk menjaga keamanan fasilitas komputer dari bencana alam, misalnya bencana kebakaran, gempa bumi dan banjir. Maka dari itu untuk mengatasi dari ancaman bencana ini di perlukan

2. Sistem jaringan keamanan internal, pada sistem keamanan jaringan internal ini membuat beragam pengamanan keamanan yang di buat untuk perangkat keras dan perangkat lunak yang handel dengan baik secara software untuk menjaga keutuhan jaringan komputer data.

2.1.3 Keamanan Jaringan Wireless

Pengguna jaringan nirkabel ini bergantung pada perangkat komputer *user* dan perangkat *user – user* lainnya yang terkoneksi dengan jaringan lokal nirkabel untuk mengakses internet untuk melakukan berbagai aktifitas kegiatan online. Karena banyak perusahaan yang mengizinkan karyawannya untuk bekerja dari rumah. Jaringan nirkabel pada rumah tanpa keamanan yang baik rentan menjadi sasaran target serangan *hacking*. Kerentanan dan pembobolan data tersebut dapat membahayakan keamanan jaringan perusahaan. [10]

Jaringan nirkabel, memiliki kerentanan terhadap serangan *hacking* yang sangat tinggi karena menggunakan gelombang radio sebagai transmisi dalam mengirimkan data. Artinya, user atau pengguna yang berada di dalam area jangkauan jaringan nirkabel akan mendapatkan menerima dan membaca informasi data yang dikirimkan. Maka dari itu, penting untuk pengguna maupun seorang administrator mengamankan perangkat jaringan nirkabel untuk menghindari berbagai macam serangan.

Serangan hacking ini dapat menyebabkan sebuah kerugian yang begitu besar bagi pribadi individu dan sebuah organisasi bisnis. Data informasi pribadi seperti alamat rumah, id identitas, nomor kartu kredit dan kata sandi dapat dicuri oleh seorang yang tidak diketahui atau *hacker* yang dapat mengakibatkan pencurian identitas, pembobolan data dan kerugian finansial. Seorang *hacker* dapat mengambil akses ahli dan mengkontrol pada perangkat jaringan yang kurang aman, sehingga dapat menyebabkan hilangnya dan bahkan kehancuran data. Maka dari itu, keamanan nirkabel penting untuk melindungi data dan perangkat jaringan komputer dari segala ancaman dan resiko. Dengan mengamankan

jaringan nirkabel dapat menjaga keamanan informasi dari peretas dan mengurangi segala resiko dan ancaman yang sangat high risk.

Keamanan nirkabel bekerja dengan menggabungkan beberapa teknologi dan teknik. Enkripsi data adalah salah satu teknologi utama yang digunakan. Enkripsi merupakan suatu proses perubahan metadata asli ke dalam sebuah format yang unik sehingga tidak dapat dimengerti atau tidak mudah di baca oleh pihak yang tidak memiliki kunci enkripsi. Dalam keamanan jaringan nirkabel, enkripsi berfungsi sebagai untuk menjaga dan melindungi semua data informasi yang dikirimkan dalam jaringan nirkabel tidak dapat terbaca ataupun tidak dapat di ambil oleh pihak atau entitas yang tidak dikenal.

Untuk saat ini terdapat macam - macam jenis keamanaan jaringan nirkabel dengan 4 mode enskripsi, yaitu :

1. *WEP (Wired Equivalent Privacy)*

   WEP ini merupakan protokol dari suatu keamanan jaringan yang digunakan untuk melindungi jaringan nirkabel *Wi-Fi*. Protokol ini dimaksudkan untuk memberikan keamanan yang sebanding dengan jaringan kabel, menjamin untuk membawa informasi data yang dimana melewati jaringan nirkabel untuk tidak mudah disadap oleh entitas yang tidak dikenal. WEP mengenkripsi komunikasi antar perangkat yang terhubung ke jaringan nirkabel. Pada saat itu WEP mulai terjadi suatu kerentanan pada masalah keamanan utama. Beberapa kelemahan yang terkenal termasuk kunci enkripsi yang mudah ditebak, prosedur inisialisasi yang tidak efektif, dan serangan terhadap transmisi data. Pada era saat ini WEP sudah tidak lagi digunakan di karenakan memiliki kerentanannya. Maka dari itu *WPA* menjadi lanjutan dari metode teknik enkripsi yang lebih baik dan mengurangi terjadinya celah kelemahan pada sistem jaringan nirkabel.

2. *WPA* (Wi-Fi Protected Access)

   Sebuah protokol keamanan yang digunakan untuk melindungi jaringan nirkabel dari suatu serangan. *WPA* dirancang sebagai pengganti metode enskripsi sebelumnya WEP (Wired Equivalent Privacy) yang rentan terhadap berbagai serangan keamanan.

   WPA memiliki tingkat lapisan keamanan dengan menggunakan enkripsi yang lebih kuat dan metode otentikasi yang lebih aman. Protokol ini berfungsi sebagai membuat perlindungan yang lebih baik terhadap serangan pada

jaringan nirkabel, seperti serangan penyadapan (eavesdropping) dan pembajakan (spoofing).

3. *WPA*2 (Wi-Fi Protected Access 2)

   Sebuah metode tingkat enskripsi dari *WPA* untuk tambahan keamanan jaringan nirkabel yang menggunakan protokol otentikasi yang lebih canggih seperti *EAP (Extensible Authentication Protocol)* dan *RADIUS (Remote Authentication Dial-In User Service),* yang cocok untuk lingkungan jaringan yang lebih besar dan memerlukan kontrol akses yang lebih granular.

4. *WPA*3 (Wi-Fi Protected Access 3)

   WPA 3 adalah versi terbaru dari protokol *WPA,* menambahkan fitur keamanan yang ditingkatkan seperti enkripsi individual untuk setiap perangkat yang terhubung (enkripsi data individual) dan perlindungan terhadap serangan *brute force*. Namun, *WPA*3 belum banyak digunakan, dan *WPA*2 tetap menjadi standar keamanan yang paling sering digunakan.

Maka dari itu PT Mitra Bhakti Informasi memiliki cara dan infrastruktur yang sangat handal untuk membuat jaringan lokal nirkabel menjadi sangat aman. Dengan dibuat nya infrastruktur dari ahli dan berpengalaman serta profesional dalam menjaga kerahasiaan data dan penjagaan komunikasi data jaringan wireless. PT Mitra Bhakti Informasi sebagai perusahaan vendor yang memiliki integritasi sistem jaringan menawarkan solusi untuk para organisasi dengan kebutuhan dan keamanaan yang sangat tinggi.

2.1.4 Keamanan Jaringan Server

Keamanan jaringan adalah serangkaian tindakan dan suatu prosedur untuk melindungi jaringan komputer dan sistem yang terhubung. Tujuan utama keamanan jaringan adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data, serta mencegah akses tidak sah dan melindungi sumber daya jaringan. Dengan menerapkan keamanan jaringan yang baik, perusahaan dapat mengurangi risiko serangan dan pelanggaran keamanan yang dapat merugikan bisnisnya.

Pada penelitian ini mengambil salah satu jenis keamanan jaringan server, yaitu *network segmentation*. *Network segmentation* melibatkan pembagian jaringan menjadi segmen pada suatu jaringan. Dengan memisahkan jaringan internet dengan lokal dan menyesuaikan dari kebutuhan serta fungsi nya agar meminimalisir suatu serangan ancaman. Maka dari itu, dibuat lah satu segmen yang tidak dapat menyebar atau terkoneksi ke segmen lain. Hal ini membantu membatasi dampak serangan dan melindungi data yang lebih sensitif.

Dari banyak nya aspek penting dari keamanan jaringan server, pada penelitian ini penulis mengambil beberapa aspek yang akan di analisa, mulai dari :

1. Otentikasi, menggunakan metode otentikasi yang kuat pada saat login untuk memastikan bahwa pengguna adalah seorang yang di perbolehkan masuk kedalam jaringan server. Seperti username dan password yang unik tanpa sepengetahuan atau default dan ditambah dengan *authentication OTP* atau *dual authintaction.*
2. Otorisasi, Mengatur user pengguna pada jaringan server terutama *role* atau arah akses dari setiap user yang terdaftar pada jaringan server ini. Dan dapat memastikan bahwa pengguna hanya memiliki akses ke departement yang sudah relevan atau sesuai dengan jobdesc pekerjaan mereka.
3. Enkripsi, Menggunakan metode enkripsi untuk melindungi data yang dikirim antara perangkat server ke perangkat komputer dan jaringan lainnya agar data yang di kirim dan simpan di server menjadi sangat aman dan tidak mudah untuk diketahui atau di analisa oleh pihak yang tidak dikenal. Hal ini juga mencegah penyadapan data atau manipulasi data oleh entitas yang tidak dikenal.
4. Firewall, Mengaktifkan atau menggunakan Firewall sebagai memantau dan mengatur service network atau lalu lintas jaringan dari perangkat jaringan server ke jaringan lain dan membantu melindungi serta membatasi server dari serangan jaringan luar.

2.1.5 Keamanan Protokol *WPA*

Protokol ini diperkenalkan pada tahun 2003 dan menggantikan WEP. Ini mirip dengan WEP, tetapi menangani kunci keamanan alias *password* dan otentikasi *username* dengan lebih baik. *WPA* merupakan singkatan dari Wi-Fi Protected Access Pre-Shared

Key adalah sebuah metode enskripsi yang digunakan oleh perangkat jaringan nirkabel dengan credential user login untuk masuk ke dalam suatu jaringan nirkabel. Yang dimana nanti nya ketika ada seseorang ingin mengakses perangkat komputer ke jaringan lokal nirkabel ini harus mengetahui credential username dan password yang valid. Pada *WPA* panjang karakater minimal dan maksimal dalam WEP menyediakan kunci unik untuk setiap sistem yang diautentikasi, sedangkan *WPA* menggunakan Key Identity Protocol (TKIP) untuk menetapkan *credential* yang digunakan oleh suatu sistem. Hal ini mencegah ada nya hacking atau pembobolan dari penyerangan encryption credential yang ada di jaringan nirkabel. Standar enkripsi TKIP kemudian digantikan oleh Advanced Encryption Standard (AES), yang dimana AES akan memeriksa integritas log data untuk di analisa apakah hacker telah melakukan pencegatan atau memodifikasi paket data. Pada saat ini, *WPA* telah menggunakan *WPA*2-PSK (AES) yang sangat sudah canggih keamanan nya. [11]

Key encryption yang digunakan dalam *WPA* adalah 256-bit, sebagai peningkatan signifikan dibandingkan kunci 64-bit dan 128-bit yang dipakai oleh *encryption WEP*. Namun, meskipun ada perbaikan ini, elemen *WPA* masih digunakan untuk membuat *WPA*2. Kunci *WPA* adalah kata sandi yang digunakan untuk terhubung ke jaringan nirkabel. [12]

WPA2-PSK merupakan keamanan jaringan nirkabel ini dengan metode enskripsi terbaru dari *WPA*. Dalam perkembangan *WPA* mencari lebih dalam untuk algoritma enskripsi terbaru yaitu *AES (Advance Encryption System)* dan terlahir lah *WPA2-PSK (AES) [11]*. Jika user ingin mengakses jaringan lokal nirkabel ini, mereka perlu mengatahui credential password untuk login atau disaat mengkoneksi kan perangkat komputer mereka ke jaringan nirkabel ini. User dapat menanyakan credential password login ke jaringan lokal nirkabel ini dengan bertanya langsung ke sang administrator secara legal. Nanti nya disaat user telah mengetahui password dan disaat mereka mencoba login ke dalam suatu jaringan lokal nirkabel ini sistem *WPA* akan memeriksa validasi dari credential tersebut apakah valid sesuai dengan credential password yang mereka setting di sisi accesspoint [12].

Walaupun digadang atau disebut dengan kata keamanan terbaru dan dengan encryption terbaru, semua sistem keamanan jaringan masih ada memliki beberapa celah kelemahan nya. Contoh nya seperti ada user yang sudah mengetahui credential password pada suatu jaringan nirkabel ini mereka menyebarkan credential tersebut ke semua

pengguna tanpa mengetahui niat dari penggunaan saat mereka mengakses jaringan nirkabel tersebut.

2.2 Penelitian Terkait

Pada tahap ini penulis menggambarkan alur penelitian dan bagaimana penelitian ini berkaitan dengan analisis keamanan network yang sudah ada sebelumnya. Pada kegiatan penelitian analisa ini, penulis mengambil beberapa referensi kepustakaan dari suatu sumber penelitian sebelumnya. Dalam hal ini yang akan berguna untuk sebagai perbandingan referensi dan contoh bahan dalam menyelesaikan kegiatan penelitian analisa ini. Adapun beberapa hal penelitian yang hampir mirip atau berkaitan dengan masalah yang di analisa pada kegiatan penelitain ini, maka dari itu untuk lebih memahami bagaimana penelitian-penelitian terdahulu terkait dengan judul "Analisis Sistem Keamanan Jaringan Wireless Dengan Metode PTES (Penetration Testing Execution Standard)" dapat membantu dalam melakukan analisis serupa, berikut adalah penjelasan rinci dari beberapa penelitian tersebut. Berikut ini beberapa sumber yang penulis telah melakukan penelitian terdahulu pada table dibawah ini atau table 2.1.

No	Judul	Tahun	Penulis	Deskripsi
1	Evaluating Wireless Network Security Using PTES Methodology: A Case Study	2019	Smith, J., & Johnson, A.	Studi ini menunjukkan bahwa PTES dan OWASP memiliki pendekatan yang berbeda dalam mengevaluasi keamanan jaringan nirkabel, dengan masing-masing memiliki kelebihan dan kelemahan. Namun, PTES menonjol dalam mengidentifikasi kerentanan yang spesifik untuk jaringan nirkabel, sementara OWASP lebih berfokus pada kerentanan umum yang dapat diterapkan pada berbagai jenis sistem.
2	ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) DENGAN METODE PENETRATION TESTING PADA PT.PLN (PERSERO) SEKTOR	2021	RIVALDI RACHMAN	Studi ini menjelaskan keamanan jaringan pada suatu jarkomdat di PT PLN Persero Pakanbaru

	PENGENDALIAN PEMBANGKITAN PEKANBARU			
3	Enhancing Wireless Network Security: A Case Study of PTES Implementation in a Financial Institution	2021	Gupta, R., & Patel, S	Penelitian ini menggunakan pendekatan studi kasus dengan menerapkan langkah-langkah PTES dalam melakukan evaluasi keamanan jaringan nirkabel di lembaga keuangan. Data dikumpulkan melalui proses tes penetrasi, analisis kerentanan, dan wawancara dengan staf keamanan informasi.
4	Assessing Wireless Network Vulnerabilities: A Comparative Study of PTES and OWASP Methodologies	2020	Chen, L., & Wang, Q.	Penelitian ini menggunakan pendekatan komparatif dengan menerapkan kedua metodologi pada beberapa organisasi dengan infrastruktur jaringan nirkabel yang berbeda. Data dikumpulkan melalui proses pengujian penetrasi dan analisis hasil tes.
5	Evaluating Wireless Network Security Using PTES: A Case Study in the Healthcare Sector	2021	Rahman, M., & Chowdhury, S.	Implementasi metode PTES berhasil mengidentifikasi kerentanan keamanan yang signifikan dalam jaringan nirkabel rumah sakit, yang memungkinkan untuk penerapan tindakan perbaikan yang tepat.

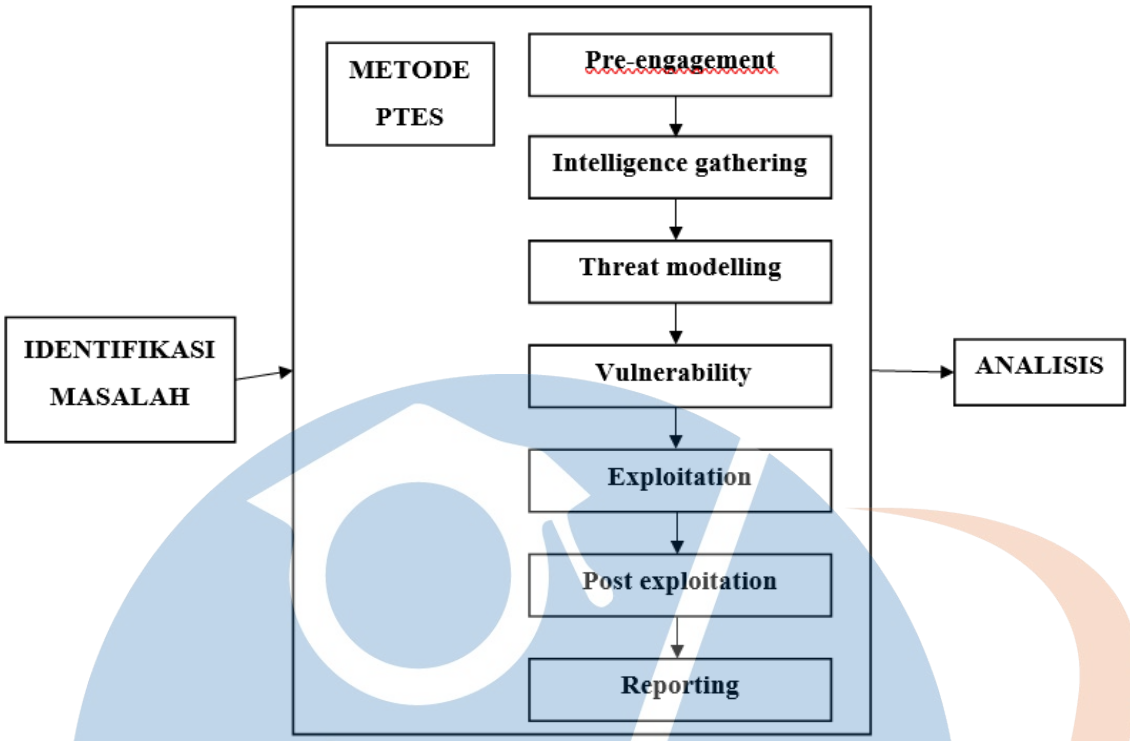
Tabel 2. 1 Peneliti terdahulu

BAB III
METODOLOGI PENELITIAN

Pada penelitian ini menggunakan jenis metode penelitian deskriptif kualitatif. Metode penelitian deskriptif kualitatif sebuah metode yang digunakan peneliti untuk menemukan pengetahuan atau teori terhadap suatu penelitian untuk memahami bagaimana interaksi dengan penggunaan teknologi informasi. Metode penelitian deskriptif kualitatif ini memungkinkan peneliti untuk menggali secara mendalam berbagai aspek dari sistem keamanan jaringan wireless dan memberikan rekomendasi yang terukur dan spesifik untuk meningkatkan keamanan di PT Mitra Bhakti Informasi. Dengan penggunaan metode deskriptif kualitatif ini, hasil dari skripsi atau tugas akhir penulis berupa sesuatu yang dapat diukur berdasarkan kualitas yang dihasilkan dari penelitian. Adapun tahapan penelitian pada bab ini akan membahas tentang tahapan penulis dalam melakukan penelitian "analisis keamanan jaringan wireless dengan metode PTES" yaitu, metode penelitian, tahapan penelitian, lingkungan penelitian, serta timeline penelitian pada PT Mitra Bhakti Informasi. Berikut ini penulis menjelaskan metodologi penelitian dan hasil suatu analisis dengan tahapan sebagai berikut.

3.1 Metodologi Penelitian

Dalam metodologi penelitian tugas akhir ini menggunakan metode Penetration Testing (PTES) yaitu suatu metode penguji keamanan pada suatu lingkup sistem jaringan di PT Mitra Bhakti Informasi dengan simulasi serangan pada jaringan wireless. Tujuan dari metode PTES adalah menemukan kelemahan dan mencegah adanya serangan dari pihak yang tidak di ingikan (*hacking*) pada suatu perusahaan. [9] Langkah – langkah dalam menggunakan metodelogi penelitain ini dengan cara mengidentifikasi masalah lalu metode PTES dan menganalisis.



Gambar 3. 1 Metode penelitian pada metode PTES

3.1.1 Identifikasi masalah

Pada penelitian ini penulis menidentifikasi masalah pada jaringan *wireless* local network guna dalam keamanan dan melindungi sistem pada PT Mitra Bhakti Informasi. Kegiatan penelitian ini juga untuk menganalisa sistem keamanan jaringan wireless.

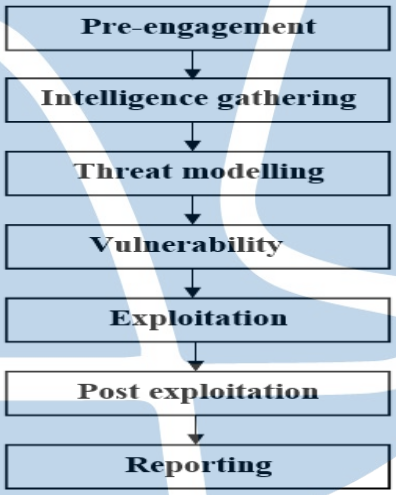
3.1.2 Metode PTES

Pada penelitian ini penulis menggunakan metode PTES dalam mengumpulkan data dan menganalisa data pada suatu jaringan *wireless.* Metode ini merupakan suatu metode yang umum dan efektif bagi para *IT Security* ataupun Audit untuk menjawab dari permasalahan utama pada penelitian ini. Dan pada metode penelitian kali ini dilakukan dengan secara teliti dari tahap awal dan serangkaian prosedur agar kegiatan penelitian ini dapat terlaksana dengan tujuan memecahkan permasalahan dan menjadi solusi bagi para pembaca dalam memecahkan masalah dalam keamanan jaringan *wireless.* [4]

Dengan menggunakan metode PTES pada metode penelitian kali ini sangat cocok dan efisien dalam topik pembahasan penelitian maupun digunakan pada

penerapan keamanan jaringan, yaitu pada penerapan uji coba standart keamanaan pada bidang Security [7]. Dengan metode PTES penulis berharap para Administrator ataupun staff bidang IT dapat membantu menganalisa suatu keamanaan jaringan nirkabel dan menjadi bahan pertimbangan untuk PT Mitra Bhakti Informasi dalam mengambil langkah atau keputusan yang sangat penting bagi keamanan jaringan dan data.

Pada metode *Penetration Testing Execution Standart (PTES)* biasanya digunakan oleh para *IT Security* untuk mencari celah dan akan menjadi sebuah audit yang berisi keamanan data dengan melewati beberapa tahapan yang sesuai dan sudah memenuhi sebuah hasil dari tujuan metode PTES sesuai harapan dari perusahaan. Dalam penelitian ini metode PTES terdiri dari 7 langkah seperti tabel 3.1 diatas yang akan dilakukan selama penelitian ini berlangsung.



Gambar 3. 2 Metode PTES

3.1.2.1 Pre-engagement

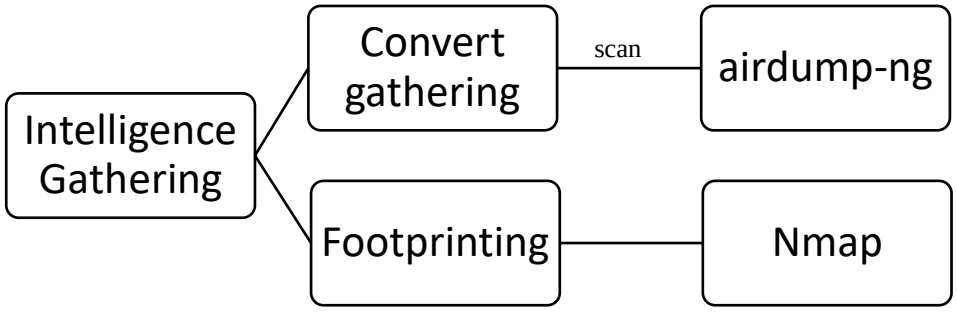
Pada tahap ini ialah tahap wawancara dan permintaan untuk perizinan pada peneliti kepada PT Mitra Bhakti Informasi untuk melakukan penetration testing pada suatu jaringan nirkabel yang ada jaringan lokal. Penulis memeberikan beberapa pertanyaan kepada *Administrator* dan Staff IT mengenai keamanan, spesifikasi jaringan nirkabel dan sistem jaringan nirkabel pada jaringan lokal di Perusahaan. Berikut beberapa pertanyaan yang di ajukan ke pada divisi atau departemen terkait.

1) Siapa yang bertanggung jawab atas pemeliharaan dan pengelola perangkat *wireless*?
2) Berapa jumlah perangkat *wireless* yang ada di PT Mitra Bhakti Informasi?
3) Apakah perangkat *wireless* dalam perawatan baik secara perawatan perangkat maupun penanganan sistem jaringan?
4) Apakah sistem perangkat wireless selalu ter *update* dan dikelola dengan baik?
5) Kapan terakhir melakukan pemeliharaan dan pengelolaan terhadap perangkat *wireless*?
6) Bagaimana Adminstrator dapat memantau perangkat *wireless* ?
7) Dimana posisi perangkat wireless diletakan?

Dari beberapa pertanyaan diatas penulis mendapatkan beberapa informasi mengenai pengelolaan perangkat wireless dan pemeliharaan yang sangat baik pada PT Mitra Bhakti Informasi. Pre engangment ini sangat berguna bagi para peneliti sebelum melakukan *PTES*.

3.1.2.2 Intelligence Gathering

Pada tahap ini penulis akan melakukan pengumpulan informasi dari suatu jaringan nirkabel untuk mendapatkan *metadata* atau sumber data yang dapat dipahami. Cara untuk mendapatkan informasi data menggunakan *tools* pemindaian perangkat dengan *Nmap* dan *airdump-ng* [13] . Dan semua data yang dicatat selama tahap ini akan menjadi suatu bahan pembahasan pokok untuk evaluasi jika adanya temuan suatu kerentanan.

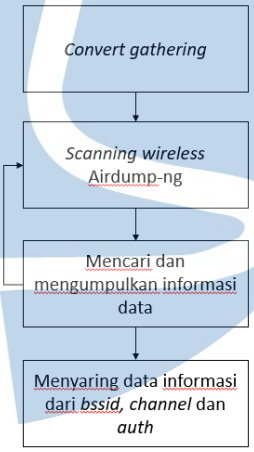


Gambar 3. 3 Intelligence Gathering

Pada gambar 3.3, adalah *flow* dari tahapan pengujian dari *intelligence gathering* dengan menggunakan cara *convert gathering* dan *footprinting.* Pada *convert gathering* peneliti menggunakan *tools* untuk *scanning bssid* yaitu *airdump-ng*. *Convert gathering* ini digunakan pada kegiatan penelitian kali ini untuk mengetahui target yang akan di uji dalam metode *PTES* di PT Mitra Bhakti Informasi. Dan untuk *footprinting* menggunakan *Nmap* sebagai *port scan.*

A. Convert gathering

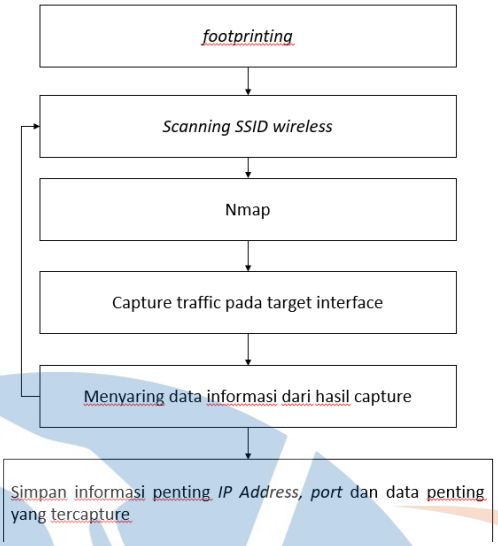
Convert gathering ini merupakan suatu proses dari *scanning wireless* yang akan berguna untuk mengumpulkan informasi yang sangat penting dan akan digunakan sebagai tujuan dari PTES ini, contohnya : *bssid, channel, auth* dan informasi sistem dari perangkat wireless. Cara ini juga dapat mengetahui informasi target perangkat *wireless*.



Gambar 3. 4 Convert Gathering

B. Footprinting

Ini merupakan suatu cara atau proses dalam pengumpulan informasi yang digunakan untuk mengambil data dari data yang melintas dari jalur jaringan yang ada di jaringan lokal wireless ini. Pada Langkah ini peneliti menggunakan tools *nmap*.

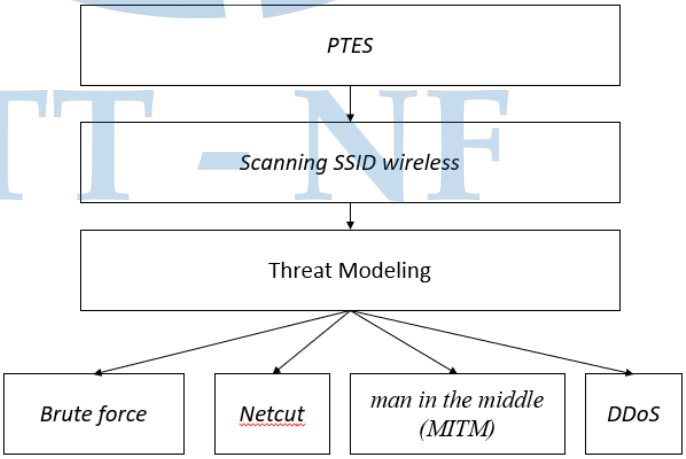


Gambar 3. 5 Footprinting

Dari hasil footprinting ini akan terlihat capture atau data yang tersaring pada traffic network wireless baik berupa IP address, port dan data lainnya.

3.1.2.3 Threat modeling

Pada tahap ini peneliti akan menentukan model atau jenis ancaman yang memungkinkan setelah mendapatkan informasi berdasarkan tahapan sebelumnya pada PT Mitra Bhakti Informasi. Pada bagian ini menggunakan model ancaman yang paling kritis sebagai tes yang wajib untuk dilaksanaan, seperti : *brute force, netcut, ddos* dan *man in the middle (MITM).*



Gambar 3. 6 Threat modeling

a. Brute force, serangan ini berguna sebagai teknik serangan mencari kata sandi pada suatu sistem dengan berbagai kata kata pada algoritma yang akan terus mencoba berulang kali. Sederhananya, sistem ini akan menyerang pada halaman login dengan cara menebak kata sandi dengan *wordlist* yang disediakan sampai sistem serangan ini menebak dengan sesuai *credential password* yang ada di target. [14]

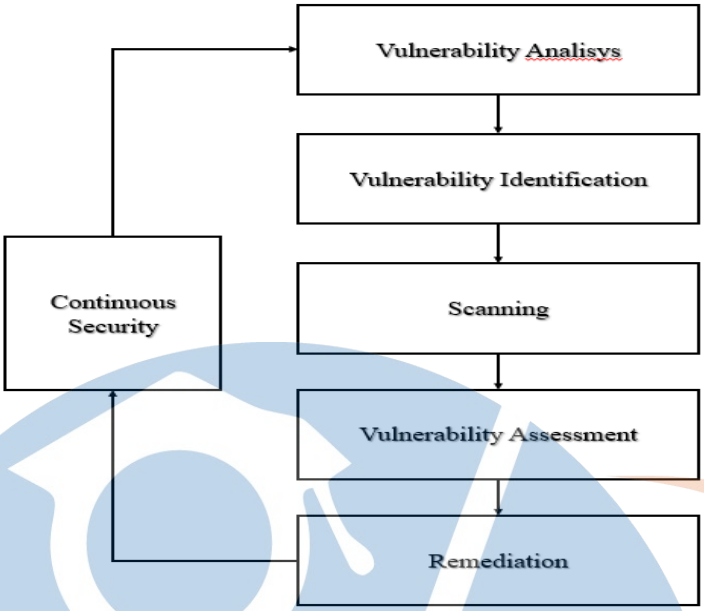
b. Netcut, Netcut atau netcat adalah sebuah utiliti tool yang digunakan untuk berbagai hal yang berkaitan dengan protokol TCP atau UDP. Yang dapat membuka koneksi TCP, mengirimkan paket-paket UDP, listen pada port port TCP dan UDP, melakukan scanning port, dan sesuai dengan IPV4 dan IPV6. Ciri – ciri dari serangan ini ialah pada saat kita menggunakan suatu jaringan begitu lambat tetapi pada perangkat wireless ping ke internet stabil, lalu pada saat merestart perangkat wireless akan kembali normal.

c. *man in the middle (MITM),* serangan ini menggunakan Teknik atau cara menyerang atau memodifikasi pada traffic pada suatu network. Dengan begitu, seorang penyerang dapat membuat suatu jaringan wireless palsu atau duplikasi pada SSID. [15]

d. *DDoS,* serangan ini menggunakan *flooding packet* data pada target. Simpelnya, serangan ini akan mengirim kan *packet data* besar ke target hingga membuat sistem target lambat sampai tidak dapat mampu berdaya menerima semua *flooding* atau *packet data* begitu banyak dan ukuran *file* yang besar [16].

3.1.2.4 Vulnerability Analysis

Pada tahap ini peneliti akan mengumpulkan semua infromasi data dari hasil tahap *intelligence gathering* dan *threat modeling* untuk dapat menemukan celah keamanan pada suatu jaringan lokal di PT Mitra Bhakti Informasi. Lalu, akan dilanjutkan ke tahap selanjutnya agar peneliti dapat menguji kerentanan yang ditemukan oleh peneliti dari hasil *Vulnerability analysis.*



Gambar 3. 7 Vulberability analysis

Dalam Proses Scanning di metode Vulnerability analysis ini menggunakan tools yang secara open source. Setelah berhasil penguji akan mendapatkan informasi yang di targetkan. Hasil dari penguji handsake ini akan menjadi sebuah format file .cap dari Access Point yang di targetkan pada lokasi sekitar.

3.1.2.5 Exploitation

Langkah ini dapat dilkakukan jika seorang penyerang sudah mengumpulkan dan informasi yang jelas dan detail. Selanjutnya dalam pengujian mengeksploitasi jaringan wireless yang ada di PT Mitra Bhakti Informasi. Pada tahapan ini penguji akan melakukan serangn terhadap salah satu jaringan *wireless* dengan 4 metode penyerangan dari tahapan sebelumnya *Threat Modeling.*

3.1.2.6 Post exploitation

Tahapan ini dilakukan setelah penguji berhasil melakukan penetration testing terhadap sistem keamaan jaringan wireless dan untuk upaya mempertahankan keamanaaan jaringan pada suatu jaringan lokal perusahaan bahkan untuk membatasi hal akses.

3.1.2.7 Reporting

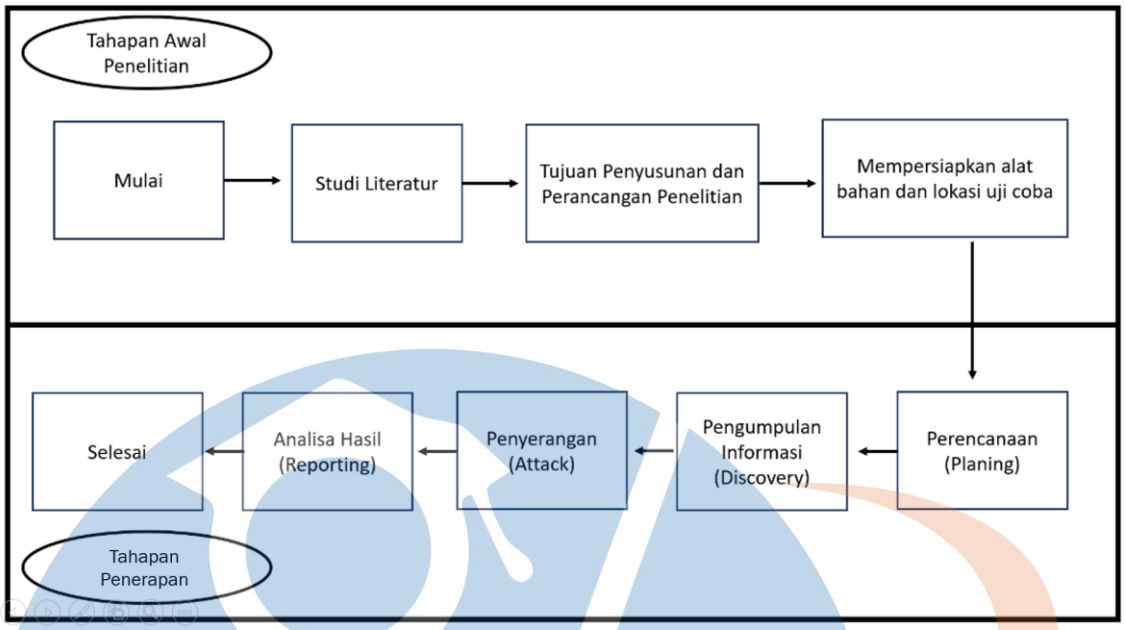
Pada tahapan ini penguji akan memberikan laporan terhapad hasil analisis tentang celah keamanan pada jaringan lokal *wireless* kepada pihak yang berwajib atas menangani jaringan lokal yang ada di PT Mitra Bhakti Informasi.

3.2 Metode Pengumpulan Data Penelitian

Didalam tahapan metode pengumpulan data ini, penelitian ini menggunakan metode deskriptif kualitatif untuk mengeksplorasi dan menganalisis sistem keamanan jaringan wireless di PT Mitra Bhakti Informasi. Metode ini dipilih karena memungkinkan peneliti untuk menggali secara mendalam fenomena yang kompleks dan dinamis dalam konteks jaringan wireless dan keamanan sibernya. penulis melakukan pengumpulan data melalu studi literature yang bertujuan untuk memberikan informasi dan membagikan beberapa teori – teori yang sangat berguna sebagai mengatasi permasalahan pada penulis sebagai bahan pembahasan hasil penelitian. Sehingga penulis dan pembaca memahami konspe dari penelitian analisis keamanan jaringan, wireshark, alfa network dan cara kerja dari metode penetration testing.

3.3 Tahapan Penelitian

Pada penelitian ini penulis membuat 2 tahapan yaitu tahapan awal dan tahapan penerapan. Pada tahapan awal berupa tahapan dari penyusunan penulisan tugas akhir ini dan tahapan akhir sebagai tahap dalam menggunakan cara Planning, Discovery, Vulnerability dan Repoting. Berikut ini langkah – langkah dalam menggunakan metode PTES ini dengan cara berikut.



Gambar 3. 8 Tahapan Penelitian

3.1.1 Studi Literatur

Di tahap ini penulis melakukan studi literatur agar dapat memahami konsep dalam suatu kegiatan analisis keamanan jaringan wireless menggunakan metode PTES. Agar hasil dari studi literatur ini menjadi landasan teori dasar yang akan dipakai dan akan menjadi pendasar yang sangat valid bagi penulis untuk memahami teori dan langkah pada teori maupun praktik yang baik pada penulisan penelitian ini.

3.1.2 Tujuan Penyusunan dan Perancangan Penelitian

Pada tahap ini penulis melakukan tujuan penyusunan dan perancagan penelitian untuk pembaca dapat memahami dari arah dan perencaan pada penelitian ini. Pada dasarnya penelitian ini ditujukan untuk meneliti atau menganalisa pada suatu jaringan wireless dengan metode PTES dan serta membuat rancangan penelitian yang mencakup alat, bahan, metode, topologi jaringan serta rangka waktu penelitian.

3.1.3 Mempersiapkan alat bahan dan lokasi uji coba

Pada tahapan ini penulis menganalisa suatu jaringan Lab network pada PT Mitra Bhakti Informasi yang dimana alat yang digunakan

accesspoint dan *alfa network* dan bahan yang digunakan adalah *airodump, ettercap* dan *hping3* sebagai implementasi dari penelitian ini. Alat dan bahan ini digunakan dalam penelitian sebagai analisa dalam keamanan jaringan wireless.

3.1.4 Perencanaan (planning)

Langkah awal dalam menggunakan metode ini adalah mengidentifikasi pada suatu sasaran, ruang lingkup dan tujuan test. Planning juga mencakup pada mentargetkan dari pengumpulan informasi pada suatu jaringan.

3.1.5 Pengumpulan Informasi (Discovery)

Adapun langkah kedua pengumpulan informasi mengenai sistem target yang diuji menggunakan scanning dan akan di kumpulkan dan dicatat. Adapun informasi yang dikumpulkan mencakup pada alamat IP, host, sistem operasi, domain name dan packet data.

3.1.6 Analisis Kerentanan (Vulnerability Detection)

Langkah ini adalah langkah lanjutan setelah mengumpulkan informasi yang banyak kita temukan lalu kita analisis untuk mencari celah keamanaan dengan perangkat Alfa Network setelah itu kita gathering semua data pada jaringan tersebut dengan wireshark agar data data yang kita kumpulkan dapat di export dan menjadi hasil analisa pada suatu jaringan.

3.1.7 Analisis Hasil (Reporting)

Pada langkah terakhir ini, Setelah data kita kumpulkan dan export hasil nya. Kita susun laporan dari hasil analisa dan temuan celah, potensi, dampak serangan dan saran untuk di perbaiki sistem tersebut.

3.4 Lingkungan Penelitian

Lingkungan penelitian tugas akhir ini, penulis melakukan uji coba penelitian di sebuah ruangan lab khusus dan bukan production (Non Prod) pada suatu network area di perusahaan sebagai bahan lab dan uji coba.

3.5 Alat dan Bahan Penelitian

Dalam metode analisis keamanan jaringan yang berbasis menggunakan wireless penulis menggunakan beberapa alat dan software sebagai tools dalam onboarding atau dalam uji coba penelitian.

3.5.1 Alat

No	Nama Alat	Model	Banyak	Keterangan
1	Access Point	TPLink TI-wa 801	1 pcs	Sebagai alat penyebar luasan area jaringan pada suatu ruangan tanpa kabel atau wireless
2	Alfa Network	AWUS036ACH	1 pcs	Sebagai alat menyambungkan ke suatu jaringan nirkabel yang tidak dapat dihubungkan oleh adaptor internal komputer.
3	Mikrotik	RB-1100	1 pcs	Router
4	Laptop	HP	1 pcs	Sebagai alat onboarding atau melakukan uji coba

Tabel 3. 1 Alat

3.5.2 Bahan

No	Nama Tools	Versi	Keterangan
1	VirtualBox	7	Sebagai menjalankan OS Kali Linux dalam
2	OS Kali Linux	Kali Linux 2021	System operasi yang digunakan sebagai bahan uji coba
3	OS Windows	Windows 11	System operasi yang digunakan sebagai bahan uji coba

4	Wireshark	2.4	Tools yang digunakan sebagai penyaring packet data yang melintas pada suatu jaringan

Tabel 3. 2 Bahan

3.6 Timeline Penelitian

Berikut ini merupakan tabel kegiatan timeline penelitian yang direncanakan oleh peneliti dalam melakukan penelitian ini dengan kurun waktu kurang lebih 7 bulan, yang dimulai dari bulan Februari 2024 sampai bulan Agustus 2024. Sebagai berikut :

No	Nama Kegiatan	Bulan						
		Feb	Mar	Apr	Mei	Jun	Jul	Agu
1	Kajian Literatur							
2	Analisis							
3	Penyusunan Proposal							
5	Perancangan Sistem							
6	Pengembangan Sistem							
8	Penarikan Kesimpulan dan Saran							
10	Sidang							

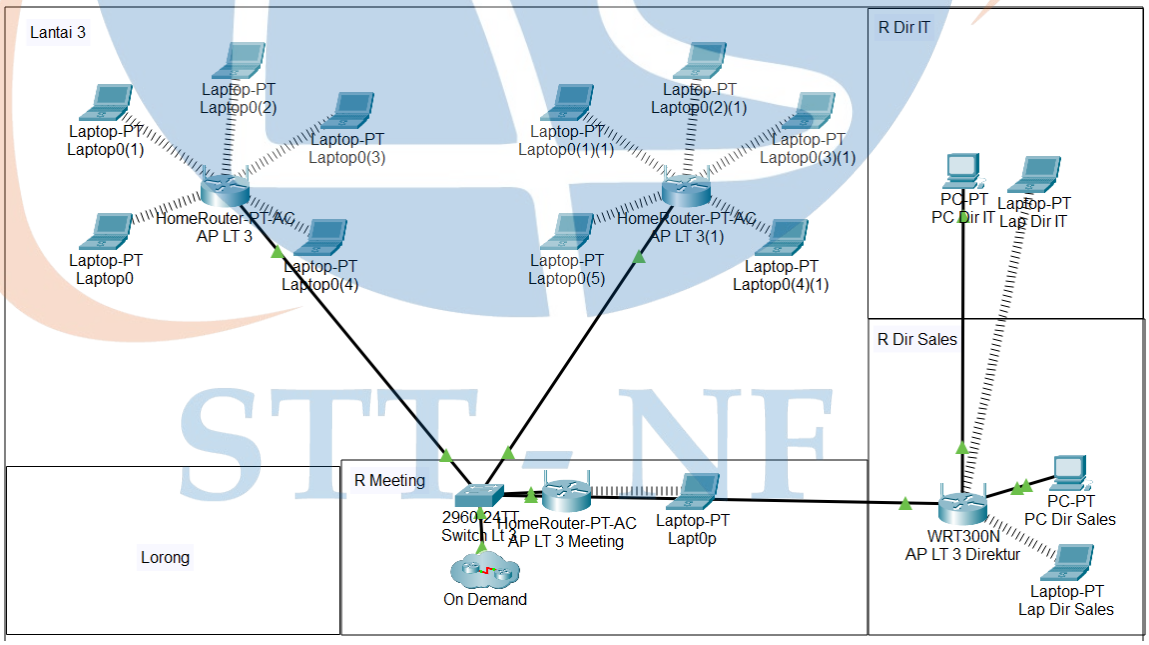
Tabel 3. 3 Timeline Penelitian

BAB IV
IMPLEMENTASI DAN EVALUASI

Pada bab ini penulis akan menjelaskan secara rinci mengenai penerapan analisi keamanan jaringan wireless dari konsep, motede dan sistem penerapan yang sudah di rancang. Maka dari itu, bab ini juga akan membahas hasil atau evaluasi dari analisis tersebut.

4.1 Perancangan

Perancangan pada pembahasan kali ini mengenai topologi yang akan di PenTesting di PT Mitra Bhakti Informasi. Topologi yang di maksud peneliti ialah salah satu raungan pada gedung kantor BPJS yang berada tepat di Jln. Gatot Subroto Jakarta Selatan sebuah *logic topologi* jaringan wireless yang kurang lebih hampir mirip berada di lantai 3 pada lantai tersebut terdapat departement *IT* dan *Bisnis Marketing* dengan model topologi star, seperti gambar berikut. *Logic topologi* dari jaringan lokal di PT Mitra Bhakti Informasi seperti berikut.



Gambar 4. 1 Topologi Jaringan

4.2 Kegiatan Penetration Test

Pada kegiatan kali ini penguji memiliki tujuh langkah-langkah metode *PTES* yaitu *pre-engagement, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post exploitation* dan *reporting*.

4.2.1 Pre-engagement

Pre-engagement yang dilakukan penguji saat penelitian berupa wawancara sebagai *assessment* dan bukan bagian dari metodelogi penelitian dengan pertanyaan mengenai perangkat *wireless, physical* dan *administrator* sistem. Wawancara ini membantu peneliti untuk mendapatkan informasi dilokasi penelitian. Berikut hasil wawancara penetration test wireless.

No	Peneliti	Narasumber
1	Siapa yang bertanggung jawab atas pemeliharaan dan pengelola perangkat wireless?	Kita memiliki divisi Staff IT yang dimana 3 posisi, yaitu Administrator, Programmer dan IT Support
2	Berapa jumlah perangkat wireless yang ada di PT Mitra Bhakti Informasi?	21 Perangkat Aktif
3	Apakah perangkat wireless dalam perawatan baik secara perawatan perangkat maupun penanganan sistem jaringan?	Perangkat selalu terjaga dalam kebersihan, melakukan update pada software dan ter-monitoring dengan software cacti.
4	Apakah sistem perangkat wireless selalu ter update dan dikelola dengan baik?	Perangkat selalu terupdate secara *software* dan selalu melakukan *backup* serta penambahan konfigurasi pada keamanan
5	Kapan terakhir melakukan pemeliharaan dan pengelolaan terhadap perangkat wireless?	Pemeliharaan dan pengolalaan dilaksanakan pada setiap seminggu sekali untuk proses backup dan membersihkan perangkat setiap hari
6	Bagaimana Adminstrator dapat memantau perangkat wireless ?	Dengan software cacti
7	Dimana posisi perangkat	Di tempat yang tidak mudah di

	wireless diletakan?	temukan oleh manusia seperti di balik plafon

Tabel 4. 1 Assesment pre-engagement

4.2.2 Intelligence Gathering

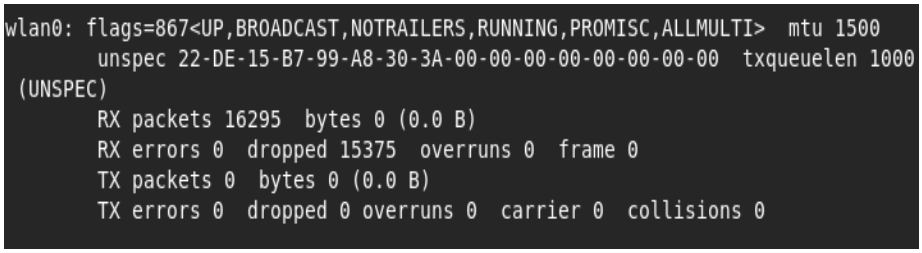
Pada kegiatana kali ini yang dilakukan saat penelitian berupa analisa jaringan, *convert gathering*, identifikasi wireless dan *footprinting*.

A. Convert Gathering

Covert gathering adalah teknik untuk mengumpulkan informasi secara *undetected* tanpa terdeteksi oleh administrator jaringan atau sistem keamanan. Pada jaringan *wireless*, *covert gathering* dapat dilakukan dengan menggunakan alat dan teknik yang meminimalkan jejak yang ditinggalkan. *Convert gathering* yang dilakukan dalam pengujian kali ini menggunakan beberapa *tools* berupa *scan wireless* seperti *airodump-ng*. *airmon-ng, tcpdump, dan wireshark* untuk mengumpulkan informasi tanpa diketahui dari sistem maupun sang adminstrator jaringan. Teknik ini ditunjukan untuk pengujian metode *penetration testing (PTES)* dan audit tanpa terdeteksi oleh sistem dan administrator jaringan. Langkah pada pengujian ini sudah mendapatkan izin legal dengan PT Mitra Bhakti Informasi sebelum melakukan aktivitas pengumpulan informasi pada jaringan *wireless*.

Pertama kita akan melakukan *Scan wireless* dipastikan perangkat di *setting mode monitor* dengan perintah:

#iwconfig wlan0 mode monitor

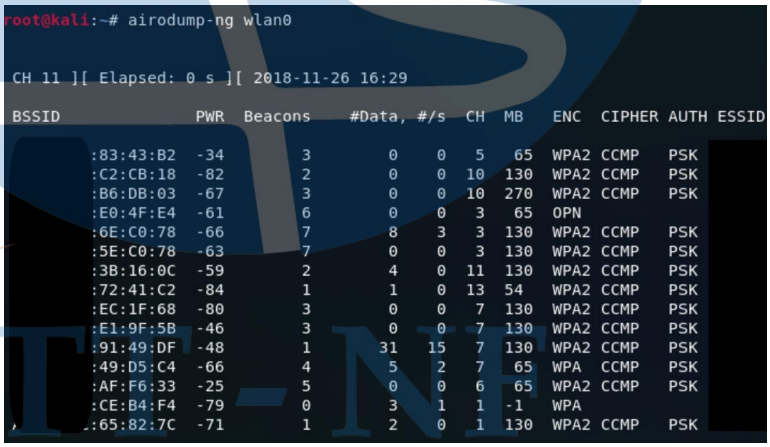


Gambar 4. 2 Mengaktifkan interface wlan0

Dari gambar diatas, bahwa perangkat *wireless* laptop menjadi *mode monitor* dengan jumlah *maximum transmission unit* (*MTU*) 1500, sedangkan *txqueuelen* diukur dari jumlah *frame* pada *ethernet* serta ukuran *buffer*. RX *packet* yang di terima dari mode monitor ini 16295, RX *dropped* yang ditahan sebanyak 15375. Sedangkan untuk TX atau *Transmitter* tidak didapati paket.

Untuk melakukan monitoring jaringan wireless dengan perintah *command*:

#sudo airodump-ng wlan0



Gambar 4. 3 Monitoring dengan airodump-ng

Hasil dari monitoring menggunakan *airodump-ng* seperti gambar diatas. Dalam proses ini mendapatkan BSSID (*mac address*) perangkat yang ada disekitar area dengan PWR yang merupakan *signal level* atau kekuatan sinyal dari perangkat wireless, PWR yang dihasilkan dibawah -

80. *Beacons* merupakan jumlah paket yang di kirimkan melalui *access point*. Data merupakan jumlah data paket yang di *capture*. #/s adalah jumlah *packet* data yang di ukur per 10 detik terakhir. CH merupakan *channel number* yang berasal dari *beacon packet* pada wireless. *MB* adalah *maximum speed* pada *access point*. ENC merupakan enkripsi algoritma yang di gunakan oleh *user*. *CIPHER* mendeteksi sandi berupa *ccmp* dan *tkip*, *ccmp* digunakan pada *WPA2* sedangkan *tkip* digunakan pada *WPA*. *Auth* atau *authentication protokol* yang digunakan adalah PSK *(Pre-Shared Key)*, *PSK* merupakan fitur keamanan yang berada pada wireless. Untuk ESSID menjelaskan nama *ssid* perangkat wireless.

Setelah kita mendapatkan data informasi dari memindai perangkat wireless yang ada disekitar kita. Gunakan command dibawah ini untuk menyimpan hasil pemindaian tsb,

#sudo airodump-ng -w output --output-format csv wlan0mon

Atau bisa kita import hasil capture sniffing atau penangkapan paket data dengan metode monitoring dan menyimpan hasil pemindaian ke format .cap

#sudo tcpdump -i wlan0mon -w capture.pcap

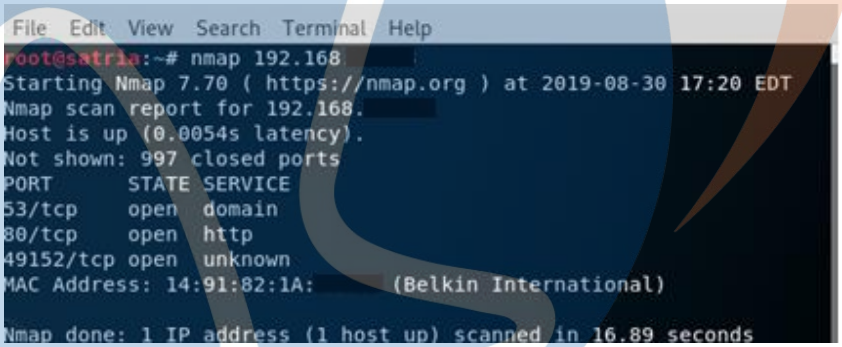
Ket :

- -i wlan0mon : Menggunakan *interface* wlan0 sebagai mode monitoring
- -w capture.pcap : Menyimpan hasil tangkapan ke file capture.pcap untuk analisis lebih lanjut

B. Footprinting

Footprinting yang dilakukan pada target *wireless* yaitu mengcapture dan *filter packet* untuk menambah informasi selama proses *information gathering* dengan menggunakan *nmap* . *Footprinting* dengan *Nmap (Network Mapper)* merupakan suatu proses pengumpulan data informasi mengenai sistem jaringan target dan perangkat yang terhubung ke dalam jaringan target tersebut. *Nmap* juga sebagai *tools* serbaguna untuk melakukan berbagai jenis pemindaian jaringan. Berikut langkah yang dilakukan dengan menggunakan *nmap*. Untuk mendapatkan informasi *packet* pada target

#nmap (ip target)



Gambar 4. 4 Scanning NMAP

Pada proses gambar diatas *nmap* dapat terlihat bahwa *nmap* melakukan proses *scanning* dari ip address yang di tergatkan. Muncul *port, state* dan *service* yang terbuka seperti *port tcp* 53 (*domain*), *tcp* 80 (*http*) dan *tcp* 49152 (*unknown*).

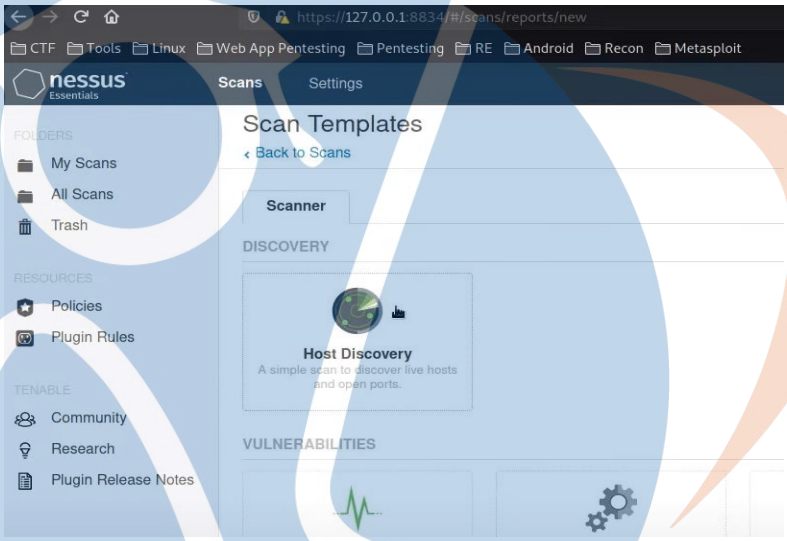
4.1.3 Threat Modelling

Threat modelling yang dilakukan dalam penelitian ini berupa pengujian beberapa serangan seperti *brute force attack, man in the middle (MITM) attack* dan *de-authentication*.

4.1.4 Vulnerability Analysis

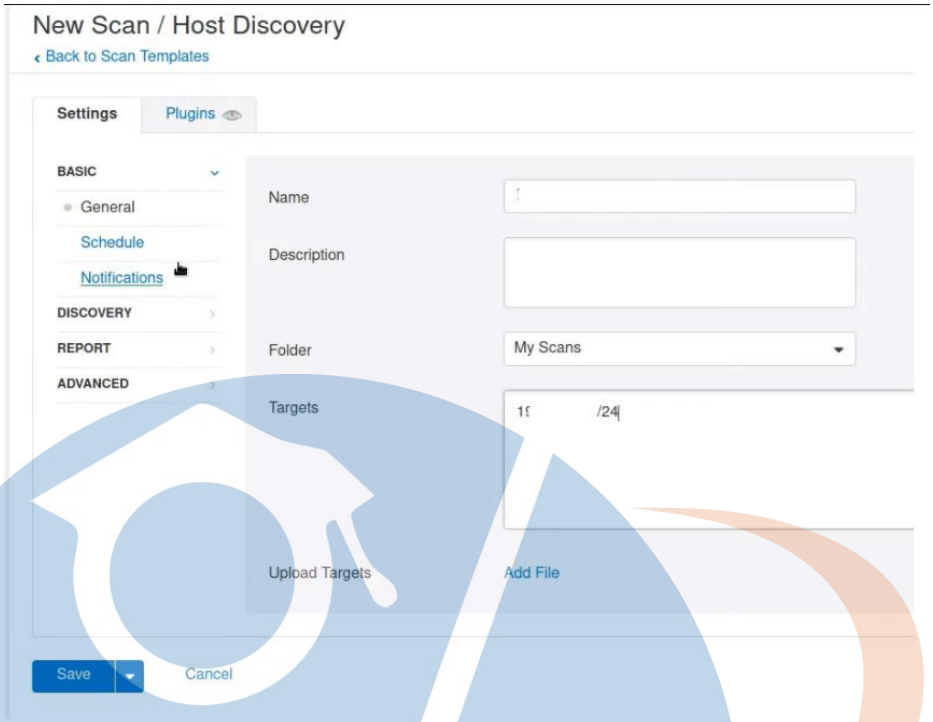
Pada kegiatan *Vulnerability analysis* yang dilakukan untuk meneliti dengan cara menganalisa kerentanan sistem wireless dengan menggunakan *nessus*.

1. Pada halaman awal nessus dashboard



Gambar 4. 5 Dashboard Nessus

2. Lalu masukan *Nama scan* dan *IP target* didalam kolom *targets*,



Gambar 4. 6 New scan Nessus

Lalu klik tanda panah bawah samping *save* dan klik *launch*.

Gambar 4. 7 Launch scan

3. Lalu kita tunggu sampai proses selesai

Gambar 4. 8 Proses Nessus Scan

Hasil dari scaning nessus ini akan ditampilkan pada Analisa dibagian 4.3 Analisa.

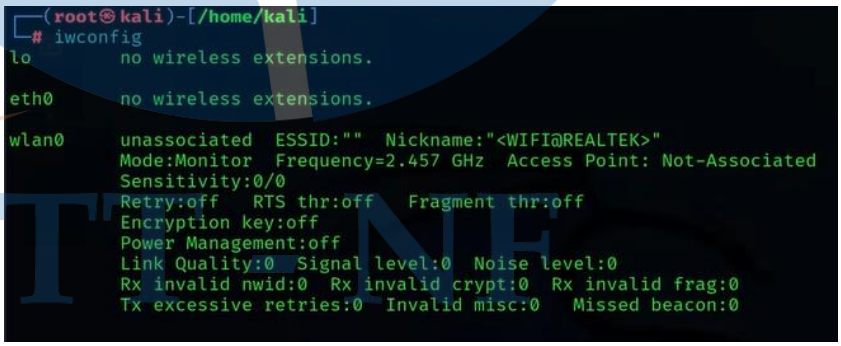
4.1.5 Exploitation

Setelah mengumpulkan semua informasi yang diperlukan untuk pengujian jaringan wireless ini, Serangan ini dapat di implementasikan dilokasi .selanjutnya akan dilakukan 3 jenis penyerangan yaitu *brute force attack, man in the middle attack (mitm)* dan *deauthentication attack*. Dari informasi sebelumnya dapat di gunakan sebagai bahan pengujian.

4.1.5.1 Brute Force Attack

Pada serangan ini adalah metode serangan dalam dunia keamanan komputer di mana penyerang mencoba untuk mendapatkan informasi yang diinginkan, seperti kata sandi atau kunci enkripsi, dengan mencoba setiap kemungkinan kombinasi secara sistematis hingga menemukan yang benar [5]. Pada kali penguji akan mencoba pada beberapa jaringan wireless secara acak. Penguji akan melakukan cara untuk mendapatkan password dari *ssid* tersebut dengan cara *brute force attack*. Berikut ini langkah – langkah untuk melakukan serangan *brute force*.

1. Mengaktifkan mode monitor airodump-ng
   Sebelum kita aktifkan mode monitor kita cek interface nya terlebih dahulu dan mengkaitkan ke interface
   #iwconfig



Gambar 4. 9 Interface Iwconfig

#sudo airmon-ng

#sudo airmon-ng start wlan0

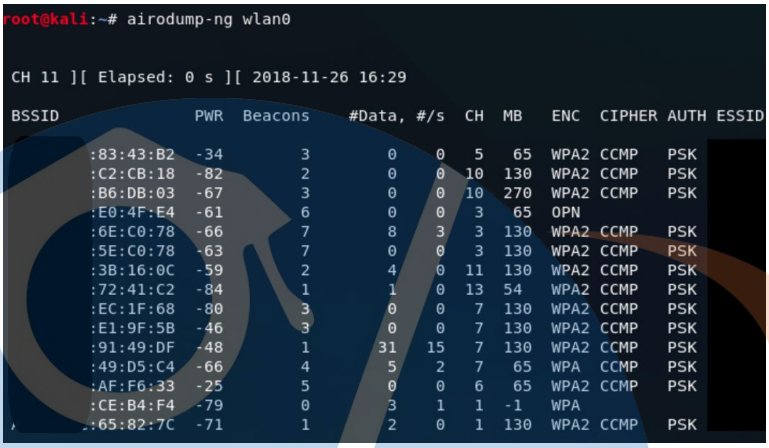
Setelah itu ubah mode monitor ke target interface

#sudo airodump-ng wlan0mon

2. Mendeteksi Jaringan Wi-Fi

Pada langkah ini penguji akan memilih perangkat wireless yang akan diserang

#sudo airodump-ng wlan0



Gambar 4. 10 airodump-ng wlan0

Ket :

- BSSID menunjukkan alamat MAC jaringan target
- PWR menunjukkan kekuatan sinyal jaringan. Semakin tinggi angkanya, semakin baik pula sinyalnya
- Beacon adalah frame yang dikirim oleh jaringan untuk menyiarkan keberadaannya
- #Data, menunjukkan jumlah paket data atau jumlah frame data
- #/s menunjukkan jumlah paket data yang kita kumpulkan dalam 10 detik terakhir
- CH menunjukkan saluran tempat jaringan bekerja
- ENC menunjukkan enkripsi yang digunakan oleh jaringan. Bisa berupa WEP, OPN, *WPA*, *WPA*2
- CIPHER menunjukkan cipher yang digunakan dalam jaringan
- AUTH menunjukkan otentikasi yang digunakan pada jaringan
- ESSID menunjukkan nama jaringan

3. Mengumpulkan target data

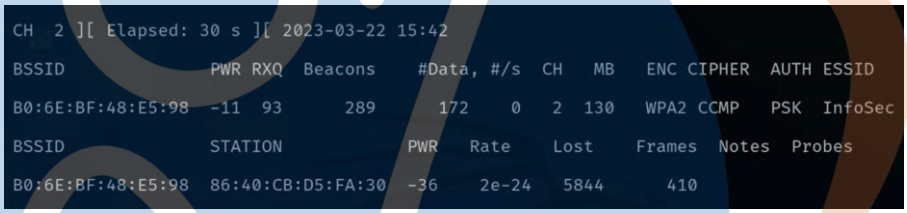
Lalu kita mengumpulkan dari nama ssid yang akan diserang

Gambar 4. 11 simpan infromasi data hasil pemindaian

#sudo airodump-ng -c [channel] --bssid [BSSID] -w [output file] wlan0mon

Ket :

- -c [channel]: Channel dari jaringan target.
- --bssid [BSSID]: BSSID dari jaringan target.
- -w [output file]: Nama file untuk menyimpan paket yang dikumpulkan.

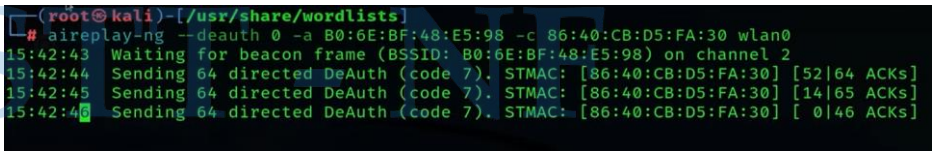


Gambar 4. 12 Handsake airodump

4. Menangkap Handsake

Dari hasil langkah diatas kita dapat menggunakan aireplay-ng dengan proses *de-authentication* pada *BSSID* dengan spesifik dan detail yang akan dijadikan *monitor* pada *BSSID* target sehingga penguji dapat *WPA Handshake* dan hasil nya akan disimpan sebagai *file* ber*format .cap*.

#sudo aireplay-ng --deauth 10 -a [BSSID] wlan0mon



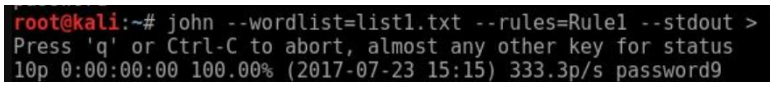
Gambar 4. 13 De – authentication handsale

5. Memecahkan kata sandi

Dari langkah hasil sebelumnya bisa kita dapatkan *capture* .cap diatas kita dapat lanjutkan untuk dijadikan sebagai penyerangan kata sandi perangkat tersebut dengan *brute force.* Sebelum mekakukan

serangan penguji mempersiapkan terlebih dahulu wordlist yang akan menjadi acuan cracking password ini. Dengan cara menggunakan *tools* dari *Jhon The Ripper* sebagai berikut.

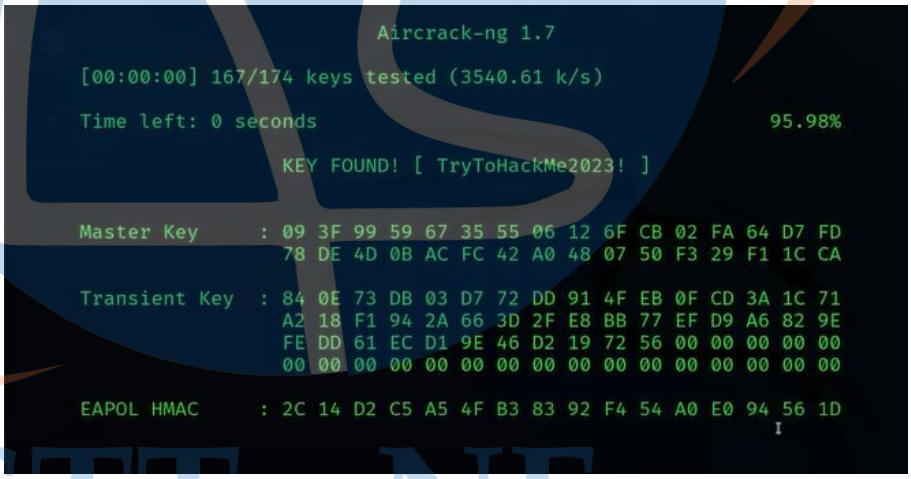
#sudo john --wordlist=list.txt –rules=Rule1 --stdout > [namafile].txt



Gambar 4. 14 Membuat wordlist untuk cracking password

#sudo aircrack-ng [output file]-01.cap -w [wordlist]

Gambar 4. 14 Cracking / brute force password



Gambar 4. 15 Hasil dari bruteforce

Dari hasil langkah yang kita lakukan dapat di penguji berhasil bahwa *password* yang kita *brute force* seperti gambar diatas dan kita telah melakukan uji coba pembobolan password pada *WPA*.

4.1.5.2 Man In The Middle Attack (MITM)

Setelah penguji telah mendapatkan kata sandi dengan metode *brute force attack* maka selanjutnya akan menguji jaringan *wifi* tersebut dengan serangan *man in the middle attack* yaitu menjadi orang ditengah-tengah komunikasi antara korban dan *wifi.* [5] Saat menguji serangan ini menggunakan *ettercap.* Berikut ini langkah – langkah dan hasil dari serangan *man in the middle (MITM)* :

1. Instalasi *Ettercap*

   #sudo apt-get update

   #sudo apt-get install ettercap-graphical

2. Memilih *Interface*

   Buka terminal dan jalankan *Ettercap* dalam *mode grafis* atau GUI.

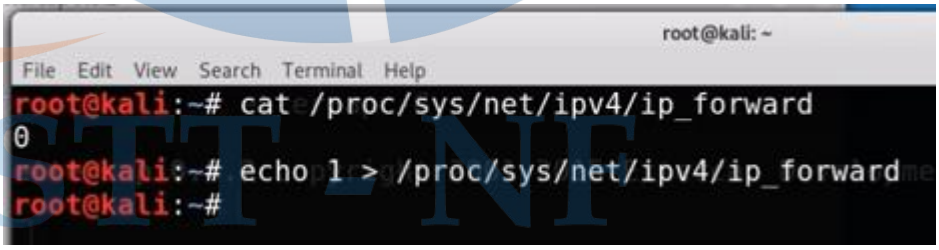
   #sudo ettercap -G

3. Aktifkan forward IPv4

   Buka terminal dan jalankan command berikut.

   #cat /proc/sys/net/ipv4/ip_forward

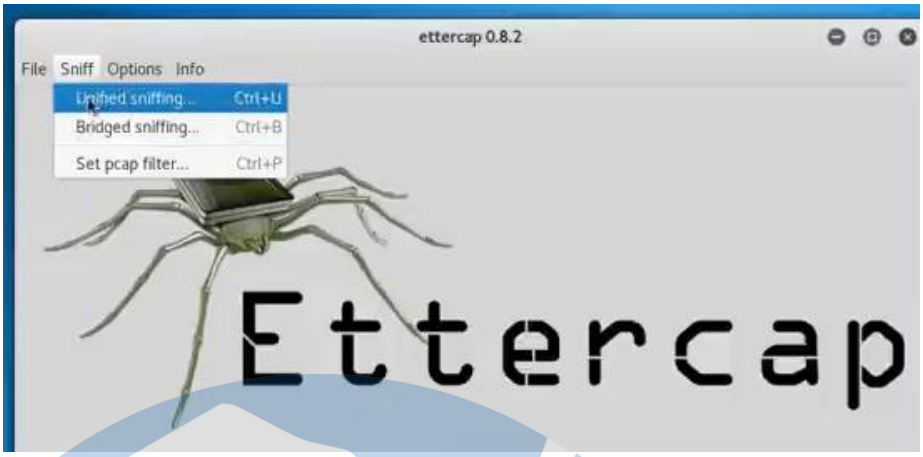
   #echo 1 > /proc/sys/net/ipv4/ip_forward



Gambar 4. 16 Mengaktifkan IP Forward IPv4

4. Memulai Scan Jaringan

   Pada antarmuka Ettercap, pilih antarmuka jaringan yang akan digunakan untuk serangan (misalnya, eth0 atau wlan0):



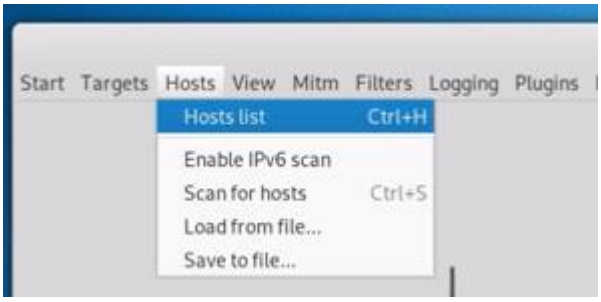
Gambar 4. 17 Halaman awal ettercap

Klik pada *Sniff* > *Unified sniffing*, Pilih antarmuka jaringan yang sesuai dan klik OK.

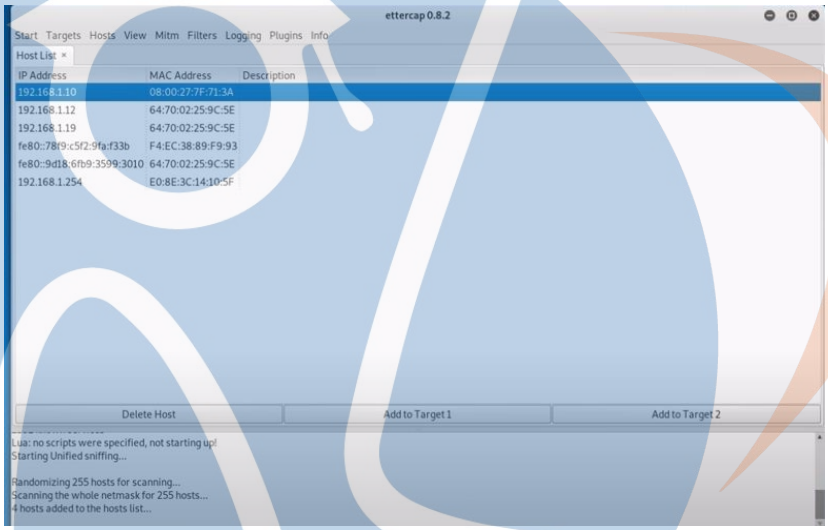
Gambar 4. 18 Memilih interface

5. Menambahkan *Target*

   Pilih menu *Hosts* > *Hosts list*

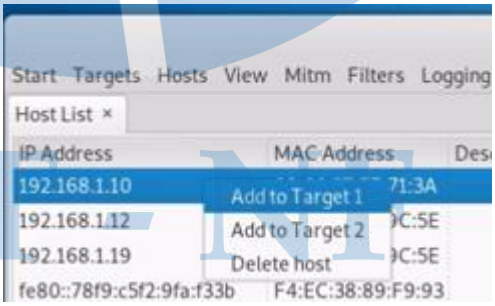


Gambar 4. 19 Menu hosts list



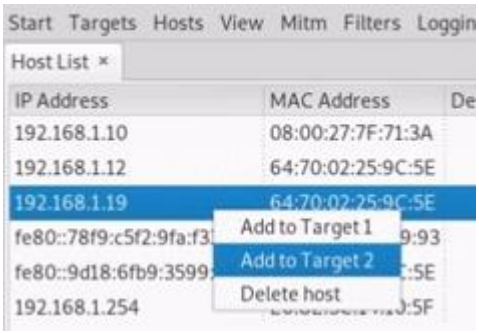
Gambar 4. 20 Host list

Lalu pilih IP yang akan menjadi target 1



Gambar 4. 21 Target 1

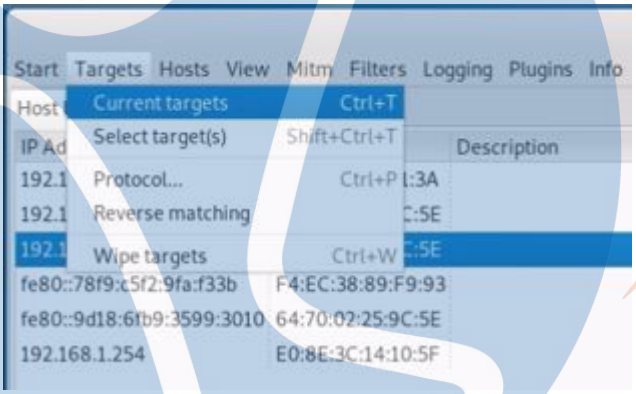
Lalu pilih IP untuk menjadi target 2



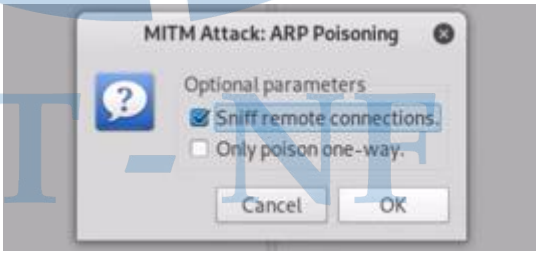
Gambar 4. 22 Target 2

6. Memulai Serangan *MITM*

   Pilih menu *Targets* > *Current targets* untuk melihat target.

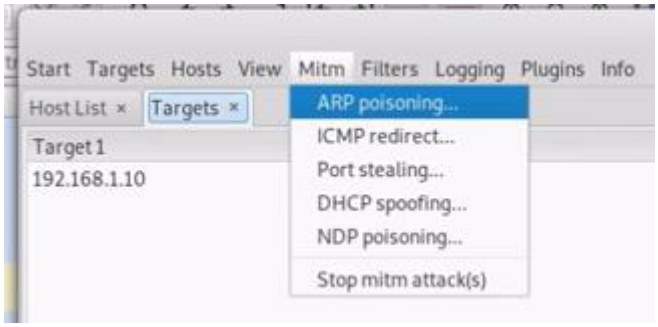


Gambar 4. 23 Current targets



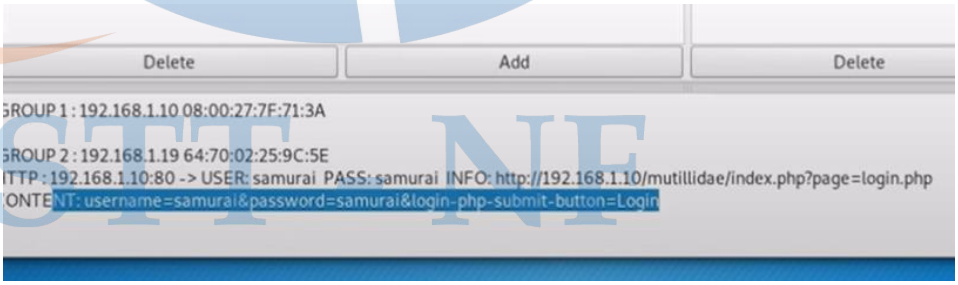
Gambar 4. 24 MITM Attack ARP Poisoning

7. Memulai *Sniffing*



Gambar 4. 25 ARP Poisoning

Gambar 4. 26 Contoh halaman web untuk tes login



Gambar 4. 27 Hasil MITM dengan Ettercap

Dari hasil gambar diatas, berupa kata sandi yang telah di *capture* selama serangan *man in the middle* (MITM) dengan *ettercap*. Proses *sniffer* menggunakan *ettercap* yang dimana target serangan ini untuk menjadi

penentu informasi perangkat *wireless*. *Protocol* disaring dengan berupa *tcp, udp* dan beberapa informasi yang disaring sesuai dengan target dan tujuan. Dengan cara penyaringan koneksi yang dilakukan secara *active* dan *pasive* terdapat keterangan bahwa user target mengakses jaringan wireless untuk masuk ke *web portal* yang perlu *login*.

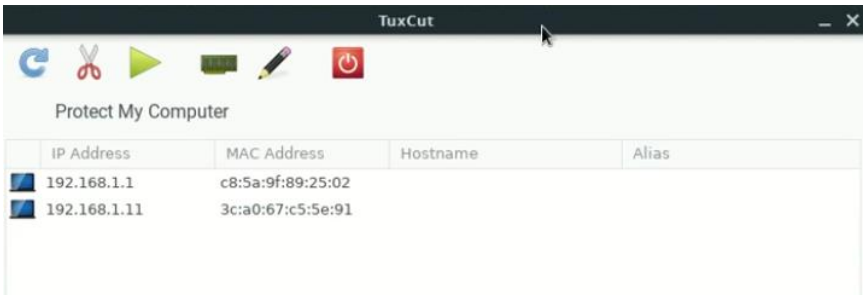
4.1.5.3 Deauthentication Attack

Setelah memonitoring korban dengan serangan *man in the middle (MITM)*, pada tahap pengujian kali ini akan melakukan metode *deauthentication attack* pembatasan penggunaan jaringan atau *limit bandwidth*. Dengan cara penguji mencari informasi tentang *bbsid* dan *mac address* dari perangkat nirkabel yang menjadi target serangan. Penguji akan menggunakan 2 metode untuk melakukan *de-authentication* yaitu *netcut* dan *Distributed Denial of Service (DDoS)*.

1. *Netcut*

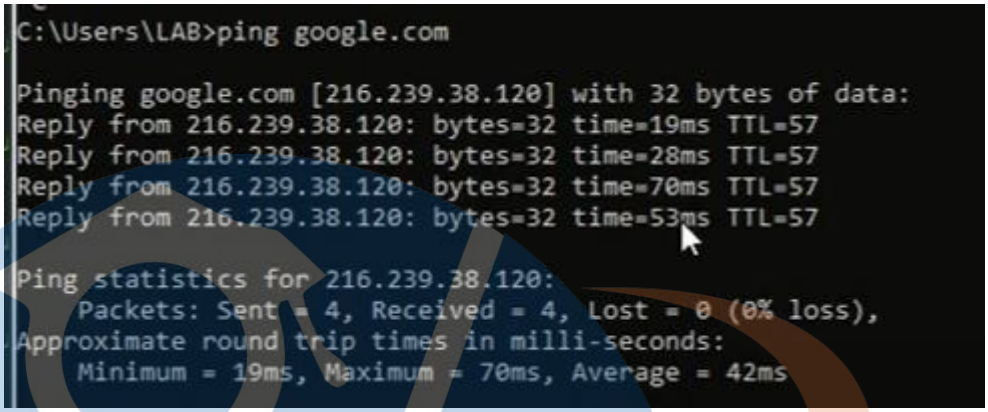
   Pada metode netcut ini ialah limit bandwith dengan menggunakan tools dari tuxcut. Nanti nya ketika korban yang sedang menikmati jaringan internet akan kita ganggu dengan tools ini, berikut langkah untuk menggunakan netcut

   a. Buka aplikasi tuxcut



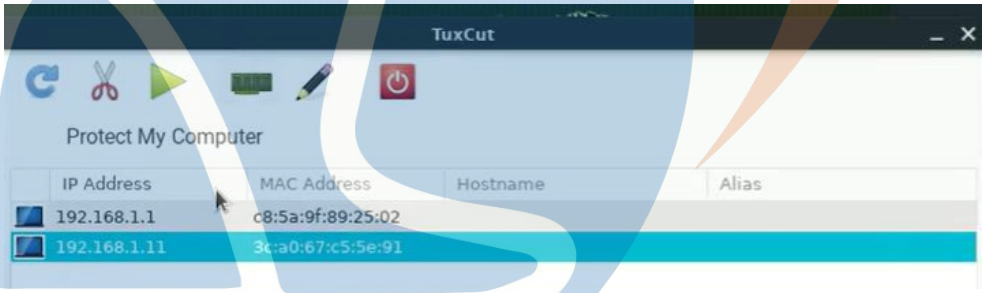
Gambar 4. 28 Tools TuxCut

b. Ini adalah point of view (POV) dari target yang sedang tes ping kecepatan bandwith internet ke google.com dan korban akan menjadi target dari penelitian.

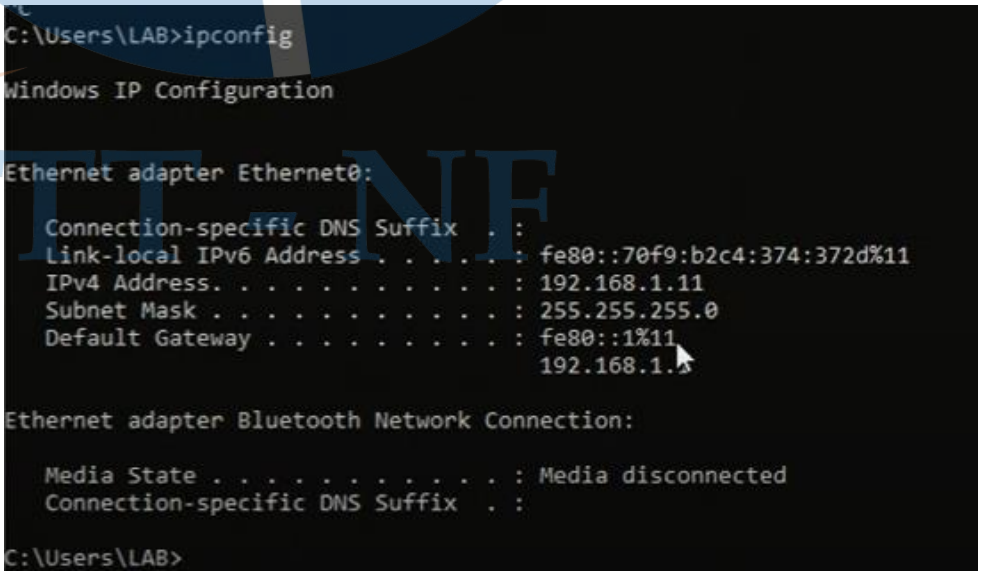


Gambar 4. 29 Tes ping google.com

c. Lalu pada tools tuxcut kita tentukan IP Target

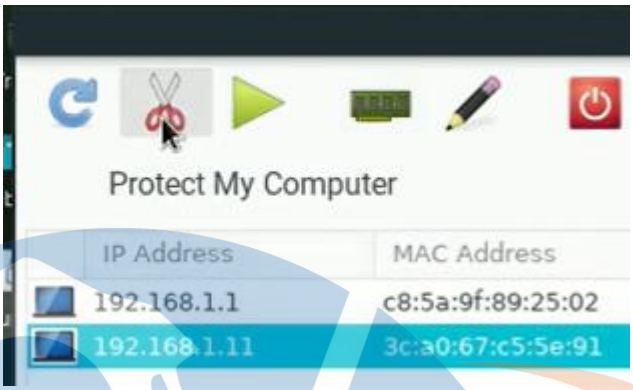


Gambar 4. 30 Memlih IP target



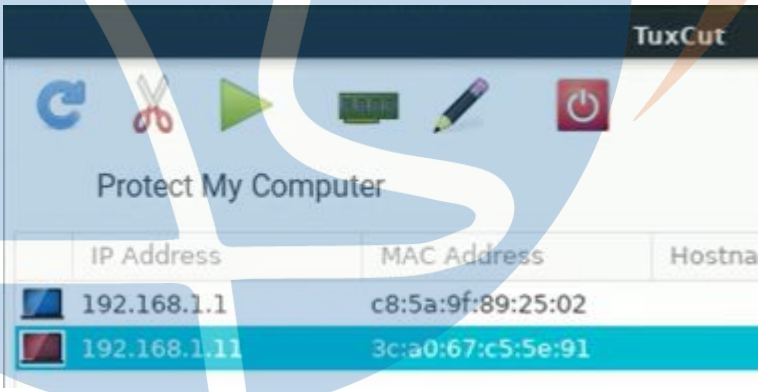
Gambar 4. 31 IP dari target

d. Jika sudah mendapatkan informasi IP target kita akan eksekusi dengan cara klik tombol pada gambar berbentuk gunting



Gambar 4. 32 Execution target

e. Tunggu sampai icon berubah menjadi warna merah, lalu korban akan mengalami lambat nya dari bandwith yang ada di jaringan tersebut.



Gambar 4. 33 Proses execution ke target

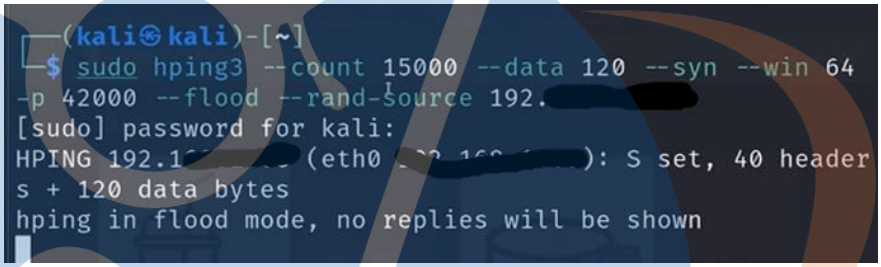
2. *Distributed Denial of Service (DDoS)*

Melakukan serangan ini adalah tindakan ilegal yang bisa menyebabkan gangguan signifikan pada layanan jaringan, kecepatan jaringan dan membahayakan data yang bisa menjadi *crash* atau *conculion*. Tujuan dari penelitian ini hanya untuk meningkatkan keamanan, bukan untuk melakukan tindakan yang merugikan. Namun, penulis dapat menjelaskan secara teknis tentang serangan *DDoS* pada jaringan *wireless* yang ada di PT Mitra Bhakti Informasi untuk

keperluan edukasi dan pemahaman tentang keamanan jaringan. Berikut ini langkah menggunakan tools dari hping3 sebagai serangan *DDoS* secara membanjiri atau flooding paket data yang akan lewat dari target ke jaringan internet yang melewati perangkat *wireless*.

a. Pertama buka aplikasi *hping3* yang tersedia pada di *tab menu*
b. Lalu ketikan *command* berikut

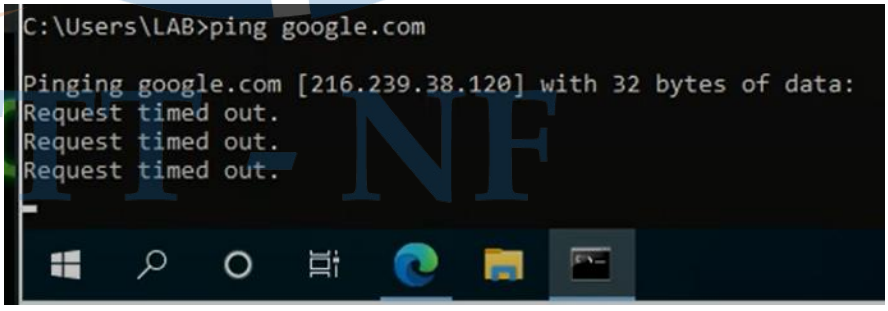
   #sudo hping3 -I wlan0 –count 15000 –data 120 –syn –win 64 -p 42000 –flood –rand-source [IP_TARGET]



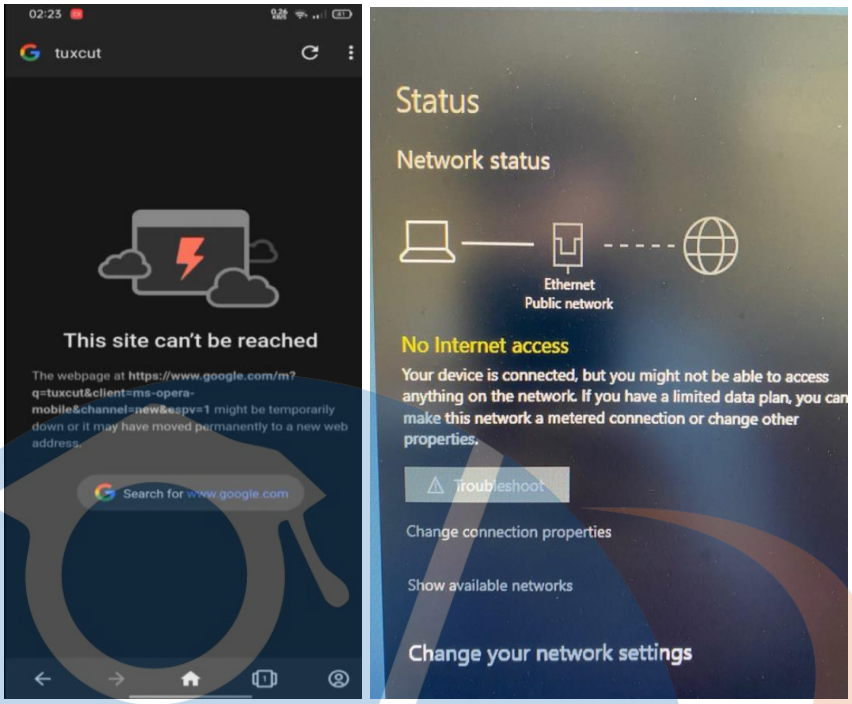
Gambar 4. 34 Command hping3

c. Setelah itu proses akan berjalan terus menerus hingga membuat gangguan pada jaringan target.

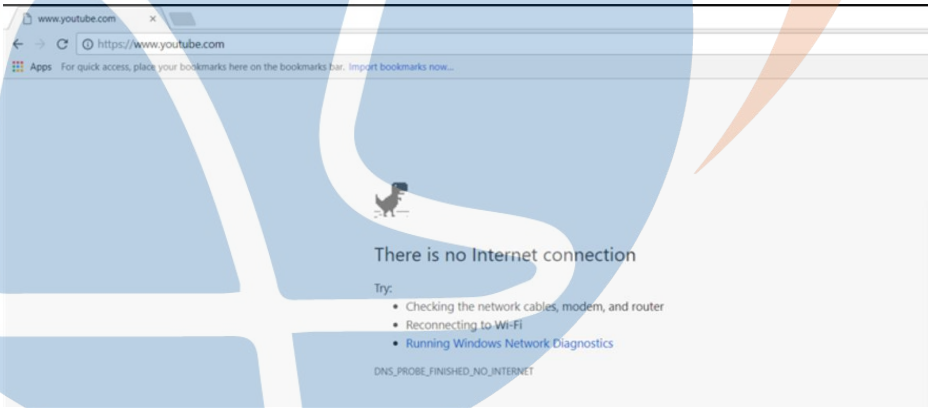
Berikut ini adalah hasil dari kedua serangan tersebut ke sisi target korban yang telah kita lakukan *netcut* dan *Distributed Denial of Service (DDoS)*



Gambar 4. 35 Tes ping google.com



Gambar 4. 36 Hasil serangan membuat korban tidak dapat akses internet



Gambar 4. 37 Korban tidak dapat mengakases google.com

Dari hasil penyerangan diatas penguji berhasil dalam menyerang korban dengan *tools tuxcut* dan *hping3* dan akan sulit untuk mengakses internet.

4.1.6 Post Exploitation

Pada tahapan *post exploitation* merupakan kelanjutan dari *exploitation* yaitu berusaha mencuri data dari korban. Sehubungan dari tahapan ini, peneliti tidak mendapatkan ijin untuk meneliti lebih dalam karena datanya terlalu *credential* .

4.1.7 Reporting

Untuk tahapan *reporting*, data yang telah di dapat dengan cara pengujian ini kami rangkum dalam bentuk laporan dalam bentuk dokumen word yang isinya mengenai langkah-langkah dari pengujian tersebut, hasil pengujian dan *severity rate* (penilaian kerentanan).

4.3 Analisa

Pada tahapan ini, kami menganalisa dari hasil yang telah didapatkan pada pengujian sebelumnya dengan dalam bentuk penilaian dalam *severity*. Penulis tidak lupa menganalisa dari dampak dari pengujian tersebut sehingga *user* mengetahui dampak dari serangan tersebut dan penulis memberikan rekomendasi dari pengujian tersebut sehingga *user* dari kementerian dalam negeri agar bisa mengantisipasi dan menutup celah keamanan pada wireless tersebut dengan rekomendasi yang diberikan.

4.3.1 Severity

Setelah melakukan penelitian diatas, tahapan *severity* ini merupakan bagian dari *vulnerability analysis* dengan menggunakan nessus dengan target wireless yang sudah ditentukan. Untuk hasil dari *vulnerability analysis* tersebut di *generate report* dalam bentuk pdf. Berikut ini hasil *severity* yang telah di lakukan proses *scanning*.

Berikut ini hasil dari pengujian menggunakan *nessus*.

0	0	1	0	18
CRITICAL	HIGH	MEDIUM	LOW	INFO

Tabel 4. 2 Hosts Executive Summary

Vulnerabilities

Severity	CVSS	Plugin	Name
Medium	5.8	50686	IP Forwarding Enabled
Info	N/A	45590	Common Platform Enumeration (CPE)
Info	N/A	11002	DNS Server Detection
Info	N/A	72779	DNS Server Version Detection
Info	N/A	35716	Ethernet Card Manufacturer Detection
Info	N/A	86420	Ethernet MAC Addresses
Info	N/A	10107	HTTP Server Type and Version
Info	N/A	24260	HyperText Transfer Protocol (HTTP) Information
Info	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	11219	Nessus SYN scanner
Info	N/A	19506	Nessus Scan Information
Info	N/A	11936	OS Identification
Info	N/A	22964	Service Detection
Info	N/A	25220	TCP/IP Timestamps Supported
Info	N/A	10287	Traceroute Information
Info	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
Info	N/A	10386	Web Server No 404 Error Code Check
Info	N/A	106628	lighttpd HTTP Server Detection
Info	N/A	66717	mDNS Detection (Local Network)

Tabel 4. 3 Hasil scan Nessus

Pada tabel diatas, menjelaskan *vulnerability* pada jaringan wireless tersebut, bahwa terdapat 1 kerentanan keamanan bersifat *medium* dan 18 anjuran keamanan. Untuk *severity medium* ini telah terbukti pada pengujian *man in the middle attack* bahwa *ip forwarding enabled*. Hasil *scanning* di atas didapatkan 1 kerentanan keamanan bersifat *medium* dan 18 anjuran keamanan. Untuk *medium range score cvss v3* bernilai 4.0 - 6.9.

4.3.2 Dampak

Setelah melakukan pengujian sebelumnya, terdapat beberapa kerentanan pada sistem jaringan wireless tersebut. Dampak yang ditimbulkan setelah pengujian sebelumnya adalah jaringan wireless tersebut menjadi rentan dari serangan *hacker*, jika seorang *hacker* mampu mendapatkan password wireless tersebut dengan cara *brute force attack*, lalu memata-matai semua asktivitas dengan *man in the middle* dan menonaktifkan jaringan internet pada wireless dengan cara *deauthentication* oleh *hacker*, bisa saja *hacker* mengambil data yang berada dilokasi tersebut.

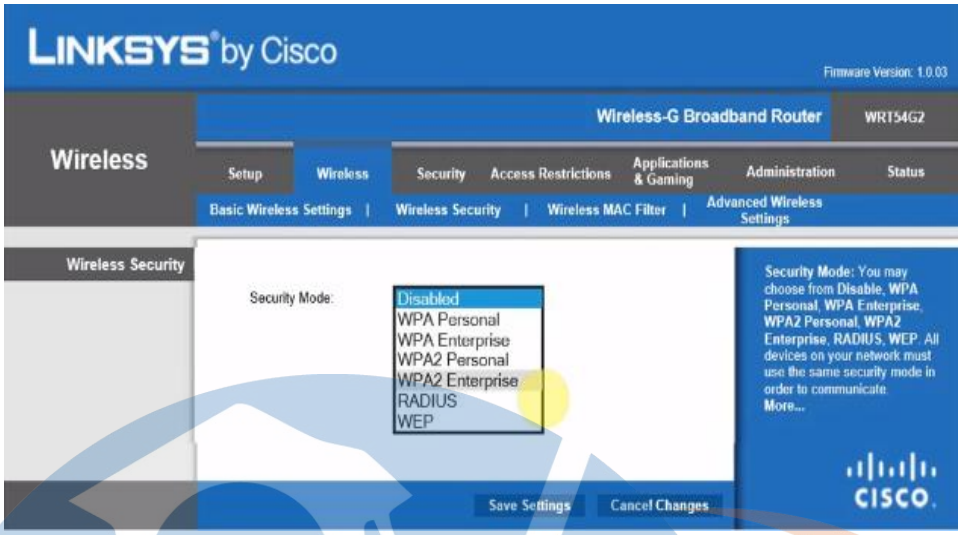
4.3.3 Rekomendasi

Pada tahapan rekomendasi merupakan tahapan dimana *pentester* memberikan saran untuk menutup celah keamanan yang berada dilokasi penelitian. Rekomendasi yang diberikan berupa saran bagi pihak yang terkait. Dalam rekomendasi ini dibagi menjadi 2 yaitu rekomendasi teknis dan rekomendasi strategi, dimana rekomendasi teknis berisi saran menanggulangi sistem keamanan wireless berupa perangkat yang terkait. Sedangan rekomendasi strategi berisi saran secara umum.

Dari pengujian diatas yang telah dilakukan di lokasi, berikut ini merupakan rekomendasi dari penguji untuk ke pihak yang terkait :

1. Rekomendasi Teknis

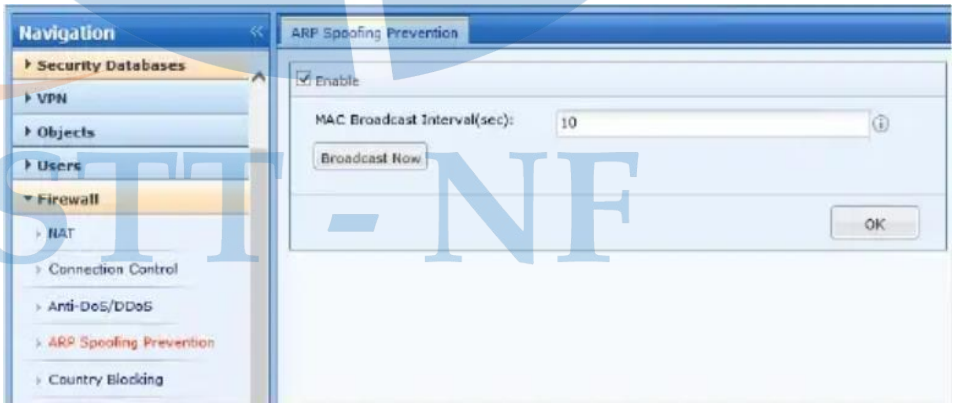
Setelah dilakukan pengujian seperti *brute force attack, man in the middle attack*, dan *deauthentication attack*. Maka langkah selanjutnya adalah penanggulangan untuk mengatasi masalah sistem keamanan wireless ini. Untuk rekomendasi kami terapkan di perangka *wireless*, kami menerapkan security mode *WPA*2 Enterprise seperti berikut ini.



Gambar 4. 38 WPA2 Enterprise

Pada gambar 4.7, Untuk mengaktifkan keamanan pada wireless kami menggunakan *security mode* yaitu *WPA2 enterprise* dengan terintegrasi dengan *active directory* dan menggunakan enkripsi AES. Langkah ini dilakukan karena perlunya autentikasi pengguna wireless dengan *login password* wireless yang berbeda-beda dan untuk menghindari serangan *brute force*.

Untuk rekomendasi di sisi perangkat sangfor, kami menerapkan perlindungan *Arp spoofing* dan perlindungan *deauthentication attack*. Untuk perlindungan Arp kami mengaktifkan *Arp Spoofing Prevention* seperti dibawah ini.

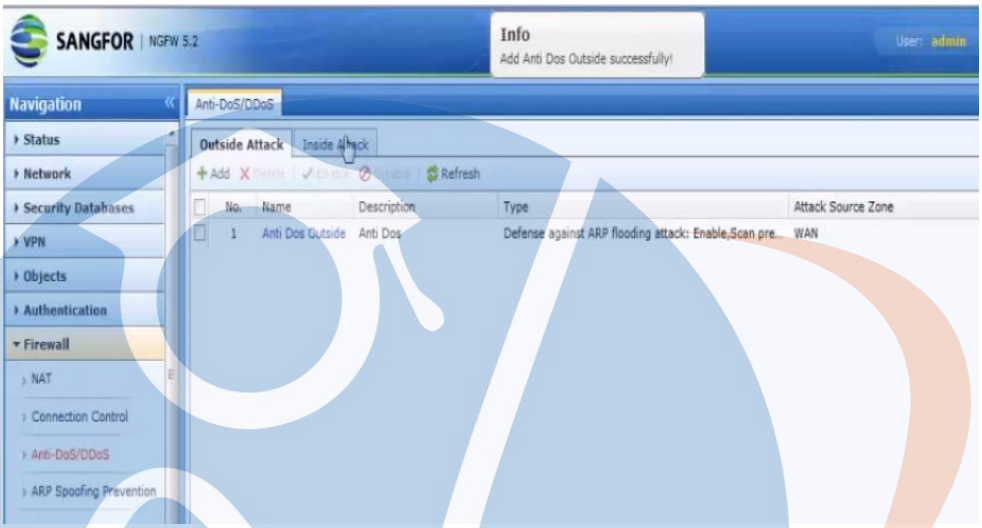


Gambar 4. 39 Arp spoofing prevention

Pada gambar 4.8, dijelaskan mengenai perlindungan *Arp spoofing* dengan *mac broadcast interval*nya adalah 10 *second*. [5]Dengan

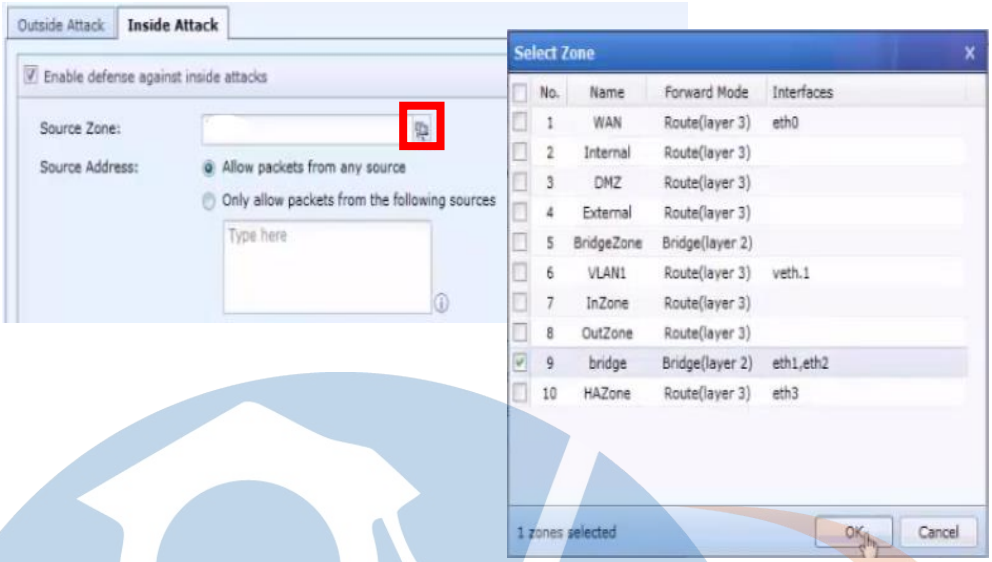
mengaktifkan perlindungan *arp spoofing* ini diharapkan tidak ada celah keamanan wireless kembali.

Untuk perlindungan *dos* atau *deauthentication*, maka kami mengaktifkan perlindungan anti *dos/ddos* di perangkat sangfor. Berikut ini hasil dari anti *dos/ddos* di sisi *outside*.



Gambar 4. 40 Dashboard Outside Attack

Pada gambar 4.9, dijelaskan penambahan *rule* untuk perlindungan *dos/ddos* dengan perlindungan *icmp flooding, udp flooding, syn flooding* serta *dns flooding*. Dengan adanya perlindungan anti *dos/deauthentication* disisi luar diharapkan tidak ada serangan *dos/deauthentication* di sisi wireless kembali. Untuk perlindungan *dos/deauthentication* disisi dalam atau *inside* maka kami menambahkan *rule* untuk perlindungan disisi dalam wireless seperti dibawah ini.



Gambar 4. 41 Anti Dos/Ddos Inside

Pada gambar diatas menjelaskan cara mengaktifkan perlindungan disisi dalam. Dengan zona sumber di sisi dalam serta mengaktifkan paket dari semua sumber. Langkah ini dilakukan berharap dapat mengurangi celah keamanan pada serangan *deauthentication*.

2. Rekomendasi Strategi

Setelah rekomendasi teknis dilakukan maka selanjutnya adalah rekomendasi strategi yaitu berisi berupa saran secara umum mengenai keamanan untuk disisi internal kemendagri. Berikut adalah rekomendasi strategi untuk meningkatkan keamanan jaringan wireless di PT Mitra Bhakti Informasi berdasarkan temuan dan analisis yang dilakukan:

a. Untuk mengantisipasi segala macam serangan, disarankan untuk membentuk divisi *security operation center (SOC)* yang berguna memonitoring sistem keamanan yang berada di PT Mitra Bhakti Informasi.

b. Setelah divisi *security operation center (SOC)* sudah di bentuk, maka selanjutnya adalah membentuk divisi *IT Security* yang berguna merancang sistem keamanan di PT Mitra Bhakti Informasi

c. Peningkatan keamanan jaringan, Segera beralih ke protokol enkripsi *WPA2* pada semua access point untuk memastikan lapisan enkripsi yang

lebih kuat dan perlindungan terhadap serangan brute force. Dan gunakan kata sandi yang sangat aman dan sulit ditebak dengan campuran *alphabet upper lower, numbering* dan *special character* dan diganti secara berkala atau terjadi temuan indikasi serangan. Jika menggunakan PSK selalu gunakan pre-shared key yang kuat dan kompleks untuk semua jaringan wireless, dan ganti secara berkala.

d. Pembaruan dan pemeliharaan sistem, rutin dalam pembaruan *firmware* atau *patch* dan terapkan kebijakan pembaruan *firmware* atau *patch* dengan secara rutin pada semua perangkat jaringan untuk menambal kerentanan yang diketahui dan meningkatkan keamanan.

e. Pengelolaan dan konfigurasi perangkat, mengubah semua pengaturan *default* pada perangkat jaringan, termasuk nama pengguna dan kata sandi yang masih dalam konfigurasi *default*, untuk mencegah terjadinya indikasi serangan.

f. Segmentasi jaringan, membuat segmentasikan jaringan wireless menjadi beberapa VLAN (Virtual LAN) atau memisahkan lalu lintas data antara karyawan, tamu, dan perangkat *network & server*.

g. Audit, dengan adanya kegiatan audit keamanan jaringan secara berkala menggunakan metode PTES atau standar lainnya untuk memastikan bahwa keamanan terus diperbarui dan diterapkan dengan benar.

h. Pelatihan mengenai keamanan, mengadakan program pelatihan dan kesadaran keamanan siber secara berkala untuk karyawan di PT Mitra Bhakti Informasi, termasuk pelatihan tentang praktik kata sandi yang aman, pengenalan phishing, ancaman bahaya serangan siber dan tanggapan terhadap insiden keamanan.

i. Monitoring berkelanjutan, mengimplementasikan IDS/IPS (Intrusion Detection System/Intrusion Prevention System) dengan berbagai *tools* atau sistem yang aman untuk mendeteksi dan mencegah aktivitas mencurigakan di jaringan wireless. Lalu memantau log dan analisis log secara teratur untuk mendeteksi pola yang tidak biasa dan mengidentifikasi potensi ancaman.

BAB V
KESIMPULAN DAN SARAN

Pada bab ini penulis merangkum semua kesimpulan dan hasil dari kegiatan dan pembuatan tugas akhir analisa keamanan jaringan wireless dan memberikan saran kepada penulis, perusahaan dan kepada pembaca untuk pengembangan lebih lanjut.

5.1 Kesimpulan

Berdasarkan rumusan masalah yang telah dijelaskan pada bab sebelumnya, berikut adalah kesimpulan rinci untuk masing-masing masalah:

a. Dari hasil penelitian yang dilakukan, dapat disimpulkan bahwa kondisi keamanan jaringan wireless di PT Mitra Bhakti Informasi memiliki beberapa aspek positif tetapi juga terdapat sejumlah kelemahan yang signifikan. Meskipun jaringan menggunakan protokol enkripsi *WPA*2 dan kata sandi yang begitu kuat, analisis lebih mendalam mengungkap adanya konfigurasi yang belum optimal. Beberapa perangkat jaringan masih menggunakan pengaturan default dan tidak ada nya integrasi sistem user login pada jaringan lokal dengan user *Active Directory* yang dimana akan digunakan sebagai *user login* pada saat atau ingin mengakses layanan internet dari perangkat *wireless* dan jaringan lokal. Tidak semua firmware perangkat diperbarui ke versi terbaru, yang merupakan kelemahan kritis dalam keamanan jaringan.

b. Metode *PTES (Penetration Testing Execution Standard)* menyediakan kerangka kerja yang terstruktur untuk melakukan pengujian penetrasi pada jaringan nirkabel. PTES terdiri dari beberapa tahap mulai dari *pre-engagement interactions* hingga *reporting*, yang memastikan setiap metode pengujian dilakukan secara sistematis dan terstukrur. *Implementasi* metode *PTES* di PT Mitra Bhakti Informasi memungkinkan perusahaan untuk mengidentifikasi kerentanan secara efisien dan memberikan solusi yang spesifik untuk meningkatkan keamanan jaringan. Setiap tahap dalam metode *PTES* memberikan panduan yang jelas tentang aktivitas yang harus dilakukan, menjadikan proses pengujian lebih efektif dan terarah.Evaluasi tingkat keamanan jaringan nirkabel harus didasarkan pada standar keamanan yang berlaku serta analisis risiko yang

komprehensif. Penilaian kepatuhan terhadap standar industri seperti *IEEE 802.11* membantu dalam memastikan bahwa konfigurasi dan kebijakan keamanan sesuai dengan praktik terbaik. Penggunaan metrik keamanan seperti jumlah kerentanan yang ditemukan, tingkat deteksi serangan, dan waktu respons insiden adalah indikator kunci untuk mengukur efektivitas sistem keamanan. Evaluasi berkala dan audit keamanan memastikan bahwa langkah-langkah perbaikan yang diimplementasikan terus ditinjau dan ditingkatkan.

Secara keseluruhan, melalui pendekatan yang terstruktur dan menyeluruh PT Mitra Bhakti Informasi dapat meningkatkan keamanan jaringan nirkabelnya, mengurangi risiko serangan dan memastikan bisnis perusahaan yang lebih stabil dan aman. Implementasi metode *PTES* memungkinkan perusahaan untuk mengidentifikasi kerentanan keamanan jaringan dengan tepat dan memberikan solusi yang efektif untuk mengatasi masalah keamanan.

5.2 Saran

Berdasarkan hasil analisis dan pengujian, beberapa saran untuk meningkatkan keamanan jaringan wireless di PT Mitra Bhakti Informasi meliputi:

1. **Peningkatan Enkripsi**, Semua access point harus segera dimigrasi ke protokol *WPA*2 atau Enskripsi terbar yang menawarkan keamanan lebih kuat dibandingkan teknologi sebelumnya, termasuk perlindungan terhadap serangan brute force. Dan, gunakan pre-shared key (PSK) yang kompleks dan kuat, serta lakukan penggantian kata sandi secara berkala untuk mengurangi risiko kompromi.

2. **Pembaruan Firmware**, Lakukan pembaruan firmware secara berkala pada semua perangkat jaringan. Pembaruan ini harus mencakup semua patch keamanan terbaru untuk menutup celah kerentanan yang sudah diketahui. Implementasikan sistem pemberitahuan otomatis untuk update firmware sehingga tidak ada perangkat yang terlewatkan.

3. **Keamanan Sistem,** Segera ubah semua pengaturan default pada perangkat jaringan, termasuk kata sandi admin dan parameter konfigurasi lainnya. Lalu untuk SSID pada setiap perangkat disarankan untuk mengunakan nama SSID yang tidak mengandung informasi sensitif dan hindari penggunaan SSID default.

4. **Segmentasi Jaringan**, Implementasikan segmentasi jaringan dengan menggunakan VLAN untuk memisahkan lalu lintas data antara karyawan, tamu, dan perangkat IoT. Hal ini akan membatasi akses dan mengurangi risiko penyebaran serangan. Terapkan kebijakan hak akses minimal untuk setiap segmen jaringan dan pastikan hanya pengguna yang berwenang yang memiliki akses.

5. **Monitoring dan Pemantauan Berkelanjutan**, Gunakan Intrusion Detection System/Intrusion Prevention System (IDS/IPS) untuk mendeteksi dan mencegah aktivitas mencurigakan di jaringan wireless. Lalu pantau dan analisis log secara teratur untuk mendeteksi anomali dan pola aktivitas yang mencurigakan.

6. **Pelatihan dan Kesadaran Keamanan**, Selenggarakan program pelatihan keamanan secara berkala untuk meningkatkan kesadaran karyawan tentang praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat dan cara mengenali phishing.

Lakukan simulasi serangan secara periodik untuk menguji kesiapan karyawan dan memperkuat kebijakan keamanan yang ada.

7. **Audit dan Penilaian Keamanan Berkala**, Lakukan audit keamanan secara berkala menggunakan standar seperti PTES untuk memastikan bahwa kebijakan dan praktik keamanan terus diperbarui dan diterapkan dengan benar. Lakukan penilaian risiko untuk mengidentifikasi potensi kerentanan baru dan menentukan prioritas perbaikan.

DAFTAR PUSTAKA

[1] Abdelrahman, R, B, M. Mustafa, A, B, A. & Osman, A, A (2015). A comparison between ieee 802.11a, b, g, n and ac standards, Sudan: IOSR Journal of Computer Engineering (IOSR-JCE).

[2] Abu-Dabaseh, F. Alshammari, E. (2018). Automated Penetration Testing: An Overview, Computer Science & Information Technology (CS & IT).

[3] Alhassana, M, M. Adjei-Quayeb, A. (2017). Information security in an organization", International Journal of Computer (IJC).

[4] Arjun K. Pillay. Farik, M. & Liava'a, E (2017). Campus area network WiFi security, Internasional Journal Of Scientific & Technology Research Vol 6.

[5] Bairwa, S, Mewara, B, & Gajrani, J. (2014). Vulnerability scanners: a proactive approach to assess web application security, International Journal on Computational Sciences & Applications (IJCSA).

[6] Bel, A. Adame, T. & Bellalta, B. (2014). An energy consumption model for IEEE 802.11ah wlans, Journal Of Latex Class Files.

[7] Brangetto, P. Caliskan, E. & Roigas, H. (2015). Cyber red teaming, Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

[8] Christopher, P, Kohlios. Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and *WPA*3, MDPI,.

[9] El-Nazeer, Nazar. Daimi, K, Evaluation of network port scanning tools, semantic sholar.

[10] Fadilah, S, I. et all (2014). Performance analysis for wireless g (IEEE 802.11g) and wireless n (IEEE 802.11n) in outdoor environment, ARPN Journal of Engineer.

[11] Gopalakrishnan, S. (2014) A survey of wireless network security, International Journal of Computer Science and Mobile Computing.

[12] Gupta, A. Anand, A (2017) Ethical hacking and hacking attacks, International Journal Of Engineering And Computer Science.

[13] Inc, Alfa Network. (2014). Alfa AWUS036ACH", Alfa Network Inc.

[14] Ijemaru, G, K. et all (2018) Security challenges of wireless communications networks: a survey, International Journal of Applied Engineering Research.

[15] Kamani, C. et all. (2019) De authentication attack on wireless network, International Journal of Engineering and Advanced Technology (IJEAT).

[16] Kesharwani, P. et all. (2018). A study on penetration testing using metasploit framework, International Research Journal of Engineering and Technology (IRJET).

[17] Kumar, S. Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures, International Journal of Advance Research in Computer Science and Management (IJSART).

[18] Manzoor, J. Kumar, A. & Kumari, S. (2016). ARP spoofing and Man In The Middle attack, International Journal of Computer Engineering and Applications.

[19] Pandikumar,T. Yesuf, M,A. (2017). Wi-Fi security and test bed implementation for WEP and *WPA* cracking, International Journal of Engineering Science and Computing (IJESC).

[20] Pavithran. M,S. Pavithran, S (2015). Advanced attack against wireless networks Wep, *WPA*/*WPA*2-personal and *WPA*/*WPA*2-enterprise, Internasional Journal Of Scientific & Technology Research Vol 4.

[21] Ram, P, R. Sindhura, D. & Shareef, O. (2014). Wi-Fi network's password strength analysis using backtrack tools, International Journal of Advanced Computational Engineering and Networking.

[22] Rani, Pooja. Arora, Punnet. (2018). Penetration testing in virtual and real environment, International Journal Of Modern Engineering Research (IJMER).

[23] Reddy P, K. Shukla, N,K. (2017). A study on WLAN security a literature review of security in wireless network, International Journal of Scientific Research and Review.

[24] Saini, S. Sharma, Y, K. (2016). A research study of wireless network security: a case study, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE).

[25] Siddiqui, F. Zeadally, S. & Salah, F. (2015). Gigabit wireless networking with IEEE 802.11ac: technical overview and challenges, Journal Of Networks.

[26] Sing, Harshdeep. Singh, Jaswinder. (2017). Analysis of various tools of penetration testing, Internasional Journal of Advance Research in Science and Engineering (ijarse).

[27] Team, The PTES. (2017). The Penetration Testing Execution Standard Documentation", PTES.

[28] Vaithyasubramanian, S. Christy, A. & Saravanan, D. (2014). An analysis of markov password against brute force attack for effective web applications, Applied Mathematical Sciences, HIKARI Ltd.

[29] Vondráček, M. Pluskal, J. & Ryšavý, O. (2018). Automated Man-in-the-Middle attack against Wi Fi networks, Journal of Digital Forensics, Security and Law.

[30] Zheng, Y. Shi, T. & Xu, X. (2017). Research on WLAN planning problem based on optimization models and multi-agent algorithm, Ningbo, China: IEEE 8th International Conference on CIS & RAM.

[31] OWASP. 2024. Penetration Testing Methodologies. https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

[32] UNIT 42. 2022. Network Security Trends and Exploit. https://unit42.paloaltonetworks.com/network-security-trends-update/

[33] Mitre ATT&CK. 2024. Network Matirk. https://attack.mitre.org/matrices/enterprise/network/

[34] SA Maherza. (2023). Penetration Testing Terhadap Website Sekolah Menengah Atas ABC dengan Metode NIST SP 800-115. https://ejournal.upnvj.ac.id/informatik/article/download/4697/2291

[35] Najoan, 2019, Analisis Dan Implementasi Sistem Redundant hot Standby Network Security Menggunakan Metode Intrusion Preventi Sistem (IPS), Bianglala Informatika,Vol. 2 No 2, Hal. 112-119

[36] Nugroho, B. A. (2012). Analisis keamanan jaringan pada fasilitas internet (wifi) terhadap serangan packet sniffing (Unpublished doctoral dissertation). Universitas Muhammadiyah Surakarta.

[37] Thommy, E. (2015). Analisis manajemen local area network. journal Ilmu Administrasi Bisnis.

[38] Bobanto, W. S., Lumenta, A. S., dan Najoan, X. (2015). Analisis kualitas layanan jaringan internet (studi kasus pt. kawanua internetindo manado). Jurnal Teknik Elektro dan Komputer.

[39] Setiawan,H, 2018, Rancangan Bangun Captive Portal Untuk Jaringan Wireless Berbasi open Source pada CV. Gempar production Palembang, Jurnal Teknologi Informasi, Vol. 7 No. 1, Hal. 36-44.

[40] Najoan, 2019, Analisis Dan Implementasi Sistem Redundant hot Standby Network Security Menggunakan Metode Intrusion Preventi Sistem (IPS), Bianglala Informatika,Vol. 2 No 2, Hal. 112-119

[41] Purwanto,D., dan Dana,RD., 2015, Sistem Keamana Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebone, Jurnal Online ICT STMIK IKM, Vol. 13 Nomor 1

[42] Simarmata Janner. 2006. Pengenalan Teknologi Komputer dan Informasi. Andi.

[43] Tanembaum, Andrews. 1996. Computer Network. Andi.

[44] EC-Council. 2012. Certified Ethical Hacker v8. Amerika. EC-Council.

[45] Dipanegara, Arya. 2009, 1 Jam Belajar Teknik Hacking. Jakarta. HP Cyber Community.

LAMPIRA

Ruangan kerja