Plagiarism Checker X Originality Report

Similarity Found: 10%

Date: Kamis, Desember 19, 2019
Statistics: 384 words Plagiarized / 3969 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN DENGAN WIRESHARK Rahma Hanipah Jurusan Teknik Informatika Universitas Indraprasta PGRI (UNINDRA) JL. Raya Tengah No.8 Gedong, Pasar Rebo, Jakarta Selatan. Telepon : (021) 87797409 Website: http://www.unindra.ac.id Abstrak: Dalam membangun suatu jaringan di dunia jaringan computer, hal yang paling sangat dibutuhkan dalam jaringan computer adalah tentang keamanan jaringan.

Komunikasi dan laju kecepatan traffic dalam suatu jaringan sangatlah rentan terhadap suatu serangan, dengan tingkat laju seperti itu, system tidak cukup hanya tentang system keamanan jaringan saja, dikarenakan system jaringan yang sangat rentan tersebut, diperlukan sebuah tools yang dapat menemukan dan mendeteksi adanya suatu kegiatan serangan dari jaringan. Macam macam serangan ada flooding dan syn flood.

Serangan ini memiliki tujuan untuk membuat computer yang terhubung dan terkoneksi mengalami gangguan dan kurang berjalan normal di dalam jaringan komputer. Software khusus yang mampu mengendalikan kondisi tersebut dinamakan wireshark, dengan wireshark aktifitas jaringan computer mampu di jaga keamanannya dan memproteksi dengan mendeteksi suatu serangan di dalam computer sehingga user tidak perlu khawatir dengan hal tersebut. Kata Kunci: Wireshark, Jaringan Komputer, Serangan Jaringan.

Pendahuluan Keamanan jaringan komputer ini mencakup ke beberapa jaringan komputer, baik swasta maupun negeri, untuk dilakukan pada pekerjaan sehari-hari dalam transaksi dan komunikasi dikalangan bisnis, instansi pemerintahan dana individu. Dari pengamatan yang telah dilakukan tentang keamanan dalam jaringan computer

dapat dilihat dari segi bentuknya,yaitu: Keamanan hardware Didalam jaringan computer dibutuhkan sebuah komponen yang bersifat perangkat keras yang digunakan untuk jaringan komputer.

Keamanan hadwere wajib menjadi hal utama yang harus kita perhatian dalam jaringan computer, namun hal tersebut sering terabaikan. Dalam keamanan hardwere, server, dan tempat penyimpanan data wajib menjadi perhatian utama. Akses melalui fisik terhadap suatu server serta data data penting dibatasi secara maksimal.

Keamanan software Sesuai dengan namanya, perangkat lunak lah yang paling wajib untuk kita perhatinkan dan kita amankan, beberapa contoh perangkat lunak yang kita maksud adalah tentang system operasi, system aplikasi, data dan informasi serta data data yang tersimpan dalam komputer jaringan terutama pada server. Seperti misalnya server bertugas sebagai router, maka software web server serta FTP server tidak perlu dipasang, Membatasi software yang dipasang dapat mengurangi konflik antar software yang membatasi akses, contohnya apabila router dipasangi juga menggunakan FTP server, maka orang dari luar dengan login anonymous mungkin bisa saja mengakses router tersebut.

Wireshark dalam memonotor suatu jaringan komputer dapat membantu memudahkan seorang administrator jaringan untuk melakukan pengawasan terhadapt suatu jaringan komputer. Dengan aplikasi wireshark ini kita dapat melakukan monitoring, meninjau serta melakukan penyimpanan informasi sebuah paket baik paket yang keluar maupun paket yang masuk didalam suatu jaringan secara detail.

Selain itu tampilan grafis (GUI) pad wireshark cukup baik sehingga lebih memudahkan dalam memonitoring semua aktifitas serta kegiatan yang dilakukan pada suatu jaringan atau terhadap jaringan yang kita punya. Keamanan Jaringan Untuk menghindari berbagai macam serangan baik itu oleh para hacker ataupun craker keamanan jaringan sangatlah diperlukan.

Ternyata serangan tersebut bukan Cuma berasal dari serangan para hacker dan craker, tetapi juga berasal dari lingkuan sekitar kita. Oleh karna itu administrator diharuskan lebih teliti dalam memilih atau menganalisa sistem jaringan yang digunakan. Pada dasarnya komputer yang terhubung ke dalam jaringan memiliki ancaman serangan yang lebih besar dibandingkan dengan komputer yang tidak terhubung kejaringan.

Resiko ini dapat dikurangi oleh network security, namun network security ini akan bertentangan dengan software network acces. Dikarenakan adanya network access, network security dapat memiliki kerawanan yang tinggi. Berikut ini merupakan jenis –

jenis keamanan jaringan computer : Didalam komputer harusnya mempunyai beberapa sistem keamanan yang baik.

Hal ini dimaksudkan untuk menghindari terjadinya serangan – serangan oleh para hacker atau pelaku lain yang dapat mengganggu kinerja komputer anda seperti yang telah dijelaskan tadi. Pada dasarnya sistem keamanan komputer memiliki 5 jenis keamanan yang dapat memperkuat system keamanan komputer: Keamanan fisik Klasifikasi keamanan yang ini makin didukung melalui hardware ataupun perangkat keras.

Dari maksud hal ini bermagsud supaya mampu melindungi hardware agar selalu dalam kondisi yang baik supaya bisa dipergunakan dalam melaksanakan operasi kepada jaringan. Keamanan Jaringan Keamanan jaringan akan makin bertipe pada abstrak. Kenapa abstrak? Karena jenis keamanan dilakukan oleh benda tidak keliatan atau tidak kasat mata, baik itu menggunakan sofwere maupun perintah tertentu.

Contoh keamanan jaringan yang satu ini yaitu, dengan menggunaka proxy maupun firewall untuk melakukan fiter pada user yang ingin menggunakan jaringan. Otorisasi Akses Jenis keamanan jaringan Otorisasi Akses adalah suatu keamanan jaringan dengan pemakaian password atau kata sandi apabila kita akan menghubungkan sesuatu pada jaringan. Hal tersebut dilakukan agar administrator bisa menentukan hanya melaui user yang sudah dipilih saja yang bisa terhubung pada sebuah jaringan.

Proteksi Virus Virus adalah metode penyerangan pada system computer dengan menggunaka program akan mampu merusak dan menjadikan sistem yang ada di komputer menjadi berantakan dan mengakibatkan kerusakan. Untuk menangani serangan virus ini, kita bisa gunakan atau menginstal sofwere anti virus pada komputer selalu update dengan database baru.

Penganan Rencana Penganan Rencana ini merupakan langkah – langkah yang harus diambil apabila terjadi bencana alam yang menangakibatkan kerusakan dan kehilangan data – data penting pada semua system jaringan computer. Perencanan bencana ini bertujuan untuk terjadinya kerusakan pada system dapat cepat teratasi. Untuk memahami mengenai pengertian dari jaringan komputer serta hal – hal penting yang terdapat pada jaringan komputer, berikut ini adalah pengertian jaringan komputer menurut para ahli serta hal – hal penting yang ada di jaringan komputer itu sendiri: Pengertian Jaringan Komputer Menurut Jafar Noor Yudianto (2007) jaringan komputer adalah sebuah sistem yang terdiri atas computer - komputer yang di hubungkan satu sama lain untuk dapat berbagi sumber daya satu sama lain seperti printer dan cpu, dan dapat saling berkomunikasi baik dalam surel atau pesan instan, serta agar dapat

melakukan akses pada suatu informasi atau peramban web.

Tujuan dari suatu jaringan komputer yaitu bertujuan agar setiap computer dapat dalam jaringan computer bisa meminta serta memberikan pelayanan atu memberikan sebuah service. Pada suatu jaringan perangkat yang mengakses baik menerima atau menggunakan layan biasadisebut perangkat klien (client) dan perangkat yang menyediakan atau mengirim layanan biasa disebut peladen (server).

Desain ini biasa disebut dengan metode sistem client-server, metode ini biasa digunakan hampir seluruh penerapan atau pembuatan suatu jaringan komputer. Sedangkan menurut Umi Proboyekti disebutkan bahwa jaringan komputer adalah kumpulan beberapa computer yang berjumlah banyak serta terletak secara terpisah-pisah tetapi sama-sama terakses dengan yang lain.

Sebuah computer bias dikatakan saling terhubung apabila computer terhbung dengan satu computer lain, atau terhubung dengan banyak computer dengan kondisi dapat saling berpindah informasi ataupun data dengan yang lain. Bentuk koneksi dalam jaringan komputer dapat melalui media kawat tembaga atau melalui kabel serat optik, delombang mikro, maupun satelit komunikasi.

Dari beberapa pendapat diatas maka dapat disimpulkan bahwa jaringan komputer merupakan suatu jaringan pada telekomunikasi yang menghubungkan satu computer dengan computer yang lain dengan tujuan agar dapat untuk saling berkomunikasi serta dapat bertukar data satu sama lain. Penyalahgunaan Protokol TCP Transmision Control Protocol (TCP) adalah sebuah layanan yang menyediakan pengiriman data oleh protokol, TCP merupakan protokol yang bersifat reliable, byte stream service, connection-oriented.

Connection oriented ialah dua aplikasi pengguna TCP dapat dilakukan pembentukan hubungan terhadap bentuk pertukaran kontrol informasi (handshaking) sebelum transmisi pada data terjadi. Realiable ialah suatu proses deteksi kesalahan paket TCP dan mentransmisikan kembali. Byte stream service adalah paket yang dikirimkan dan sampai ketempat tujuan dengan secara berurutan. Dasarnya jenis protkol TCP sulit untuk disalah gunakan.

Kecuali penyusup mengontrol router pada diantara dua sistem, penyusup itu bisa selalu dilacak keberadaannya sehingga penggunaan seperti penggunakan syn attack, Penyalahgunaan yang sering dilakukan dalam protokol ini adalah syn attack, syn attack adalah jenis serangan yang memanfaatkan kelemahan koneksi TCP, penyerang mengirimkan paket TCP SYN secara acak ke host tujuan akan mengirim kembali paket

SYN ACK.

Serangan berjenis ini sangat sulit untuk dideteksi untuk alamat pengumannya karena alamat IP dari pengirim tersebut telah disaruhkan dengan menyeleksi paket router dengan menghubungkan jaringan internet, terlihat seperti gambar 1. Gambar 1: SYN TCP Attack. Gambar diatas tersebut adalah sebuah paket SYN yang dalam proses pengiriman yang telah disamarkan, ketika paket SYN sampai ke server, selanjutnya akan diteruskan untuk mengalokasikan buffer pada memori yang dibutuhkan.

Flooding data Data Data merupakan kumpulan huruf atau angka yang belom diolah sehingga tidak memiliki ari, atau bisa juga disebut sebagai catetan atas kumpulan fakta. Data merupakan bentuk Dalam bentuk jamak data dapat disebut datum. yang kalau diubah kedalam bahasa latin, data memiliki arti "suatu yang harus diberikan". Data dalam sebuah peryataan berarti yang telah diterima dalam penggunaan sehari – hari secara apa adanya, Pernyataan ini didapat dari sebuah hasil pengamatan atau survei yang berupa angka dan kata – kata citra secara fakta yang disatukan untuk menjadi data.

Kemudian data diolah agar dapat diaturkan dengan jelas sehingga orang lain dapat dengan mudah mengerti apa yang telah mereka alami, hal ini disebut deskripsi. Pemilihan banyak data sesuai dengan persamaan atau perbedaan yang dikandunganya dinamakan klarifiasi. Flooding Data yang pengirimannya berlebihan besar kecilnya sebuah paket atau besar kecilnya jumlah paket dalam jaringan, umumnya data yang tidak terpakai dapat disebut dengan Flood Data. adakalanya data-data yang berbeda dalam aktifitas didalam jaringan komputer merupakan data yang tidak dibutuhkan.

Data-data tersebut menang sengaja dikirim oleh seseorang meneruskan jaringan data yang ada. Lambatnya jalur traffic diakibatkan oleh adanya pengiriman data kedalam jaringan yang juga dapat mengakibatkan kerugian lain. Adanya intruder dari kerusakan program yang masuk kedalam jaringan. Suatu jaringan mengalami turun naik selama pemakaianya pada Traffic data.

Traffic Akan terjadinyaa turun naik selama pemakaian pada traffic data yang ada dalam jaringan. Akan adanya keterlambatan dalam penerimaan dan pengiriman data, sampai pada data yang dikirim ataupun data yang akan datang mengalami antrian data, sehingga traffic data akan mengalami gangguan, karna pada jam sibuk traffic data sangat padat.

Jenis-jenis Flood attack: Ping of death Pengiriman echo request ICMP secara berlebihan dalam suaru jaringan. Terjadinya system crash karna pengiriman paket ini, yauitu reboot

atau hang. Smurf Attack Smurcf attack paket ICMP memiliki kemiripan dengan Ping of death akan tetapi perbedaannya terdapat pada pengirimannya, Smurf Attack tidak akan dikirim secara langsung kepada korban melainkan akan melalui perantara.

Pada awalnya ini dikirim sebuah paket ICMP echo request ke sebuah host lain, supaya host tersebut bisa mengirimkan paket ICMP PING secara terus menerus kepada korban terakhirnya. Syn Floodingh flood SYN terjadi bila suatu host hanya mengirimkan paket SYN TCP saja secara kontinyu tanpa mengirimkan paket CK sebagai konfirmasinya. Hal ini akan menyebabkan host tujuan akan terus menunggu paket tersebut denngan menyimpannya kedalam backlog.

Walaupun besar paket kecil, tetapi apabila pengiriman SYN tersebut terus menerus akan memperbesar backing. Hal tersebut mengakibatkan penolakan otomatis dari host tujuan semua paket SYN yang datang, jadi host pun tidak dapat terkoneksi oleh host yang lain. UDP flood Pengiriman data UPD yang berlebihan kesuatu jaringan, sehingga pnegiriman UDP flood dapat terbentuk suatu lajur hubungan denga UDP dari host tujuan.

Serangan dapat terjadi pada saat administrator sedang bekerja maupun tidak pada server jaringan komputer. Oleh karena itu dibutuhkan system pertahanan pada server itu sendiri yang dapat menganalisa secara langsung, jadi pada setiap paket yang masuk itu adalah data yang diharapkan atau data yang tidak diharapkan.

Kalo paket itu merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan yaitu dengan mengeblok atau memblokir IP asal paket tersebut. Pemodelan suatu system yang digunakan untuk mengatasi flooding data pada suatu jaringan. System ini membuat suatu firewall yang aktif yang dapet mengdeviniskan pada tiap data yang masuk keserver, apakah data yang datang adalah sebuah data flood atau data yang dibutuhkan oleh user.

Pemodelan dibuat dengan menggunakan bahas pemograman Delphi 7 dan dalam lingkungan jaringan komputer berbasis IP address local area Network. Flooding data hanya bisa dicegah hanya sampai pada titik server saja, dan hanya bisa mencegah data masuk ke dalam yang bisa menyebabkan kerusakan lebih parah. Akan tetapi proses pengiriman data oleh pelaku flooding masih tetap berlangsung tanpa bisa dihentikan, sebagai aktibat pengiriman data yang terus menerus itu tentunya traffic yang ada akan mengalami keterlambatan, sehingga masih diperlukan suatu system untuk menyempurnakan system ini dengan menambahkan suatu komunikasi dari server kepada server. Untuk hal ini hubungan server local keserver yang lebih tinggi.

Tujuan komunikasi ini merupakan untuk membuat pemblokiran IP pada server yang

lebih tinggi sehingga jika terjadi gangguan lebih dapat dikurangi lagi. Traffic di jaringan local dapat menjadi normal karena data sebelumnya terjadi sudah diblokir ditingkat lebih atas. Wireshark Wireshark adalah salah satu dari alat analisa jaringan yang biasa dipakai oleh seorang Network Administrator untuk melakukan pemecahan masalah yang ada dalam jaringan, menganalisa, perangkat lunak atau untuk pengembangan sebuah protocol dalam komunikasi, dan atau dalam pendidikan.

Pertama kali wireshar muncul dengan nama Ethereal, lalu pada bulan Mei tahun 2006 proyek ini mengganti namanya menjadi Wireshark karena ada permasalahan mengenai merk dagang. Bahasa Pemrograman yang dipakai dalam wireshark adalah bahasa C dengan public licenci GNU. Wireshark banyak digemari karena interface wireshark yang telah menggunakan tampilan grafis atau GUI.

Seperti namanya, aplikasi Wireshark dapat menangkap beberapa paket data yang berkeliaran dalam lalu lintas jaringan yang kita lihat. Seluruh jenis informasi paket dalam bermacam-macam format protokol pun bisa dengan mudah ditangkap dan dianalisis. Oleh karena itu, tool ini sering digunakan untuk sniffing (mendapatkan informasi penting seperti username dan password) dengan menangkap paket yang berkeliaran dalam lalu lintas jaringan dan menganalisanya. Untuk dapat menjalankan tool ini caranya cukup mudah.

Kita hanya perlu memberikan perintah untuk Perancangan Sistem Menggunakan Wireshark. Berbeda dengan perancangan dalam jurnal sebelumnya, dalam perancangan system menggunakan wireshark lebih menujuk pada aktifitas illegal. Seperti yang telah dijelaskan dalam jurnal, uses diberikan hak akses berupa proses upload maka pada system yang akan dibangun menggunakan pembatas harddisk dengan menggunkan disk quota, jadi user tidak bisa melakukan upload secara sembarang karena telah dibatasi quota untuk melakukan proses upload.

Proses yang dilakukan tersebut diawasi oleh wireshark agar uses dapat dengan aman meng-upload data tanpa perlu mengkawatirkan ada yang mengusupi pada saat melakukan upload data. Tujuan, kegunaan, dan manfaat Wireshark Manfaat dari penggunaan aplikasi wireshark ini yaitu sebagai berikut : Menangkap informasi atau data paket yang dikirim dan diterima dalam jaringan computer Mengetahui aktifitas yang terjadi dalam jaringan computer Mengetahui dan menganalisa kinerja jaringan computer yang kita miliki seperti kecepatan akses/shere data dan koneksi jaringan ke internet Mengamati keamanan dari jaringan computer yang kita miliki Kegunaan Wireshark Beberapa kegunaan wireshark diantaranya: Wireshark digunakan oleh seorang network administrator untuk menganalisis lalu lintas dalam jaringannya.

Wireshark dapat mengambil paket data atau pun informasi yang sedang terjadi di dalam sebuah jaringan dan semua jenis informasi yang diperoleh ini bisa dengan mudah untuk dianalisis, salah satu caranya menggunakan sniffing , dengan menggunakan sniffing maka memungkinkan kita untuk memperoleh informasi penting seperti username dan password yang ada didalam jaringan kita.

Wireshark adalah apliaksi yang digunakan untuk menganalisis lalu – lintas yang terjadi dalam jaringan komputer, dimana software ini memiliki beberapa fungsi yang cukup bermanfaat bagi seorang profesional jaringan, peneliti, administrator jaringan, atau pun pengembang perangkat lunak jaringan. Wireshark bisa meng-tracking data secara realtime melalui Ethernet, FDDI, Token Ring, serial (PPP dan SLIP), wireless LAN 802.11, ataupun koneksivitas ATM.

Program ini pun marak dipakai oleh seorang chatters untuk mendapatkan alamat ip korban ataupun alamat IP para chatter lain melalui typing room. Alat dalam wireshark bisa menganalisis perpindahan paket data pada sebuah jaringan, yakni proses koneksi dan transmisi data antar beberapa komputer. Selama kita dapat memperoleh paket langsung melalui jaringan, dalam tool seperti pada wireshark, maka kita pun dapat menggunakan wireshark untuk 'menyadap' percakapan melalui Voice over IP.

Cara Instalasi wireshark Download wireshark lalu lakukan Installasi, Wwreshark bisa didapat dengan cara mendownload dengan Gratis melalui situs Official Wireshark. Di situs officialnya wireshark tersedia untuk sistem operasi macOS dan juga Windows. Selama proses installasi berlangsung pada windows, terkadang kita akan diminta untuk menginstal WinPcap, karena WinPcap merupakan library atau software pendukung yang nantinya akan digunakan untuk pengambilan data secara realtime.

Untuk penginstalan wireshark dikomputer ataupun laptop caranya seperti menginstal softwere-softwere additional tasks yang berukuran kecil dan tidak perlu kapasitas yang besar pada hardisk kita, yang pasti kita harus memiliki softwere installernya atau jika belom memiliki bisa didownlod pada situs resminya dan bisa searching digoogle atau dapat juga minta kepada teman anda yang memiliki, agar lebih jelasnya cara instalasi wireshark yaitu sebagai berikut: Double klik pada palikasi installer wireshark Kemudian klik next kontak dialog tersebut dalam memulai instalasi Lalu dibaca terlebih dahulu untuk license agreement dan klik I agree Selanjutnya kita bisa pilih komponen yang ingin kita instal pada wireshark kita, terdapat 5 komponen, kita pilih atau centang semua agar wireshark yang kita instal lengkap lalu kita pilih next Selajutnya pada additional tasks pilih shortcut tambahan yang diperlukan seperti desktop icon dan quick launch icon.

Jadi kita tentukan lokasi instalasi/direktori pada computer dengan kapasitas memori yang dibutuhkan 84MB lalu klik next Kemudian untuk install aplikasi winCap dimana aplikasi ini berfungsi untuk mengakat netwock data atau paket data secara live kemudian klik install Tunggu hingga proses instalasi selesai Terakhir kita klik next dan instalasi telah selesai lalu klik finish, bearti Wireshark telah resmi terinsal diLaptop atau PC kita Menggunakan Wireshark untuk Menitoring Jaringan Setelah wireshark terinstal maka kita dpat langsung menggunaknnya untuk mencoba menitoring jaringan pada kali ini saya akan melakukan untuk monitoring application layer protocol HTTP.

Paket data yang kita dilihat berasal dari tansmisi ketika kita membuka webpage atau paket data yang melewati HTTP protocol Jalankan wireshark dengan klik dua kali pada desktop icon wireshark Selanjutnya kita tunggu sebentar ketika muncul seperti berikut Setelah itu akan muncul seperti berikut, maka wireshark sudah dapat digunakan. Selanjutnya kita klik interface list dapat melihat daftar interface yang akan kita capture.

Saya memilih Microsoft yang merupakan wireless network yang sedang aktif pada laptop saya, Beri tanda centang dulu pada interface Microsoft, baru kemudian klik start Wireshark menampilkan paket-paket data yang ada dijaringan sebagai berikut yang dapat kit lihat. Lalu kita buka google chrome untuk membuka blog saya sendiri http://iyaksatria.blogsop.com/ untuk melihar transmisi paket data pada halaman web untuk monitoring aplikasi protocol layer HTTP Pada filter kita ketikkan ‘http’ untuk melihat paket data yang hanya transmisi protokol HTTP Untuk lebih memudahkan kita dalam melihat transmisi ke http://iyaksatria.blogsopt.com/ tadi maka kita harus mengetahui IP dari http://iyaksatria.blogsopt.com/ yaitu dengan command prompt ping ke http://iyaksatria.blogsopt.com/ Dapat diketahui IP address dari http://iyaksatria.blogsopt.com/ yaitu 74.125.235.12 Selanjutnya untuk melihat transmisi paket data yang menuju ke protocol halaman web http;//iyaksatria.blogsopt.com/ berarti kita harus melakukan filter paket data yang menuju ke http://iyaksatria.blogsopt.com/ dengan cara menuliskan syntax ini ke filetr : ip.dst==74.125.235.12 lalu tekan entar. (ip.dst adalah ip destination atau tujuan) Sebelumnya kita sudah melihat transmisi paket yang menuju ke http://iyaksatria.blogspt.com/ (ip:74.125.235.12) lalu kita akan melihat paket yang melalui protocol HTTP halaman web, maka kita filter agi yaitu dengan syntax filter: Dapat kita lihat pada hasil setelah filter ip.dst==74.125.235.12 && http, terdapat 2 transmisi paket data yang menuju ke http://iyaksatria.blogspot.com/ pada jaringan computer saya.

Disini akan sedikit kita analisis yaitu : Number disini merupakan urutan nomer paket data yang ditangkap oleh wireshark secara langsung yang dapat dilihat 2 tranmisi paket data yang menuju ke http://iyaksatria.blogsopt.com/ memiliki nomer 3960 dan 6862.

Time disini merupakan waktu saat paket yang menuju ke http://iyaksatria.blogsopt.com/ tersebut ditangkap, dapat dilihat time paket pertama yaitu 1770.82690.

Source disini merupakan ip sumber dari paket tersebut, dimana IPnya sesuai dengan IP laptop saya yang terhubung dengan wireless network adapter yaitu 192.168.0.108. Destination disini merupakan IP tujuan dari paket diatas dimana IP tujuan sesuai dengan IP dari webpage http://iyaksatria.blogsopt.com/ yaitu 74.125.235.12. Protocol disini merupakan tampilan protocol apa yang dipakai paket data diatas yaitu HTTP.

Length disini merupakan lamanya transmisi paket data menuju ke ip tujuan, yaitu kita lihat sebesar 627 untuk yang pertama dan yang kedua sebesar 391, yang kedua lebih kecil karena hanya me-reload page dari halaman web http://iyaksatria.blogsopt.com/. Info disini merupakan tampilan informasi mendeatil tentang paket tersebut di atas.

Dalam memcahkan traubleshootng dijaringan untuk memeriksa keamanan jaringan wireshark banyak digunakan, sehingga juga men-debug implementasi proctocol jaringan pada softwere mereka, sehingga melakukan protocol, implementasi paket dan belajar, untuk sniffer atau mengendus data privasi jaringan dalam menggunkan protocol. Wireshark yang digunakan oleh uses untuk penggunaanya sebagi media atau tool, entah untuk kejahatan atau kebaikan.

Oleh karena iu wireshrak digunakan dalam mencari informasi sensitive yang berkeliaran dijaringan, contoh cookie, kata sandi dan lainya. Wireshark mampu menganalisi paket data secara real time, yang artinya aplikasi ini mampu mngawasi semua paket data yang masuk keluar melalu antar muka yang telah ditentukan oleh user sebelumnya.

Dan wireshark akan tarsus mengawasi semua paket dsta yang keluar masuk melalui berbagai antar muka yang sudah ditentukan dan selajutnya akan menampilkan.Aplikasi berbasis jaringan yang digunakan komputer jika pada saat komputer terhubung dengan jaringan dengan kecepatan tinggi, aplikasi wiresharkpun dapan menampilkan berbagai macam oaket data jaringan yang akan muncul dan wireshark mampu memfilter jenis-jenis protocol tertentu yang ingin ditampilkan.

Analisa dan Perancangan Analisa Sistem aktivitas illegal di dalam jaringan Analisa ini yang digunakan, adalah anilsa yang pengembangan system. Penelitian yang digunakan dengan pendekatan pengembangan, yaitu suatu penelitian dalam berusaha mencari pengaruh variable tertentu, dalam kondisi yang terkontrol dalam variable yang lain.

Dibawah ini adlah flowchatdalam proses penangkapan aktivitas illegal yang terjadi dalam jaringan denagn dilakukan eksperimen secara langsung dlaam metode penelitian.

Gambar 2. flowchart pendeteksian aktivitas illegal Perancangan Sistem jaringan untuk aktivitas ilegal Ini adalah uji coba dalam menggunakan system operasi windows yang akan dijelaska pada gambar dibawah ini, gambar tersebbut adalh bagian wireshark yang akan mejelaskan proses penangkapan aktivitas illegal yang sering terjadi dijaringan komputer. Gambar 3.

penangkapan aktivitas illegal Gambar tadi menunjukan user akan diberikan hak akses berupa proses upload pada sistem yang dibangun menggunakan pembatas harddisk dengan menggunakan disk quota, sehingga user tidak mampu melakukan upload dengan cara sembarang karena sudah dibatasi quota untuk melakuakan proses upload. Proses ini dilakukan sehingga diawasi oleh wireshark supaya user dapat dengan aman meng-upload data tanpa harus mengkawatirkan ada yang menyusupi saat melakukan upload data.

Untuk melakukan capture packet sesuai dengan keinginan dari user dimana setelah memilih pada salah satu interface yang akan dipantau aktivitas jaringan secara online sehingga akan muncul seperti gambar dibawah ini Gambar 4. Capture packet Didalam jaringan untuk proses anlissa aktivitas ilegal, wireshark bisa mnganalisis dan melihat pada paket secara offline seperti pada gambar 5, penulis juga menyimpan file terlebih dahulu kedalam sebuah filter *.pcap. Untuk melakukan perancangan ini penulis ia dapat peroleh 500 aktivitas data pada file ini.

Gambar 5. Penangkapan paket secara offline Hasil Pengujian Hasil pengujian ini yaitu pengujian aktivitas yang sudah berhasil di-ca pture oleh wireshark pada informasi sumber, maka tujuan protocol dan waktu ca pture-nya.

Pemfilteran Aktivitas Jaringan Dengan Secara Langsung Jika saat memfilter aktivitas paket data jaringan dengan secara langsung, dapat kita lakukan ketika membuka interface yang ingin digunakan seperti terlihat gambar dibawah ini. Gambar 6. Interface untuk pemfilteran paket Gambar 6 menjelaskan bahwa wireshark mampu menangkap aktivitas illegal di dalam jaringan setelah memillih interface yang akan ditangkap pada dianalisa, namun proses tersebut sudah selesai maka harus klik tombol mulai untuk memulai suatu proses capture packet lalu aplikasi ini akan melakukan pemfilteran dan hasil tersebut tampil pada layar wireshark untuk pengujian, menganlisa paket HTTP tcp port 80 dan penulis memfilter maka hasil penangkapan sebuat paket itu seperti gambar dibawah ini.

Keaimpulan Wireshark adalah salah satu alat dari analisa jaringan yang biasa dipakai oleh seorang Network Administrator untuk melakukan pemecahan maslah yanga da dalam jariangan, manganalisa, perangkat lunak atau untuk pengembangan sebuah

protocol dalam komunikasi, dan atau dalam pendidikan, dan dengan mengguanakan software dalam melakukan memonitoring sebuah jaringan komputer dapat memudahkan seorang administrator jaringan dalam melakukan kegiatan yang memantau terhadap jaringan komputernya dan dapat juga membantu ketesediaan dari jaringan tersebut, dan hasil data yang didapatkan dalam mengenal protocol jaringan hasil pemfilteran paket data bahwa menggunakan wireshark sangat cukup mudah dilakukan dibandingkan dengan aplikasi yaitu forensic tools short sangat memerlukan penyetingan pada snort conf, sedengkan dengan wireshark hanya perlu memilih filter paket yang berada pada kolom filter. Sehingga administrator jaringan mampu menganalisa jaringan saat berlangsung.

Daftar Pusaka Ariyus, D. (2007). Intrusion Detection System. Penerbit Andi: Yogyakarta. Ariyus, D. (2006). Computer Security. Penerbit Andi: Yogyakarta. Pratama, A. J. (2010). Design And Implementation Of Data Flooding Prevention On Computer Network dalam Undergraduate Theses Teknik Informatika ITS Surabaya (ict.binus.edu/metamorph/file/research/MA ID_JOURv2.0.pdf diakses tanggal 9 November 2015). Kurniawan, A. (2010). Network Forensics Wireshark. Penerbit Andi: Yogyakarta. Ramadhani, K. B. (2011).

Penggunaan Jaringan Komputer Pascasarjana UPN 'Veteran" Jatim menggunakan metode 'IDS (Intruzion Detection System)" Dari Aktifitas dalam tesis Pasca sarjana UPN Veteran Jatim.
https://dosenit.com/jaringan-komputer/pengertian-jaringan-komputer-menurut-para-ahli
http://fauziadnan.blogspot.com/2018/04/apa-itu-wireshark-kegunaan-cara-kerja.html

INTERNET SOURCES:

<1% -
https://text-id.123dok.com/document/7qvxdry5-analisis-jenis-jenis-sistem-keamanan-jaringan-wireless-hotspot.html
1% - http://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/download/229/93
<1% - https://tichacuaem93.wordpress.com/author/tichaunes/
<1% -
https://kumpulaninformasidanmateri.blogspot.com/2013/07/materi-sistem-keaman-jaringan.html
<1% - https://rangga677.blogspot.com/2016/
<1% - https://www.mastekno.com/id/jenis-sistem-keamanan-jaringan/
<1% - https://taatpadaillahi.blogspot.com/2015/12/makalah-mengenai-internet.html
<1% -

https://blog.dimensidata.com/pengertian-jenis-dan-fungsi-switch-pada-jaringan-komputer/
<1% -
http://www.tipsnewtechnology.com/2018/08/pengertian-topologi-jaringan-dan-jenis.html
<1% - https://ezagren.blogspot.com/2012/02/laporan-praktikum-i.html
<1% -
https://www.wixapedia.com/jaringan-komputer-pengertian-topologi-dan-contohnya-lengkap/
<1% - https://yuanamuzika.blogspot.com/#!
<1% -
http://www.stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/229/93
<1% - https://jaringandasar26.wordpress.com/protokol-tcp-ip/
<1% - https://effvz.blogspot.com/2018/08/
<1% - https://www.academia.edu/17562780/Do_S-1
<1% - https://ejournal.unsrat.ac.id/index.php/elekdankom/article/download/6520/6045
<1% - https://jurnal.stmikroyal.ac.id/index.php/jurteksi/article/download/48/41
<1% - https://fauzult.blogspot.com/2012/01/tugas-makalah-basis-data.html
<1% - https://tekhpro.blogspot.com/2010/
<1% - https://rahmadteknology.blogspot.com/
<1% -
https://susi-melani.blogspot.com/2011/10/koneksi-internet-hardware-dan-topologi.html
<1% - https://luthfiliaworld.wordpress.com/page/2/
<1% - https://izzahpechex.wordpress.com/software-jaringan/
<1% - https://ahmadimam321.blogspot.com/#!
<1% - https://putrajatim.blogspot.com/2012/04/
<1% - https://israwatifazri.blogspot.com/
<1% -
https://dananguye97.blogspot.com/2015/04/cara-memonitoring-jaringan-dengan.html#!
<1% - https://lanaibrahim.blogspot.com/
<1% - http://eprints.umm.ac.id/36115/3/jiptummpp-gdl-amiribnual-48821-3-bab-ii.pdf
2% -
https://www.kompasiana.com/iyaksatria/software-wireshark-untuk-monitoring-jaringan-komputer_55204a08813311f77319f744
<1% - https://kalisya27.blogspot.com/2016/
<1% - https://mobilemultimedia301.wordpress.com/2011/11/
<1% - https://blogasmart.blogspot.com/2012/09/metode-penelitian-jenis-jenis.html
<1% - https://www.anakit.id/2019/05/cara-instal-netbeans.html

<1% - https://bobotoh-v3.blogspot.com/2010/04/jaringan-infrastruktur.html