Analisa Keamanan Jaringan *Wireless* Di Universitas Sam Ratulangi

Abraham Yano Suharmanto, Arie S.M Lumenta, Xaverius B.N. Najoan
Teknik Elektro Universitas Sam Ratulangi Manado, Indonesia, 95115
South.ridder@gmail.com, al@unsrat.ac.id, xnajoan@unsrat.ac.id

***Abstrak* - Masyarakat telah menikmati perkembangan teknologi khususnya di bidang informasi salah satunya yang telah berkembang saat ini adalah internet. Dalam penggunaannya, jaringan yang dipakai oleh masyarakat adalah kabel LAN maupun Wireless LAN (Tanpa Kabel) serangan dari pihak yang tidak bertanggung jawab yaitu hacker yang bisa mengeksploitasi data penting dari pengguna, menyadap data seperti password dan mengubah data penggunanya. Wireshark adalah tools yang digunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Serta Acunetix Web Vulnerability Scanner yang digunakan untuk mencari celah keamanan suatu web. Suatu Jaringan pun bisa down akibat serangan dari DDOS (Disc Denial Of Service) Universitas Sam Ratulangi atau yang dikenal dengan singakatan Unsrat, beralamat Jalan Bahu, Kota Manado, Provinsi Sulawesi Utara. Merupakan lembaga pendidikan tingkat perguruan tinggi dan merupakan Salah Satu Universitas Negeri terbaik Di Sulawesi Utara. Universitas Sam Ratulangi saat ini telah menyediakan fasilitas jaringan komputer kabel maupun nirkabel atau lebih sering dikenal wireless sebagai sarana untuk pertukaran data, pencarian informasi seperti materi mata kuliah, chatting, Pengisian Kartu Rencana Studi (KRS), penelitian ini adalah untuk menganalisis keamanan jaringan yang berada di Universitas Sam Ratulangi, terhadap ancaman serangan pihak luar yang dapat dilakukan.**

Kata kunci : Wireless, Sniffing, DDOS, Universitas Sam Ratulangi

I. PENDAHULUAN

Dalam Era modern ini masyarakat telah menikmati perkembangan teknologi khususnya di bidang informasi salah satunya yang telah berkembang saat ini adalah internet, dimana masyarakat memanfaatkan teknologi ini untuk kegiatan seperti mencari informasi, berbagi data dengan teman, bertransaksi keuangan menggunakan fasilitas *e-banking*, serta berinteraksi sosial menggunakan layanan sosial media dan lain – lain. Dari seluruh kegiatan yang dilakukan masyarakat dalam internet tersebut agar bisa saling terhubung satu sama lain menggunakan fasilitas jaringan internet.

Dalam penggunaannya, jaringan yang dipakai oleh masyarakat adalah kabel *LAN* maupun *Wireless LAN* (Tanpa Kabel) dan dalam jaringan internet tersebut bukan berarti pengguna aman dari serangan dari pihak yang tidak bertanggung jawab yaitu *hacker* yang bisa mengeksploitasi data penting dari suatu instansi, menyadap data seperti *password* dan mengubah data penggunanya. Maka dalam perancangan sistem keamanan jaringan internet harus dirancang dengan dengan teliti agar bisa meminimalisir segala jenis serangan yang dilakukan dari pihak – pihak yang tidak bertanggung jawab untuk dapat melindungi *user.*

Adapula Keamanan informasi dalam sebuah *website* menjadi sangat penting. Keamanan informasi sebuah *website* merupakan salah satu prioritas yang sangat utama bagi seorang *web development*. Jika seseorang mengabaikan keamanan tersebut maka seorang *hacker* dapat mengambil data penting dan bahkan mengacak-acak tampilan *web* tersebut. Ada tiga tujuan penting tercapainya keamanan informasi (Vacca, 2009): (1) *Confidentiality* (kerahasiaan) yaitu informasi hanya tersedia untuk orang atau sistem perlu akses kesana; (2) *Integrity* (kesatuan) yaitu informasi hanya dapat ditambah atau diperbaharui oleh orang yang telah diautorisasi: (3) *Avability* (ketersedian) yaitu informasi harus tersedia dalam waktu yang tepat ketika dibutuhkan.

Universitas Sam Ratulangi atau yang dikenal dengan singakatan Unsrat, beralamat Jalan Bahu, Kota Manado, Provinsi Sulawesi Utara. Merupakan lembaga pendidikan tingkat perguruan tinggi dan merupakan Salah Satu Universitas Negeri terbaik Di Sulawesi Utara. Unsrat saat ini telah menyediakan fasilitas jaringan komputer kabel maupun nirkabel atau lebih sering dikenal *wireless* sebagai sarana untuk pertukaran data, pencarian informasi seperti materi mata kuliah, *chatting,* Pengisian Kartu Rencana Studi (KRS), penginputan nilai, *e-learning* atau kuliah jarak jauh dan lain – lain. fasilitas layanan jaringan komputer tersebut diberikan secara gratis kepada mahasiswa, dosen dan pegawai yang terdaftar di Universitas Sam Ratulangi yang dilaksanakan oleh UPT Teknologi Informasi dan Komunikasi Unsrat.

Untuk menguji keamanan dari jaringan server UPT Teknologi Informasi dan Komunikasi Unsrat peneliti akan melakukan uji penetrasi jaringan menggunakan metode *Action Research* terhadap server dan website Unsrat dan kepada user yang aktif terutama yang dalam cakupan penggunaan *Wireless* dengan batasan – batasan seperti tidak melakukan perusakan terhadap jaringan atau yang dapat merugikan pihak – pihak yang terkait.

A. *Penelitian Action Research (Penelitian Tindakan)*

Menurut Arikunto (2006:18), penelitian tindakan adalah penelitian tentang hal-hal yang terjadi di masyarakat atau kelompok sasaran, dan hasilnya langsung dapat dikenakan pada masyarakat yang bersangkutan. Karakteristik utama penelitian ini adalah partisipasi dan kolaborasi antara peneliti dengan anggota sasaran. Penelitian tindakan adalah salah satu strategi pemecahan masalah yang memanfaatkan tindakan nyata dalam bentuk proses pengembangan inovatif yang 'dicoba sambil jalan' dalam mendeteksi dan memecahkan masalah.

Kemmis (dalam Arikunto, 2006:19) menyatakan bahwa penelitian tindakan merupakan upaya mengujicobakan ide-ide ke dalam praktek untuk memperbaiki atau mengubah sesuatu agar memperoleh dampak nyata dari situasi. Selanjutnya Kemmis dan Taggar (dalam Zuriah, 2003:54) juga menyatakan bahwa penelitian tindakan adalah suatu bentuk penelitian reflektif diri yang secara kolektif dilakukan peneliti dalam situasi social untuk meningkatkan penalaran dan keadilan praktek pendidikan dan social mereka, serta pemahaman mereka mengenai praktek dan terhadap situasi tempat dilakukan praktek-praktek tersebut. Davison, Martinsons & Kock (2004) membagi *Action research* dalam 5 tahapan yang merupakan suatu siklus, yaitu :

1. Melakukan diagnosa (*diagnosing*)
   Melakukan identifikasi masalah-masalah pokok yang ada sehingga terjadi perubahan.
2. Membuat rencana tindakan (*action planning*)
   Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.
3. Melakukan tindakan (*action taking*)
   Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah.
4. Melakukan evaluasi (*evaluating*)
   Setelah masa implementasi (*action taking*) dianggap cukup kemudian peneliti melaksanakan evaluasi hasil dari implementasi.
5. Pembelajaran (*learning*)
   Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahap pertahap yang telah berakhir kemudian penelitian ini dapat berakhir. Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi dievaluasi oleh peneliti dan dikomunikasikan, peneliti merefleksi hasil proyek yang akan dilaporkan secara lengkap dan hasilnya secara eksplisit dipertimbangkan dalam hal implikasinya terhadap penerapan tindakan.

B. *Konsep Jaringan Komputer*

Dalam ilmu komputer dan teknologi informasi, dikenal istilah jaringan komputer. Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi, sehingga dapat saling berbagi data, informasi, program, dan perangkat keras (printer, harddisk, webcam, dsb). Berbeda dengan konsep jaringan dalam ilmu biologi –yaitu kumpulan sel yang fungsinya sejenis komputer-komputer yang terhubung dalam jaringan komputer tidak harus sejenis. Komputer-komputer tersebut bisa saja memiliki tipe yang berbeda-beda, menggunakan sistem operasi yang berbeda, dan menggunakan program/aplikasi yang berbeda pula. Tetapi komputer-komputer yang terhubung dalam jaringan komputer harus memakai aturan komunikasi (protokol) yang sama. Hal ini dimaksudkan agar masing-masing komputer dapat berkomunikasi yang baik dengan komputer lainnya. Protokol yang menjadi Standar Internasional adalah TCP/IP (*Transmission Control Protocol / Internet Protocol*).

(Modul Praktikum Universitas Gunadarma)

C. *Konsep Keamanan Jaringan*

Menurut Bayu Arie Nugroho (2012) Pada penelitiannya yang berjudul Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) terhadap Serangan Packet Sniffing yang berisi Jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*, baik jaringan *LAN* maupun *Wireless.* Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam pembangunan perancangannya, system keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisiterjadinya serangan oleh para *hacker.* Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman , kelemahan, dan *policy* keamanan jaringan.

D. *Jenis – Jenis Ancaman Serangan*

Ancaman Serangan yang bisa terjadi dalam jaringan terutama jaringan *Wireless (WIFI)* ada bermacam – macam seperti yang akan dipaparkan di bawah ini berdasarkan penelitian yang dikutip oleh penulis dari Bayu Arie Nugroho (2012) dengan penelitiannya Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) terhadap Serangan Packet Sniffing, yaitu :

1. Packet sniffer

Packet sniffer adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun nirkabel. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan karena pada dasarnya semua koneksi ethernet adalah koneksi yang bersifat broadcast, di mana semua host dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah host. Cukup sulit untuk melindungi diri dari gangguan ini karena sifat dari packet sniffing yang merupakan metode pasif (pihak penyerang tidak perlu melakukan apapun, hanya perlu mendengar saja).

2. Denial of service (Dos)

Sumber daya jaringan yang berharga antara lain komputer dan database, serta pelayanan-pelayanan (service) yang disediakan oleh organisasi pemilik jaringan. Kebanyakan user jaringan memanfaatkan pelayananpelayanan tersebut agar pekerjaan mereka menjadi efisien. Bila pelayanan ini tidak dapat dipergunakan karena sebab-sebab tertentu, maka tentu saja akan menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab *denial of service*. Berikut ini adalah contoh penyebab terjadinya *denial of service* :

a) Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran traffic.
b) Kemungkinan ada virus yang menyebar dan menyebabkan system komputer menjadi lamban atau bahkan lumpuh.
c) Kemungkinan device yang melindungi jaringan dirusak.

D. Penelitian Terkait

Penelitian sebelumnya digunakan untuk dapat dijadikan bahan pertimbangan dan diharapkan dapat membantu dalam pembuatan teknik yang baru. Penelitian yang dibuat penulis tidak 100% persen adalah hasil kerja sendiri melainkan penulis mengambil dasar – dasar dari beberapa penelitian dari beberapa penulis lain yang terkait dengan penelitian ini yaitu salah satunya penelitian dari Bayu Arie Nugroho (2012) dengan judulnya Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) terhadap Serangan Packet Sniffing dimana penelitian ini berfokus pada pengujian keamanan terhadap serangan sniffing (pendapan) yang bertujuan merekam segala data penting dari target untuk bisa diambil data penting seperti username dan password.

Jaringan komputer mempunyai dua media transmisi data yaitu kabel dan nirkabel. PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta merupakan salah satu Badan Usaha Milik Negara (BUMN) yang mempunyai fasilitas jaringan nirkabel (wifi). Jaringan wifi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Diperlukan system pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar terhindar dari serangan yang dilakukan oleh orang–orang yang tidak bertanggung jawab.

Penelitian ini membahas evaluasi tingkat keamanan fasilitas wifi di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta dengan menggunakan aplikasi netstumbler, inSSIDer dan ettercap. Netstumbler adalah tools wifi hacking yang digunakan untuk mendeteksi dan mengidentifikasi sinyal wireless yang terbuka. inSSIDer adalah software alternatif yang fungsinya sama persis dengan netstumbler. Ettercap adalah tools packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Dalam penelitian ini dilakukan dua tahap, yang pertama mengidentifikasi keberadaan dan keamanan wifi yang dipakai menggunakan software inSSIDer. Tahap kedua melakukan serangan packet sniffing menggunakan software Ettercap sebagai langkah pengujian keamanan di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta. Hasil dari penelitian ini adalah dengan terdeteksinya keberadaan dan keamanan wifi yang terbuka atau tanpa pengamanan dan terekamnya username dan password. Hal ini dapat membahayakan keamanan lalulintas data para pengguna jaringan wifi maupun LAN kabel khususnya para karyawan/i, sehingga diperlukan peningkatan keamanan yang baik untuk dapat mencegah/menangani serangan packet sniffing dan yang lebih lanjut.

Penelitian lainnya yang penulis ambil adalah dari Adi Fajaryanto (2015) yang berjudul Penerapan Metode ISSAF dan OWASP Versi 4 Untuk Uji Kerentanan Web Server dimana penelitian ini bertujuan untuk pengujian serangan terhadap web server dengan menggunakan metode ISSAF dan OWASP dimana salah satu metode ini digunakan oleh penulis untuk digunakan.test terhadap server mereka sendiri. Melalui self test ini, para pemilik web server akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode self test ini adalah penetration test. Metode ini sama dengan aktivitas hacking namun dilakukan secara legal. Penelitian ini, metode implementasi penetration test yang akan digunakan adalah ISSAF (Information Systems Security Assessment Framework) dan OWASP versi 4. IKIP PGRI Madiun sebagai salah satu instansi pendidikan sudah mempunyai web server sendiri sejak tahun 2010. Berdasarkan wawancara dengan pengelola web server IKIP PGRI Madiun, sejak pertama kali web server online sampai saa tini web server berhasil dibobol oleh hacker beberapa kali dalam setahun dan belum pernah dilakukan penetration test pada web servernya. Hasil pengujian dan analisa dengan metode ISSAF menunjukkan bahwa sistem web server IKIP PGRI Madiun masih dapat ditembus dan mengambil alih hak akses administrator, sedangkan dengan metode OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik.

Serta penelitian dari Sudarmawan (2013) yang berjudul Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing (Kasus : Universitas Muhammadiyah Magelang) yang dalam penelitiannya melakukan uji penetrasi terhadap Wireless LAN untuk mengevaluasi tingkat keamanan jaringan dengan menerapkan pula metode ISSAF sebagai framework dalam penelitian ini.

Wireless Local Area Network (WLAN) merupakan jaringan yang banyak digunakan pada beberapa institusi untuk menyediakan akses informasi secara bersama. Keamanan jaringan wireless menjadi perhatian utama bagi pengelola jaringan untuk menjaga kualitas sistem jaringan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan evaluasi terhadap sistem keamanan yang ada dalam jaringan tersebut. Salah satu metode yang dapat digunakan untuk mengevaluasi adalah dengan penetration testing terhadap jaringan tersebut. Penetration testing adalah tindakan pengujian sistem dengan cara mensimulasikan bentuk-bentuk serangan terhadap system tersebut sehingga akan diketahui tingkat kerentanannya. Pengujian dengan metode ini tentunya akan beresiko yang dapat mempengaruhi sistem. Serangan yang dilakukan terhadap sistem dapat merugikan pihak target pengujian dan bagi pelaku tentunya merupakan sebuah tindakan pelanggaran apabila tidak adanya kesepakatan atas tindakan yang akan dilakukan dan konsekuensi terhadap akibat dari tindakan tersebut. Oleh sebab itu untuk menerapkan pada institusi perlu adanya perencanaan dan persiapan yang baik agar tidak merugikanmasing-masing pihak. Penelitian ini menggunakan kasus di Universitas Muhammadiyah Magelang sebagai institusi yang dijadikan objek untuk menerapkan model evaluasi keamanan WLAN dengan penetration testing.

II. METODOLOGI PENELITIAN

Penelitian ini dilaksanakan di lokasi – lokasi yang terdapat hotspot (wifi) di area Universitas Sam Ratulangi Manado. Peneliti malaksanakan penelitian di area tersebut karena dalam cakupan hotspot yang berada di Universitas Sam Ratulangi selalu ramai dalam kegiatan mengakses internet baik itu mencari informasi, penggunaan sosial media, dan aktifitas input / output data fakultas atau universitas. Adapun lokasi akses point yang dijadikan tempat penelitian yaitu di UPT – TIK (Unit Pelayanan Terpadu – Teknologi Informasi dan Komunikasi), serta Akses point yang berada di kantor jurusan Elektro serta berada diLaboraturium Teknologi Informasi dan komunikasi.

1. Langkah – Langkah penelitian

a. Mencari informasi penting berupa alamat ip dengan menggunakan tools whois dan mendapatkan alamat ip, domain, dan server yang dipakai serta informasi lainnya.
b. Mencari celah yang terbuka dengan menggunkan *tools Acunetix Web Vulnerability* hasilnya terdapat kurang lebih 150 celah yang didapat tapi celah yang ditemukan masih kategori sangan aman karena tingkan ancaman tingkat berbahaya karena hanya ancaman level 2 saja .
c. Melakukan *DDOS* dengan *LOIC (Low Orbit Ion Canon)* dan target berhasil di *flooding*
d. Penetrasi menggunakan *HOIC (High Orbit Ion Canon)* berhasil mengirim package
e. *DoSHTTP* gagal melakukan *flooding*
f. Mengetes keamanan wifi dengan metode *Sniffing /* Penyadapan dengan memakai *Wireshark* dan penyadapan tidak berhasi

Pada tahap ini merupakan hasil dan pembahasan sebelumnya dan berhubungan dengan tahap penelitian di atas. Adapun dalam tahap penelitian menggunakan *Action research* (penelitian tindakan). Metode penelitian ini ada 5 tahapan yang merupakan siklus dari metode ini yang akan diterapkan di penelitian ini :

2. Melakukan diagnosa (diagnosing).

Pada tahap diagnosa peneliti akan melakukan identifikasikan masalah-masalah pada saat melakukan penelitian Analisis Keamanan Jaringan wireless di Universitas Sam Ratulangi. Pokok – pokok apa saja yang menjadi permasalah maka menjadi pembahasan dalam penelitian. Peneliti mengidentifikasi Jaringan wireless Dan website di Universitas Sam Ratulangi sehingga keamanan yang berguna. Langkah yang ditempuh adalah melakukan tes kepada website Universitas Sam Ratulangi yang terkait langsung maupun tidak langsung. Masalah yang terkait langsung dalam penelitian ini adalah mengenai keamanan website.

a. Membuat rencana tindakan (action planning).

Penulis bisa memahami pokok pokok permasalahan yang akan dilanjutkan pada tahap rencana tindakan ini, pada tahap ini melakukan rencana tindakan yang akan dilakukan pada website Unsrat dengan membuat perancangan dan pengujian sistem keamanan website . Pada tahap ini peneliti mempelajari pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat sebagai pencegahan terhadap masalah yang ada. Dengan demikian, Analisis Keamanan Jaringan Wireless di unsrat harus terlebih dahulu membuat rencana pencarian celah. Dengan memperhatikan kebutuhan website Peneliti membuat rancangan tahapan dengan menggabungkan teknik pencarian celah.

b. Melakukan tindakan (action taking)

Peneliti menerapkan rencana dengan tindakan yang telah dibuat dengan menjalankan tahapan-tahapan mengikuti fase penetrasi testing terhadap website Unsrat untuk mencari celah keamanan pada website . Pada tahapan ini, Peneliti sebagai penguji mengimplementasikan rencana tindakan dengan harapan dapat menemukan celah keamanan Website Unsrat

Proses pelaksanaannya, pertama kali peneliti mengecek menggunakan aplikasi Aplikasi Whois untuk mendapatkan informasi seperti alamat ip dan informasi lainnya selanjutnya dilanjutkan dengan penggunaan tools *Acunetix Web Vulnerability Scanner untuk* melakukan uji pencariani celah untuk mengetahui sejauh mana keamanan Website Universitas Sam Ratulangi Unsrat. Setelah praktik dilakukan, peneliti kemudian memeberikan solusi berupa rangkuman.

3. Melakukan evaluasi (evaluating)

Peneliti melaksanakan evaluasi hasil dari penetrasi yang menemukan celah keamanan website Unsrat, dalam tahap ini yang dilihat adalah apakah system keamanan website berjalan dengan baik dan sesuai dengan rencana. Setelah tahap implementasi (action taking), Peneliti melakukan evaluasi terhadap implementasi celah keamanan Website dengan melakukan uji penetrasi peneliti menuliskan masalah sesuai dengan proses yang telah ditempuh selama pengujian berlangsung. Dari Laporan pengujian ini peneliti dapat melihat sejauh mana keamanannya

4. Pembelajaran (learning)

Tahap ini merupakan bagian akhir tahap-tahapan yang telah di lakukan oleh peneliti. Dimana tahap ini merupakan Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi dievaluasi oleh peneliti dan dikomunikasikan, peneliti merefleksi hasil proyek dalam bentuk skripsi yang merupakan inti dari penelitian ini dan hasilnya secara eksplisit dipertimbangkan dalam hal implikasinya terhadap penerapan tindakan. Tahap ini merupakan bagian akhir tindakan yang telah dilalui dengan. Seluruh kriteria dalam prinsip keamanan, termasuk yang terjadi, kemudian dikomunikasikan kepada Website Bazma Pertamina RU III Plaju Palembang. Peneliti kemudian merefleksikan analisis celah keamanan yang telah dilaksanakan, termasuk pertimbangan dan masukan untuk memperbaiki solusi keamanan yang telah diterapkan. Selanjutnya, Peneliti merangkum seluruh hasil penelitian dalam bentuk laporan skripsi penelitian. Setelah tahap demi tahap peneliti melakukan analisa dan uji coba dengan beberapa tools yaitu *Acunetix Web Vulnerability Scanner* yang digunakan untuk mencari informasi celah menunjukkan bahwa website dalam level kerentanan *Low*, hal ini ditunjukkan dengan ditemukannya *web alerts* dengan kategori *Low* dan *informational* berdasarkan beberapa tingkatan *high*, *medium* dan *low* menghasilkan tingkatan celah keamanan yang tinggi.

Dari hasil *Acunetix Web Vulnerability Scanner* ditemukan celah yang terdiri dari beberapa tingkatan

diantaranya :

1. Tingkatan high dengan total nilai 0 celah
2. Tingkatan medium dengan total nilai 44
3. Tingkatan low dengan total nilai 1

Dari analisis menggunakan tool *Acunetix Web Vulnerability Scanner* ini peneliti melanjutkan untuk menguji celah tersebut dengan beberapa tools diantarannya LOIC (Low Orbit Ion Canon) untuk melakukan pengujian DDOS untuk melakukan flooding terhadap jaringan dan website unsrat, HOIC (High Orbit Ion Canon) untuk melakukan flooding dengan cara pengiriman Package secara besar sehingga karena banyaknya *request* yang masuk membuat *web server* menjadi *down*, serta *DoSHTTP 2.5* digunakan untuk melakukan penetrasi flooding, selanjutnya mencoba melakukan sniffing atau penyadapan dengan menggunakan Wireshark. Maka dari hasil uji coba menggunakan aplikasi-aplikasi tersebut didapatlah beberapa kerentanan atau *Vulnerability* dari *website* Unsrat

A. *Metode Pengumpulan Data*

Untuk mendapatkan data dan informasi pada penelitian ini, maka peneliti menggunakan metode dalam proses penumpulan data adalah sebagai berikut:

1. Pengamatan (*Observation*)

Peneliti mengadakan peninjauan langsung jaringan website unsrat serta meninjau lokasi yang bisa dijadikan spot untuk melakukan penelitian di unsrat dengan objek penelitian yang ada.

2. Pengujian (*Testing)*

Untuk mendapatkan informasi dan mendapatkan data-data secara langsung, maka dalam hal ini peneliti melakuakan pengujian terhadap jaringan yang akang diteliti agar bisa memperoleh gambaram model pengujian yang lebih detail.

3. Studi Kepustakaan (*Literature*)

Data juga diperoleh melalui studi kepustakaan (*literature*) yaitu dengan cara mencari bahan dari internet, jurnal dan perpustakaan serta buku yang sesuai dengan objek yang akan diteliti.

B. *Tools yang digunakan*

1. *Whois*

Whois atau disuarakan “who is” digunakan untuk mendapatkan data informasi domain tertentu seperti nama pemilik domain, ip address, name server dan umur domain. Whois lookup yaitu sebuah aplikasi berbasis command line digunakan untuk melakukan query terhadap database whois.

Namun dalam perkembangannya, data whois suatu domain bisa dilihat di situs whois seperti domaintools atau whois.net. Sehingga user biasa seperti kita bisa mendapatkan informasi kepemilikan suatu domain dengan mudah. Walaupun demikian program whois berbasis command-line masih sering digunakan oleh Administrator jaringan.

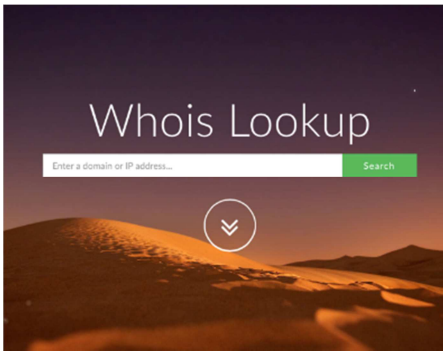
2. *Kegunaan whois*

Selain mendapatkan informasi suatu domain, whois memiliki kegunaan sebagai berikut :

1. Mendukung keamanan dan kestabilan dari internet dengan menyediakan informasi kontak yang bisa dihubungi yang berhubungan dengan jaringan, ISP, dan pemilik domain.
2. Untuk mendapatkan informasi ketersediaan domain. Sehingga jika domain tersedia dalam artian belum diregistrasi oleh orang lain, maka Anda bisa melakukan registrasi atas nama domain tersebut.

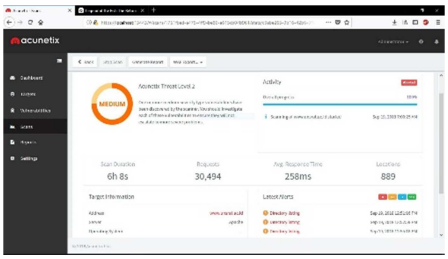
1. *Acunetix*

Acunetix Web Vulnerability Scanner adalah sebuah alat layanan aplikasi web untuk pengujian keamanan otomatis yang mengaudit aplikasi web Anda dengan memeriksa kerentanan seperti SQL Injection, Cross site scripting, dan kerentanan web yang dieksploitasi lainnya. Acunetix merupakan alat otomatis yang dapat membantu perusahaan memindai aplikasi web mereka untuk mengidentifikasi dan menyelesaikan kerentanan dieksploitasi. Acunetix Vulnerability Scanner juga telah menjadi alat pilihan bagi banyak pelanggan di Pemerintahan, Militer, Pendidikan, Telekomunikasi, Perbankan, Keuangan, dan perusahaan E-Commerce, dan termasuk perusahaan-perusahaan besar lainnya dari berbagai negara. Acunetix Vulnerability Scanner juga dapat mendeteksi dan melaporkan berbagai macam kerentanan dalam aplikasi yang dibangun pada arsitektur seperti WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails dan masih banyak lainnya. Acunetix Vulnerability Scanner membawa fitur-set yang luas dari kedua alat pengujian penetrasi otomatis dan manual, memungkinkan analis keamanan untuk melakukan penilaian kerentanan yang lengkap, dan melakukan perbaikan acaman yang terdeteksi dan memberikan laporan lengkap mengenai hasil dari scan secara jelas.

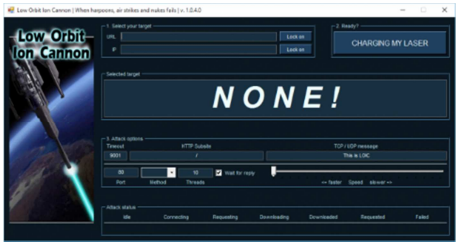


Gambar 1 : Tampilan Logo Whois

Gambar 2 : Logo Acunetix

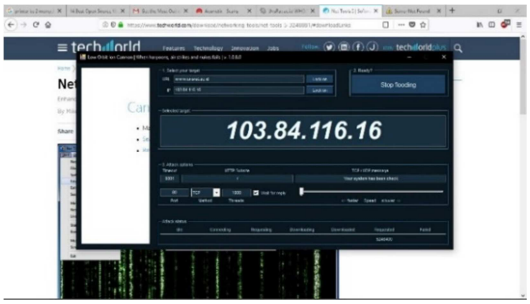


Gambar 3 : Logo Acunetix

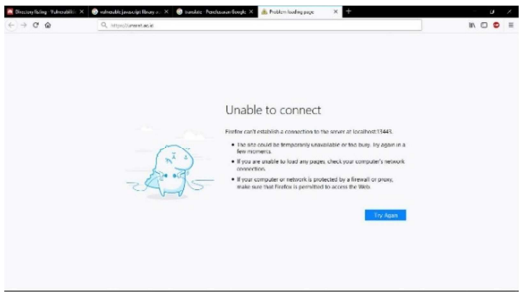


Gambar 4 : Tampilan Loic (Low Orbit Ion Canon)

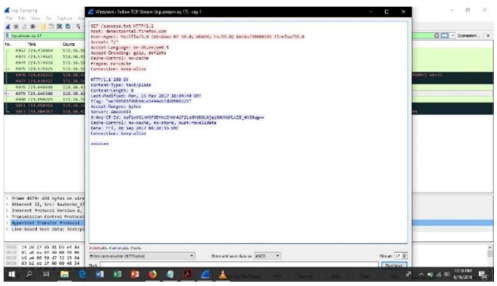
Gambar 5 : Logo Wireshark



Gambar 5: tampilan salah satu tools yang digunakan untuk melakukan DDOS



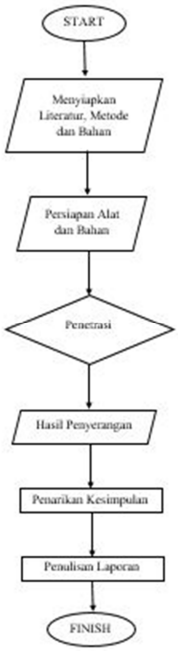
Gambar 6 : Web https://unsrat.ac.id/ gagal masuk akibat ddos



Gambar 7 : hasil uji coba wireshark tidak mendapatkan sesuatu

Tabel 1 : Rekapitulasi hasil pengujian

No	Jenis Serangan	Tools	Keterangan	Status
1	Port Scanner	*Acunetix web Vulnerability*	Mencarport yang terbuka	Berhasil
2	Deniel of Service (DoS)	LOIC (Low Orbit Ion Canon)	Melakukan Flooding	Berhasil
		HOIC (High Orbit Ion Canon)	Mengirimkan request untuk membanjiri server	Berhasil
		DoSHTTP 2.5	Membanjiri server	Gagal
3	Sniffing	Wireshark	Melakukan penyadapan antara 2 host	Gagal



Gambar 8 : table alur

A. Teknologi Acusensor
B. Industri yang paling canggih dan mendalam dalam SQL injection dan pengujian Cross site scripting.
C. Mendukung HTML5 penuh dengan Acunetix DeepScan Teknologi
D. Aplikasi scanning komprehensif baik untuk Halaman Single dan situs berbasis JavaScript
E. Mendukung Mobile web site
F. Dapat mendeteksi kerentanan Blind XSS dengan layanan AcuMonitor
G. Dapat mendeteksi otomatis kerentanan XSS berbasis DOM
H. Alat pengujian penetrasi Canggih, seperti HTTP Editor dan HTTP Fuzzer
I. Fasilitas pelaporan ekstensif termasuk laporan kepatuhan PCI
J. Multi-berulir dan petir scanner cepat merangkak ratusan ribu halaman dengan mudah.

3. LOIC (Low Orbit Ion Canon)

Low Orbit Ion Cannon (Loic) adalah open source network stress tools dan denial-of- service attack, yang ditulis dalam C #. Loic awalnya dikembangkan oleh Praetox Technologies, namun kemudian dilepaskan ke domain publik, dan sekarang di-host di beberapa platform open source

Serangan DDoS diluncurkan secara online dengan "toolkit" yang dirancang khusus untuk menyebabkan serangan semacam itu. Salah satu toolkit yang paling terkenal, versi awal, diberi nama berdasarkan meriam Ion, senjata fiktif dalam franchise permainan video yang dikenal sebagai Command & conquer, the Low Orbit Ion Cannon (LOIC) adalah pengujian tegangan jaringan sumber terbuka dan Aplikasi serangan DDOS yang digunakan oleh mesin klien untuk secara sukarela bergabung dengan botnet.

Serangan penolakan layanan terdistribusi mengacu pada banjir lalu lintas data yang diterima server saat beberapa sistem mengirimkan data dengan tujuan membanjiri bandwidthnya. Atau sumber daya. Dalam kebanyakan kasus, banjir data ini dimaksudkan untuk mengganggu penerimaan lalu lintas yang sah oleh server, 'menolak layanan' kepada klien yang mengirimkan permintaan ke server. Untuk pengguna akhir, ketika serangan DDOS tampak seperti penundaan permintaan layanan, di mana koneksi baru tidak lagi diterima.

LOIC telah bertanggung jawab atas beberapa serangan DDOS di situs web utama seperti PayPal, MasterCard dan Visa, biasanya Dilakukan oleh kelompok hacking seperti Anonymous. Aplikasi LOIC tersedia dalam dua versi: yang pertama adalah versi biner atau alat LOIC asli yang pada awalnya dikembangkan untuk jaringan uji stres dan LOIC berbasis web atau JS LOIC.

Aplikasi LOIC, yang pertama kali dikembangkan oleh Praetox Technologies, mengirimkan urutan besar permintaan HTTP, UDP atau TCP ke server Target. LOIC mudah digunakan bahkan oleh pengguna yang kurang memiliki kemampuan hacking dasar. Semua yang dibutuhkan adalah URL target. Untuk mengendalikan LOIC dari jarak jauh, beberapa hacker menghubungkan klien tersebut untuk meluncurkan serangan ke Relay Internet Chart menggunakan protokol IRC.

Dengan menggunakan protokol ini, mesin pengguna menjadi bagian dari botnet. Botnet adalah jaringan sistem komputer yang dikompromikan yang dikendalikan oleh malware atau virus dan mengirimkan banjir lalu lintas ke sistem target saat diminta.

LOIC DDOS menggunakan tiga jenis serangan terhadap mesin target. Ini termasuk HTTP, UDP dan TCP. Ini menerapkan mekanisme serangan yang sama yaitu membuka beberapa koneksi ke mesin target dan mengirim rangkaian pesan yang kontinyu ke mesin target. Alat LOIC terus mengirimkan lalu lintas ke server yang ditargetkan, sampai server kelebihan beban. Begitu server tidak dapat menanggapi permintaan pengguna yang sah, secara efektif akan dimatikan.

JS LOIC yang dirilis pada bulan Desember 2010 adalah alat berbasis web yang berjalan pada browser web JavaScript yang diaktifkan, maka akronim JS . LOIC mengirim sebuah ID dan pesan dengan banyak permintaan koneksi untuk setiap ID dan pesan. Alat serangan LOIC DDOS memudahkan untuk menemukan penyerang, dan akibatnya tidak umum digunakan oleh klien biasa. Di sisi lain, peretas dengan beberapa keterampilan dapat menggunakan jaringan IRC untuk meluncurkan serangan di dalam Tim sehingga sulit untuk mengidentifikasi orang-orang yang sebenarnya di balik serangan tersebut.

Alat serangan DDOS LOIC telah diunduh jutaan kali Karena mudah digunakan dan mudah dikenali.

Administrator jaringan dapat menggunakan firewall yang kuat untuk mencegah atau meminimalkan serangan. Administrator server kemudian dapat melihat log untuk mengidentifikasi IP yang mengirim lalu lintas dan memblokir IP dari server. Aturan firewall yang ditulis dengan baik dapat membentuk filter hebat dari LOIC DDOS yang mencegah serangan agar tidak sepenuhnya efektif.

Beberapa ahli mengklaim bahwa penyaringan UDP dan lalu lintas ICMP juga dapat menangani serangan LOIC secara efektif. Agar efektif di tingkat firewall, aturan harus diimplementasikan di awal link jaringan misalnya di operator situs ISP, di mana server terhubung ke tulang punggung melalui jalur broadband.

Penting juga untuk memeriksa Jalur broadband untuk memastikan tidak memiliki keterbatasan. Jika paket dikirim melalui bandwidth yang sempit maka penyumbatan pada jalur ini akan tetap terjadi sebelum lalu lintas bisa sampai ke firewall dan disaring.

LOIC Serangan DDOS dapat dikurangi dengan menggunakan dua dasar Pendekatan, kontrol heuristik atau tanda tangan. Kontrol tanda tangan menggunakan pola yang telah ditentukan untuk menyaring pola lalu lintas masuk yang sesuai dan menghilangkan serangan tersebut. Meskipun efektif untuk serangan berulang, ini menjadi masalah ketika pola serangan baru diluncurkan, dan akan terus menjadi masalah sampai tanda tangan diperbarui.

Di sisi lain sistem kontrol serangan DDOS heuristik membuat 'tebakan terdidik' Dari serangan yang akan datang dan tindakan untuk menghilangkan atau meminimalkan dampaknya.

Biasanya berdasarkan uji coba dan coba, metode ini memberikan solusi aproksimasi di mana kecepatan diperlukan untuk mencegah serangan DDOS . Tanda tangan heuristik karenanya dapat memberikan pendekatan real-time untuk masalah ini. Teknologi berpemilik lainnya mungkin termasuk interaksi manusia-komputer dengan menyediakan antarmuka pengguna, yang memungkinkan administrator sistem mendapatkan peringatan saat tanda tangan heuristik terdeteksi.

4. Wireshark

Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkin kan kita untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia dan merupakan kelanjutan dari proyek yang dimulai oleh Gerald Combs pada tahun 1998.wireshark di buat dengan bahasa C, C+

A. Pemeriksaan mendalam dari ratusan protokol, dengan lebih banyak yang ditambahkan setiap saat
B. Pengambilan langsung dan analisis offline
C. Browser paket tiga-panel standar
D. Multi-platform: Berjalan di Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, dan banyak lainnya
E. Data jaringan yang diambil dapat diakses melalui GUI, atau melalui utilitas TShark TTY-mode
F. Filter tampilan paling kuat di industri
G. Analisis VoIP yang kaya
H. Baca / tulis berbagai format file tangkapan yang berbeda: tcpdump
I. (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Monitor
J. Jaringan Microsoft, Jaringan Umum Sniffer® (terkompresi dan tidak
K. terkompresi), Sniffer® Pro, dan NetXray®, Pengamat Instrumen Jaringan ,NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN Analyzer, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek, dan banyak lainnya
L. File tangkap yang dikompresi dengan gzip dapat didekompresi dengan cepat
M. Data langsung dapat dibaca dari Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, dan lainnya (tergantung pada platform Anda)
N. Dukungan dekripsi untuk banyak protokol, termasuk IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP, dan WPA / WPA2
O. Aturan mewarnai dapat diterapkan pada daftar paket untuk analisis cepat dan intuitif
P. Output dapat diekspor ke XML, PostScript, CSV, atau teks biasa

III. HASIL DAN PEMBAHASAN

Rekapitulasi hasil penelitian ini merupakan hasil dari analisa dan pembahasan peneliti selama melakukan ujicoba dalam lingkup jaringan Wifi Unsrat lihat table 1.

1. Solusi *Testing Acunetix Web Vulnerability Scanner*

Berikut merupakan table uraian celah kemanan yang terbuka pada hasil *Testing Acunetix Web Vulnerability Scanner* beserta dampak beserta solusinya. Dalam mencari hasi celah keamanan yang ditemukan dalam hasil scan terdapat ancaman yang didapat dalam tengkatan level yang ada dalam aplikasi *Acunetix Web Vulnerability Scanner* celah yang ditemukan selain tertulis dalam kotak juga terdapat warna yang menunjukkan tingkat ancaman celah keamanan dengan warna dan serta jumlah nilai ancaman dalam bentuk angka

Hijau (informasi), dengan jumlah nilai 99+
Biru (ancaman terendah) , dengan jumlah nilai 1
Orange (ancaman menengah) dengan jumlah nilai 41
Merah (ancaman bahaya) dengan jumlah nilai 0

Adapun hasil celah keamanan yang didapat dari hasil scan Aplikasi *Acunetix Web Vulnerability Scanner* yaitu : Email address found

Dari hasil celah keamanan ini, ditemukan satu atau lebih alamat email di website https://Unsrat.ac.id/ bisa terlihat. Yang bisa memunculkan Spam-Bots yang

Mayoritas spam berasal dari alamat email yang diambil dari internet. Dan bisa menjadi celah untuk merekam alamat email yang terlihat.

1. Documentation file

   Pada direktori ini dari hasil scan acunetix ditemukan file dokumentasi . dari file dokumentasi ini pula dapat digunakan oleh penyerang untuk mengidentifikasi aplikasi web yang digunakan dalam hal ini terdapat di https://Unsrat.ac.id/

   /Script/PerFolder/Readme_Files.script

2. Application error message

     pada Lansiran ini memerlukan konfirmasi manual </ span> </ div>
 Kesalahan aplikasi atau pesan peringatan dapat mengekspos informasi sensitif tentang internal aplikasi bekerja untuk penyerang.

 Acunetix menemukan pesan kesalahan atau peringatan yang dapat memperlihatkan informasi sensitif. Pesan itu juga dapat berisi lokasi file yang menghasilkan permasalahan yang tidak tertangani.

   /script/Perscheme/Error_Message.script

3. Directory Listing

   Server web dikonfigurasi untuk menampilkan daftar file yang ada di direktori ini. Ini tidak disarankan karena direktori mungkin berisi file yang biasanya tidak terpapar melalui tautan di situs web ini

4. HTML form without CSRF protection

     Lansiran ini memerlukan konfirmasi manual </ span> </ div>
 Pemintaan Permintaan Lintas-Situs (CSRF, atau XSRF) adalah kerentanan di mana penyerang dapat menipu korban untuk membuat permintaan yang tidak diinginkan korban. Oleh karena itu, dengan CSRF, penyerang menyalahgunakan kepercayaan yang dimiliki suatu aplikasi web dengan browser korban.

 Acunetix menemukan bentuk HTML tanpa perlindungan anti-CSRF yang jelas diterapkan. Lihat bagian 'Detail serangan' untuk informasi lebih lanjut tentang formulir HTML yang terpengaruh.

5. Vulnerable Javascript library

   digunakan pustaka javascript yang rentan. satu atau lebih kerentanan dilaporkan versi pustaka javascript ini. periksalah rincian serangan dan referensi web untuk informasi lebih lanjut tentang libarari yang terkena dampak dan kerentanan yang dilaporkan

5. Hasil uji DDOS

Dari hasil percobaan pengujian *flooding* selama kurang lebih 7 jam dengan menggunakan beberapa tools DDOS peneliti berhasil melumpuhkan sementara waktu akses untuk masuk dalam website https://unsrat.ac.id/ sehingga proses masuk user dalam memasuki web tersebut terganggu seperti terlihat pada gambari ini dimana peneliti menggunakan komputur yang berbeda untuk membuka website tetapi tidak bisa dilakukan

Dari masalah yang terdapat pada acuntix peneliti mencoba menggalai informasi penting yang terdapat pada website https://unsrat.ac.id/ dengan melakukan metode sniffing yang bertujuan untuk menyadap aktifitas yang dilakukan, dan peneliti menggarapkan bisa mndapatkan sesuatu yang penting dan melakukan scanning sniffing menggunakan tools wireshark tapi. Setelah mendapat hasil peneliti mencoba menggali apa yang ditemukan dalam hal ini peneliti mengharapkan mendapat password yang terekam seperti yang disimulasikan tapi tidak menedapat apapun hanya didapat report biasa dalam wireshark seperti terlihat pada gambar di bawah ini.

Makadari hasil ini bisa dipastikan pihak Unsrat menggunakan semacam alat anti penyadapan / tools untuk menghalau aktifitas penyadapan / sniffing untuk menjaga keamanan data dan user

IV. PENUTUP

1. Kesimpulan

Berdasarkan hasil penelitian serta pembahasan yang telah diuraikan pada bab sebelumnya, dalam penelitian yang berjudul Analisa Keamanan Jaringan Wireless di Unsrat maka dapat disimpulakan bahwa :

Bahwa keamanan jaringan dan website Unsrat belum sepenuhnya dapat dikatakan aman, walaupun masih dikatakan belum aman tetapi tingkat ancaman yang ditunjukkan hanya berada di level 2 dan tidak mendapatkan tingkat keamanan pada level high pada web alert akan tetapi jaringan unsrat masih bisa terkena *Flooding* dan metode penyerangan DDOS masih bisa dilakukan. Sedangkan pada *level Medium* yang mengandung informasi sensitif, dan sehingga keamanan website Unsrat berhasil dan dapat penetrasi dan *server* terganggu.

2. Saran

Berikut beberapa saran yang dapat peneliti berikan setelah melakukan
penelitian ini :

1. Periksa referensi dengan detail tentang cara mengatasi masalah Alamat email yang diposting di situs web agar tidak tertumpuk menjadi spam.
2. Hapus atau batasi akses ke semua file dokumentasi yang dapat diakses dari internet agar bira ada data penting tidak langsung dapat diakses public.
3. Verifikasi pada halaman Application error message. Tamampilkan pesan atau peringatan dan konfigurasikan aplikasi dengan benar untuk mencatat kesalahan ke file dalam hal menampilkan kepada pengguna.
4. Harus memastikan direktori tidak mengandung informasi sensitif atau Anda mungkin ingin membatasi daftar direktori dari konfigurasi server web.

Verifikasi apakah formulir ini memerlukan perlindungan anti CSRF dan implementasikan tindakan CSRF jika diperlukan

DAFTAR PUSTAKA

[1] Nugroho, Bayu. 2012 Analisa Keamanan Jaringan Pada Fasilitas Internet (wifi) terhadap serangan packet sniffing : Tugas Akhir Universitas Muhammadiyah Surakarta.
[2] Arikunto, Suharsimi. 2006. Prosedur Penelitian. Jakarta: Rineka Cipta.
[3] Zuriah, Nurul. 2003. Penelitian Tindakan Dalam Bidang Pendidikan dan Sosial. Malang: Bayumedia.
[4] Davison, R.M., Martinsons, M.G., & Kock N. 2004. Jurnal: *Information Systems* dan *Principles of Canonical Action Research*.
[5] Hidayat, Nurman. 2011 *Hacking* Jaringan *Lan* Menggunakan Metode Sniffing : Tugas Akhir Universitas Sumatera Utara, Medan.
[6] Pasaribu, Try. 2014 Monitoring dan identifikasi paket *data protokol HTTP dan sniffing password* menggunakan *wireshark.* Tugas akhir : Politeknik Negeri Medan

Sekilas dari penulis dengan Nama lengkap Abraham Yano Suharmanto, anak tunggal dari pasangan suami isteri ayah Tarcisius Suharmanto dan ibu Meiske Sangi. Lahir di Kota Manado, Provinsi Sulawesi Utara pada tanggal 29 Mei 1992. Dengan alamat tempat tinggal sekarang di Kelurahan Kolongan 1, Kecamatan Tomohon Tengah, Kota Tomohon. Mulai menempuh pendidikan di sekolah dasar GMIM 6 Tomohon dan setelah naik ke kelas 4 SD pindah sekolah ke SD Katolik Santa Clara Tomohon. Setelah itu melanjutkan pendidikan di Sekolah Menengah tingkat Pertama Negeri 1 Tomohon. Selanjutnya menempuh pendidikan Ke Sekolah Menengah Atas Negeri 1 Tomohon dan selesai studi SMA pada tahun 2010. Lalu Setelah lulus belum langsung masuk ke perguruan tinggi, Nanti di Tahun 2011 saya melanjukan pendidikan ke salah satu perguruan tinggi yang berada di kota Manado yaitu Universitas Sam Ratulangi, dengan mengambil Program Studi S-1 Teknik Informatika di Jurusan Elektro, Fakultas Teknik. Penulis membuat Penelitian demi memenuhi syarat memperoleh gelar S1 Sarjana Komputer dengan penelitian berjudul Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi, yang dibimbing oleh dua dosen pembimbing yaitu Arie S.M. Lumenta, ST., MT. dan Xaverius B.N. Najoan, ST., MT pada tanggal 25 September 2018 penulis selesai melaksanakan pendidikan di Fakultas Teknik Universitas Sam Ratulangi, Jurusan Teknik Elektro, Progam Studi Teknik Informatika