SKRIPSI

ANALISA KEAMANAN JARINGAN WIRELESS UNIMMA MENGGUNAKAN METODE PENETRATION TESTING

MUHAMMAD A. HANAFI
NPM. 19.0504.0029

PROGRAM STUDI TEKNIK INFORMATIKA S1
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MAGELANG
2022/2023

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Jaringan nirkabel memanfaatkan gelombang radio yang dipancarkan secara *broadcast* dan bergerak bebas diudara. Tingkat keamanan jaringan nirkabel yang kurang baik jika dibandingkan dengan jaringan kabel perlu mendapatkan perhatianserius. Hal ini dikarenakan jaringan nirkabel bisa diakses secara diam-diam dan tidak memerlukan akses fisik ke gedung. Oleh karena itu, perancangan dan implementasi sauatu topologi jaringan komputer yang menggunakan nirkabel memerlukan adanya suatu pent tes untuk menguji tingkat keaman suatu jaringaan nirkabel. Tujuannya adalah menentukan dan mengetahui macam-macam serangan yang mungkin dilakukan pada sistem serta akibat yang bisa terjadi karena adanya kelemahan keamanan pada sistem komputer atau jaringan yang dimiliki. Kerentanan dalam aplikasi server web akan memberikan peluang bagi peretas untuk mengeksploitasi dan menyerang secara bertahap pada sistem dan tidak dapat menutup kemungkinan bahwa sistem yang diserang akan diambil alih sepenuhnya.Selama pengujian penetrasi, batasan pengujian yang cermat diperlukan untuk menghindari gangguan dan untuk menunjukkan apakah suatu serangan dapat dilakukan. Namun, pengujian ini dapat menyebabkan kondisi penolakan layanan (DOS). Di sisi lain, setelah pengujian destruktif dilakukan dan dipetakan, serangan penolakan layanan dan buffer overflows dapat dikurangi.(Riadi & Yudhana, 2020)

Jaringan nirkabel pada Universitas Muhammadiyah Magelang banyak diakses oleh Mahasiswa untuk mempermudah proses pembelajaran. Jaringan ini dikelola oleh Biro Sistem Informasi (BSI). Jaringan pada Fakultas Teknik dibagi menjadi beberapa ruangan, seperti ruang lab S1, ruang lab D3 dan ruang Tata Usaha. Setiap jaringan pada ruangan tersebut bisa dikembangan menjadi jaringan wireless. Namun karena dikembangkan secara mandiri maka keamanan jaringan nirkabel tersebut belum terjamin. Jaringan nirkabel saat ini menjadi sorotan karena keamanannya, sehingga diperlukan perhatian khusus karena jaringan nirkabel

menggunakan gelombang radio yang disiarkan dan bergerak bebas melalui udaradan dapat diterima oleh siapa saja dan kapan saja.(Delsi Samsumar & Gunawan, 2017)

Oleh karena itu, banyak attacker yang tertarik untuk menguji celahkeamanan pada jaringan nirkabel UNIMMA. Penelitian ini melakukan percobaan pen test terkait kerentanan pada jaringan nirkabel Fakultas Teknik dan diambil kesimpulan dari percobaan tersebut sebagai bahan Analisa kerentanan jaringan nirkabel tersebut. Analisis terhadapsistem keamanan yang ada dalam jaringan merupakan tindakan yang paling tepatuntuk mengetahui celah keamanan jaringan. Penelitian yang akan dilakukan evaluasi ini dilakukan untuk meningkatkan kesadaran pengelolaan masalah keamanan atau *intrusion detection* dan seberapa cepat kemampuan respon terhadapadanya ancaman (*threat)*(Delsi Samsumar & Gunawan, 2017). Evaluasi ini jugadilakukan sebagai bahan pertimbangan dalam pengambilan keputusan olehmanajemen yang lebih tinggi pada Universitas Muhammadiyah Magelang dalam hal kerentanan akan keamanan sistem jaringan. Manajemen kampus mungkin tidakingin atau tidak mampu untuk mengatasi semua kerentanan yang ditemukan dalampenilaian kerentanan, tetapi mungkin ingin untuk mengatasi kelemahan sistem yang ditemukan dianggap paling berbahaya, sehingga disinilah fungsi dari evaluasi ini melalui tes penetrasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka rumusan masalah pada penelitian ini adalah meninjau keamanan jaringan wireless yang dikelola oleh BSI UNIMMA menggunakan metode Penetration Testing.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dijelaskan, maka tujuan penelitianyang akan dicapai adalah untuk melakukan analisa terhadap sistem keamanan wireless di Universitas Muhammadiyah Magelang dengan menggunakan metode penetration testing

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah diuraikan diatas maka hasil dari penelitian ini didapatkan Beberapa manfaat menggunakan teknik Penetration Testing (PenTest):

1. Untuk mengetahui kerentanan terhadap serangan jaringan wireless.

BAB 2
TINJAUAN PUSTAKA

2.1 Penelitian Relevan

Menurut Muhammad Adam, Erick Irawadi Alwi, dan Ihwana As'ad pada penelitiannya yang berjudul "ANALISIS FORENSIK TERHADAP SERANGAN DDOS PING OF DEATH PADA SERVER" menjelaskan bahwa pada Penelitian ini menjelaskan tentang alat yang dapat mendeteksi serangan DDoS ataupun mengurangi serangan yang muncul pada jaringan, kerangka forensik disajikan dengan mempertimbangkan data yang tercatat pada data yang tersimpan(Adam et al., 2022).

Menurut Yudi Mulyanto dan Akbar Algi Fari pada penelitian yang berjudul "ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN *BRUTEFORCE* MENGGUNAKAN METODE *PENETRATION TESTING*" berdasarkan wawancara yang dilakukan oleh peneliti dengan Dwita hadisyahputraselaku kepala IT di SMK Negeri 2 Sumbawa menyatakan bahwa serangan yangpaling sering terjadi adalah *Brute Force* yaitu metode *hacking* yang dilakukandengan mencoba login berkali-kali hingga *password* berhasil ditebak, baik secara manual maupun otomatis (robot). Yang mengakibatkan jaringan menjadi tidakstabil dan semua prangkat yang tersambung kedalam jaringan router mikrotik akanterputus secara tiba-tiba.Maka perlu dilakukan analisa terhadap *login* pada *router mikrotik* dengan menggunakan metode *Penetration Testing*(Yudi Mulyanto, 2022).

Pada penelitian yang mengidentifikasi bukti forensik jaringan virtual router menggunakan metode NIST berhasil mendapatkan bukti-bukti digital, baik dengancara pengamatan secara langsung maupun tidak. Penggunaan metode NIST yang meliputi, koleksi, pemeriksaan, analisis dan pelaporan, dapat diulang dandipertahankan dengan data yang sama. Peneliti juga menyimpulkan bahwa tahapan analisis membuktikan adanya serangan yang dilakukan oleh alamat 192.168.10.10 dan 192.168.234.10, hal ini dapat digunakan investigator sebagai identifikasi bukti

serangan siber(Yasin et al., 2021)

Dalam penelitiannya, Imam Riadi mengatakan bahwa saat ini terdapat banyak kasus penghapusan barang bukti kejahatan untuk menghilangkan jejak pelaku. Barang bukti yang telah dihapus menjadi problem bagi pihak berwajib untuk membuktikan kejahatan pelaku dalam persidangan. Untuk itu diperlukan *tools forensic* dengan kinerja yang paling optimal untuk memudahkan pihak berwajib saat mengumpulkan kembali bukti-bukti yang sengaja dihapus maupun tidak sengaja terhapus. Penelitian ini menerapkan metode NIST yang memiliki kerangka kerja dan proses forensik terstruktur yang menjamin investigator sehinggahasilnya dapat dipertanggung jawabkan. Tujuan penelitian ini adalah membandingkan dua *tools forensic* yaitu Wondershare dr. Fone for Android dan Oxygen Forensics Suite 2014. Untuk mendukung penelitian ini dibutuhkan dua *smartphone* yang masing-masing sudah terpasang *tools forensic*. Penelitian ini berhasil mengembalikan data yang terhapus menggunakan kedua *tools forensic* dengan hasil presentase yang berbeda yaitu, Wondershare pada *smartphone* 1 berhasil mengembalikan data terhapus dengan persentase keberhasilan 31%, sementara Oxygen mencapai keberhasilan 67%. Sedangkan pada *smartphone* 2 Wondershare berhasil mengembalikan data terhapus dengan persentase keberhasilan mencapai 35% dan Oxygen memiliki persentase keberhasilan 69%. Dari hasil penelitian tersebut disimpulkan bahwa Oxygen Forensics Suite 2014 memiliki kinerja yang lebih baik daripada Wondershare dr. Fone for Android dalammengembalikan data yang telah dihapus(Riadi, 2020).

Menurut Harry Dwi Sabdho dan Maria Ulfa pada penelitiannya yang berjudul "ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE PENETRATION TESTING PADA KANTOR PT. MORA TELEMATIKA INDONESIA REGIONAL PALEMBANG" menjelaskan bahwa mengidentifikasi kerentanan keamanan dalam keadaan terkendali, sehingga dapat menghapusnya. Pakar sistem komputasi menggunakan pengujian pentesting untukmemecahakan masalah yang melekat dalam penilaian kerentanan, dengan fokus sensitivitas terhadap tingkat keparahan tinggi. Pengujian penetrasi adalah alat penilaian nilai yang bermanfaat bagi bisnis dan operasinya.

Menurut Haeruddin dan Arif Kurniadi dari penelitian yang berjudul "ANALISIS KEAMANAN JARINGAN WPA2-PSK MENGGUNAKAN METODE PENETRATION TESTING (STUDI KASUS: TP-LINK ARCHER A6)" Media transmisi yang digunakan wireless adalah gelombang radio yang dipancarkan ke semua area yang bisa dijangkau oleh gelombang radio tersebut. Beberapa vendor menyediakan fitur - fitur yang memudahkan pengguna maupun administrator jaringan untuk menggunakannya, sehingga sering dijumpai masih menggunakan konfigurasi default dari vendor. Oleh karena itu, para hacker sering melakukan aksinya untuk menguji kemampuan yang telah dipelajari sebelumnya. Kemudian terhubung dalam satu jaringan yang sama dan mengambil data penggunalainnya secara illegal(Haeruddin & Kurniadi, 2021).

Menurut Gidion Aryo Nugraha Pongdatu, Aryo Michael dan Enohk EightryPatalo pada penelitian yang berjudul "ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE PENETRATION TESTING DI SMK XYZ TANA TORAJA" menjelaskan bahwa Akses yang mudah terhadap jaringan wireless memerlukan perhatian yang lebih khususnya pada segi keamanan, mengingat keamanan data adalah sesuatu yang penting apalagi di dalam suatu instansi atau lembaga. Sebab pada jaringan wireless Service Set Identifier (SSID) akan di broadcast sehingga koneksi akan mudah diretas oleh orang-orang yang tidakbertanggung jawab. Jaringan Wireless yang terhubung langsung ke server yang di dalamnya terdapat data siswa, data guru dan pegawai, serta data keuangan. Sehingga keamanan pada jaringan wireless perlu diperhatikan agar dapat mengantisipasi ancaman dari luar yang dapat merusak seperti serangan malware ataupun dari orang-orang yang ingin mencuri data-data penting yang dimiliki olehsekolah. Metode yang dapat digunakan untuk pengujian sistem keamanan jaringanWireless LAN (WLAN) yaitu dengan metode penetration testing yang dilakukan pada jaringan instansi terkait untuk menemukan kelemahan yang ada pada jaringan tersebut. Kesimpulan dari penelitian ini adalah dari 4 rangkaian serangan yang dilakukan seperti MiTM Attack: Arp Poisoning, Deauth Attack, MAC Spoofing, Cracking WPA2 Key Encryption semua serangan ini terbukti berhasil membobol jaringan di sekolah tersebut(Aryo et al., 2022).

Menurut Ismail dan Pramudita pada penelitian yang berjudul "METODE PENETRATION TESTING PADA KEAMANAN JARINGAN WIRELESS WARDRIVING PT.PUMA MAKMUR ANEKA ENGINEERING BEKASI" menjelaskan bahwa mengidentifikasi kerentanan keamanan dalam keadaan terkendali, sehingga dapat menghapusnya. Pakar sistem komputasi menggunakan pengujian pentesting untuk memecahkan masalah yang melekat dalam penilaian kerentanan, dengan fokus sensitivitas terhadap tingkat keparahan tinggi. Pengujianpenetrasi adalah alat penilaian nilai yang bermanfaat bagi bisnis dan operasinya. Kesimpulan dari penelitian ini adalah dari 4 rangkaian pengujian terdapat 3 pengujian yang aman dan 1 pengujian yang tidak aman yaitu pada pengujian WPA2 Cracking, Password Router Wireless Cracking, Access Point Isolation pengujian ini dinyatakan aman dan pada pengujian Dos dinyatakan tidak aman(Ismail & Pramudita, 2020).

Menurut Rusdi & Prasti pada penelitian yang berjudul "PENETRATION TESTING PADA JARINGAN WIFI MENGGUNAKAN KALI LINUX"
menjelaskan bahwa dikarenakan kemudahan untuk instalasi jaringan nirkabel, sangat rentan terhadap gangguan keamanan eksternal. Enkripsi ganda ini telah diterapkan untuk melindungi kemanan jaringan wireless ini. Namun, enksripsi ini mudah dipecahkan oleh hacker. Oleh karena itu perlu ditingkatkan keamanan jaringan di perusahaan tersebut(Rusdi & Prasti, 2019).

2.2 Landasan Teori

Analisis serangan yang akan dilakukan pada penelitian ini adalah dengan mengimplementaskan metode PenTes (Penetrasi Testing) berupa Planning, Scanning, Gaining Access, Maintaining Access, dan Analysis agar mendapatkan bukti untuk menunjang keberhasilan dalam penelitian ini penulis menggunakan berbagai macam teori. Teori-teori tersebut terdiri dari teori POD (PING Of Death), Pentes (Penetrasi Testing), Brute Force dan Route

2.2.1 *PenTes (Penetration Testing)*

Pengujian penetrasi (pentesting) adalah kegiatan di mana seseorang mencoba mensimulasikan serangan yang dapat dilakukan terhadap organisasi / jaringan bisnis tertentu untuk menemukan kerentanan dalam sistem jaringan. Orang yang melakukan aktivitas ini disebut sebagai penetration tester (pentester)(Mushlih et al., 2019). seperangkat keterampilan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan informasi. Dalam menganalisa keamanan suatu jaringan Wireless dilakukan dengan prosedur penetration test yang mensimulasikan bentuk serangan terhadap jaringan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal ini adalah Kali Linux(Harry Dwi Sabdho & Ulfa Maria, 2018).

2.2.2 *GoldenEye*

Pada bulan Maret 2016, diperoleh pengamatan menarik tentang evolusi tingkat rendah ransomware, khususnya Petya, digabungkan denganransomware lain Mischa dan Ransomware baru bernama GoldenEye telah keluar. GoldenEye didistribusikan melalui email. Malware ini dapat memblokir akses sepenuhnya komputer(Cholid Fitra Fahriza, 2022).

2.2.3 Keamanan Jaringan

Merupakan bagian sistem yang sangat penting untuk menjaga akurasi dan integritas data serta memastikan ketersediaan layanan pagi bagipengguna di mana saja dan kapan saja. Di sisi lain, masyarakat sangat bergantung pada sistem informasi. Akibatnya, statistik kegagalan keamanan data di jaringan terus meningkat tajam dari tahun ke tahun. Sehingga diperlukan solusi untuk mengatasi hal tersebut, salah satunya adalah simulasi. Simulasi dilakukan untuk meniru sistem keamanan jaringan nyata yang karakteristiknya lebih mudah diamati daripada sistem asli untuk mengetahui kinerja sistem(Fachri & Harahap, 2020)

2.2.4 *Brute Force*

Brute force adalah sebuah metode serangan keamanan komputer yang mencoba semua kemungkinan kombinasi kata sandi hingga menemukan kata sandi yang tepat untuk mengakses suatu sistem atau akuntertentu. Dalam Brute Force attack, attacker akan mencoba semua kemungkinan kata sandi hingga menemukan yang benar atau berhasil menebak kata sandi dengan menguji kombinasi yang paling umum atau mudah ditebak. Brute Force attack dapat dilakukan secara manual, namun sering kali menggunakan perangkat lunak yang dirancang untuk mengotomatisasi proses pengujian kata sandi dengan kecepatan yang tinggi.Brute force attack seringkali digunakan oleh hacker untuk mencoba memecahkan keamanan sistem, mengakses akun pribadi, atau merusak sistem. Dari hasil penyerangan yang dilakukan dengan Brute Force pada jaringan yang ada, membuat jaringan menjadi lemot dan semua pengguna jaringan akan terputus dari jaringan tersebut(Mulyanto et al., 2022).

Serangan Brute Force adalah serangan cryptanalytic yang secara teoritis dapat digunakan untuk mendekripsi data terenkripsi (kecuali untuk data yang telah dienkripsi dengan cara yang aman secara teoritis). Serangansemacam itu dapat digunakan ketika tidak mungkin mengeksploitasi kerentanan lain dalam sistem enkripsi (jika ada) yang akan membuat tugas lebih mudah. Saat menebak kata sandi, metode ini sangat cepat jika semua kata sandi pendek. Namun, untuk kata sandi yang lebih panjang, metode lainseperti serangan kamus digunakan karena pencarian Brute Force terlalu lama. Kata sandi, frasa sandi, dan kunci yang lebih panjang memiliki lebih banyak kemungkinan nilai, membuatnya secara eksponensial lebih sulit diretas daripada yang lebih pendek(Sampurna et al., 2022).

2.2.5 *(National Institute of Standard and Technology)*

Badan nasional non-regulator dari Amerika Serikat yang dikenal dengan nama National Institute of Standards and Technology (NIST) memiliki tujuan untuk mempromosikan dan memperbaiki pengukuran,

standar, dan teknologi demi meningkatkan produktivitas, mendukung perdagangan, serta meningkatkan kualitas hidup masyarakat secara keseluruhan. Salah satu program penting yang dijalankan oleh NIST adalahprogram keamanan siber (cybersecurity), yang bertujuan untuk mengembangkan dan menerapkan teknologi dan metodologi keamanan yang praktis dan inovatif untuk mengatasi tantangan keamanan komputer dan informasi saat ini maupun di masa depan. Memiliki panduan teknis SP800-127 berjudul "Panduan untuk Mengamankan Jaringan Wi-Fi" yang memberikan pedoman umum dan rekomendasi mengenai konfigurasi, otentikasi, dan enkripsi untuk meningkatkan keamanan jaringan Wi-Fi. Didirikan pada tahun 1901 untuk meningkatkan inovasi industri dan daya saing di Amerika Serikat sehingga dapat meningkatkan kemampuan negaradalam hal keamanan informasi(Mushlihudin, 2020)

2.2.6 *Wireles*

Menurut Sari MW pada jurnal “Metode Penetration Testing Pada Keamanan Jaringan Wireless Wardriving Pt. Puma Makmur Aneka Engineering Bekasi” Jaringan wireless adalah jaringan yang memungkinkan pengiriman informasi (atau data) antar host dilakukan tanpa menggunakan media kabel. Jaringan wireless atau teknologi wireless ini mengunakan gelombang elektromagnetik untuk membawa informasi antara satu host dengan host lainnya(Ismail & Pramudita, 2020).

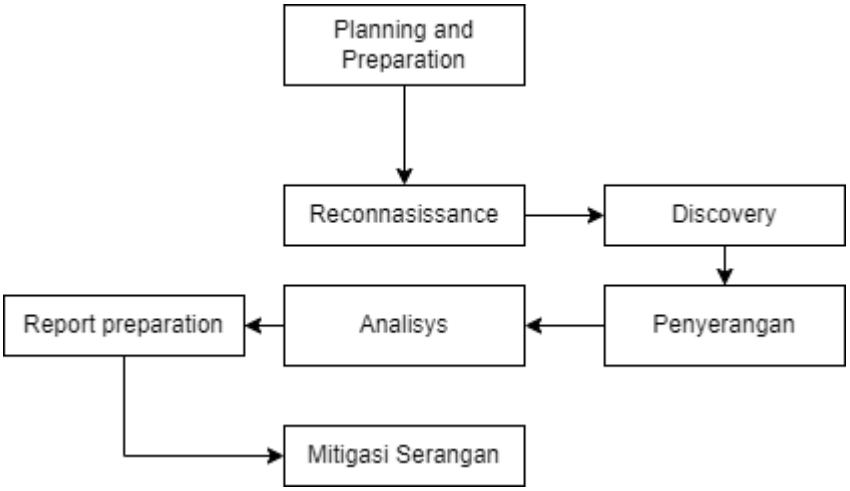
2.2.7 *Router*

Router adalah perangkat jaringan yang tugasnya menghubungkan beberapa jaringan komputer dan mengontrol lalu lintas di antara mereka. Router beroperasi pada lapisan 3 (lapisan jaringan) dalam model referensi OSI (Open System Interconnection) dan bertindak sebagai gateway yang menghubungkan jaringan area lokal (LAN) ke jaringan area luas (WAN) atau Internet.

BAB 3
METODOLOGI PENELITIAN

3.1 Prosedur Penelitian

Pada penelitian ini menggunakan tahapan meliputi planning and preparation, reconnasissance, discovery, analyzing information and risk, active intrusion attempts, final analysis, dan report preparation seperti pada Gambar 3.1 berikut:



Gambar 3. 1 Tahap Penelitian

3.1.1 Planning and Preparation

Planning and Preparation atau tentukan ruang lingkup dan tujuan pengujian, termasuk sistem yang akan dicakup dan metode pengujian yang digunakan. Mengumpulkan informasi (nama jaringan dan server domain, server email) untuk lebih memahami operasi target dan potensi kerentanan.

Pada tahapan ini penulis mengambil fokus pada penyerangan wireless kampus UNIMMA. Pengujian dilakukan pada jaringan wireless kampus UNIMMA menggunakan metodePenTes dan Brute Force.

Sebelum melakukan serangan penulis menyiapkan tools Kali Linux yang akan digunakan untuk menyerang jaringan UNIMMA dengan teknik Cracking Password

3.1.2 Reconnasissance

Reconnasissance atau sering disebut sebagai pendataan, dapat diklasifikasikan sebagai pengujian penetrasi data pasif melalui pendataan manual, dokumen terkait atau informasi publik, atau melalui pertanyaan langsung kepada pihak sistem.

Pada tahap ini penulis melakukan wawancara kepada pihak BSI dan Laboran S1 mengenai alur dan keamanan jaringan yang terdapat pada fakultas teknik.

3.1.3 Discovery

Discovery adalah tahap pengumpulan informasi menggunakan alattools kali linux untuk memindai jaringan yang ada di sekitar kampus UNIMMA.Untuk mengetahui MAC (Media Access Control) unik dari titik akses (Access Point) yang terdeteksi di jaringan (BSSID), nomor kanal pada frekuensi WiFi yang digunakan oleh titik akses (CH), Metode otentikasi yang digunakan pada jaringan (AUTH) dan Nama dari jaringan nirkabel (SSID)

3.1.4 Penyerangan

Setalah ditemukan beberapa data dari hasil scanning wifi di area UNIMMA peneliti melakukan penyerangan. Penyerangan dilakukan dengan teknik yaitu Brute Force dan Cracking.

3.1.5 Analysis

Setelah melakukan serangan, peneliti menganalisa hasil penyerangan lalu merangkum hasilnya kedalam bentuk gambar tangkapan layar saat penyerangan.

3.1.6 Report preparation

Report preparation tahap terakhir dari kegiatan pengujian ini adalah laporan hasil investigasi, yang diberikan kepada semua pihak yangterkait dan bertanggung jawab terhadap sistem dan menjadi acuan untuk meningkatkan keamanan sistem.

Setelah hasil analisa didapatkan dalam bentuk dokumen selanjutnyapenulis memberikan dokumen tersebut kepada pihak yang terkait.

3.1.7 Mitigasi Serangan

Penulis memanfaatkan alat Wireshark pada tahap mitigasi serangan untuk mengurangi dampak dan risiko keamanan informasi atau siber. Beberapa tahap mitigasi serangan yang umumnya diterapkan mencakup:

a. Analisis Risiko:

1. Identifikasi potensi ancaman dan risiko keamanan informasi.
2. Penilaian terhadap kerentanan yang dapat dieksploitasi oleh penyerang.
3. Penentuan tingkat risiko yang dapat diterima.

b. Perencanaan:

1. Pengembangan strategi mitigasi berdasarkan analisis risiko.
2. Penetapan prioritas mitigasi berdasarkan dampak dan kemungkinan terjadinya.
3. Pembuatan rencana darurat untuk tanggap cepat terhadap serangan.

c. Proteksi:

1. Implementasi kontrol keamanan seperti firewall, antivirus, enkripsi data, dan sistem deteksi ancaman.
2. Pembaruan dan pengelolaan keamanan perangkat lunak secara berkala.
3. Pengaturan kebijakan keamanan yang ketat.

d. Deteksi:

1. Penerapan sistem deteksi intrusi dan pemantauan keamanan yang aktif.
2. Analisis log dan peristiwa untuk mendeteksi indikasi serangan atau perilaku mencurigakan.
3. Penggunaan teknologi kecerdasan buatan (AI) untuk deteksi dini.

e. Respons:

1. Pembentukan tim respons keamanan yang siap bertindak setelah terdeteksi serangan.
2. Penyusunan prosedur tanggap cepat dan perbaikan setelah serangan terjadi.
3. Pelaksanaan pelatihan dan simulasi tanggap darurat.

f. Pemulihan:

1. Penetapan proses pemulihan sistem dan data setelah serangan.
2. Implementasi solusi cadangan dan pemulihan untuk mengembalikan operasional normal.
3. Evaluasi dan pembelajaran dari serangan untuk meningkatkan ketahanan keamanan.

g. Edukasi dan Kesadaran:

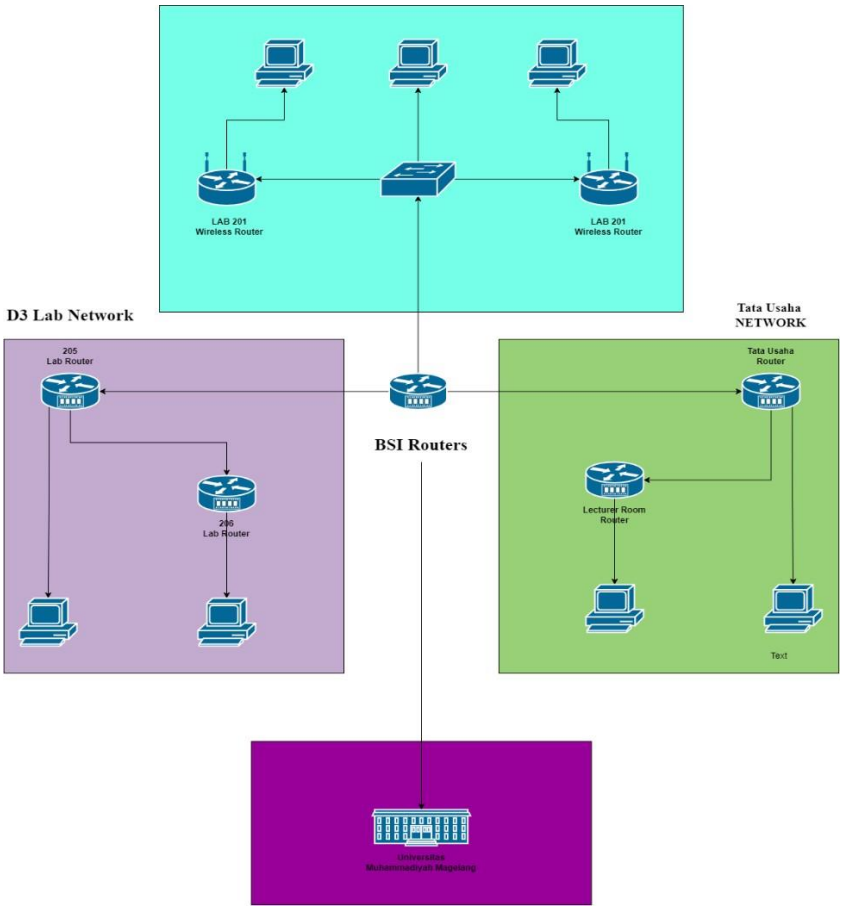
1. Pelaksanaan program pelatihan keamanan untuk karyawan.
2. Peningkatan kesadaran keamanan informasi dalam organisasi.
3. Penggalakan budaya keamanan informasi.

h. Pengujian dan Pemantauan Terus-menerus:

1. Pelaksanaan uji penetrasi dan pengujian keamanan secara reguler.
2. Pemantauan terus-menerus terhadap ancaman keamanan dan perubahan lingkungan keamanan.
3. Pembaruan kebijakan dan kontrol keamanan berdasarkan hasil evaluasi.

3.2 Pengumpulan Data

Pada fase ini, penulis mengumpulkan berbagai studi penelitian, jurnal, dan sumber informasi lain yang terkait dengan metode, alat, dan teknik forensik digital yang diterapkan pada bukti digital. Data yang digunakan adalah data sekunder karena skenario ilustrasi yang telah direncanakan sebelumnya digunakan dalam penelitian ini. Informasi yang menggambarkan skenario tersebut merupakan hasil wawancara denganKetua Biro Sistem Informasi (Agus Setiawan M.Eng.) dan dengan teknisi laboratorium Laboratorium S1 Teknologi Informasi (Qosim Nurdin Haka, S.Kom). Selain itu, dokumentasi serangan dibuat menggunakan alat dan teknik forensik digital yang dapat digunakan untuk mempersiapkan upaya pertahanan dan pengembangan di masa mendatang.



Gambar 3. 2 Topologi Jaringan Fakultas Teknik

3.3 Membuat Skenario

Skenario pengujian mengacu pada perumusan masalah yaitu memberikan solusi atas instalasi keamanan. Untuk itu skenario pengujian nya di buat sebagai berikut:

1) Melakukan observasi terhadap router UNIMMA sebagai objek serangan (lansung ke router yang ada).

2) Uji coba terhadap router UNIMMA melaui infrastuktur jaringan UNIMMA dengan menggunakan 2 tools serangan yaitu:

a. Brute Force

Disini penulis mencoba utuk menyerang jaringan pada router dengan mencoba semua kemungkinan kombinasi username dan password. Serangan brute force pada organisasi atau instansi pemerintah akan mengalami dampak yang serius terhadap instalasi jaringan, serangan ini termasuk kedalam jenis DDoS (*Distributed Denial of Service*) *attack* yang akan menyebabkan *down time* pada jaringan. Jadi diperlukan pertahanan jaringan yang bisa menghalangi serangan DDoS tersebut.

b. Cracking

Disini penulis mencoba menyerang dengan membanjiri requestHTTP pada router Lab dan UNIMMA. Serangan yang dilakukan menggunakan *tools goldeneye,* setelah dianalisis goldeneye menggunakan eksploitasi *Eternalblue* yang sama seperti yang digunakan oleh *Wannacry* untuk mereplika secara lateral, yang bisa disebut komponen "*Worm*" dari malware. Komponen ini memungkinkan malware mereplika dirinya pada sistem yang rentan diseluruh jaringan. Jadi perlu penanganan untuk menangani masalah tersebut.

3) Membuat skenario kasus dengan mengidentifikasi alamat IP, nama pengguna, dan kata sandi untuk melakukan serangan. Skenario dibuat di ruang laboratorium 201 S1 Fakultas Teknik Informatika, dengan menggunakan virtual box dan Kali Linux. Berikut adalah fungsi dari masing-masing alat:

Tabel 3. 1 Tools dalam Skenario

NO	Nama Tools	Funsi
1	*Virtual Box*	Tempat menginstall tools yang akan digunakan
2	*Kali Linux*	Sebagai alat serangan

Selama pengumpulan data peneliti menggunakan seperangkat komputer dengan spesifikasi sebagai berikut:

a. *Hardware*

1) Laptop Lenovo G40-PC

- CPU : Intel Celeron N2840
- Kartu grafis : Intel® HD Graphics
- RAM : 8 GB DDR4
- Penyimpanan : 500 GB

2) *Router Board* RB951Ui-2HnD

- CPU : AR9344
- CPU nominal frequency : 600 MHz
- License level 4
- RAM : 128 MB
- Storage size : 128 MB
- PoE in : Passive PoE
- PoE in input Voltage : 9-30 V
- PoE out : Passive PoE
- PoE-out ports : Ether5
- Number of DC inputs : 2 (DC jack, PoE-IN)
- DC jack input Voltage : 9-30 V
- Max out per port output (input < 30 V) : 500 mA
- Max total out (A) : 500 mA
- Max power consumption : 6.5 W

3) Wifi Adapter TP-Link TL-WN722N

- Interface : USB 2.0
- Button : WPS Button
- Dimensions (W x D x H) : 3.7 x 1.0 x 0.4 in. (93.5 x 26 x 11mm)
- Antenna Type : Detachable Omni Directional (RP-SMA)
- Antenna Gain : 4dBi

- Wireless Standards : IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
- Frequency : 2.400-2.4835GHz
- Signal Rate 11n: Up to 150Mbps(dynamic)

  11g: Up to 54Mbps(dynamic)

  11b: Up to 11Mbps(dynamic)
- Reception Sensitivity : 130M: -68dBm@10% PER

  108M: -68dBm@10% PER

  54M: -68dBm@10% PER

  11M: -85dBm@8% PER

  6M: -88dBm@10% PER

  1M: -90dBm@8% PER
- Transmit Power : <20dBm
- Wireless Modes : Ad-Hoc / Infrastructure mode
- Wireless Security : Support 64/128 bit WEP, WPA-PSK/WPA2-PSK
- Modulation Technology : DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

b. *Software*

1) Oracle VM VirtualBox
   - versi : 6.1.40 r154048
2) Kali Linux
   - PRETTY_NAME="Kali GNU/Linux Rolling"
   - NAME="Kali GNU/Linux"
   - ID=kali
   - VERSION="2021.3"
   - VERSION_ID="2021.3"

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang mengevaluasi keamanan jaringan wireless BSI UNIMMA dengan menggunakan metode Penetration Testing, disimpulkan bahwa Aircrack memiliki kemampuan untuk melakukan scanning, monitoring, dan merekam lalu lintas data dalam jaringan Wi-Fi tersebut. Penggunaan "deauth attack tool" pada Aircrack dapat memaksa perangkat pengguna atau access point untuk memutuskan koneksi Wi-Fi yang aktif, menyebabkan gangguan pada akses internet. Akibatnya, terdapat potensi untuk melakukan peretasan (cracking) terhadap jaringan Wi-Fi dengan menggunakan wordlist, yaitu daftar kata sandi yang mungkin digunakan. Kesimpulan ini mencerminkan potensi risiko keamanan dalam pengelolaan jaringan wireless yang perlu mendapatkan perhatian lebih lanjut dan penerapan langkah-langkah mitigasi yang tepat.

5.2 Saran

Penulis menyarankan BSI UNIMMA untuk memperkuat keamanan jaringan dengan menerapkan metode enkripsi yang lebih kuat, seperti migrasi ke protokol WPA3, guna mengurangi risiko pemantauan dan merekam data oleh alat-alat seperti Aircrack. Implementasi sistem pemantauan aktif, yang mampu mendeteksi dan merespons cepat terhadap aktivitas mencurigakan seperti scanning dan serangan deauth, menjadi langkah krusial untuk mengidentifikasi potensi serangan dan meminimalkan dampaknya. Dalam upaya pertahanan dari serangan luar, perlu diperbarui dan dikonfigurasi firewall pada tingkat perangkat keras dan perangkat lunak, sambil menerapkan kebijakan pemutakhiran rutin guna menutup celah keamanan yang dapat dimanfaatkan oleh alat seperti Aircrack. Melalui kampanye kesadaran keamanan berkala, organisasi dapat meningkatkan pemahaman pengguna terhadap risiko penggunaan jaringan Wi-Fi, serta memberikan edukasi tentang praktik keamanan yang baik, termasuk penggunaan kata sandi yang kuat dan kebijakan keamanan yang harus diikuti. Penerapan kebijakan kontrol akses yang ketat, khususnya terhadap alat-alat keamanan seperti Aircrack, akan membantu mencegah penggunaan alat-alat tersebut secara tidak sah atau tidak etis. Keseluruhan langkah-langkah ini dapat diintegrasikan ke dalam

kebijakan keamanan organisasi untuk menciptakan lingkungan yang lebih aman dan andal.

DAFTAR PUSTAKA

Adam, M., Alwi, E. I., & As'ad, I. (2022). *ANALISIS FORENSIK TERHADAP SERANGAN DDOS PING OF DEATH PADA SERVER* (Vol. 5, Issue 1).

Alliance, W.-F. (2005). *{D}eploying {W}i-{F}i {P}rotected {A}ccess ({W}{P}{A}{\texttrademark}) and {W}{P}{A}2{\texttrademark} in the {E}nterprise*. *March*.

Aryo, G., Pongdatu, N., Michael, A., Patalo, E. E., Studi, P., Informatika, T., Kristen, U., Toraja, I., Toraja, T., & Selatan, S. (2022). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing di SMK Xyz Tana Toraja. *Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Di SMK Xyz Tana Toraja*, *2*(2), 1–7. https://doi.org/10.47178/infinity.v2i2

Cholid Fitra Fahriza. (2022). *Analisis Ransomware secara Statis dan Dinamis untuk PemetaanEvolusi Ransomware*.

Delsi Samsumar, L., & Gunawan, K. (2017). ANALISIS DAN EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL (WIRELESS LAN); STUDI KASUS DI KAMPUS STMIK MATARAM. In *Jurnal Ilmiah Teknologi Informasi Terapan: Vol. IV* (Issue 1).

Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *4*(2), 413. https://doi.org/10.30865/mib.v4i2.2037

Haeruddin, H., & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *Conference on Management, Business, Innovation, Education and Social Science*, *1*(1), 508–515. https://journal.uib.ac.id/index.php/combines/article/view/4475

Harry Dwi Sabdho, & Ulfa Maria. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. *Seminar Hasil Penelitian Vokasi (SEMHAVOK)*, *1*(1), 15–24.

Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi. *Jurnal Mahasiswa Bina Insani*, *5*(1), 53–62.

Mulyanto, Y., Herfandi, H., & Candra Kirana, R. (2022). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI

ABDULKADIR). *Jurnal Informatika Teknologi Dan Sains*, *4*(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mushlih, M., Fitri, R., & Wardiah, I. (2019). Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. *Prosiding SNRT (Seminar Nasional Riset Terapan)*, A41–A47. https://www.polman-babel.ac.id/

Mushlihudin, A. N. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *CYBERNETICS*, *4*(02), 79–92. https://centralops.net

Owens, L., & Devices, H. (2015). *Wireless Network Security Tom Karygiannis*. *1*.

Riadi, I. (2020). *PERBANDINGAN TOOL FORENSIK DATA RECOVERY BERBASIS ANDROID MENGGUNAKAN METODE NIST*. *7*(1), 197–204. https://doi.org/10.25126/jtiik.202071921

Riadi, I., & Yudhana, A. (2020). *Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)* (Vol. 2, Issue 1). http://ars.ilkom.unsri.ac.id300

Rodrigues, T. (2022). *TP-Link Archer C64 blends simplicity and efficiency*. Showmetech.

Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. In *Seminar Nasional Teknologi Informasi dan Komputer*.

Sampurna, M. R., Korespondensi, P., Muhammad, :, & Sampurna, R. (2022). Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA. *NetPLG Journal of Network and Computer Applications*, *1*(2).

Yudi Mulyanto, A. A. F. (2022). *ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus SMK …*. *4*, 145–155.

Adam, M., Alwi, E. I., & As'ad, I. (2022). *ANALISIS FORENSIK TERHADAP SERANGAN DDOS PING OF DEATH PADA SERVER* (Vol. 5, Issue 1).

Alliance, W.-F. (2005). *{D}eploying {W}i-{F}i {P}rotected {A}ccess ({W}{P}{A}{\texttrademark}) and {W}{P}{A}2{\texttrademark} in the {E}nterprise*. *March*.