ANALISIS KEBUTUHAN KEAMANAN INFORMASI MENGGUNAKAN METODE SQUARE PADA APLIKASI HUMAN RESOURCES INFORMATION SYSTEM (HRIS) STUDI KASUS PT. PERKEBUNAN NUSANTARA V AMO-II SEI LALA

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau

DISUSUN OLEH :

MUHAMAD ILHAN
163510341

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2020

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, serta kita hadiahkan shalawat kepada junjungan kita Nabi Muhammad SAW sehingga penulis dapat menyelesaikan proposal penelitian ini untuk menyelesaikan program studi strata 1 (S1) pada jurusan Teknik Informatika UNIVERSITAS ISLAM RIAU dengan judul "Analisis Kebutuhan Keamanan Informasi Menggunakan Metode SQUARE Pada Aplikasi Human Resources Information System (HRIS) Studi Kasus PT.Perkebunan Nusantara V AMO-II Sei Lala"

Penulis menyadari bahwa dalam penelitian ini masih terdapat kesalahan dan kekurangan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran dari para pembaca sehingga pada penelitian yang akan datang akan lebih baik dari penelitian ini. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Prof, Dr. H. Syarinaldi, S.H.,M.C.L selaku Rektor Universitas Islam Riau.
2. Bapak Dr. Eng Muslim, ST, MT selaku Dekan Fakultas Teknik Universitas Islam Riau
3. Ibu Dr. Mursyidah, M.Sc selaku Wakil Dekan I Fakultas Teknik
4. Bapak Dr. Anas Puri, ST., MT selaku Wakil Dekan II Fakultas Teknik

5. Bapak Akmar Efendi, S.Kom. M.Kom selaku Wakil Dekan III Fakultas Teknik sekaligus Pembimbing Akademik penulis yang selalu memberikan motivasi, serta arahan dan dukungan kepada penulis selama proses perkuliahan
6. Bapak Dr. Arbi Haza Nasution, B. IT (Hons)., M. IT selaku Ketua Program Studi Teknik Informatika Universitas Islam Riau
7. Bapak Yudhi Arta, ST., M.Kom selaku Pembimbing Skripsi yang selalu memberikan dukungan, motivasi dan memberikan arahan serta saran agar penulis dapat menyelesaikan skripsi dengan baik dan memberikan kelancaran bagi penulis untuk menyelesaikan skripsi ini.
8. Ibu Ana Yulinti, ST., M.Kom selaku Sekretaris Ketua Program Studi
9. Segenap Dosen Program Studi Teknik Informatika Universitas Islam Riau yang telah membrikan ilmu yang begitu berharga, membimbing, mendidik, dan membrikan kesempatan kepada penulis untuk dapat belajar
10. Segenap pengurus Tata Usaha Fakultas Teknik Universitas Islam Riau beserta Staff yang telah banyak membantu dalam berbagai urusan administrasi selama proses penyelesaian skripsi
11. Teruntuk yang teristimewah Orang Tua yang selalu memberikan dukungan, motivasi yang luar biasa, dan kasih sayang yang tak henti-hentinya diberikan kepada penulis untuk dapat menyelesaikan sripsi ini dengan baik. Terimakasih untuk do'a yang selalu di panjatkan disetiap shalat, terimakasih telah menjadi pendengar yang baik disaat penulis sedang merasa lelah, kehilangan arah, orang

tua selalu menjadi alasan penulis untuk kembali semangat menyelesaikan skripsi ini.

12. Terimakasih untuk Partner terbaik Mega Purnamawati Firdaos S.Psi yang selalu memberikan semangat dan motivasi kepada penulis untuk dapat menyelesaikan skripsi ini dengan sebaik-baiknya
13. Terimakasih untuk seluruh keluarga besar yang selalu memberikan do'a dan kasih sayang kepada penulis
14. Untuk seluruh teman-teman yang tidak dapat disebutkan satu-persatu penulis ucapkan terimakasih karena telah bersama-sama belajar dibangku perkuliahan, memberikan candatawa setiap harinya, semoga apa yang telah kita perjuangkan dapat membuahkan hasil yang baik. Skripsi ini mungkin masih banyak kekurangan dan jauh dari kata sempurna, semoga kekurangan dalam skripsi ini dapat menjadikan masukan dan pertimbangan bagi penulis lain agar dapat menjadi referensi penulis karya ilmiah selanjutnya.

Pekanbaru, 16 Desember 2020

Penulis

Muhammad Ilhan

DAFTAR ISI

Hal

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

ABSTRAK

Keamanan dalam suatu sistem tentunya sangat dibutuhkan untuk menjaga integritas data penting yang tersimpan dalam sistem tersebut. Oleh sebab itu untuk menjaga integritas data ini bermula setelah sistem tersebut terkoneksi dengan jaringan internet. Dalam penelitian ini hanya menggunakan mrtode SQUARE yang akan di gunakan untuk mencari celah kemanan sistem. Dengan adanya masalah keamanan maka penggunaan metode SQUARE dapat mengetahui celah keamanan sistem dan melihat seberapa aman sistem terhadap serangan yang kemungkinan terjadi dan memberikan rekomendasi yang dapat mengatasi kelemahan sistem dengan melakukan pengujian dan melakukan beberapa observasi terhadap sistem. Hasil dalam analisis yang telah di lakukan sebelumnya dengan metode SQUARE, sangat membantu dalam menganalisa dan mengetahui celah atau kelemahan sistem yang dapat merusak sistem sekaligus memberikan rekomendasi terhadap kebutuhan keamanan sistem yang bertujuan untuk menjaga availibilitas dan kerahasiaan serta integritas sistem.

Kata Kunci : *Human Resources Information System* (HRIS), Keamanan, SQUARE.

.

ABSTRACT

Security in a system is certainly needed to maintain the integrity of important data stored in the system. Therefore, to maintain security in a system is certainly needed to maintain the integrity of important data stored in the system. Therefore, to maintain the integrity of this data begins after the system is connected to the internet network. In this study only use SQUARE mrtode that will be used to find system security gaps. With security issues, the use of SQUARE method can find out system security gaps and see how secure the system is against possible attacks and provide recommendations that can overcome system weaknesses by testing and conducting several observations on the system. The results in the analysis that has been done before with SQUARE method, is very helpful in analyzing and knowing the gaps or weaknesses of the system that can damage the system while providing recommendations on the security needs of the system aimed at maintaining the availability and confidentiality and integrity of the system.

Keywords: Human Resources Information System (HRIS), Security, SQUARE.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan sebuah sistem tentunya sangat diperlukan untuk menjaga integritas data yang tersimpan dalam sistem tersebut. Tantangan untuk menjaga integritas data ini bermula setelah sistem terkoneksi dengan jaringan komputer yang terhubung ke internet. Integritas data ini digunakan oleh dua perspektif yaitu penyelenggara dan pengguna. Salah satu sistem yang digunakan yaitu sistem Human Resources Information System (HRIS) atau sistem data karyawan pada perusahaan PT. Perkebunan Nusantara V.

Keamanan dalam sistem Human Resources Information System (HRIS) tentunya bersesuaian dengan informasi dasar yang harus dipenuhi suatu sistem keamanan dalam web application. Semisal kemungkinan pemalsuan data yang dilakukan oleh orang luar ataupun karyawan untuk memasuki sistem yang ada. Hal ini bersesuaian dengan informasi keamanan CIA (*Confidentiality, Integrity and Availability*) dan authentification. CIA (*Confidentiality, Integrity and Availability*) merupakan prinsip dasar keamanan informasi, Ketika ingin membangun sebuah sistem yang aman, maka CIA yang dijadikan sebagai acuan yang harus di capai dan di lindungi, misalnya akses bagi pengguna yang berperan sebagai admin harus berbeda dengan seorang user, oleh karena itu harus ada

langkah pengamanan untuk hal tersebut, sehingga tidak ada pengguna yang dapat memalsukan informasi yang tersimpan pada sistem, sedangkan *Authentication* merupakan Tindakan mengkonfirmasi kebenaran suatu bagian dari sebuah data user yang telah tersimpan.

Integritas dan keamanan data dalam sistem harus dijaga, sehingga membantu mengurangi risiko data tidak dipalsukan sehingga keasliannya tetap terjaga, kecuali data yang fleksibel untuk dimodifikasi. Sistem yang dapat diakses di mana saja juga harus diperhatikan, sehingga ketersediaan sistem dapat terpenuhi. Dengan sistem yang terhubung ke jaringan internet, kemungkinan mengubah atau merusak data akan semakin besar, karena pengguna yang berpotensi berbahaya akan dengan mudah memasuki sistem melalui jaringan internet.

Penulis menerapkan analisis keamanan aplikasi Sistem HRIS, yang menyimpulkan bahwa untuk mencegah serangan terhadap Sistem Informasi HRIS, diperlukan langkah-langkah pengendalian akses di dalam sistem. Namun, ada beberapa teknologi kontrol akses yang tidak efektif dalam mencegah serangan eksternal karena ada celah keamanan ketika serangan dapat dilakukan di dalam sistem oleh pengguna internal dan pengguna di luar sistem. Oleh karena itu diperlukan keamanan informasi yang tepat untuk memastikan keamanan sistem HRIS sehingga penulis fokus pada penggunaan metode menggunakan metode SQUARE.

1.2 Masalah Penelitian

Masalah yang terdapat pada penelitian ini yaitu keamanan pada sistem Human Resouces Information System (HRIS) karena sistem tersebut tidak memiliki keamanan yang cukup yang dapat menjaga integritas data yang sangat penting, oleh karena itu keamanan pada sistem HRIS tersebut sangat rentan terhadap manipulasi maupun tindak kejahatan lainnya oleh orang yang tidak bertanggung jawab. Maka dilakukan Analisis sebuah kebutuhan keamanan informasi dalam sebuah sistem dengan metode SQUARE untuk mengetahui tingkat ancaman dan celah yang dapat meruskan dan merugikan perusahaan.

1.2.1 Identifikasi Masalah

Berdasarkan latar belakang masalah di atas, maka dapat diidentifikasikan masalah sebagai berikut:

1. Perusahaan memerlukan sebuah analisis kebutuhan terhadap keamanan sebuah sistem, jaringan maupun sebuah data karyawan yang sangat penting. Dan sistem tersebut sangat rentan terhadap serangan atau orang yang tidak bertanggung jawab yang dapat mengakibatkan pencurian data, manipulasi data bahkan penyerangan melalui jaringan internet yang terkoneksi ke Sistem HRIS tersebut.
2. Kurangnya metode keamanan sistem informasi di perusahaan PT. Perkebunan Nusantara V AMO-II Sei Lala yang dapat hilang dan

keamanan identitas yang sangat minim akan Beresiko terkena ancaman pencurian, perusakan sistem dan manipulasi data yang dapat merugikan perusahaan.

1.2.2 Ruang Lingkup Masalah

Penulisan Penelitian di batasi pada ruang lingkup di bawah ini :

1. Analisis kebutuhan keamanan informasi pada sistem Human Resources Information System (HRIS).
2. Impelementasi keamanan informasi sesuai standar ISO 27001 yang di terapkan pada perusahaan PT. Perkebunan Nusantara V
3. Evaluasi Keamanan pada suatu sistem Human Resouces Information System (HRIS)

1.2.3 Rumusan Masalah

Berdasarkan latar belakang di atas, adapun rumusan masalah dalam tugas akhir ini yaitu :

1. Bagaimana membuat analisis kebutuhan sistem keamanan pada aplikasi Human Resources Information System (HRIS)?
2. Bagaimana metode SQUARE dapat menganalisis sebuah kebutuhan keamanan pada sistem Human Resources Information System (HRIS) ?
3. Bagaimana hasil dari sebuah analisis kebutuhan keamanan sistem HRIS dengan menggunakan Metode SQUARE?

1.3 Tujuan dan Manfaat Penelitian

Adapun tujuan dan manfaat pada penelitian ini yaitu:

A. Tujuan Penelitian

1. Melakukan penilaian pada persyaratan keamanan menggunakan metode SQUARE.agar dapat mengetahui ancaman apa saja yang dapat mengganggu proses aplikasi dari segi keamanan yang dijalankan agar dapat ditanggulangi secara tepat.
2. Menganalisa kebutuhan keamanan sistem dari segi kerentanan informasi penting karyawan.

B. Manfaat Penelitian

1. Meningkatkan keamanan sistem pada informasi penting dan biodata karyawan khususnya.
2. Membantu karyawan dan perusahaan dalam memahami konsep eksperimental atau konsep memahami sebab akibat dalan sebuah sistem aplikasi.
3. Mendapatkan sebuah hasil analisa keamanan sehingga di jadikan antisipasi terhadap sistem yang akan di buat.

BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Untuk menyusun laporan skripsi ini, penulis juga menggunakan acuan kepustakaan yang bersumber pada penelitian sebelumnya. Hal ini berguna sebagai perbandingan dan bahan referensi bagi penulis. Pada penelitan ini, penulis mengambil referensi berdasarkan penelitian yang di lakukan oleh Muhammad Agreindra Helmiawan, (2018) dengan judul "Analisis Keamanan Sistem Informasi E-Learning Menggunakan Metode Squre". Pada penelitian ini di jelaskan secara detail bagaimana evaluasi menganalisa keamanan sistem yang gunakan oleh admin dengan cermat, sehingga perusahaan tidak lagi harus khawatir akan kehilangan data akibat orang yang tidak bertanggung jawab.

Dimuat dalam jurnal Umar et al., (2019) bahwa "Tujuan penerapan sistem keamanan informasi adalah untuk mengatasi segala kendala baik secara teknis maupun secara non-teknis yang dapat berpengaruh dalam kinerja sistem. Keamanan informasi adalah suatu keharusan dimana keamanan di maksudkan menjaga sistem dari ancaman berupa serangan sistem. Keamanan di angap penting karena jika informasi tersebut dapat diakses oleh orang yang tidak bertanggung jawab, maka akurasi informasi akan meragukan sehingga tidak lagi dapat di percaya informasinya. Adanya masalah keamanan memicu prosedur untuk

mengendalikan hak akses pada sebuah sistem informasi. Kualitas data informasi yang baik memnimbulkan pengaruh yang penting dalam pelayanan, produk, operasional dan keputusan bisnis sehingga diharapkan kualitas data dan informasi dapat di nilai tingkat objektifitasnya Penelitian ini bertujuan untuk melakukan evaluasi terkait keamanan sistem informasi yang telah diimplementasikan pada sebuah institusi untuk mendapatkan nilai maturity level keamanan sistem informasi dari sebuah institusi.

Keamanan sistem informasi merupakan salah satu topik dalam perkembangan teknologi informasi dan komunikasi di era digitalisasi. Untuk menyelesaikan masalah keamanan dibutuhkan penerapan metode yang menjamin keamanan data, transaksi, dan komunikasi (Martsanto & Nabihi, 2016)

Dari hasil penelitian sebuah jurnal tersebut maka penulis dapat simpulkan bahwa hasil Analisa sistem dengan metode SQUARE dapat digunakan sebagai metode analisis dan pengujian keamanan sebuah sistem dan dapat mengatui bagian atau celah keamanan yang dapat di masuki oleh pengguna berbahaya serta sangat membantu dalam melakukan analisis yang memberikan rekomendasi terhadap kebutuhan keamanan sistem untuk menjaga availibilitas, conidentility dan integritas sistem HRIS yang akan penulis buat.

2.2 Landasan Teori

2.2.1 Definisi Metode SQUARE

Metode *System Quality Requirements Engineering* (SQUARE) adalah proses sembilan langkah yang dirancang untuk menganalisis informasi tentang kebutuhan keamanan. Dikembangkan oleh Carnegie Mellon Institute of Software Engineering, metode ini menawarkan penerimaan industri yang efisien dalam pengembangan perangkat lunak dan aplikasi sistem yang aman. Saat mengevaluasi dokumen dengan persyaratan teknis perangkat lunak, seringkali ada bagian terpisah tentang persyaratan keamanan umum.

Persyaratan yang didokumentasikan biasanya umum, seperti perlindungan kata sandi, firewall, deteksi virus, dan semacamnya. Persyaratan untuk ekstraksi dan analisis sangat jarang. Bahkan jika itu ada, dari sepuluh persyaratan yang dikembangkan secara terpisah dari sisa kegiatan teknik dan tidak terintegrasi dengan kegiatan. Akibatnya, persyaratan keamanan yang melekat dalam melindungi layanan dan aset sering dilupakan. kerentanan besar perusahaan besar terletak pada sistem aplikasi.

Pada era teknologi yang begitu pesat ini penulis mengambil referensi berdasarkan metodologi SQUARE. Untuk mengetahui masalah penyalahgunaan maka dilakukan pembagian kategori ancaman. Berikut ini merupakan pengkategorian ancaman yang terjadi sebagai berikut :

1. SQL Injection
2. Data Sniffing
3. Mac Address Spooffing
4. Spyware dan Trojans
5. Denial of Services

Tabel 2.1 Kategori Ancaman

No	Kategori Ancaman	Kondisi	Dampak
1	SQL Injection	Melakukan acak login pada menu login klien	Kehilangan data pengguna dan password pengguna yang legal
2	Data Sniffing	Melakukan pengintipan lalulintas jaringan	Penyerang dapat melihat dengan jelas dan mengetahui aktifitas data di sistem.
3	Mac Address Spooffing	Mengambil IP Address yang ada di dalam jaringan untuk di palsukan	Penyerang dapat mengambil informasi yang tersedia pada pengguna legal
4	Spyware dan Trojans	Melakukan perusakan, pencurian aktifitas sebuah computer	Dapat melihat aktivitas admin, mengendalikan komputer serta dapat mencurri data user
5	Denial of Serices	Mengirim data dalam jumlah banyak terhadap server agar server mengalami kerusakan.	Membuat jaringan menjadi padat sehingga komputer tidak menanggapi permintaan layanan

Metode SQUARE adalah metode yang paling tepat dengan perbandingan Metode Lain untuk melukan Analisis dengan perbandingan yaitu:

1. Anggaran dan waktu sangat murah dan cepat

2. Cakupan analisis yang sangat luas menggunakan Sembilan proses
3. Memiliki akurasi yang tepat.

Salah satu sumber masalah adalah persyaratan kualitas yang diungkapkan atau dianalisis dengan buruk, seperti keamanan dan privasi. Cacat rekayasa persyaratan membutuhkan biaya 10 hingga 200 kali lebih banyak untuk diperbaiki selama penerapan daripada jika terdeteksi selama pengembangan persyaratan. Selain itu, sulit dan mahal untuk meningkatkan keamanan aplikasi secara signifikan setelah berada dalam lingkungan operasionalnya.

Perbandingan pada metode lain yaitu ada berupa metode PENTEST, tetapi pada metode ini hanya mengevaluasi dan mengindentifikasi kelemahannya saja. Begitu juga pada metode Suricata yaitu hanya memecahkan maslakah tanpa memberikan rekomendasi atau solusi, dan ada juga metode Brute Force yaitu hanya menguji coba keamanan password. Maka metode yang tepat masih berada pada metode SQUARE yang mencari celah serta memberikan rekomendasi nya.

Dari sebuah keunggulan metode tersebut maka Security Quality Requirements Engineering (SQUARE) adalah proses sembilan langkah tepat yang membantu perusahaan membangun keamanan, termasuk privasi, ke dalam tahap awal siklus produksi. Bahan ajar tersedia untuk diunduh yang dapat digunakan untuk mengajarkan metode SQUARE.

Dimuat dalam jurnal Akbar, (2015) Security Quality Requirements Engineering (SQUARE) adalah merupakan sebuah model yang dikembangkan untuk memprediksi proses persyaratan. SQUARE merupakan langkah untuk mengkategorikan persyaratan keamanan yang utamakan pada sarana dan infrastruktur teknologi informasi, banyak metode yang dapat dijelaskan dengan menggunakan metode SQUARE yaitu kaitannya dengan kasus penyalahgunaan dalam sistem

2.2.2 Definisi CIA (*Confidentiality, Integrity, Availability*)

Keamanan Informasi dibangun atas tiga kunci dasar dari prinsip kunci dasar keamaan informasi yaitu *confidentiality* (kerahasiaan), *Integrity* (integritas) dan *Availability* (ketersediaan).

A. Confidentility

Merupakan keamanan informasi yang menjamin, memastikan dan menjaga kerahasiaan aset, bahwa hanya dapat diakses oleh mereka yang memiliki wewenang (Apriandari & Sasongko, 2018).

B. Integrity

Merupakan keamanan informasi yang menjaminkelengkapan aset, menjamin asset ersebut tidak berubah dan dimodifikasi maupun dihilangkan tanpa otorisasi yang tidak jelas. Menjaga keakuratan dan ancaman dari pihak luar yang tidak berkepentingan (Apriandari & Sasongko, 2018)

C. Availability

Merupakan keamanan informasiyang menjamin bahwa aet tetap tersedia, dapat diakses ketika dibutuhkan tanpa adanya gangguan dari pihak lain (Apriandari & Sasongko, 2018)

2.2.3 ISO 27001

ISO 27001 adalah standar manajemen keamanan informasi yang digunakan oleh bisnis dan organisasi untuk menjaga keamanan informasi di seluruh dunia, ISO 27001 juga didefinisikan sebagai sistem manajemen keamanan informasi (ISMS), yang memberikan gambaran tentang apa yang perlu dilakukan lembaga untuk menilai, mengimplementasikan, dan memelihara keamanan informasi. ISO 27001 berfokus pada pengurangan risiko informasi yang penting bagi organisasi (Ramadhani et al., 2018)

2.2.4 Pengertian Keamanan Infomasi Sistem

Keamanan sistem informasi merupakan salah satu topik dalam perkembangan teknologi informasi di era digitalisasi. Untuk memecahkan masalah keamanan maka dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi. Keamanan informasi dapat dicapai dengan menerapkan seperangkat kontrol yang sesuai. Kontrol ini perlu ditetapkan, diterapkan, dimonitor, direview, ditingkatkan dimana yang perlu untuk

memastikan bahwa tujuan bisnis dan keamanan yang spesfifik bagi organisasi dipenuhi. Penerapan keamanan informasi ditujukan untuk mengatasi masalah teknis dan non-teknis seperti faktor aksesibilitas, kerahasiaan dan integritas sehingga tingkat keamanan informasi dapat dinilai. Keamanan data adalah perlindungan karakteristik informasi (confidentiality, integrity, dan availability) baik itu dalam memperoses informasi, menyimpan maupun mengirimkanya untuk menjaga keberlangsungan dan memperluas kesempatan bisnis (Umar et al., 2019).

2.2.5 Definisi Sistem Human Resources Information System (HRIS)

Human Resources Information System(HRIS) Adalah sistem untuk mengelola kegiatan personel menggunakan sistem yang dinetralisir. Ini termasuk data gaji, pembayaran, biodata karyawan, proses rekrutmen, kehadiran dan cuti, dan tinjauan kinerja karyawan (Ambo & Ghufron, 2015).

Aplikasi yang memungkinkan admin mudah menginput data mengenai biodata karyaawan di aplikasi HRIS tersebut. Dengan mengakses aplikasi HRIS admin bisa melihat dan menginput biodata karyawan yang bekerja di PT. Perkebunan Nusantara V Sei Lala tersebut. Ketika admin ingin menambah karyawan atau mengubah data karyawan, admin PTPN V Sei Lala harus melakukan login terlebih dahulu, ini bermaksud untuk memudahkan proses penginputan. ketika admin berhasil login maka akan dapat melihat segala informasi tentang karyawan dari semua informasi PT PN V Sei Lala mulai dari mencari data karyawana melalui NRK yang bekerja di perusahaan tersebut.

Dengan aplikasi yang di usulkan ini maka dapat mempermudah admin dalam mencari dan melihat serta mengubah data karyawan.

Aplikasi HRIS PTPN V Sei lala yang memungkinkan admin mudah menginput data mengenai biodata karyawan di aplikasi HRIS tersebut. Dengan mengakses aplikasi HRIS maka dapat melihat dan menginput biodata karyawan yang bekerja di PT. Perkebunan Nusantara V Sei Lala tersebut. Aplikasi ini bermaksud untuk memudahkan proses penginputan. Dengan aplikasi ini maka dapat mempermudah admin dalam mencari dan melihat serta mengubah data karyawan sesuai fungsi nya yaitu mengelola informasi yang ada di PT tersebut.

Gambar 2.1 Sistem HRIS PTPN V

Dengan HRIS, para pimpinan bisnis memiliki akses ke berbagai data karyawan, seperti data pribadi, pekerjaan, penggajian, dan banyak lagi. manajer

juga dapat membatasi pengguna sistem ini informasi apa yang dapat dilihat dan diakses oleh karyawan. Salah satu modul dalam sistem ERP yang juga dapat diintegrasikan dengan beberapa modul lain yang dibutuhkan perusahaan. seperti HRIS, sistem ERP tersedia dalam berbagai jenis solusi, yaitu perangkat lunak desktop.

2.2.6 Pengertian Password Attack

Password Attack adalah proses serangan yang mendapatkan kata sandi dari jaringan. Kata sandi adalah kata sandi untuk membuka kunci sistem yang terkunci, seperti transaksi online dalam sistem, ATM, dll., Bahkan sistem online di perusahaan sangat berbahaya kecuali mereka dilengkapi dengan perangkat lunak keamanan seperti SSL (Martsanto & Nabihi, 2016)

2.2.7 Pengertian Dread

Dread Model ialah untuk menghitung resiko berdasarkan jenisnya, Tujuan dari Dread model adalah menggambarkan area resiko bisnis yang di ketahui dengan kelangsungan dari sebuah penyerangan, penyerangan dari model ancaman dapat di katarogrikan sebagai berikut :

1. Demage Potential (Potensial kerusakan) : Bagaimana luas kerusakan dari terbukanya sebuah kerentanan apabila menjadi berhasil diekploitasi? Ini membantu untuk menentukan dampak keseluruhan dari penyerangan terhadapa kerentanan yang teridenfikasi jika berhasil diluncurkan.

2. Reproductability (Reproduksifitas): seberapa mudah jenis dari serangan untuk di reproduksi ? Ini membantu mengidentifikasi apakah serangan dapat diulang.
3. Exploitability (Ekploitas): Seberapa mudah kerentanan dikenal untuk dieksploitas? Faktor ini mambahas masalah pada tingkat keahlian atau sumberdaya yang dibutuhkan untuk mengekploitas sebuah kerentanan yang ditemukan.
4. Affected User (Efek Pengguna): Menjawab pertanyaan prediksi dampak pada basis pengguna melalui aset informasi mereka atau lingkungan aplikasi yang dimanfaatkan beberapa pengguna.
5. Discoverability: Ini membantu mengidentifikasi seberapa mudah sebuah kerentanan terdeteksi untuk lingkungan aplikasi tertentu. Informasi itu membantu mengidetifikasi seberapa mudah kerentanan dapat ditemukan untuk diekploitasi.

Seperti banyaknya sistem rating resiko yang lainnya, DREAD meliputi *High,Medium,Low* deskriptor kualitatif resiko bersama dengan nilai resiko kuantitatif 3, 2, 1 yang diterapkan masing masing. Pada basis informasi model ancaman mungkin memiliki pada kedua kerentanan berpotensi dieksploitas dan sumberdaya dari penyerang, analisis yang sama dapat dilakukan untuk mempresentasikan sebuah penyerangan bercabang untuk semua tree model (Saputra et al., 2017).

2.2.8 Pengertian SQL Injection

SQL injection adalah serangan untuk mendapatkan akses ke sistem database berbasis SQL. Saat melakukan metode injeksi SQL, peretas akan mengeksploitasi celah keamanan di Internet atau aplikasi. Mereka memasukkan perintah SQL ke dalam database sehingga mereka dapat masuk tanpa memiliki nama pengguna dan kata sandi. Suntikan SQL ini dapat terjadi karena kurangnya pemrosesan keamanan sistem dan dapat mengakibatkan aplikasi disuntikkan ke perintah SQL (Yulianingsih, 2016).

Metode ini dapat merusak sistem apa pun yang menggunakan database SQL, seperti myS'L, Oracle, SQL Server, dan lainnya, yang dapat berbahaya dalam mengakses data sensitif seperti informasi pribadi, rahasia dagang, dan lain-lain. Tindakan yang berbeda dapat dirancang untuk mencegah serangan injeksi, yaitu:

1. Membatasi panjang inputan. Dengan membatasinya, maka *hacker* tidak dapat melakukan penyuntikan dengan perintah yang panjang.
2. Memfilter inputan oleh user, terutama penggunaan tanda kutip tunggal (Input Validation)
3. Menyembunyikan pesan error yang muncul dari SQL server yang sedang berjalan.

2.2.9 Pengertian Data Sniffing

Data Sniffing ini adalah proses pemantauan atau menangkap semua data yang melewati lalu lintas jaringan tertentu, yang sengaja dihasilkan oleh alat

pengintaian seperti merekam melalui saluran kabel telepon dan mendengarkan panggilan. Sniffer biasanya mengonversi sistem NIC ke mode promisscous sehingga dapat merekam semua data yang dikirim pada setiap segmen(Susanto et al., 2018).

Sniffer dapat Sniffing informasi penting melalui jaringan computer seperti:

1. Lalu Lintas Email
2. Kata Sandi FTP
3. Lalu Lintas Web
4. Kata Sandi Telnet
5. Konfigurasi Router
6. Sesi Obrolan
7. Lalu Lintas DNS

2.2.10 Pengertian Mac Address Spoofing

Spoofing meniru fungsionalitas program asli, ini biasanya dilakukan oleh peretas. Dan Mac Address Spoofing adalah cara penyerang memodifikasi atau memalsukan alamat Mac yang ditemukan di perangkat NIC seperti laptop, komputer, Android Router, dan lainnya. Dan tujuan Spoofing adalah untuk mendapatkan akses ke jaringan internet untuk menyembunyikan identitas penyusup (Veny Charnita Br Ginting et al., 2019).

2.2.11 Pengertian Spyware dan Trojans

Spyware ini adalah sistem yang mengumpulkan dan mengirimkan informasi tentang penggunaan komputer tanpa sepengetahuan pengguna, berbahaya, seperti pola otomatis, terutama ketika menggunakan Internet, seperti kartu PIN untuk perbankan elektronik dan kata sandi akun (Zulfa & Subiyanta, 2015).

Sedangkan Trojans adalah tiruan atau duplikat sebuah virus yang di masukkan sebagai virus. Sifat trojan adalah mengontrol komputer secara otomatis, contoh trojan email, Remote Access Trojans (RATS) di mana sebuah komputer di kendalikan oleh program tertentu.

2.2.12 Pengertian Denial of Service (DoS Attack)

Denial of Service adalah serangan berbasis server pada jaringan Internet, yang menggunakan pengiriman sumber daya computer berlebihan sehingga komputer tidak dapat menjalankan fungsinya dengan benar, sehingga pengguna lain tidak dapat mengakses layanan dari komputer yang diserang (Geges & Wibisono, 2015).

2.3 Hipotesis

Hipotesis adalah respon sementara terhadap perumusan masalah penelitian, di mana perumusan masalah penelitian dinyatakan dalam bentuk pertanyaan. Hipotesis terdiri dari kerangka pemikiran yang merupakan respon sementara

terhadap masalah yang dirumuskan. Berdasarkan studi teori dan struktur pemikiran di atas, hipotesis dapat dirumuskan sebagai berikut:

Hipotesis 1 : Terdapat pengaruh positif keamanan terhadap sistem aplikasi berbasis web secara online di PT.Perkebunan Nusantara V.

Hipotesis 2 : Terdapat pengaruh positif kemudahan pengamanan terhadap sistem HRIS di PT.Perkebunan Nusantara V.

Hipotesis 3 : Terdapat pengaruh negatif risiko kinerja terhadap Aplikasi.

Hipotesis 4 : Terdapat pengaruh keamanan, kemudahan, dan risiko kinerja secara bersamaan terhadap sistem HRIS secara online di PT. Perkebunan Nusantara V.

BAB III

METODE PENELITIAN

3.1 Gambaran Umum Objek Penelitian

Pada bab sebelumnya telah dijelaskan bahwa setiap perusahaan harus memiliki tingkat keamanan yang sangat tinggi, oleh karena itu dengan menggunakan metode SQUARE ini dapat mengetahui ancaman keamanan yang akan di terima dari sebuah sistem tersebut. Penulis akan melakukan penelitian menggunakan metode SQUARE, karena metode ini sangat efisien dalam melakukan Analisa kebutuhan keamanan sistem dan seberapa amankah sistem tersebut melalui 9 langkah Analisa dari metode tersebut. Penulis sangat mempertimbangkan hal tersebut karena minim nya referensi terhadap metode yang di ambil sesuai dengan kebutuhan.

3.2 Alat dan Bahan Penelitian

Adapun Alat dan bahan yang digunakan dalam penelitian ini adalah sebagai berikut :

3.2.1 Alat Penelitian

Berikut ini adalah beberapa alat dan spesifikasi alat yang di gunakan untuk penelitan yaitu berupa hardware. Untuk dapat melakukan analisis sebuah penelitian tentu saja *hardware* atau perangkat keras harus memenuhi spesifikasi perangkat keras yang sesuai sesuai kebutuhan.

Adapun kebutuhan perangkat keras (Hardware) dan spesifikasinya yang akan di gunakan dalam melakukan analisis sebagai berikut :

a. Processor : Intel core i3
b. Monitor : LCD 14 Inc
c. Mouse : Optical Wheel Mouse
d. HardDisk : 320GB
e. RAM : 4GB

3.2.2 Bahan Penelitian

Berikut ini adalah beberapa bahan yang di gunakan untuk penelitan yaitu berupa perangkat lunak atau *software*. Untuk dapat melakukan analisis sebuah penelitian tentu saja *software* sangat penting untuk melancarkan proses analisis yang sesuai dengan kebutuhan. Dan *sistem* yang digunakan dalam penelitian ini adalah berupa sebagai berikut.

a. Sistem Operasi Windows 10

   Sistem Operasi di gunakan untuk mengendalikan sumber daya Laptop yang Penulis gunakan untuk penelitian.

b. Cisco Packet Tracer 7.1

   Aplikasi yang di gunakan untuk membuat arsitektur dan topologi jaringan pada sistem HRIS yang terhubung ke internet.

c. Mozilla FireFox

Aplikasi yang di gunakan untuk mengakses Aplikasi HRIS yang ada di PT. Perkebunan Nusantara V Sei Lala

d. SQLMap

Aplikasi ini digunakan untuk menjalankan sebuah *Tools* Python(*Command Line*) yang akan melakukan penyuntikan sql kedalam sistem.

e. Python

Tools ini di gunakan untuk menulis script serangan SQL Injeksi yang dapat melihat celah keamanan.

f. BurpSuite

Tools ini di gunakan melakukan serangan Sniffing yang dapat merekam aktifitas website dalam satu jaringan dan melihat aktifitas login

g. Winbox

Tools ini di gunakan untuk melakukan serangan Sniffing untuk konektivitas dan konfigurasi MikroTik menggunakan MAC Address atau protokol IP

h. Command Prompt

Tools ini di gunakan untuk menulis script untuk mencari IP Address target untuk membuat IP bayangan yang akan di arahkan ke IP pembajak

3.3 Alur Penelitian

Dalam melakukan analisis keamanan Sistem menggunakan metodologi SQUARE maka harus menggunakan Sembilan Langkah untuk membantu proses menganalisis kebutuhan keamanan sistem

Gambar 3.1 Langkah-langkah Penelitian dengan Metode SQUARE

Ada pun Sembilan Langkah tersebut sebagai berikut :

1. *Agree on Definitions* (Mendefinisikan kebutuhan Sistem)

Pada tahap ini melakukan deskripsikan aplikasi HRIS yang akan di analisa dan mendefinisikan istilah keamanan informasi untuk aplikasi HRIS tersebut.

HRIS PTPN V adalah sistem entri data biodata yang menggunakan media. HRIS PTPN V adalah konsekuensi logis dari pengembangan teknologi informasi dan komunikasi. HRIS secara luas dapat mencakup semua pekerjaan di sebuah perusahaan, baik gaji maupun data pribadi karyawan. hal ini disebabkan oleh beberapa kerentanan yang dapat ditembus peretas untuk memalsukan data. Dengan demikian, perlu analisis proses yang dapat menjaga integritas sistem HRIS dengan menerapkan sembilan langkah metode SQUARE.

2. *Identify Security Goals* (Mengidentifikasi tujuan keamanan)

Pada tahap kedua ini melakukan Analisis tujuan dan persyaratan keamanan sistem yang di perlukan oleh perusahan PT. Perkebunan Nusantara V untuk menjaga keamanan secara menyeluruh terhadap ketersediaan (*availability*)

3. *Develop Artifact* (Pengembangan Artefak)

Pada tahap ini akan Menjelaskan arsitektur sistem HRIS yang sedang berjalan yang berupa :

a. Diagram Arsitektur

Pada perencanaan artefak maka merencanakan artefak, arsitektur sistem jaringan, deskripsi kinerja sistem.

b. Diagram *Use Case*

Use case merupakan skenario artefak untuk menanggapi tindakan yang terjadi dalam proses bisnis, menyediakan konteks bagi operasi, pemangku kepentingan, dan tim teknik untuk memahami interaksi komponen sistem

c. Diagram *Misuse Case*

Misuse cases merupakan Insiden penyalahgunaan termasuk serangkaian serangan yang terjadi pada sistem, pengguna ilegal mencoba masuk ke sistem menggunakan langkah atau metode illegal.

d. At*tack Tree*

Pohon serangan merupakan tindakan formal yang menggambarkan ancaman keamanan terhadap sistem dengan jenis serangan yang dapat terjadi dan diimplementasikan.pohon serangan yang terjadi dalam proses sistem HRIS diantaranya :

1. Pohon serangan SQL Injection (MC-01)
2. Pohon serangan Spyware and Trojans (MC-02)
3. Pohon serangan Sniffing (MC-03)
4. Pohon serangan Spoofing (MC-04)

5. Pohon serangan Denial of Service (MC-05)

4. *Perform Risk Assesment* (Penilaian Risiko)

Pada tahap ini melakukan analisa penilaian risiko untuk mengidentifikasi ancaman terhadap sistem yang kemungkinan terjadi, ada beberapa penilaian resiko yang kemungkinan terjadi sebagai berikut:

1. Serangan SQL Injection (MC-01)
2. Serangan Sniffing (MC-02)
3. Serangan Spoofing (MC-03)
4. Serangan Spyware and Trojans (MC-04)
5. Serangan Denial of Service (MC-05)

5. *Select Elicitation Technique* (Memilih Teknik Elisitasi)

Pada tahap kelima ini Memilih teknik elisitasi yang cocok untuk melakukan penanganan terhadap pekerjaan yang dilakukan dengan Pengumpulan data terkait kondisi sistem secara menyeluruh antara melalui metode observasi, *interiew*, atau analisa *use case*.

Pemilihan elisitasi teknik yang dilakukan yaitu dengan melakukan interview, kuesioner dan observasi. Karena metode elisitasi ini sangat baik karena langsung mengetahui dari instansi apa saja yang perlu di pecahkan dan mengenali Batasan

Batasan sistem dan mengenali siapa saja pemangku kepentingan untuk tujuan sebuah sistem.

6. *Elicit Security Requirements* (Permintaaan persyaratan keamanan)

Pada tahap enam melakukan Elisitasi persyaratan keamanan untuk menyediakan solusi bagaimana melakukan elisitasi keamanan yang baik dan dari hasil observasi, analisa *use case* dan studi pustaka kemudian dibuat kedalam bentuk daftar kebutuhannya

7. *Categorize Requirement* (Kategori Persyaratan)

Setelah persyaratan yang dihasilkan maka selanjutnyayaitu mengelompokan persyaratan keamanan yang dipilih, dalam hal ini menggabungkan langkah-langkah pengelompokan, penamaan, dan kategorisasi bersama-sama, berikut adalah kategori yang di jadikan persyaratan

1. Kerahasiaan
2. Akses Kontrol
3. Integritas Data
4. Pengelolaan
5. Penggunaan
6. Authentifikasi

8. *Prioritize Requirements* (Prioritas Persyaratan)

Pada proses ini akan dilakukan persyaratan prioritas mengenai sistem keamanan di jaringan nirkabel dan LAN di jaringan PT berdasarkan kasus Misusecases yang dibuat sebelumnya. Untuk memprioritaskan serangan yang membuat ancaman lebih berbahaya, Tujuan berikut prioritas ancaman diharapkan dapat mengatasi masalah ini,

1. Kebutuhan
2. Kategori
3. Rekomendasi

9. *Requirement Inspection* (Penilaian Kebutuhan)

Membuat table penilaian dan pada metode ini bertanggung jawab kepada anggota tim inspeksi dan pengembangan log dengan arsitektur terperinci dan rekomendasi kebijakan untuk persyaratan penyebaran keamanan sistem berdasarkan tingkat prioritas *misuse case.*

BAB IV

HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Dalam melakukan analisis keamanan Sistem menggunakan metodologi SQUARE maka harus menggunakan Sembilan Langkah untuk membantu proses menganalisis kebutuhan keamanan sistem. Pada hasil Penelitian ini, penulis menggunakan 3 metode teknik pengumpulan data yang digunakan dalam penelitian sebagai berikut:

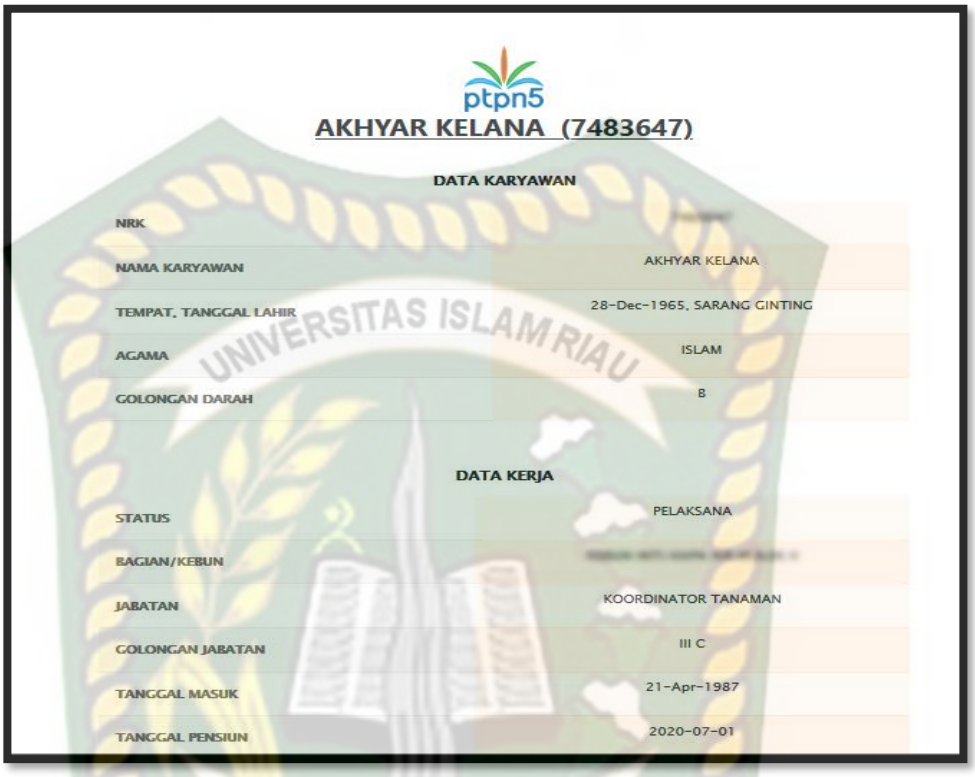
1. Melakukan pengambilan data dengan mencari berbagai sumber tertulis, baik berupa buku-buku, arsip, artikel, dan jurnal, atau dokumen-dokumen yang relevan.
2. Melakukan metode Observasi pengamatan langsung suatu subjek atau objek, yaitu proses penggunaan aplikasi HRIS PTPN V.
3. Melakukan metode wawancara untuk mendapatkan informasi dengan cara bertanya langsung kepada pemangku instansi yaitu karyawan di perusahan atau institusi sehingga data yang diperoleh bersifat objektif dan data dapat dipertanggung jawabkan

Dalam penggunaan Aplikasi HRIS PTPN V Sei lala yang memungkinkan admin mudah menginput data mengenai biodata karyawan di aplikasi HRIS tersebut. Dengan mengakses aplikasi HRIS maka dapat melihat dan menginput biodata karyawan yang bekerja di PT. Perkebunan Nusantara V Sei Lala tersebut. Aplikasi ini bermaksud untuk memudahkan proses penginputan. Dengan aplikasi ini maka dapat mempermudah admin dalam mencari dan melihat serta mengubah data karyawan sesuai fungsi nya yaitu mengelola informasi yang ada di PT dan berikut adalah sistem yang akan di uji untuk keamanannya.

Gambar 4.1 Sistem HRIS PTPN V

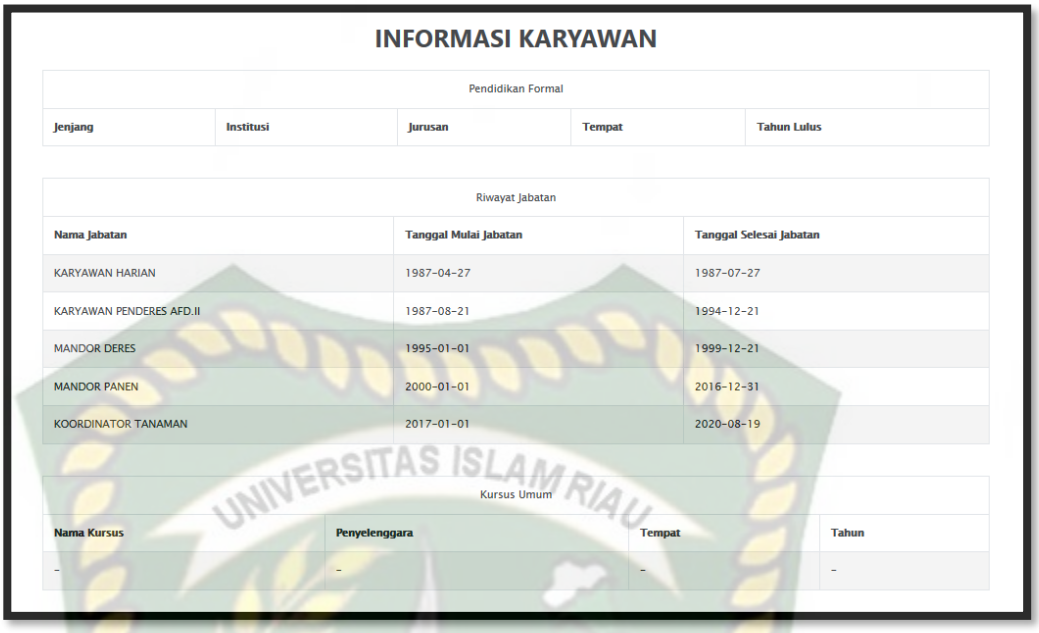
Halaman seluruh data karyawan adalah tampilan output utama ketika admin ingin melihat data karyawan mulai dari data pribadi, data Pendidikan, data riwayat

jabatan, data riwayat golongan, data kursus, data batih, data reward dan data pengalaman organisasi terdapat pada gambar di bawah.



Gambar 4.2 Biodata Karyawan

Pada gambar 4.2 merupakan tampilan *view*, dari hasil pencarian jika admin ingin mencari biodata karyawan maka sebelum mencari data karyawan bisa di cari berdasarkan nrk yang telah di simpan dan admin dapat menghapus maupun mengubah data tersebut.



INFORMASI KARYAWAN

Pendidikan Formal

Jenjang	Institusi	Jurusan	Tempat	Tahun Lulus

Riwayat Jabatan

Nama Jabatan	Tanggal Mulai Jabatan	Tanggal Selesai Jabatan
KARYAWAN HARIAN	1987-04-27	1987-07-27
KARYAWAN PENDERES AFD.II	1987-08-21	1994-12-21
MANDOR DERES	1995-01-01	1999-12-21
MANDOR PANEN	2000-01-01	2016-12-31
KOORDINATOR TANAMAN	2017-01-01	2020-08-19

Kursus Umum

Nama Kursus	Penyelenggara	Tempat	Tahun
-	-	-	-

Gambar 4.3 Data Akademik Karyawan

Pada gambar 4.3 merupakan hasil output dari Pendidikan Formal, Riwayat Jabatan, Kursus Umum dan Kursus Jabatan dari karyawan yang sebelumnya telah di Inputkan datanya. Admin yang mengelola layanan ini di beri aksess untuk menginputkan nya.

Riwayat Golongan

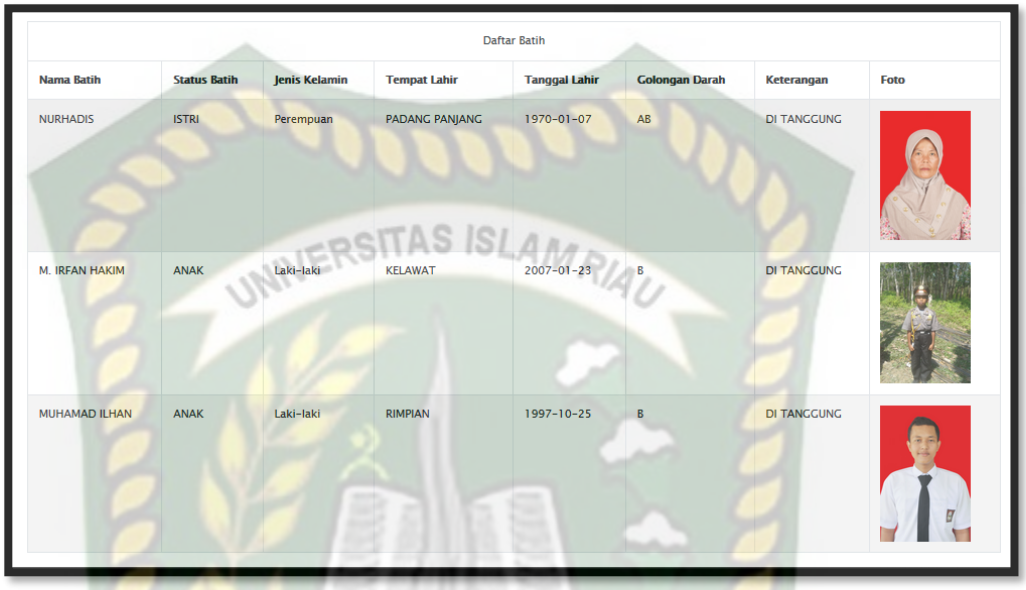
Tahun	Golongan	Berkala
1988	I A	0
1992	I B	0
1994	I C	1
2000	I D	1
2005	II A	0
2013	II B	1
2017	II C	0
2018	III A	1
2019	III C	1

Riwayat Orgnisasi

Organisasi	Tahun Mulai	Tahun Selesai	Jabatan	Tujuan Organisasi
SP.Bun	2010	2015	ANGGOTA	KESEJAHTERAAN KARYAWAN
KOPERASI KARYAWAN	2010	2016	ANGGOTA	KESEJAHTERAAN KARYAWAN

Gambar 4.4 Data Golongan Karyawan

Pada gambar 4.4 merupakan hasil output dari Reward/Punishment dan Riwayat Golongan dari karyawan yang sebelumnya telah di Inputkan datanya. Admin yang mengelola layanan ini di beri aksess untuk menginputkan nya.



Daftar Batih

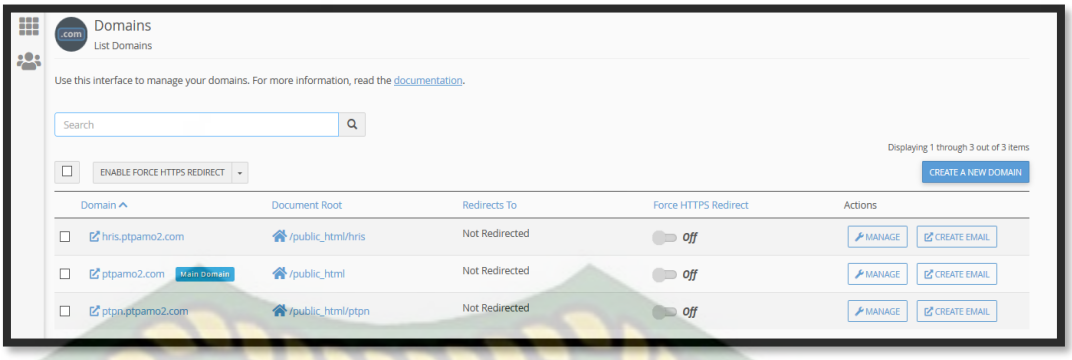
Nama Batih	Status Batih	Jenis Kelamin	Tempat Lahir	Tanggal Lahir	Golongan Darah	Keterangan	Foto
NURHADIS	ISTRI	Perempuan	PADANG PANJANG	1970-01-07	AB	DI TANGGUNG	
M. IRFAN HAKIM	ANAK	Laki-laki	KELAWAT	2007-01-23	B	DI TANGGUNG	
MUHAMAD ILHAN	ANAK	Laki-laki	RIMPIAN	1997-10-25	B	DI TANGGUNG	

Gambar 4.5 Data Batih Karyawan

Pada gambar 4,5 merupakan hasil rekam data Batih dari karyawan yang mana sistem tersebut menampilkan data tersebut melalui nrk dan Admin di beri hak akses untuk menginputkan data tersebut.

Adapun informasi mengenai sistem secara mendalam yaitu sebagai berikut:

a. URL pada sistem Human Resources Information System ini yaitu “ptpn5.co.id” yang di gunakan untuk mengidentifikasi sebuah website dalam dunia internet atau di sebut juga sebagai Domain, pada domain co.id adalah untuk Badan Usaha yang mempunyai badan hukum yang sah.

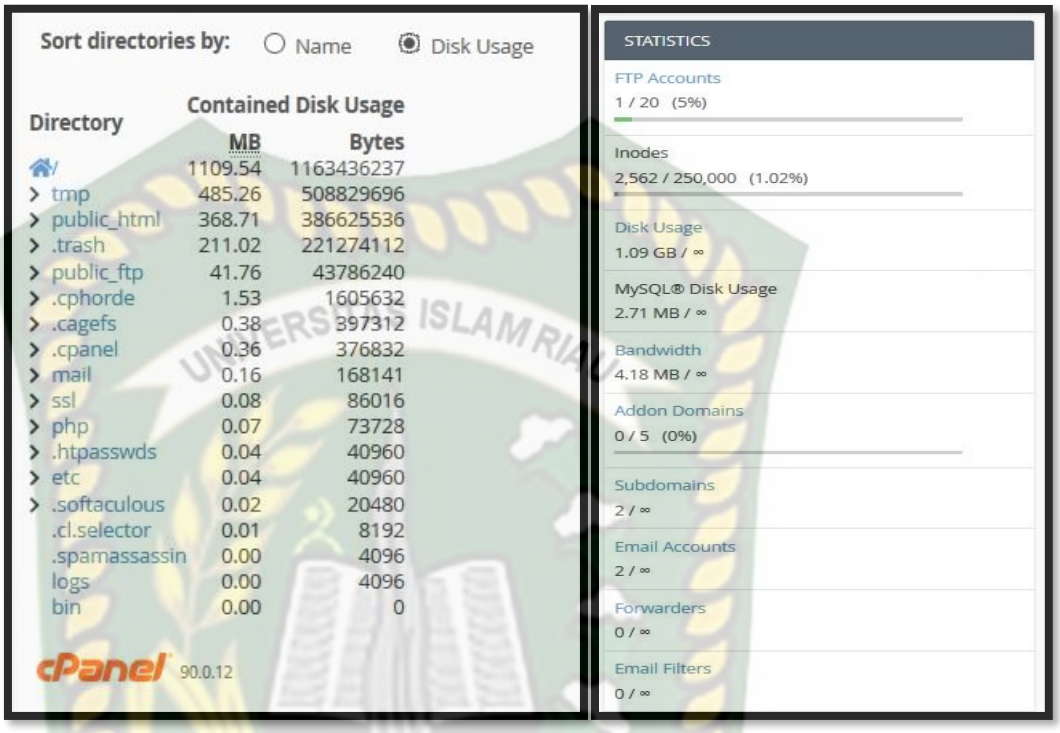


Gambar 4.6 *Domains*

b. Pada *Web Hosting* sistem ini memiliki penyimpanan tanpa batas atau unlimited storage, penyimpan ini berupa data file, gambar, video, data email, statistic, database yang mana akan di tampilkan pada website.

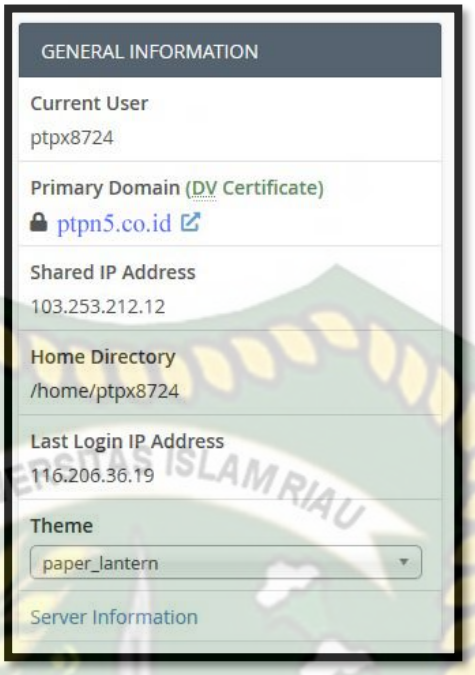
Gambar 4.7 *Web Manager(cPanel)*

c. Berikut adalah storage penyimpanan dari sistem HRIS



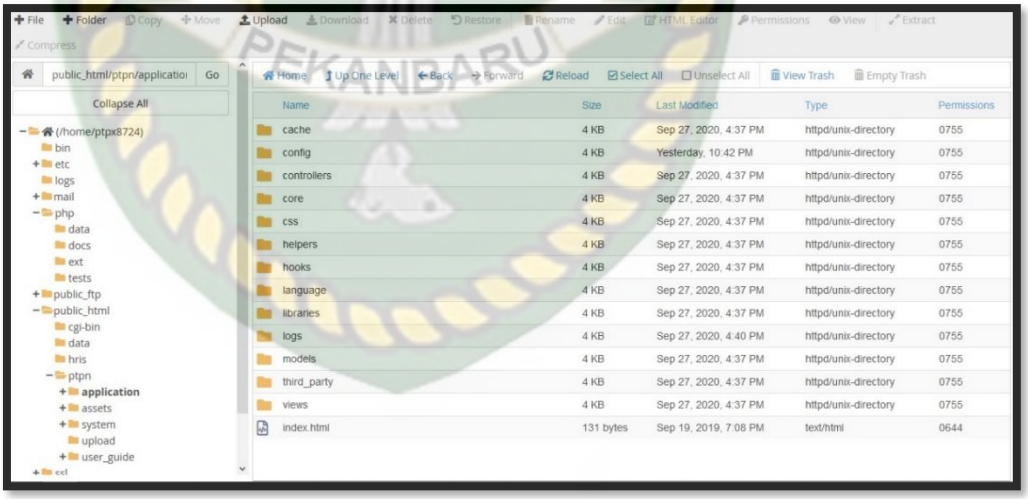
Gambar 4.8 *Disk Usage*

d. Pengguna saat ini sistem user yang di berikan secara *default* oleh cPanel yaitu "ptpx8724" yang memiliki domain "ptpn5.co.id" dan memiliki *Home Directory* /home/ptpx8724 dengan *IP Address* "103.253.212.12".



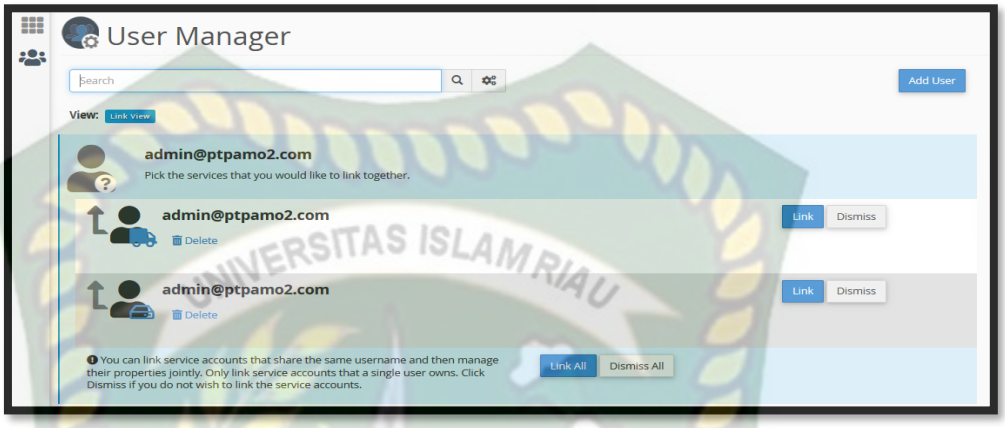
Gambar 4.9 *General Information*

e. File Manager pada sistem HRIS, file manager ini berupa storage untuk menyimpan file yang berkaitan untuk menampilkan sebuah website.



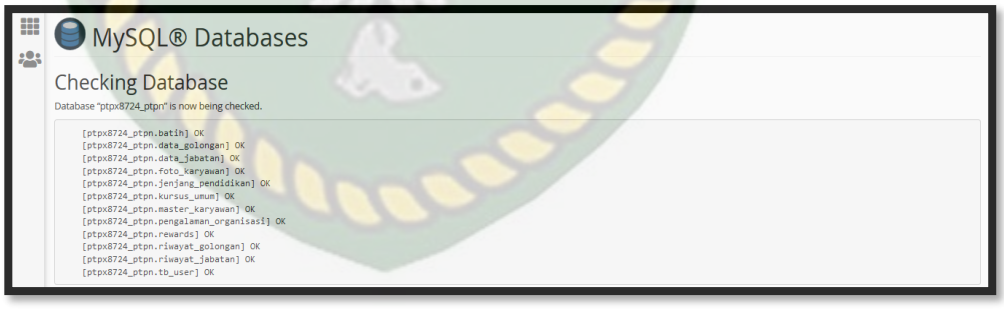
Gambar 4.10 *File Manager* Sistem HRIS

f. User Manager yang ada pada sistem HRIS tersebut hanya satu yang di beri hak akses terhadap sistem, yang mana hak akses tersebut dapat menggunaka sistem sebagaimana mestinya.



Gambar 4.11 *User Manager*

g. Pada aplikasi HRIS juga terdapat database yaitu "ptpx8724_ptpn" yang memungkinan penyimpanan kumpulan data untuk merekam semua aktifitas pada aplikasi HRIS dan juga dapat membuat data baru, mengubah data, melihat data dan menghapus data.



Gambar 4.12 *Database* ptpx8724_ptpn

4.2 Hasil Analisis dan Pembahasan

Analisa dilakukan dengan tahapan yang akan di buat berdasarkan proses dari metodologi yang telah di tentukan yaitu metode SQUARE.

4.2.1 *Agree on Definitions* (Mendefinisikan kebutuhan Sistem)

HRIS PTPN V merupakan sistem pengelola karyawan yang menggunakan media. HRIS PTPN V pengembangan teknologi informasi dan komunikasi. HRIS PTPN V dalam arti luas dapat mencakup semua kegiatan yang dilakukan di perusahaan, baik gaji maupun sertifikat personil

Ada beberapa ancaman keamanan dalam sistem HRIS, hal ini disebabkan oleh kerentanan yang dapat diperkenalkan oleh peretas untuk memalsukan data sehingga peretas dapat mengutak-auli keamanan sistem HRIS. Dengan demikian, perlu analisis kebutuhan sistem keamanan yang dapat menjaga integritas sistem HRIS. menentukan kondisi keamanan yang akan disepakati. Kondisi keamanannya adalah sebagai berikut: :

Beberapa definisi serangan pada sistem :

Tabel 4.1 Definisi serangan Sistem HRIS

No.	Keterangan Definisi serangan
1	Serangan Injeksi SQL ini objek yang diserang berupa halaman web yang menggunakan Structured Query Language (SQL) untuk melakukan query dan memalsukan database.
2	Serangan Data Sniffing, pada serangan ini melakukan sniffing terhadap data yang ada dalam jaringan untuk mengetahui data dalam jaringan
3	Serangan Spoofing, Penyerang ini untuk mendapatkan informasi yang disediakan atau mengambil mac address
4	Password Attack, serangan untuk crack sebuah password
5	Daniel of Service (DoS), jenis serangan dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sehingga komputer tersebut tidak dapat menjalankan fungsinya dengan benar.
6	Sistem HRIS tidak di lengkapi dengan keamanan yang berupa *Secure Socket Layer* (SSL). Tujuan utama pemasangan SSL adalah sebagai pengaman pertukaran data yang terjadi melalui jaringan internet. sistem HRIS tidak di lengkapi dengan pengaman SSL dan dapat di buktikan pada gamabar berikut

Gambar 4.13 URL Tanpa SSL

Pada gambar tersebut, ptpn5.co.id tidak memilik keamanan SSL karena URL terdapat simbol gembok yang di silang merah yang artinya sertifikat SSL tidak Valid dan pada URL tidak terdapat HTTPS karena website yang memiliki sertifikat SSL, URL di awali dengan HTTPS dan bukan HTTP

4.2.2 Pengujian Serangan Sistem

A. Serangan Injeksi SQL

Serangan Injeksi SQL dilakukan dengan cara menyuntikkan data yang bebas, paling sering menjadi query database, menjadi string yang akhirnya dieksekusi oleh database melalui aplikasi web (misalnya form login)

Ada pun bahan untuk melakukan serangan sql injection yaitu:

- Mozilla Firefox
- Sistem Operasi Windows 10
- Burp Suite

Biasanya serangan yang di lakukan yaitu dengan cara menyuntikan melalui input pengguna, Injeksi melalui field cookie yang berisikan string serangan Dan Injeksi Melalui Variabel server.

Berikut alat serangan SQL Injection yang di gunakan terhadap website ptpn5.co.id:

a. Laptop Acer Aspire 4739

Tabel 4.2 Spesifikasi Acer Aspire 4739

Tipe	Jenis	Laptop
Spesifikasi Dasar	CPU Model Processor Kecepatan Processor Model GPU	Core i3 Core i3 370M 2.4 GHz Intel® HD Graphics
Memori & Penyimpanan	RAM Slot Memori Tipe Penyimpanan HDD Kecepatan Rotasi Drive Optical	4 GB 2 DIMMs HDD 320 GB 5400 rpm DVD±RW
Layar	Ukuran Layar Resolusi	14inc CineCrystal LED 1280x800
Network	WiFi	802.11b/g/n

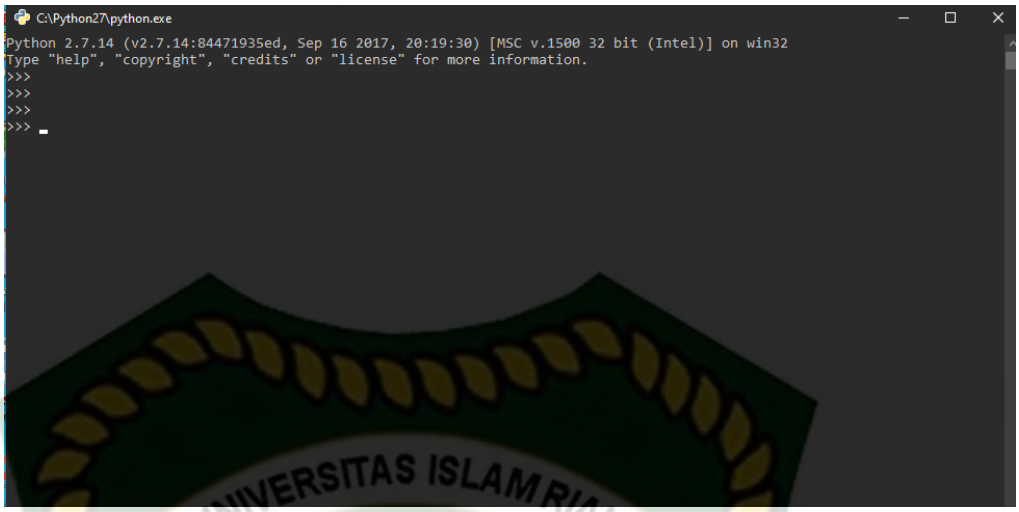
Konektifitas	Konektifitas	HDMI,USB2.0,Card Reader
Ukuran	Berat	2.2 Kg
Sistem Operasi	OS	Windows 10 Profesional

b. SQLMap

Gambar 4.14 sqlmap.py

File sqlmap ini di gunakan untuk menjalankan sebuah *Tools* Python(*Command Line*) yang akan melakukan penyuntikan sql kedalam sistem.

c. Python (*Command Line*)



Gambar 4.15 *Python*

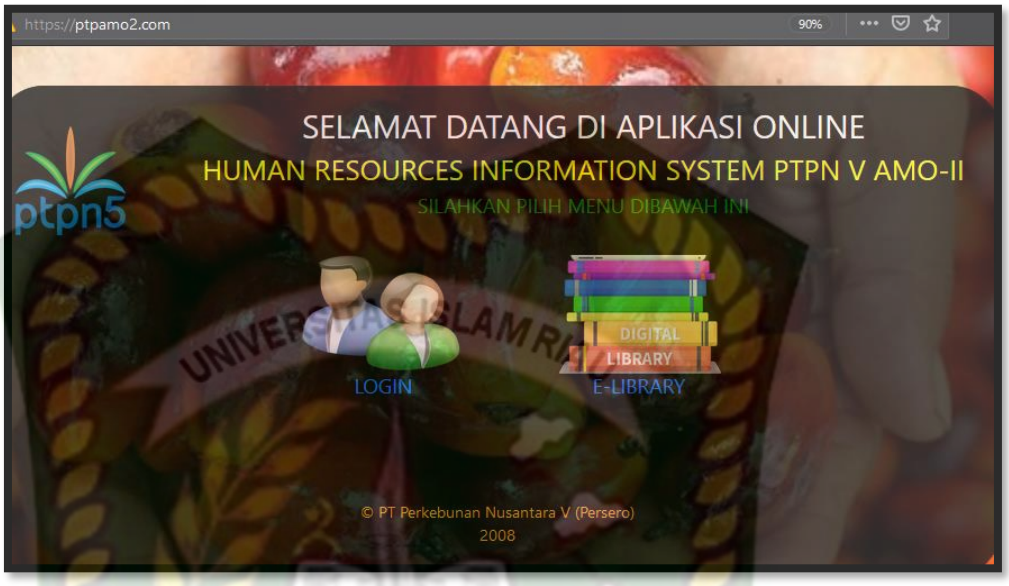
Tools ini di gunakan untuk menulis script serangan SQL Injeksi yang dapat melihat celah keamanan nya..

Adapun Langkah serangan *sql injection* sebagai berikut :

Comand yang di gunakan sqlmap untuk melakukan sql injection :

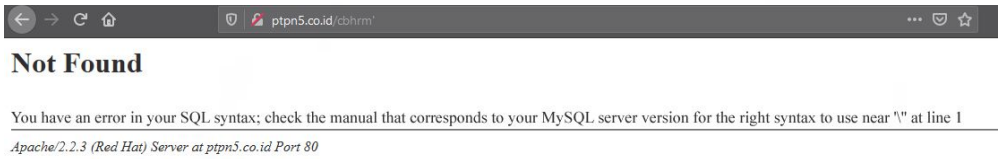
- U (fungsinya untuk memanggil url yang ingin di inject)
- dbs (untuk melihat list database yang terdapat pada web target)
- D (untuk memilih suatu database untuk di tampilkan)
- tables (untuk melihat list tabel pada database yang di pilih)
- T (untuk memilih tabel pada list tabel yang berhasil di tampilkan)
- Columns (untuk menampilkan list kolom pada tabel yang di pilih)
- C (untuk memilih kolom pada list kolom yang berhasil di tampilkan)
- dump (untuk melihat isi dari suatu kolom atau tabel juga bisa)

1. Pertama ketikan url target seperti ptpn5.co.id pada browsher sebelum melakukan sqlmap.



Gambar 4.16 *URL PTPN V*

2. Kemudian untuk mencari celah keamanan dari sistem ini maka *vulnerability* dengan cara tambahkan tanda (‘) di akhir url contoh ptpamo2.com/karyawan/get_data_by_karyawan_id2/2180652’ . Ketika ada pesan error maka perhatikan pesan nya yang akan memberitahukan letak *syntax error* nya seperti : *You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1*.



Gambar 4.17 Pesan *Error*

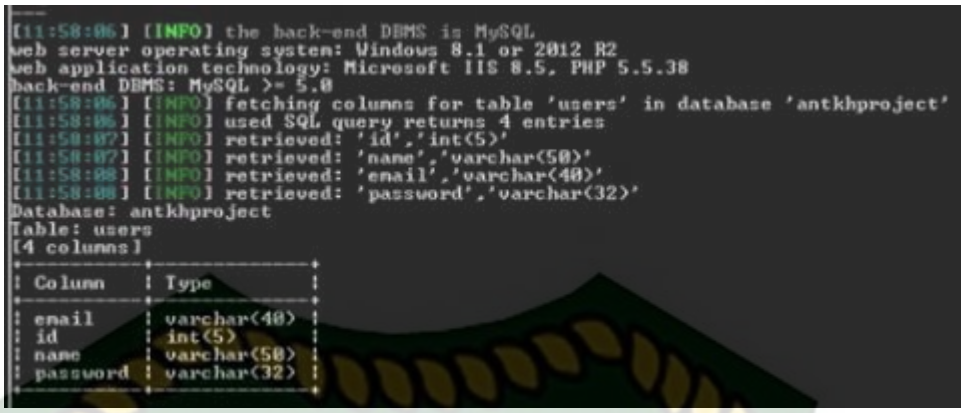
3. Kemudian jalankan Sqlmap nya dan ketikkan printah cd Document, dan ketikkan directory penyimpanan file sqlmap nya seperti cd sqlmap lalu ketikkan perintah -u , sqlmap.py -u dan tambahkan url target asli tanpa tanda (‘) kemudian diakhiri –dbs kemudian enter sampai ada tulisan got a 302 redirect to 'http://ptpn5.co.id:80/web_intranet_1/home.php'. *Do you want to follow?* [Y/n] lalu ketik “y” dan tunggu sampai selesai dan menampilkan database web tersebut.

Gambar 4.18 *IP SQLmap running*

4. Selanjutnya jika sudah menemukan database nya maka ketikkan perintah sqlmap.py -u ptpn5.co.id -D ptpx8724_ptpn –tables. Dan tunggu sampai menampilkan table nya.

Gambar 4.19 Menampilkan Tabel database ptpx8724_ptpn

5. Kemudian pilih salah satu table dan skrg pilih table user dengan mengetikkan perintah sqlmap.py -u ptpn5.co.id ptpx8724_ptpn -T tb_users --columns. Dan tunggu sampai menampilkan isi dari table tb_users



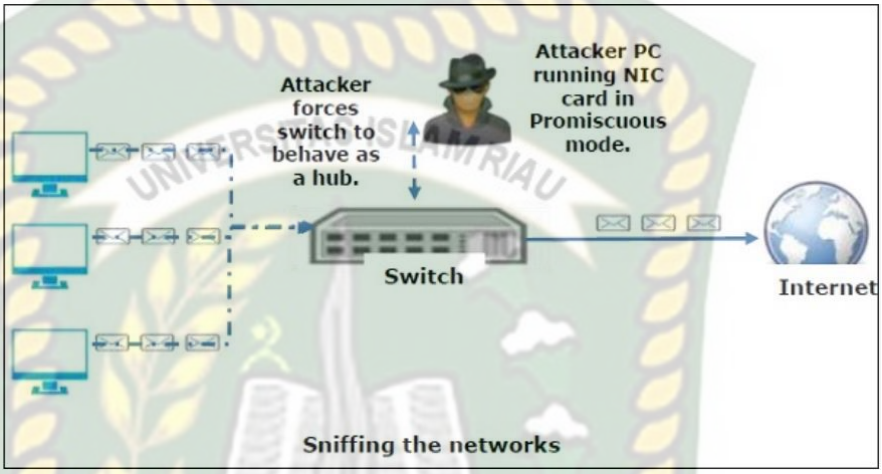
Gambar 4.20 Menampilkan table tb_users

6. Kemudian ketikkan perintah sqlmap.py -u ptpn5.co.id -D ptpx8724_ptpn -T tb_users -C email,password --dump. Dan tunggu sampai menampilkan email dan password nya

Gambar 4.21 Menampilkan email dan password

B. Serangan Data Sniffing

Serangan ini penyadapan dengan tujuan utama ekstraksi ilegal data dan informasi rahasia ketika sistem terhubung ke jaringan publik, ketika sistem mengirimkan data dari server klien dan sebaliknya.



Gambar 4.22 Cara kerja Serangan Sniffing

Untuk melakukan serangan ini maka di butuhkan *tools* sebagai berikut :

a. Laptop Acer Aspire 4739

Tabel 4.3 Spesifikasi Acer Aspire 4739

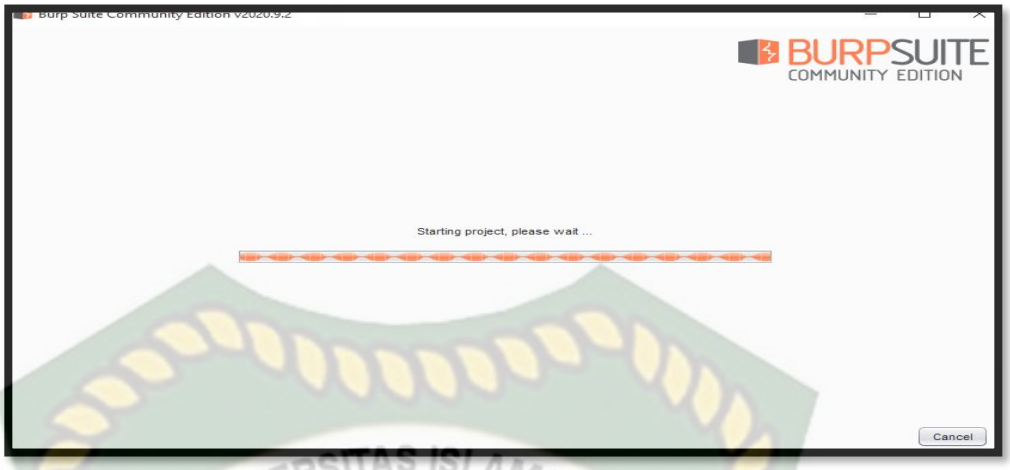
Tipe	Tipe Laptop	NoteBook
Spesifikasi Dasar	CPU Model Processor Kecepatan Processor	Core i3 Core i3 370M 2.4 GHz

	Model GPU	Intel® HD Graphics
Memori & Penyimpanan	RAM Slot Memori Tipe Penyimpanan HDD Kecepatan Rotasi Drive Optical	4 GB 2 DIMMs HDD 320 GB 5400 rpm DVD±RW
Layar	Ukuran Layar Resolusi	14inc CineCrystal LED 1280x800
Network	WiFi	802.11b/g/n
Konektifitas	Konektifitas	HDMI,USB2.0,Card Reader
Ukuran	Berat	2.2 Kg
Sistem Operasi	OS	Windows 10 Profesional

b. Mozilla FireFox

Tools ini di gunakan untuk mengakses Website dan untuk mengirimkan data seperti data login yang akan terekam oleh aplikasi WireShark.

c. BurpSuite

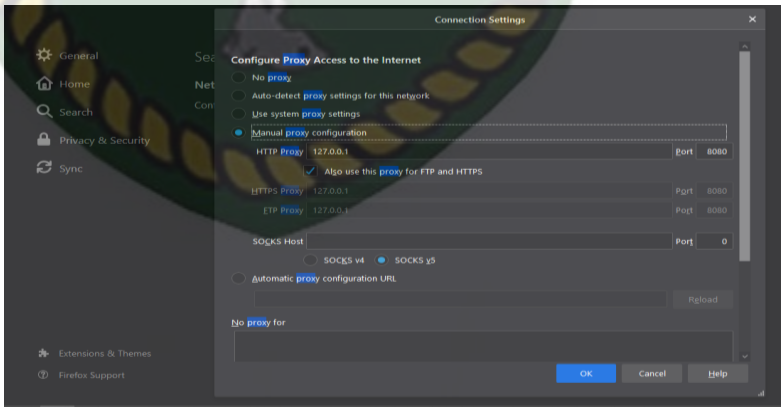


Gambar 4.23 *BurpSuite*

Tools ini di gunakan melakukan serangan Sniffing yang dapat merekam aktifitas website dalam satu jaringan local termasuk merekam kata sandi .

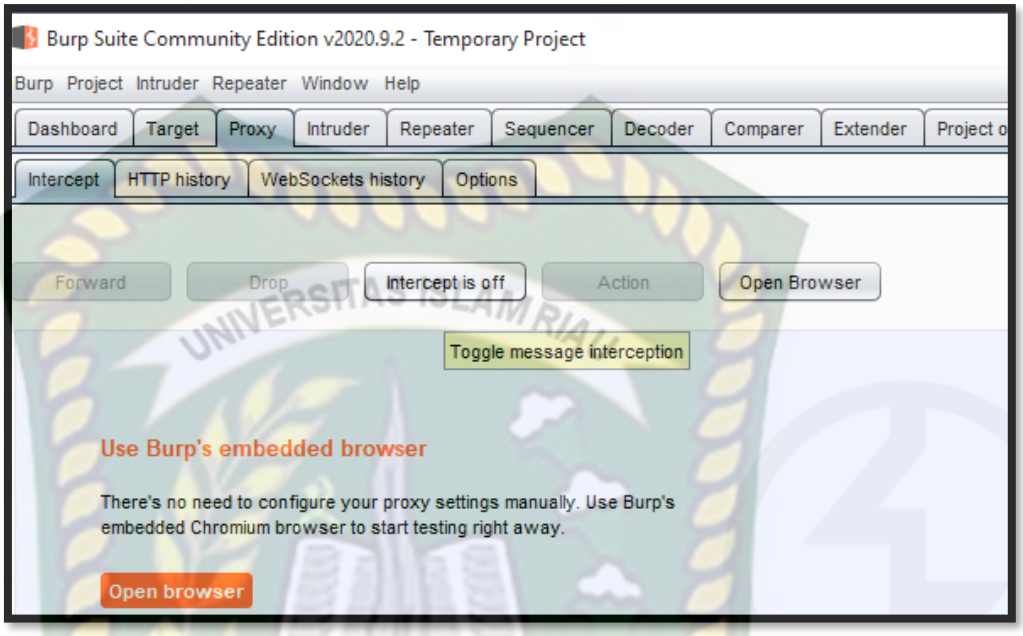
Adapun Langkah serangan Sniifing sebagai berikut :

1. Pertama Jalankan Mozilla FireFox kemudan setting Proxy manual yaitu IP 127.0.0.1 dan Port nya 8080 agar dapat membuka akses terhadap aplikasi BurpSuite sehingga *capturing* aktifitas dari lalu lintas jaringan tersebut dapat berjalan.



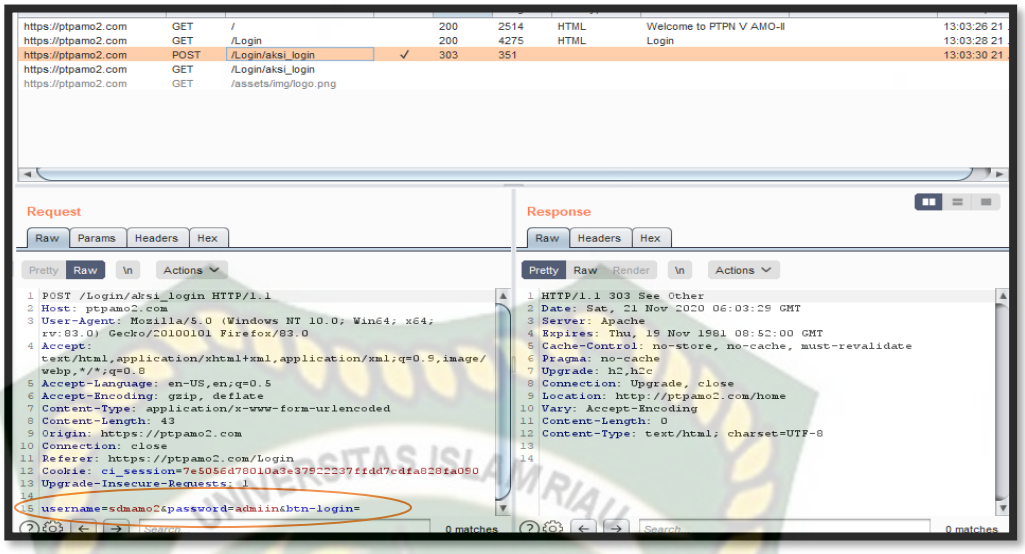
Gambar 4.24 Konfigurasi Proxy

2. Langkah kedua yaitu menjalankan Aplikasi BurpSuite dan Setting pada Intercept Proxy menjadi Off agar browsher dapat di jalankan.



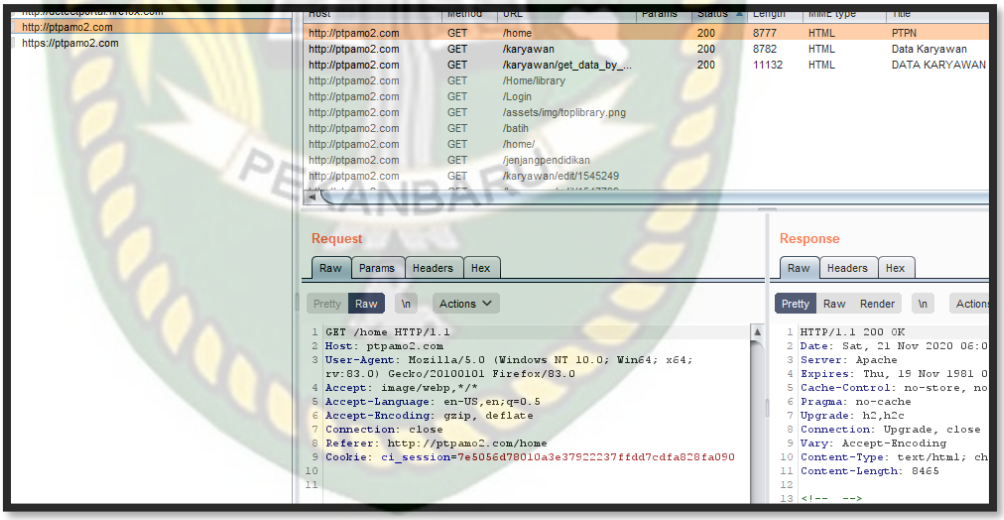
Gambar 4.25 *Setting Intercept Proxy*

3. Kemudian buka Mozilla dan jalankan website ptpn5.co.id dan lakukan aktifitas terhadap website tersebut seperti login akun, maka BurpSuite dapat merekam aktifitas login berikut hasil rekam data login website pada HOST.



Gambar 4.26 *Hasil Capturing data HOST*

4. Selanjutnya apa pun aktifitas pada web target maka dapat akan terekam oleh Burpsuite tersebut.



Gambar 4.27 Rekam Aktfitas Sistem

C. Serangan Spoofing

Spoofing adalah meniru fungsi dari program yang asli, hal ini biasanya dilakukan oleh seorang *hacker*. Dan Mac Address Spoofing adalah sebuah cara dimana seorang attacker mengubah atau memalsukan sebuah Mac Address yang terdapat pada suatu perangkat NIC seperti Laptop, Komputer, Android Router dan lain lain. Dan tujuan dari sebuah Spoofing adalah untuk mendapatkan akses ker jaringan atau menyembunykan siapa identitas attacker.

Adapun Tools yang di gunakan sebagai berikut :

a. Laptop Acer Aspire 4739

Tabel 4.4 Spesifikasi Acer Aspire 4739

Tipe	Tipe Laptop	NoteBook
Spesifikasi Dasar	CPU	Core i3
	Model Processor	Core i3 370M
	Kecepatan Processor	2.4 GHz
	Model GPU	Intel® HD Graphics
Memori & Penyimpanan	RAM	4 GB
	Slot Memori	2 DIMMs
	Tipe Penyimpanan	HDD
	HDD	320 GB
	Kecepatan Rotasi	5400 rpm
	Drive Optical	DVD±RW

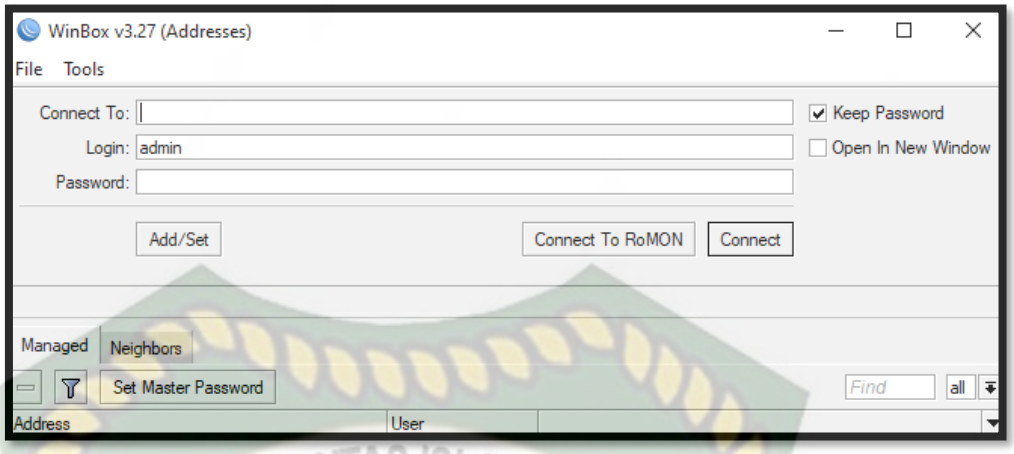
Layar	Ukuran Layar	14inc CineCrystal LED
	Resolusi	1280x800
Network	WiFi	802.11b/g/n
Konektifitas	Konektifitas	HDMI,USB2.0,Card Reader
Ukuran	Berat	2.2 Kg
Sistem Operasi	OS	Windows 10 Profesional

b. Mozilla FireFox

Gambar 4.28 *Mozilla FireFox*

Tools ini di gunakan untuk mengakses Website dan untuk mengirimkan data seperti data login yang akan terekam oleh aplikasi WireShark.

c. Winbox



Gambar 4.29 *Winbox*

Tools ini di gunakan melakukan serangan Sniffing yang digunakan untuk konektivitas dan konfigurasi MikroTik menggunakan MAC Address atau protokol IP.

d. CMD

Gambar 4.30 *Command Prompt*

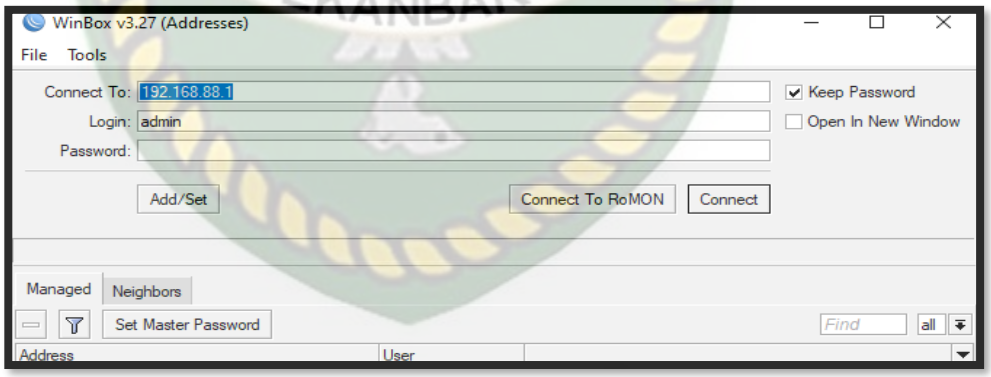
Tools ini di gunakan untuk mencari IP Address target untuk membuat IP bayangan yang akan di arahkan ke IP pembajak.

Adapun Langkah serangan DDoS sebagai berikut :

1. Pertama Jalankan cmd dengan mengetikkan nslookup ptpn5.co.id untuk menemukan IP Address server pada website tersebut.

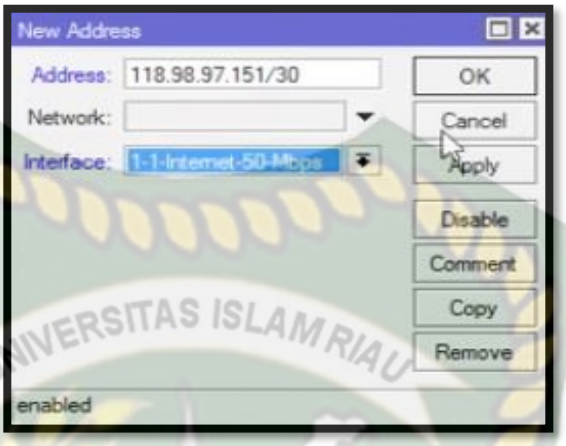
Gambar 4.31 CMD

2. Lalu connect ke IP Router melalui aplikasi Winbox.



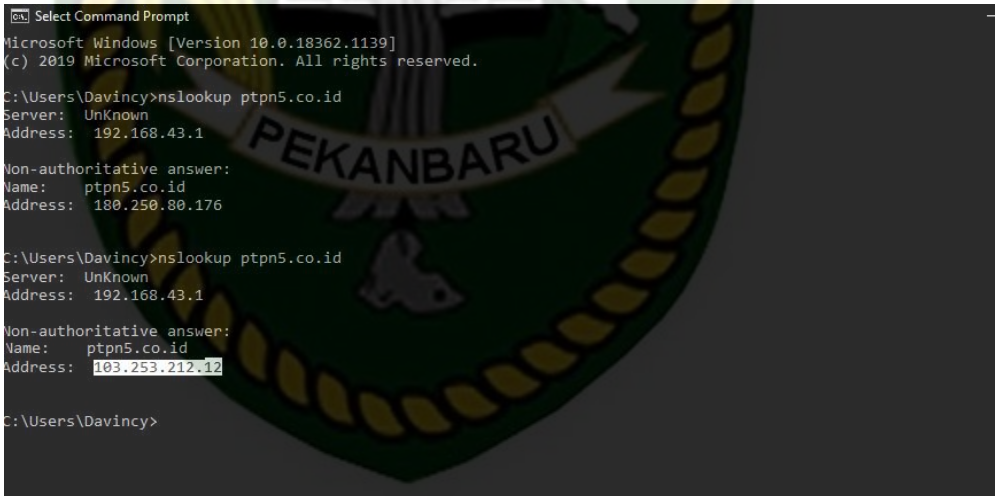
Gambar 4.32 *Connect to IP Router*

3. Setelah sudah terkoneksi ke IP router maka tambahkan IP Address website pada winbox nya dan ubah interface nya menjadi internet lalu klik OK.



Gambar 4.33 Menambahkan *Ip Address web server*

4. Selanjutnya cek Kembali IP address dari website ptpn5.co.id dengan cara nslookup ptpn5.co.id ENTER. Maka otomatis Ip Address berubah.

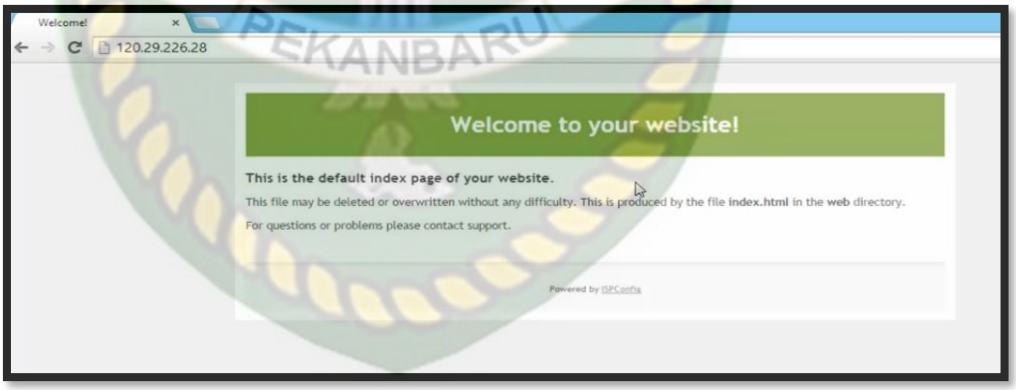


Gambar 4.34 *Ip Address* yang telah di palsukan

5. Selanjutnya mengarahkan IP tersebut ke sebuah hostingan yang milik sendiri dengan cara menambahkan NAT Rule nya dengan IP yang di arahkan.

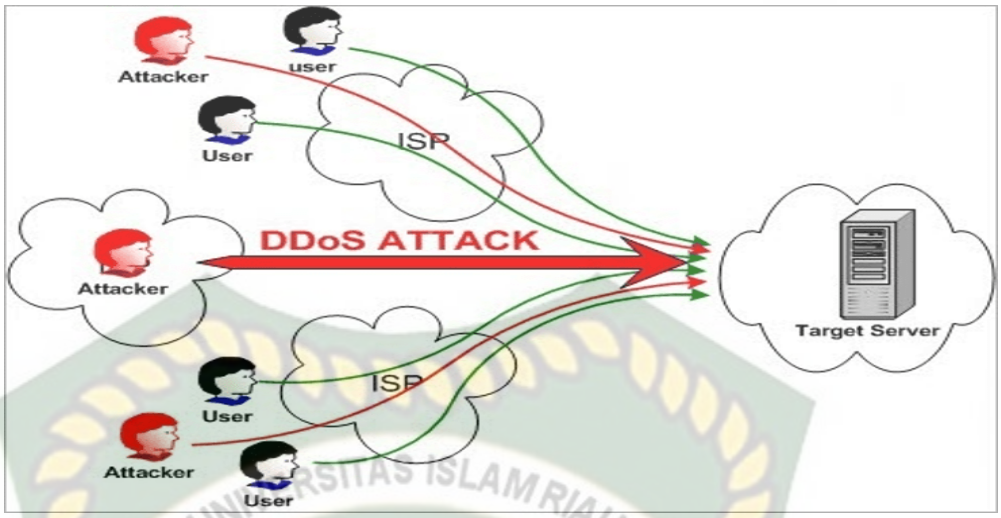
Gambar 4.35 Mengalihkan Ip ke Hosting lain

6. Selanjutnya mengakses IP address yang telah di alihkan ke hosting lain dengan membuka browser dan ketikkan Ip nya.



Gambar 4.36 Output Akses IP pengalihan

D. Serangan DDOS



Gambar 4.37 Serangan DDOS

Serangan DDoS adalah jenis serangan dalam sebuah jaringan internet yang menghabiskan sumber *resource* yang di miliki oleh komputer dengan cara mengirimkan atau membanjiri lalu lintas jaringan sehingga komputer tidak dapat berfungsi dengan benar dan user tidak dapat menggunakan layanan web tersebut.

Pada serangan DDOS ini memiliki tiga jenis serangan yaitu

- *Volume-based Attacks*
- *Protocol Attacks*
- Dan *Aplication Attacks*

Dan metode penyerangan DDOS ini juga banyak digunakan contohnya seperti UDP Flood, ICMP(ping) Folood, Ping of Death, HTTP Flood dll.

Dan berikut adalah Langkah serangan DDoS dengan menggunakan proses Command Promt atau cmd. Software ini akan melakukan pengirimn

permintaan pada HTTP, UDP, dan TCP ke server yang bisa melalui Ip Server pada website yang akan kita serang. Adapun alat yang di gunakan untuk serangan DDoS sebagai berikut :

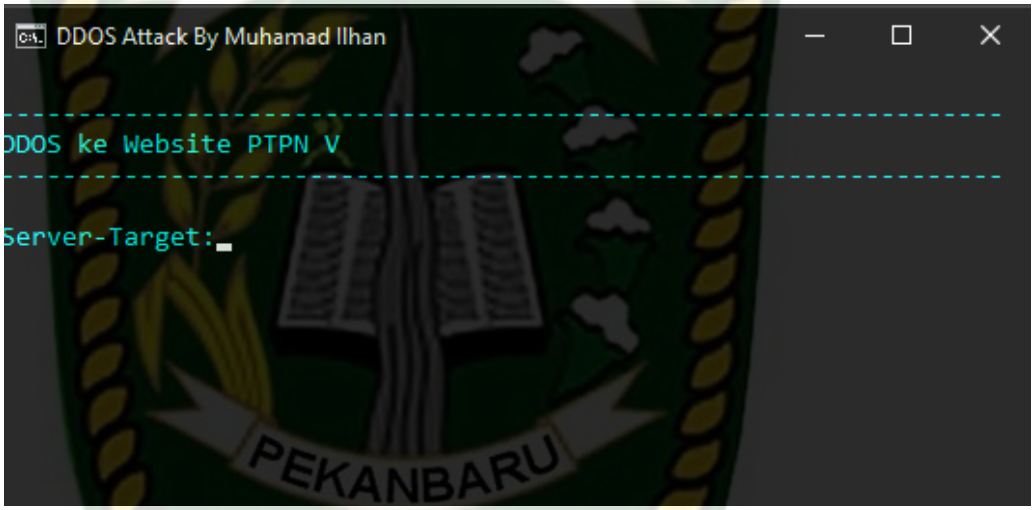
d. Laptop Acer Aspire 4739

Tabel 4.5 Spesifikasi Acer Aspire 4739

Tipe	Tipe Laptop	NoteBook
Spesifikasi Dasar	CPU	Core i3
	Model Processor	Core i3 370M
	Kecepatan Processor	2.4 GHz
	Model GPU	Intel® HD Graphics
Memori & Penyimpanan	RAM	4 GB
	Slot Memori	2 DIMMs
	Tipe Penyimpanan	HDD
	HDD	320 GB
	Kecepatan Rotasi	5400 rpm
	Drive Optical	DVD±RW
Layar	Ukuran Layar	14inc CineCrystal LED
	Resolusi	1280x800
Network	WiFi	802.11b/g/n

Konektifitas	Konektifitas	HDMI,USB2.0,Card Reader
Ukuran	Berat	2.2 Kg
Sistem Operasi	OS	Windows 10 Profesional

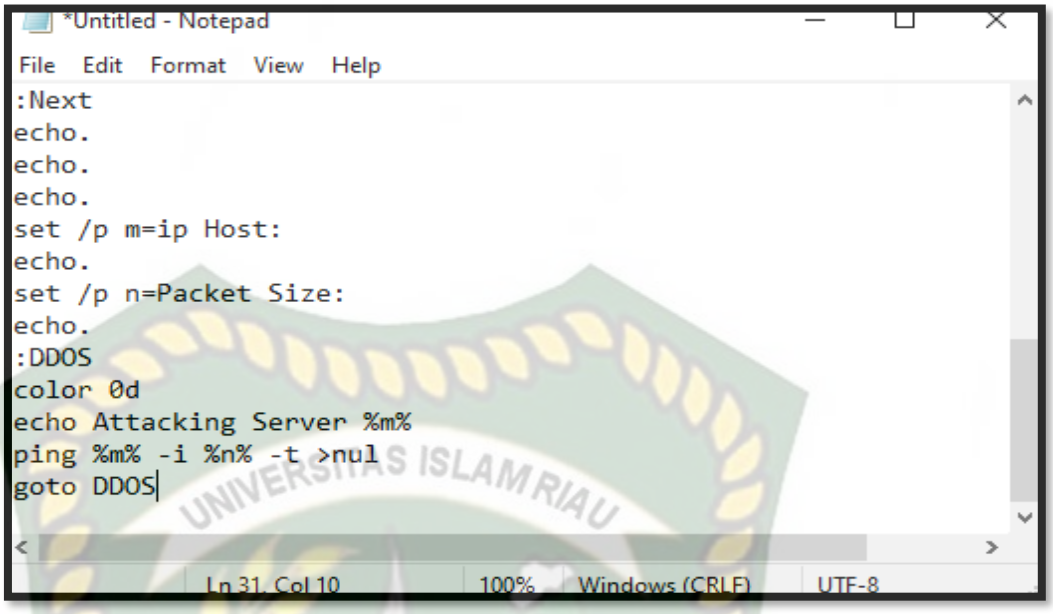
e. Command Prompt



Gambar 4.38 *Command Prompt*

Tools ini di gunakan untuk menuliskan *script* serangan kepada target yang akan di serangan.

f. Notepad



Gambar 4.39 *Notepad*

Tools ini di gunakan untuk menulis script serangan dengan mengubah ekstensi .bat yang akan menjadikan file tersebut menjadi sebuah prompt cmd untuk serangan DDoS nya.

Adapun Langkah serangan DDoS sebagai berikut :

1. Pertama Ketikkan Script berikut ini kedala Notepad

@echo off

mode 67,16

color 0b

cls

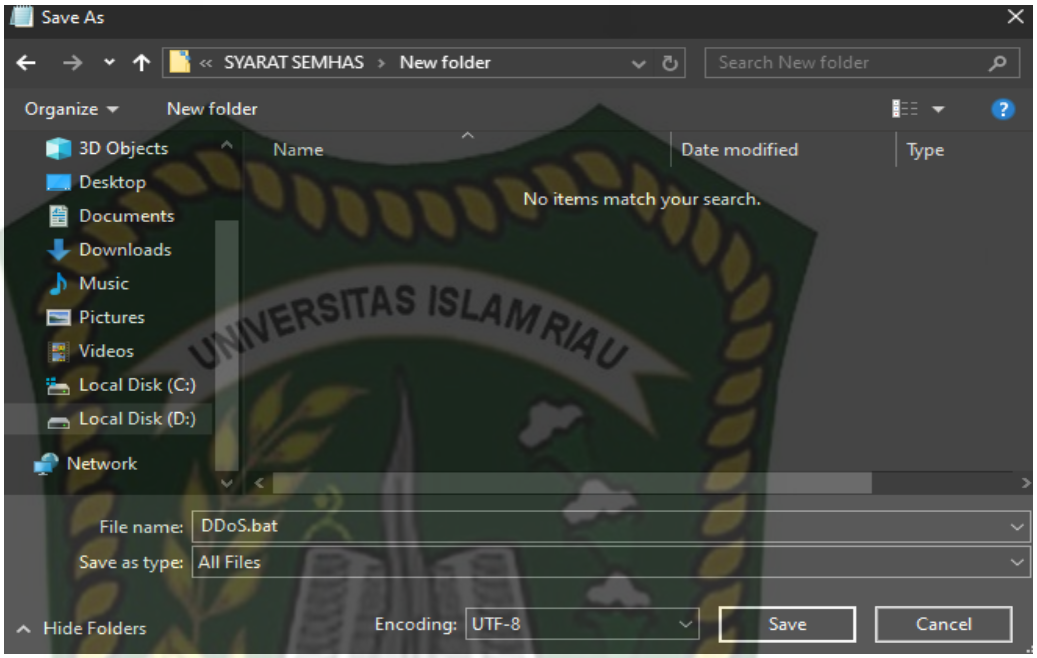
echo.

echo

echo

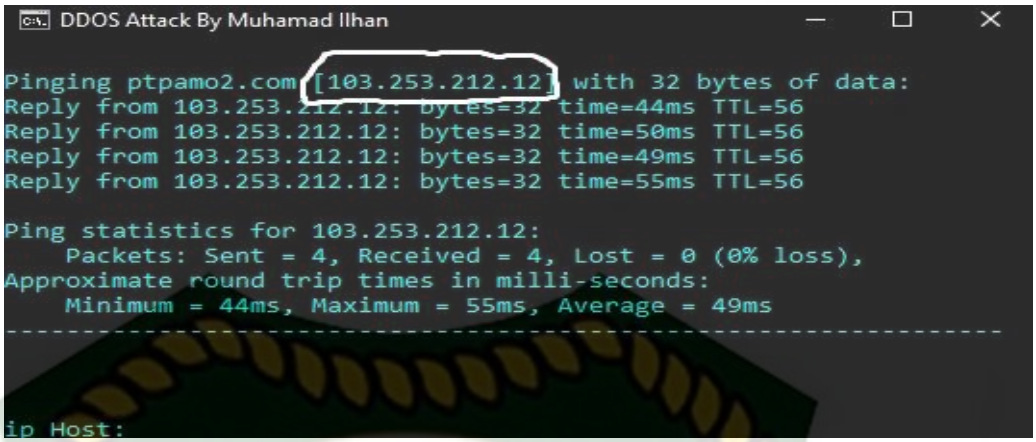
```
echo.
set /p x=Server-Target:
echo.
echo
ping %x%
echo
@ping.exe 127.0.0.1 -n 5 -w 1000 > nul
goto Next
:Next
echo.
echo.
echo.
set /p m=ip Host:
echo.
set /p n=Packet Size:
echo.
:DDOS
color 0d
echo Attacking Server %m%
ping %m% -i %n% -t >nul
goto DDOS
```

2. Kemudian script itu di ketik ke dalam notpad dan di save as dengan format .bat agar cmd nya berjalan.



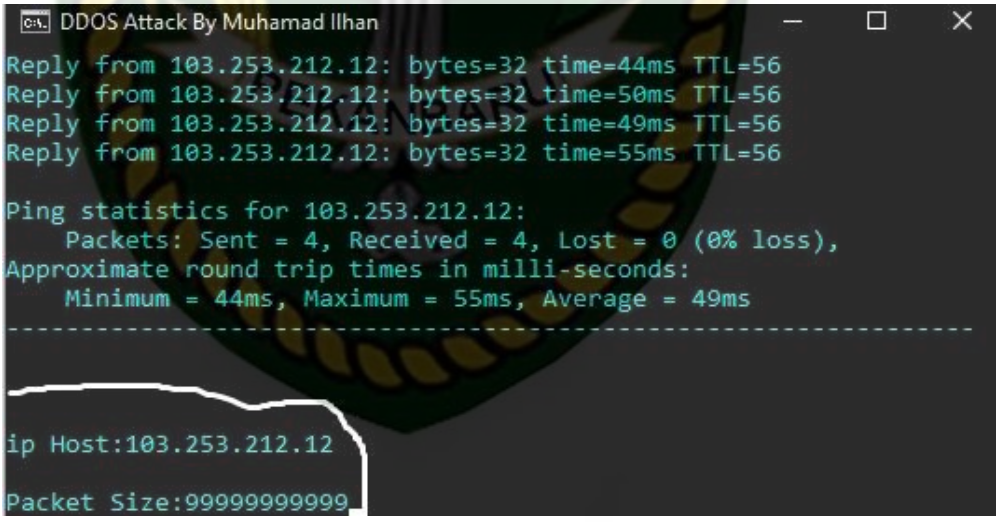
Gambar 4.40 *Save as .bat*

3. Kemudian jalankan file DDoS.bat dengan cara double click dan masukan domain target untuk mencari IP Server target. Karena untuk DDoS memerlukan IP Server nya. Dan berikut IP dari domain ptpn5.co.id 103.253.212.12



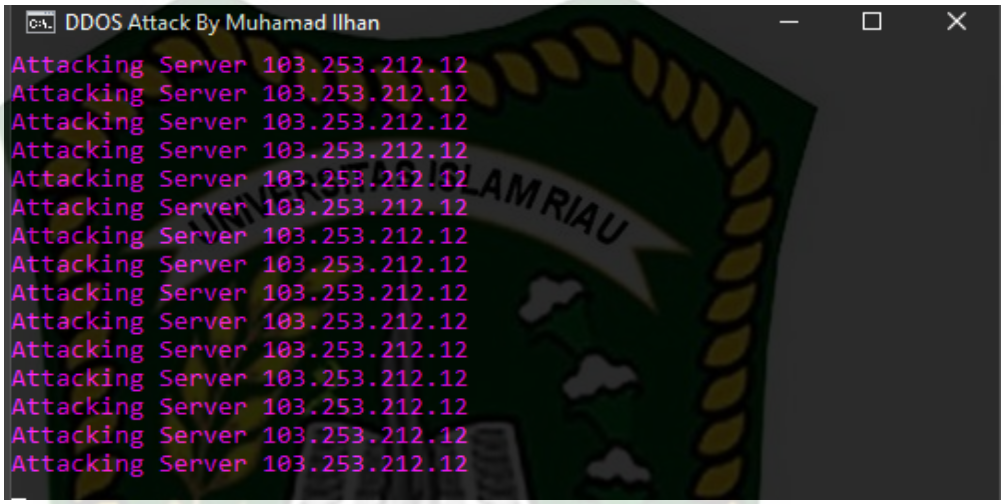
Gambar 4.41 *IP Addres Server* ptpn5.co.id

4. Selanjutnya pada Ip Host menginputkan IP yang telah di dapat yaitu 103.253.212.12 dan Isi *Packet Size* kemudian tekan *Enter*. *Packet Size* bermaksud jumlah paket yang dikirimkan ke server tersebut dan harus dengan jumlah yang besar agar server down, contoh *Packet Size* : 99999999999 lalu tekan Enter.



Gambar 4.42 *Ip Host and Packet Size*

5. Dan berikut adalah proses serangan yang sedang berjalan akan ada informasi *Attacking Server* 103.253.212.12. semakin banyak Packet Size maka semakin cepat membuat server down dan lebih baik lagi di lakukan dengan tim.



Gambar 4.43 Proses Serangan DDoS

4.2.3 *Identify Security Goals* (Mengidentifikasi tujuan keamanan)

Hasil pada tahap kedua ini melakukan Analisis tujuan dan persyaratan keamanan sistem dengan menggunakan cara *interiew* yang di perlukan oleh perusahan PT. Perkebunan Nusantara V untuk memastikan keamanan secara menyeluruh terhadap ketersediaan (*availability*)

Tabel 4.6 Tujuan Bisnis (*Business Goals*)

No.	Keterangan
1	Sistem HRIS di bangun untuk keperluan proses penyimpanan data karyawan dan identitas perusahaan
2	Sistem HRIS dapat melayani karyawan untuk melakukan penginputan data baru dan data pensiun serta informasi terkait masa jabatan
3	Sistem HRIS dapat menjaga privasi *user*. Dalam hal ini karyawan di awasi oleh admin sebagai pengelola sistem HRIS

Tabel 4.7 Tujuan Keamanan (*Security Goals*)

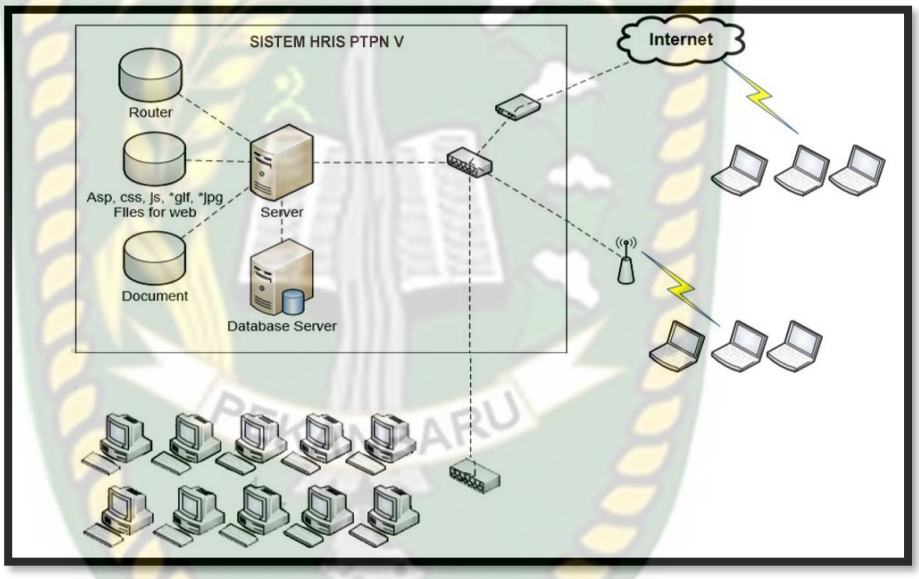
Goals		Tujuan Keamanan
G-01	Kerahasiaan (*Confidentiality*)	Data admin, data pengguna, dan informasi pengguna harus dirahasiakan dari akses pengguna ilegal. untuk mencegah pengguna ilegal mengetahui data autentikasi pengguna.
G-02	Integritas Data (*Data Integrity*)	Data admin, data pengguna, dan informasi pengguna harus tetap otentik. pengguna yang ingin terhubung dapat mengikuti semua prosedur di atas.
G-03	Ketersediaan (*Availabilty*)	Semua data dan informasi harus tersedia dalam sistem, terutama jika data diperlukan dan akan digunakan oleh pengguna.
G-04	Kontrol Akses (*Access Control*)	1. Hanya admin yang berwenang yang dapat melakukan penginoutan data pada system 2. Adanya kontrol akses terhadap pengguna dan komponen sistem
G-05	Penggunaan (*Aplication*)	1. Keamanan harus terkelola secara terstruktur dan terencana agar tidak menghambat proses bisnis 2. Menghindari resiko dari aktifitas yang merugikan sistem

4.2.4 *Develop Artifact* (Pengembangan Artefak)

Pada tahap ini akan Menjelaskan secara detail arsitektur sistem HRIS yang sedang berjalan yang berupa :

a. Diagram Arsitektur

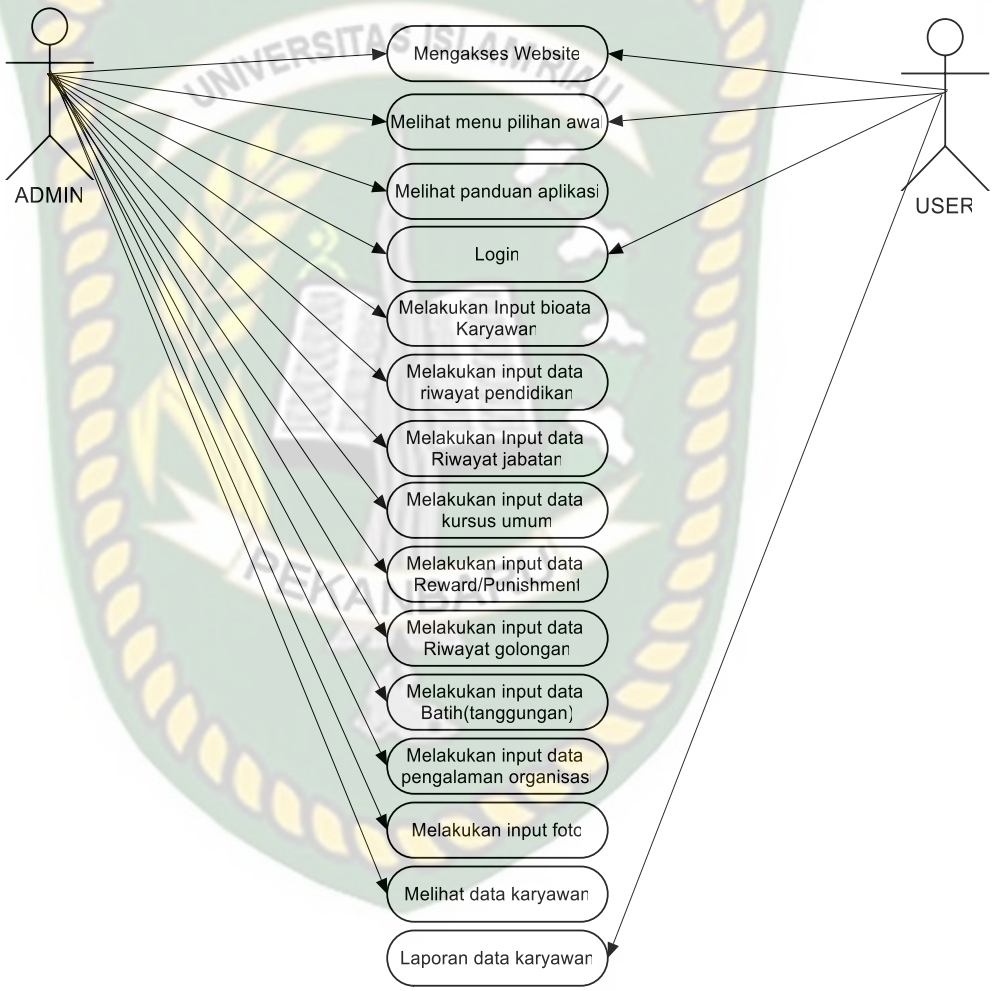
Pada perencanaan artefak maka merencanakan artefak, arsitektur sistem jaringan, deskripsi kinerja sistem.



Gambar 4.44 Arsitektur HRIS

b. Diagram *Use Case*

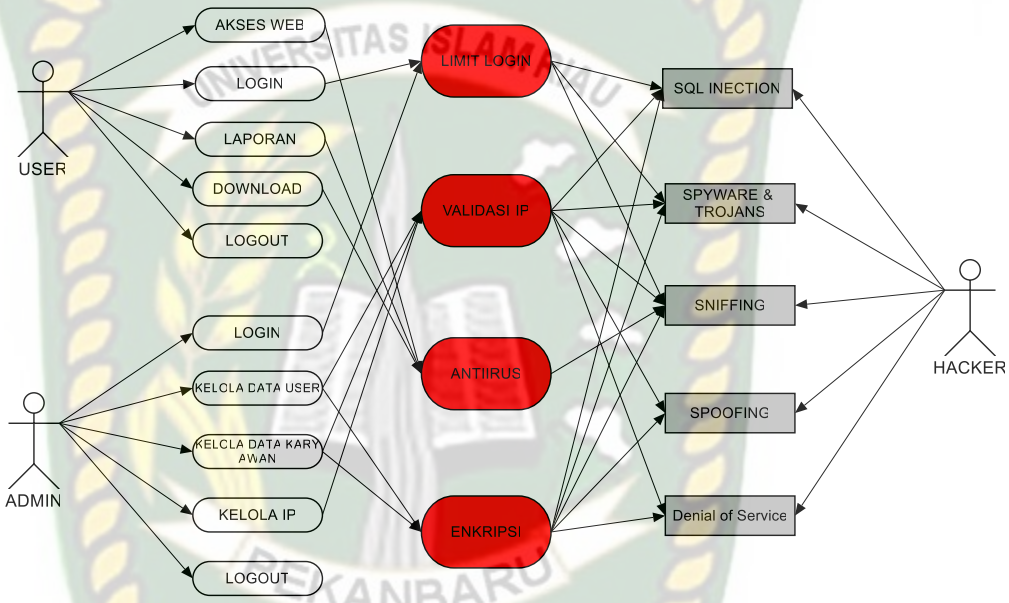
Use case merupakan skenario artefak untuk menanggapi tindakan yang terjadi dalam proses bisnis, menyediakan konteks bagi operasi, pemangku kepentingan, dan tim teknik untuk memahami interaksi komponen sistem



Gambar 4.45 Use Case Diagram Aplikasi HRIS

c. Diagram *Misuse Case*

Misuse cases merupakan Insiden penyalahgunaan termasuk serangkaian serangan yang terjadi pada sistem, pengguna ilegal mencoba masuk ke sistem menggunakan langkah atau metode illegal

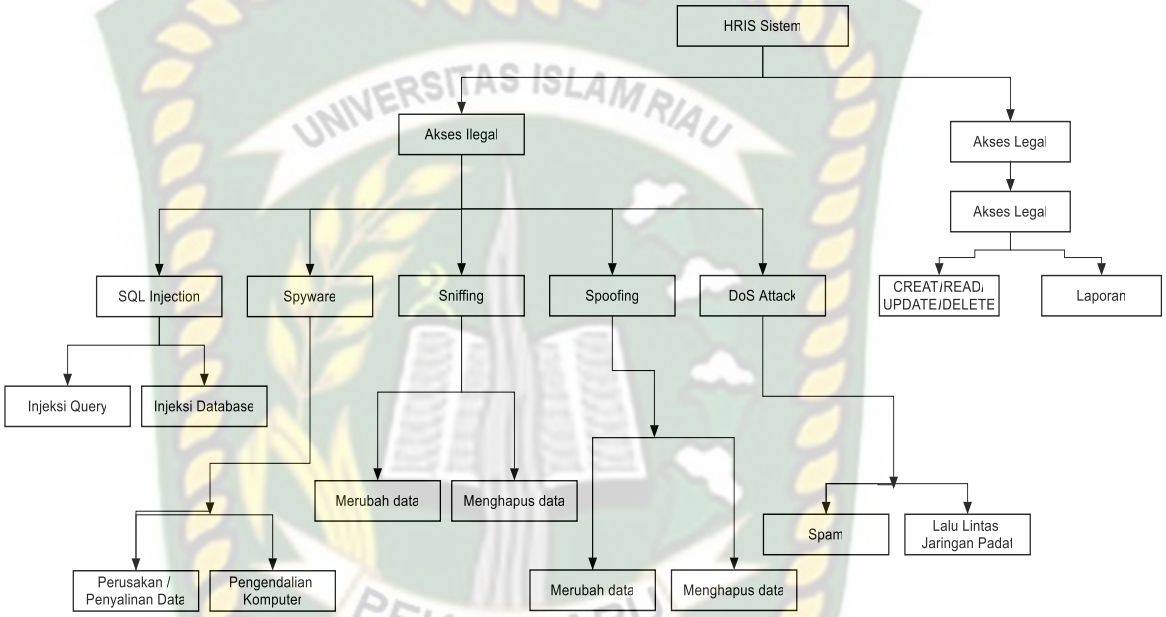


Gambar 4.46 Misuse Case Aplikasi HRIS (MU-01)

d. At*tack Tree*

Pohon serangan merupakan tindakan formal yang menggambarkan ancaman keamanan terhadap sistem dengan jenis serangan yang dapat terjadi dan diimplementasikan.pohon serangan yang terjadi dalam proses sistem HRIS diantaranya:

- Pohon serangan SQL Injection (MC-01)
- Pohon serangan Spyware and Trojans (MC-02)
- Pohon serangan Sniffing (MC-03)
- Pohon serangan Spoofing (MC-04)
- Pohon serangan Denial of Service (MC-05)



Gambar 4.47 Attack Tree Sistem HRIS

4.2.5 *Perform Risk Assesment* (Penilaian Risiko)

Pada tahap ini melakukan analisa Penilaian risiko secara kualitatif dan bertahap untuk mengidentifikasi ancaman terhadap sistem yang kemungkinan terjadi dan ini adalah hasil dari penilaian risiko dengan melakukan metode *interview*.

Tabel 4.8 Penilaian Risiko

No	Kategori Ancaman	Kondisi	Dampak	Kategori
1	SQL Injection	Melakukan acak login pada menu login klien	Kehilangan data pengguna dan password pengguna yang legal	Medium
2	Data Sniffing	Melakukan pengintipan lalulintas jaringan	Penyerang dapat melihat dengan jelas dan mengetahui aktifitas data di sistem.	Low
3	Mac Address Spooffing	Mengambil IP Address yang ada di dalam jaringan untuk di palsukan	Penyerang dapat mengambil informasi yang tersedia pada pengguna legal	High
4	Trojans	Melakukan perusakan sebuah komputer	komputer mengalami kerusakan berupa virus yang di suntikkan.	Low
5	Denial of Serices	Mengirim data dalam jumlah banyak terhadap server agar server mengalami kerusakan.	Membuat jaringan menjadi padat sehingga komputer tidak menanggapi permintaan layanan	Medium

4.2.6 *Select Elicitation Technique* (Memilih teknik elisitasi)

Pemilihan Teknik elisitasi yang dilakukan penulis yaitu dengan cara interview, sumber tertulis dan observasi. Karena metode elisitasi ini sangat efisien karena langsung mengetahui dari instansi apa saja yang perlu di pecahkan dan mengenali

batasan batasan sistem dan mengenali siapa saja pemangku kepentingan untuk tujuan sebuah sistem.

4.2.7 *Elicit Security Requirements* (Permintaaan persyaratan keamanan)

Untuk melakukan Elisitasi persyaratan keamanan maka melakukan elisitasi keamanan yang baik dan dari hasil interview, sumber tertulis dan observasi, kemudian dibentuk dalam daftar kebutuhannya. Berikut adalah hasil dari persyaratan keamanan.

R : *Requerements*

Tabel 4.9 Persyaratan Keamanan

R-01	Kebutuhan untuk memverifikasi di gateway dengan hanya membatasi komputer dengan resolusi alamat IP tertentu yang terdaftar di komputer server sehingga tidak dapat memalsukan data.
R-02	Persyaratan untuk kontrol akses berbasis peran yang mengontrol elemen sistem (data, fungsi, dll.), Pengguna dapat berkomunikasi dengan sistem. Karakter yang ditentukan hanya memperbolehkan huruf a - z, A - atau angka 0 - 9 dan melarang karakter unik atau symbol.
R-03	diperlukan untuk rencana kerja ketersediaan sistem. Setiap pengguna diharuskan menggunakan nama pengguna dan kata sandi kominasi, seperti angka, huruf besar, atau huruf kecil.
R-04	Sistem ini diperlukan bagi personel keamanan yang ditunjuk untuk memantau status dan penggunaan, termasuk peralatan keamanan
R-05	Petugas yang ditunjuk diperlukan untuk memantau sumber daya sistem dan penggunaannya secara teratur.
R-06	Sistem diperlukan untuk komunikasi jaringan yang dilindungi dari informasi yang tidak sah, menguping enkripsi, dan metode lainnya. Enkripsi sangat membutuhkan penyebaran, seperti otentikasi login. karena untuk mencegah peretas membobol sistem agar tidak mengetahui akses login.
R-07	Memerlukan izin proses penting untuk mencegah perangkat di gunakan secara ilegal.

R-08	Lindungi perangkat dari kerusakan, pencurian, atau penggantian perangkat yang tidak dikenal, kecuali bencana alam.
R-09	Implementasi komponen keamanan virus perangkat lunak yang dirancang untuk keamanan perangkat lunak yang lebih baik, seperti antivirus

4.2.8 *Categorize Requirements* (Mengkategorikan Persyaratan)

Setelah persyaratan yang dihasilkan maka selanjutnyayaitu mengelompokan persyaratan keamanan yang dipilih, dalam hal ini menggabungkan langkah-langkah pengelompokan, penamaan, dan kategorisasi bersama-sama. Berikut table pengkategorian nya:

Tabel 4.10 Kategori Persyaratan

A. KERAHASIAAN	B. AKSES KONTROL
- Admin yang mengakses internet melalui LAN dan wireless harus terjaga kemananan nya agar data rahasia tidak diketahui oleh pengguna yang tidak sah atau illegal.	1. Hanya user yang terdaftar saja yang dapat melakukan akses pada kontrol sistem. 2. Adanya pengaturan akses kontrol terhadap keamanan jaringan
C.INTEGRITAS DATA	D.PENGELOLAAN
- setting secara rutin terhadap data user, akses control agar tidak dapat di serang pengguna ilegal.	- Adanya proses manajemen hak akses yang dapat dipertanggung jawabkan atas kebenaran data yang ada.
E.PENGGUNAAN	F.AUTHENTIFIKASI
1. Penerapan manajemen terhadap Sistem keamanan agar dapat di Kelola dan tidak mengganggu aktifitas sistem.	- Melakukan authentikasi dengan baik dan sesuai dengan prosedur ketentuan.

2. Melakukan Authentikasi terhadap akses user yang harus selalu tersedia. 3. Menghilangkan risiko terhadap aktifitas yang dapat merusak sistem.	

4.2.9 *Prioritize Requirements* (Prioritas Persyaratan)

Proses ini memprioritaskan pemilihan persyaratan keamanan untuk jaringan nirkabel dan LAN pada jaringan di PT berdasarkan penyalahgunaan yang dibuat sebelumnya. Untuk memprioritaskan serangan yang membuat ancaman lebih berbahaya, tabel prioritas ancaman diharapkan dapat mengatasi masalah ini..

Tabel 4.11 Prioritas Keamanan

Tujuan	***Confidentiality* , *Integrity* dan *Availability***
Kebutuhan	- Keamanan sistem login dan server - Keamanan pada alamat IP - Database yang terjaga kerahasiaannya
Kategori	- Unauthorize Attack - Access Control - Privacy - Authentication
Rekomendasi	- Pemasangan firewall pada server

	- Penggunaan tanda tangan digital untuk sistem login - Patching pada sistem apikasi. - Pemasangan Anti virus. - Menerapkan enkripsi pada system database Perubahan password admin secara rutin - Installasi SSL pada cPanael

Tabel 4.12 Kategori Prioritas

Requirements	Missusecase	Prioritas
Penerapan *Password* Enkripsi	MU-01	MEDIUM
Menerapkan Anti Virus	MU-01	LOW
Pemasangan Firewall pada Server	MU-01	HIGH
Menerapkan Enkripsi dan Authentifikasi	MU-01	HIGH
Instalasi SSL pada cPanel	MU-01	HIGH

4.2.10 *Requirement Inspection* (Penilaian Kebutuhan)

Membuat table penilaian dan dalam metode ini memberikan tanggung jawab kepada anggota tim inspeksi dan mengembangkan log dengan tinjauan rekomendasi masalah terperinci untuk arsitektur dan persyaratan kebijakan implementasi keamanan sistem berdasarkan tingkat prioritas penyalahgunaan

Tabel 4.13 Penilaian Kebutuhan

Goal(s)	Melindungi akases jaringan computer serta data yang terdapat didalamnya dari serangan pihak lain.
Requerement(s)	Sistem harus memenuhi ketentuan : • Sistem harus dapat melindungi dirinya sendiri dari virus dengan menggunakan perangkat lunak pendeteksi virus dengan data yang terupdate • Sistem harus dapat mendeteksi Ketika serangan seperti *SQL Injection dan* DoS Ketika itu terjadi sistem harus memberi admin atau melalui notifikasi sehingga dapat langsung di cegah . • Sistem harus menggunakan Teknologi *Firewall* • Sistem harus memiliki enkripsi data yang baik. • Sistem harus di pasangkan SSL.
Category	Unauthorize Attack, Access Control, Privacy, Authentication, Encryption,
Missuse Case	MU-01
Implementation	Fitur yang telah di implementasi dalam sistem: • *Virus Detection* dengan menggunakan *Software* Antivirus • *Encode/Decode* algoritma • Pengamanan pada *Web Server* • Pembenahan pada Konfigurasi *Firewall* • Penerapan ACL pada jaringan • *Double Autentication* pada setiap aktifitas

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian ini, penulis dapat menyimpulkan bahwa metode SQUARE sangat berguna untuk menganalisis dan membuat rekomendasi kebutuhan keamanan sistem yang bertujuan untuk meningkatkan ketersediaan, kontinuitas dan integritas Sistem Informasi HRIS PT. Perkebunan Nusantara V AMO-II Sei Lala. Metode SQUARE ini memungkinkan Anda untuk mengetahui bahwa bagian kerentanan yang dapat dimasukkan oleh pengguna jahat dan dapat digunakan sebagai perencanaan saat membangun sistem dan infrastruktur.

5.2 Saran

Adapun saran yang dapat peneliti berikan yaitu:

A. Bagi Perusahanan

Untuk dapat meningkatkan sistem keamanan yang lebih baik, diharapkan untuk melakukan Pemasangan Firewall pada server agar dapat mengawasi arus data yang mengalir pada jaringan internet dan lakukan keamanan tambahan berupa tanda tangan digital untuk sistem login. Lebih baik lagi jika menerapkan Enkripsi pada database agar orang lain tidak dapat melihat *source* aslinya dan lakukan Instalasi SSL pada cPanel agar dapat mengamankan

pertukaran data yang terjadi melalui jaringan internet dan merubah menjadi https, selanjutnya kontrol rutin di area kontrol akses sehingga ancaman yang mungkin timbul secara tak terduga dapat dipertahankan dan dihindari dan diharapkan dapat menambahkan kebijakan dan prosedur keamanan jaringan yang sepenuhnya lebih baik untuk menjaga kelangsungan operasi bisnis untuk lebih meminimalkan segala jenis ancaman dan serangan dengan sengaja atau tidak sengaja dilakukan oleh pengguna atau orang yang bekerja dengan perusahaan.

B. Bagi Peneliti Selanjutnya

Penggunaan metode SQUARE, baiknya dilakukan oleh tim, agar pada saat uji dan analisis mendapatkan hasil yang lebih rinci terhadap sistem Human Resources Information System (HRIS) PT. Perkebunan Nusantara V AMO-II Sei Lala dan Hasil dari metode SQUARE ini, ada baiknya dibandingkan dengan hasil metode yang lain, metode yang berhubungan dengan keamanan.

DAFTAR PUSTAKA

Akbar, (2015). *Evaluasi Keamanan jaringan Wireless Hotspot Menggunakan Metode SQUARE*. Jurnal Teknik Informatika, STMIK Sumedang.

Ambo & Ghufron, (2015). *Rancang Bangun Aplikasi Human Resources Information System (HRIS) Menggunakan Metode Model View Controller (MVC).* Jurnal Teknik Informatika, Universitas Muhammadiyah Jakarta.

Apriandari & Sasongko, (2018). *Analisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Diskominfo Kota Sukabumi).* Jurnal Ilmiah SANTIKA, Universitas Muhammadiyah Sukabumi. Vol. 8, No. 1

Geges & Wibisono, (2015). *Pengembangan Pencegahan Serangan Distributed Denial of Serices (DDoS) Pada Sumber Daya Jaringan dengan Integrsi Network Behavior Analysis dan Client Puzzle.* Jurnal Ilmiah Teknologi Informasi, Institut Teknologi Surabaya. Vol. 13, No. 1

Martsanto & Nabihi, (2016). *Analisis Kebutuhan Keamanan Informasi Menggunakan Metode SQUARE pada Aplikasi Remittance.* Jurnal Ilmiah Ilmu Komputer, Universitas Budi Luhur Jakarta Selatan. Vol. 2, No. 1

Muhammad Agreindra Helmiawan, (2018). *Analisis Keamanan Sistem Informasi E-Learning Menggunakan Metode Square.* Jurnal Manajemen Informatika, STMIK Sumedang.

Ramadhani et al., (2018). *Manajemen Risiko Keamanan dengan Menggunakan Metode OCTAVE ALLEGRO dan Kontrol ISO 27001 Pada Instansi Pelayanan Penyelenggara Publik.* Jurnal Seminar Teknologi Nasional, Uniersitas Gajah Mada

Saputra et al., (2017). *Penilaian Ancaman pada Website Transkrip Aktivitas Kemahasiswaan Politeknik Negeri Batam Menggunakan Metode DREAD.* Jurnal Integrasi, Politeknik Negeri Batam. Vol. 9, No. 1

Susanto et al., (2018). *Analisis Sniffing Password Menggunakan Aplikasi Cain Dan Abel Pada Jaringan Wifi Universitas Semarang.* Jurnal Teknik Informatika, Universitas Semarang. Vol. 16, No. 1

Umar et al., (2019). *Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI).* Jurnal Sistem Informasi Bisnis, Universitas Ahmad Dahlan Yogyakarta. Vol. 9, No. 47-54

Veny Charnita Br Ginting et al., (2019). *Deteksi Serangan ARP Spoofing Berdasarkan Analisis Lalu Lintas Paket Protokol AR.* Jurnal Pengembangan Teknologi Informasi dan Imu Komputer, Universitas Brawijaya. Vol. 3, No. 5

Yulianingsih, (2016). *Menangkal Serangan SQL Injection dengan Parameterized Query*. Jurnal Edukasi dan Penelitian Informatika, Universitas Indraprasta PGRI. Vol. 2, No. 1

Zulfa & Subiyanta, (2015). *Pemanfaatan Spyware untuk Monitoring Aktivitas Keyboard dalam Jaringan Microsoft Windows.* Jurnal Emitor, Universitas Cirebon. Vol. 15, No. 1