DoubleClick: Journal of Computer and Information Technology E-ISSN: 2579-5317
P-ISSN: 2685-2152
Vol. 4, No. 1, Agustus 2020, Pages 11-23 http://e-journal.unipma.ac.id/ind ex.php/doubleclick

ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN DENGAN WIRESHARK

Rahma Hanipah dan Harry Dhika
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
dhikatr@yahoo.com

Abstrak. Faktor kemanan jaringan komputer adalah satu hal yang mutlak dalam membangun suatu jaringan. Pada dasarnya sistem keamanan yang dimiliki oleh sistem operasi tidaklah cukup untuk mengamankan jaringan komputer. Oleh karena itu untuk mendapatkan sebuah keamanan jaringan komputer maka diperlukan suatu tools yang dapat mendeteksi adanya suatu mekanisme serangan dari jaringan. Jenis serangan yang terjadi bisa *flooding* ataupun *syn flood*. Dimana tujuan serangan ini adalah untuk membuat komputer yang mengakses tidak bisa berjalan dengan normal jaringan komputer. Wireshark merupakan software yang dapat menganalisa aktivitas jaringan komputer sehingga dapat membantu mendeteksi serangan yang akan terjadi sehingga pengguna tidak perlu khawatir dengan serangan 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 pada keamanan maka keamanan jaringan komputer dapat dilihat dari segi bentuknya, yaitu keamanan *hardware* berhubungan pada perangkat keras yang digunakan dalam jaringan komputer. Keamanan hadwere kadang diabaikan padahal hal utama untuk menjaga jaringan supaya tetap stabil. Dalam keamanan hardwere, server, dan tempat penyimpanan data wajib menjadi perhatian utama. Akses melalui fisik terhadap server dan data - data penting dibatasi semaksimal mungkin. Keamanan software, sesuai dengan namanya, maka yang perangkat lunak yang harus diamankan. Perangkat lunak yang dimaksud disini bisa berupa system operasi, system aplikasi, data dan informasi yang tersimpan dalam komputer jaringan terutama pada server. Contohnya, jika server hanya bertugas menjadi *router*, tidak perlu software web server dan FTP server diinstal, Membatasi software yang dipasang akan mengurangi konflik antar software yang membatasi akses, contohnya jika *router* dipasangi juga dengan FTP server, maka orang dari luar dengan login anonymous mungkin akan dapat mengakses router tersebut.

Wireshark(Ben-Eid, 2015) dalam memonitor suatu jaringan komputer dapat membantu memudahkan seorang administrator jaringan untuk melakukan pengawasan terhadapt suatu jaringan komputer. Dengan aplikasi wireshark ini 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 pada jaringan yang dimiliki.

Metode Penelitian

Untuk menghindari berbagai macam serangan baik itu oleh para hacker ataupun craker keamanan jaringan sangatlah diperlukan(Agus et al., 2019). Ternyata serangan tersebut bukan Cuma berasal dari serangan para hacker dan craker, tetapi juga berasal dari lingkuan sekitar. 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(Sutarti et al., 2018) 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*(Ning et al., 2013) memiliki tingkat kerawanan yang tinggi.

Berikut ini merupakan jenis – jenis keamanan jaringan komputer :

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(Dhody, 2014; Hasibuan, 2016; Hidayatulloh, 2014):

a. Keamanan fisik
   Klasifikasi keamanan didukung melalui *hardware* ataupun perangkat keras. Tujuan dari keamana fisik yakni mampu melindungi *hardware* agar selalu dalam kondisi terbaik sehingga dapat digunakan dalam melaksanakan operasi jaringan.
b. Keamanan Jaringan
   Keamanan jaringan merupakan hal yang abstrak. Hal tersebut dikarenakan jenis keamanan dilakukan oleh benda tidak keliatan atau tidak kasat mata, baik itu menggunakan *sofwere* maupun perintah tertentu. Contoh keamanan jaringan yaitu, dengan menggunaka *proxy* maupun *firewall* untuk melakukan filter pada *user* yang ingin menggunakan akses dalam jaringan.
c. Otorisasi Akses
   Jenis keamanan jaringan atau otorisasi akses merupakan suatu keamanan jaringan dengan menggunakan password atau kata sandi, ketika akan menghubungkan perangkat dalam jaringan. Hal tersebut dilakukan agar administrator dapat membatasi akses user yang sudah terpilih saja yang bisa terhubung pada sebuah jaringan.
d. Proteksi Virus
   Virus mampu melakukan metode penyerangan pada system komputer dengan menggunakan program, dan menjadikan sistem yang ada di komputer menjadi berantakan dan mengakibatkan kerusakan. Untuk menangani serangan virus, dapat menggunakan atau menginstal *sofwere* anti virus pada komputer selalu *update* dengan *database* baru.
e. 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 komputer. Perencanan bencana ini bertujuan untuk terjadinya kerusakan pada system dapat cepat teratasi.

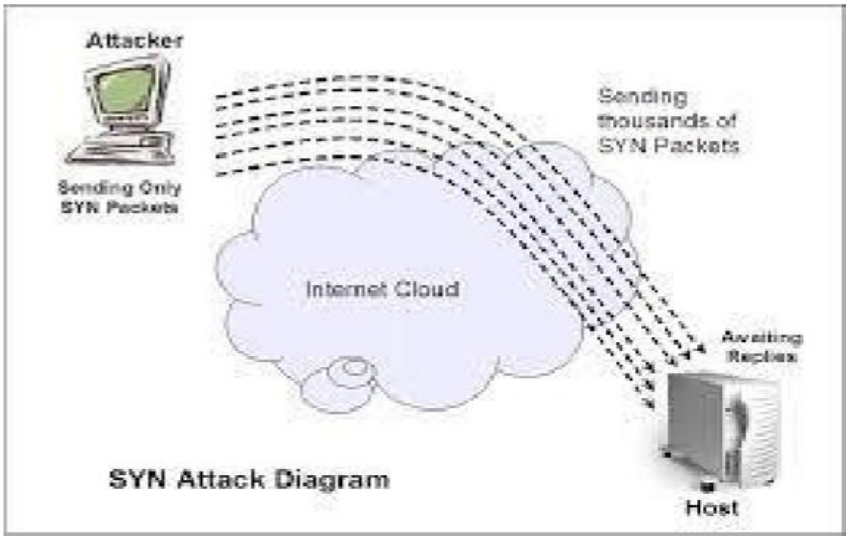
Untuk memahami mengenai pengertian dari jaringan komputer serta hal – hal penting yang terdapat pada jaringan komputer, berikut ini adalah pengertian jaringan komputer menurut para ahli serta hal – hal penting yang terdapat dalam

jaringan komputer. Jaringan komputer(Sonny & Dhika, 2017) adalah sebuah sistem yang terdiri atas komputer - 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 komputer dapat dalam jaringan komputer 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. Jaringan komputer(Simanjuntak et al., 2019) merupakan kumpulan beberapa komputer yang berjumlah banyak serta terletak secara terpisah-pisah tetapi terhubung dengan lainnya. Sebuah komputer dapat dikatakan saling terhubung apabila komputer terhubung dengan satu komputer lain, atau terhubung dengan banyak komputer dengan kondisi dapat saling mengirimkan informasi ataupun data dengan komputer lainnya . 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 komputer dengan komputer yang lain dengan tujuan agar dapat untuk saling berkomunikasi serta dapat bertukar data satu sama lain.

Hasil dan Pembahasan

Transmision Control Protocol (TCP)(Held, 2010; Zhang et al., 2017) adalah sebuah layanan yang menyediakan pengiriman data oleh protokol, TCP merupakan protokol yang bersifat *connection-oriented, reliable, byte stream service*. *Connection oriented* berarti dua aplikasi pengguna TCP harus melakukan pembentukan hubungan dalam bentuk pertukaran kontrol informasi (*handshaking*) sebelum transmisi data terjadi. *Realiable* merupakan proses deteksi kesalahan paket TCP dan mentransmisikan kembali. *Byte stream service* merupakan paket yang dikirimkan dan sampai ketempat tujuan secara berurutan. Pada dasarnya jenis protkol TCP sulit untuk disalah gunakan. Kecuali penyusup mengontrol suatu *router* diantara dua sistem, penyusup itu dapat selalu dilacak keberadaannya serta 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 yang berjenis ini cukup sulit untuk dideteksi alamat pengumannya karena alamat IP dari pengirim tersebut telah disamarkan dengan menyeleksi paket router yang menghubungkan jaringan internet, terlihat seperti gambar 1.



Gambar 1: SYN TCP *Attack*.

Gambar diatas tersebut adalah sebuah paket SYN(Bogdanoski et al., 2013; Eddy, 2007; Mohammadi et al., 2017) yang dalam proses pengiriman yang telah disamarkan, ketika paket SYN sampai ke server, selanjutnya akan diteruskan untuk mengalokasikan *buffer* pada memori yang dibutuhkan. Lalu apabila pengalokasian memori sudah diberikan kepada *host* penyerang maka, *host* penyerang akan terus mengirimkan paket SYN yang telah dimanipulasi oleh penyerang dan alamat IP yang telah disamarkan. *Host* penyerang akan memaksa server untuk mengakumulasi koneksi setengah terbuka "*half open connection*" sehingga pada posisi puncaknya server tidak mampu mengakumulasi *half open connection* sehingga sumber daya yang dimiliki server lumpuh total. Karena serangan SYN dengan alamat IP pengirim yang dipalsukan pada awalnya bukanlah suatu bentuk serangan yang mengonsumsi bandwidth, namun lebih kepada serangan yang mengonsumsi sumber daya server.

Flooding data

Flooding Data(Melnik et al., 2002) 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 "sesuatu yang 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 dikumpulkan 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 dinamakan *deskripsi.* Pemilihan banyak data sesuai dengan persamaan atau perbedaan yang dikandunganya dinamakan klarifiasi.

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 bisa mengakibatkan kerugian lain. Adanya intruder dari kerusakan program yang masuk kedalam

jaringan. Suatu jaringan akan mengalami turun naik selama pemakaianya pada Traffic data. 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.

Akan terjadinyaa turun naik selama pemakaian pada traffic data yang ada dalam suatu 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*:(Bogdanoski et al., 2013; Chen, 2010; Saied et al., 2016)

1) *Ping of death,* Pengiriman *echo request ICMP* secara berlebihan dalam suaru jaringan. Terjadinya system crash karna pengiriman paket ini, yauitu *reboot* atau *hang*.
2) *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 dikirim sebuah paket ICMP *echo request* ke sebuah *host* lain, agar host tersebut dapat mengirimkan paket ICMP PING secara terus menerus ke korban terakhirnya.
3) *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. Meskipun besar paket kecil, tetapi apabila pengiriman SYN tersebut terus menerus akan memperbesar backing. Hal yang terjadi apabila backlog sudah besar akan mengakibatkan host tujuan akan otomatis menolak semua paket SYN yang datang, sehingga host tersebut tidak bisa dikoneksi oleh host-host yang lain.*
4) *UDP flood,* Pengiriman data UDP secara berlebihan kedalam suatu jaringan, pengiriman UDP *flood* ini akan membentuk suatu jalur hubungan dengan suatu *sevis* UDP dari *host* tujuan. Flood UDP ini akan mengirimkan karakter-karakter yang akan mengetes jaringan korban. Sehingga terjadi aliran data yang tidak perlu dalam jaringan korban tersebut.

Suatu serangan kedalam server jaringan komputer dapat terjadi kapan saja pada saat administrator sedang bekerja maupun tidak. Dengan demikian dibutuhkan suatu system pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalo paket tersebut 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 setiap data yang masuk kedalam server, apakah data yang datang merupakan sebuah data flood atau data yang diperlukan oleh user. Pemodelan dibuat dengan menggunakan bahas pemograman Delphi 7 dan dalam lingkungan jaringan komputer berbasis IP address local area Network.

Flooding data yang terjadi hanya bisa dicegah sampai titik server saja, dan hanya bisa mencegah data masuk kedalam

yang bisa menyebabkan kerusakan yang 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 ke server.

Dalam hal ini hubungan server local keserver yang lebih tinggi. Tujuan komunikasi ini adalah untuk mengadakan pemblokiran IP pada server yang lebih tinggi sehingga gangguan yang ada lebih bisa dikurangi lagi. Traffic dijaringan local akan kembali normal karena data yang sebelumnya datang sudah diblokir ditingkat lebih atas.

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 dilihat. 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, 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.

a. Tujuan dan Manfaat Wireshark
   Manfaat dari penggunaan aplikasi wireshark ini yaitu sebagai berikut :
   - Menangkap informasi atau data paket yang dikirim dan diterima dalam jaringan komputer
   - Mengetahui aktifitas yang terjadi dalam jaringan komputer
   - Mengetahui dan menganalisa kinerja jaringan komputer yang dimiliki seperti kecepatan akses/shere data dan koneksi jaringan ke internet
   - Mengamati keamanan dari jaringan komputer.

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 untuk memperoleh informasi penting seperti *username* dan *password* yang ada didalam jaringan. Wireshark merupakan 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, ataupun 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 dapat memperoleh paket langsung melalui jaringan, dalam tool seperti pada wireshark, maka dapat menggunakan wireshark untuk 'menyadap' percakapan melalui Voice over IP.

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 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 atau laptop caranya seperti menginstal softwere-softwere additional tasks yang berukuran kecil dan tidak perlu kapasitas yang besar pada *hardisk*, yang pasti harus memiliki *softwere installer*-nya atau jika belom memiliki bisa didownlod pada situs resminya bisa *searching* di *google* atau bisa juga minta kepada rekan anda yang memiliki, agar lebih jelasnya cara instalasi wireshark yaitu sebagai berikut:

- Double klik pada palikasi installer wireshark
- Kemudian klik *next* kontak dialog berikut untuk memulai instalasi
- Dibaca terlebih dahulu untuk *license agreement* dan setelah itu klik *I agree*
- Kemudian pilih komponen apa saja yang ingin di instal pada *wireshark*, terdapat 5 komponen, pilih atau centang semua agar wireshark yang *instal* lengkap lalu pilih *next*
- Selajutnya dalam *additional tasks* pilih shortcut tambahan yang diperlukan seperti *desktop icon* dan *quick launch icon.*
- Tentukan lokasi instalasi/direktori pada komputer dengan kapasitas memori yang dibutuhkan 84MB lalu klik *next*
- Jangan lupa 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 klik *next* dan instalasi telah selesai lalu klik *finish,* berarti Wireshark telah resmi terinsal diLaptop atau PC.

Menggunakan Wireshark untuk Menitoring Jaringan. Setelah wireshark terinstal maka dapat langsung menggunaknnya untuk mencoba menitoring jaringan dan monitoring *application layer protocol HTTP.* Paket data yang akan dilihat berasal dari tansmisi ketika membuka *webpage* atau paket data yang melewati HTTP *protocol*

- Jalankan wireshark dengan klik dua kali pada desktop icon wireshark

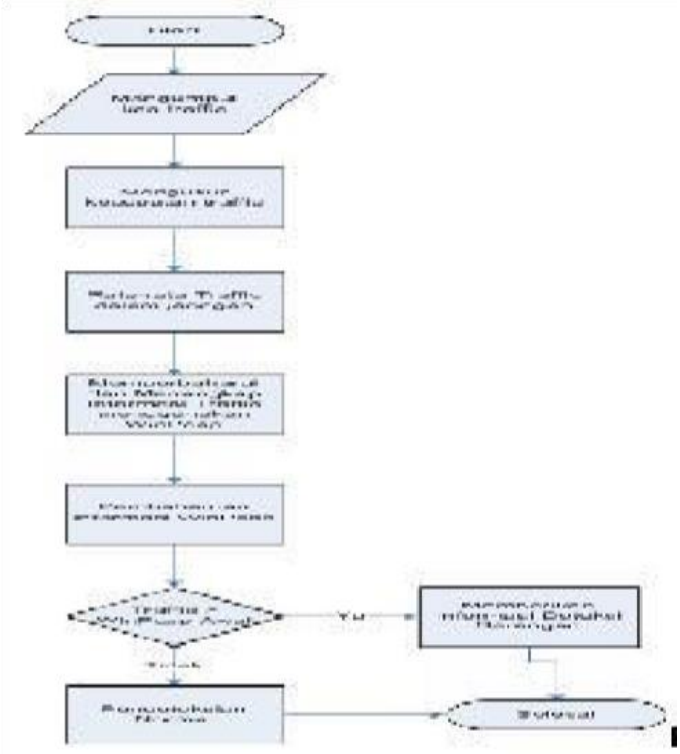
- Setelah itu tunggu sebentar ketika muncul
- Setelah itu akan muncul seperti berikut, berarti wireshark sudah dapat gunakan. Selanjutnya klik *interface list* untuk melihat daftar interface yang akan di *capture.* Pilih Microsoft karena merupakan *wireless network* yang sedang aktif pada laptop, Beri tanda centang dulu pada interface Microsoft, baru kemudian klik *start*
- Dapat dilihat disini wireshark menampilkan paket-paket data yang ada dijaringan sebagai berikut
- Kemudian buka google chrome untuk membuka blog sendiri http://iyaksatria.blogsop.com/ untuk melihar transmisi paket data pada halaman web untuk monitoring aplikasi protocol layer HTTP
- Pada filter ketikkan 'http' untuk melihat paket data yang hanya transmisi protokol HTTP
- Untuk lebih memudahkan dalam melihat transmisi ke http://iyaksatria.blogsopt.com/ tadi maka 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 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 sudah melihat transmisi paket yang menuju ke http://iyaksatria.blogspt.com/ (ip:74.125.235.12) lalu akan melihat paket yang melalui protocol HTTP halaman web, maka filter lagi yaitu dengan s*yntax filter:*

Dapat di 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 komputer.
Disini akan sedikit analisis yaitu:

1. *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.
2. *Time* disini merupakan waktu saat paket yang menuju ke http://iyaksatria.blogsopt.com/ tersebut ditangkap, dapat dilihat time paket pertama yaitu 1770.82690.
3. *Source* disini merupakan ip sumber dari paket tersebut, dimana IPnya sesuai dengan IP laptop yang terhubung dengan wireless network adapter yaitu 192.168.0.108.
4. *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.
5. *Protocol* disini merupakan tampilan protocol apa yang dipakai paket data diatas yaitu HTTP.
6. *Length* disini merupakan lamanya transmisi paket data menuju ke ip tujuan, yaitu 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/.
7. *Info* disini merupakan tampilan informasi mendeatil tentang paket tersebut di atas.

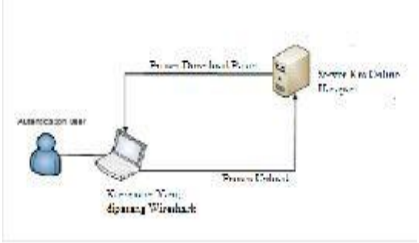
Wireshark banyak digunakan dalam memecahkan troubleshooting dijaringan untuk memeriksa keamanan jaringan, men-debug implementasi protocol jaringan dalam software mereka, melakukan debugging implementasi paket, protocol, serta belajar[4]. protocol dan banyak juga digunakan untuk sniffer atau mengendus data-data privasi dijaringan. Wireshark ini diibaratkan sebagai media atau tool yang dapat dipakai oleh user untuk penggunaanya, apakah untuk kebaikan atau kejahatan. Hal ini karena wireshark dapat digunakan untuk mencari informasi yang sensitif yang berkeliaran pada jaringan, contohnya kata sandi, cookie dan lain sebagainnya. Wireshark dapat menganalisis paket data secara real time. Artinya aplikasi wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah ditentukan oleh user sebelumnya. Wireshark dapat menganalisa paket data secara real time artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya. Jika Komputer terhubung dengan jaringan kecepatan tinggi dan pada komputer sedang digunakan aplikasi berbasis jaringan, aplikasi wireshark akan menampilakan banyak sekali paket data dan menimbulkan kebingungan karena ada begitu banyak paket data jaringan yang muncul. Aplikasi wireshark dapat memfilter jenis protocol tertentu yang ingin ditampilkan[5].

Analisa Sistem aktivitas illegal di dalam jaringan. Analisa yang digunakan, yaitu analisa pengembangan sistem. Penelitian dengan pendekatan pengembangan, adalah suatu penelitian yang berusaha mencari pengaruh variabel tertentu, terhadap variabel yang lain dalam kondisi yang terkontrol. Metode penelitan yang dilakukan dengan menggunakan eksperimen secara langsung, dibawah ini adalah flowchart untuk proses aktivitas illegal di dalam jaringan.



Gambar 2. Flowchart Pendeteksian Aktivitas Illegal

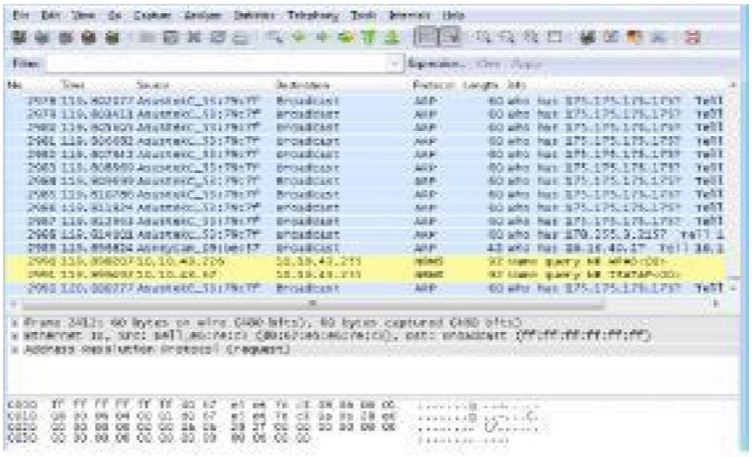
Perancangan Sistem jaringan untuk aktivitas illegal. Pada bagian ini wireshark yang diuji coba menggunakan sistem operasi windows akan dijelaskan pada gambar 4 dimana pada gambar tersebut akan menjelaskan proses penangkapan aktivitas illegal yang terjadi dijaringan komputer.



Gambar 3. Penangkapan Aktivitas Illegal

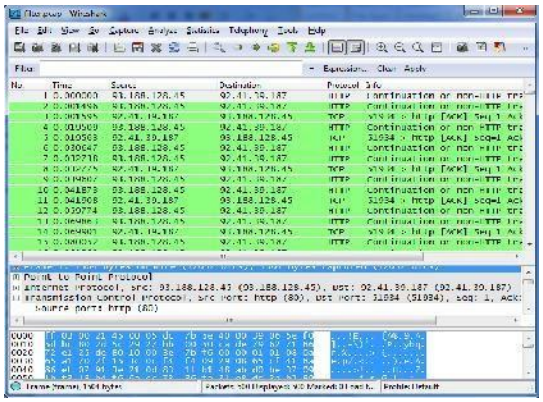
Gambar diatas menjelaskan user diberikan hak akses berupa proses upload maka pada sistem yang akan dibangun menggunakan pembatas *harddisk* dengan menggunakan *disk quota*, jadi user tidak bisa melakukan upload secara sembarang karena telah dibatasi quota untuk melakuakan proses upload. Proses yang dilakukan tersebut diawasi oleh wireshark agar user dapat dengan aman meng-upload data tanpa perlu mengkawatirkan ada yang menyusupi pada saat melakukan upload

data tersebut. Untuk melakukan capture packet sesuai dengan keinginan dari user dimana setelah memilih salah satu interface yang akan dipantau aktivitas jaringan secara online maka akan muncul seperti gambar dibawah ini



Gambar 4. Capture Packet

Dalam proses analisa aktivitas illegal didalam jaringan, wireshark mampu untuk melihat atau menganalisis paket secara offline seperti ditunjukkan gambar 6, dimana penulis menyimpan file terlebih dahulu kedalam filter *.pcap. Dalam melakukan perancangan ini penulis memperoleh 500 aktivitas data dalam file ini.



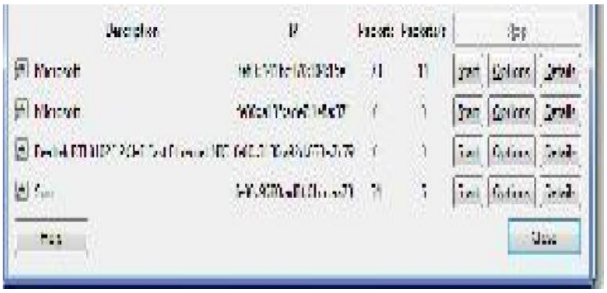
Gambar 5. Penangkapan Paket Secara Offline

a. Hasil Pengujian

Hasil pengujian dibawah ini adalah pengujian aktivitas yang berhasil di-ca pture oleh wireshark terhadap informasi sumber, tujuan protocol dan waktu ca pture-nya.

b. Pemfilteran Aktivitas Jaringan Secara Langsung

Apabila ingin memfilter aktivitas paket data jaringan secara langsung, dapat dilakukan ketika membuka interface yang ingin digunakan seperti terlihat gambar dibawah ini.



Gambar 6. Interface Untuk Pemfilteran Paket

Gambar 6 menjelaskan bagaimana wireshark dapat menangkap aktivitas illegal di dalam jaringan setelah memillih interface yang akan ditangkap untuk dianalisa, apabila dalam proses tersebut sudah selesai maka klik tombol start untuk memulai proses capture packet kemudian aplikasi wireshark akan melakukan pemfilteran dan hasilnya akan di tampilkan pada layar wireshark untuk pengujian, penulis memfilter dan menganalisa paket HTTP tcp port 80 maka hasil penangkapan paket tersebut seperti gambar dibawah ini.

5. Simpulan

Dari data yang didapatkan mengenal protocol jaringan hasil dari pemfilteran paket data menggunakan wireshark adalah pada wireshark untuk memfilter paket caranya cukup mudah dibandingkan dengan aplikasi seperti *forensic tools short* karena memerlukan penyetingan pada snort.conf sementara pada wireshark hanya cukup memilih filter paket pada kolom filter. Sehingga *administrator* jaringan dapat menganalisa paket jaringan yang sedang berlangsung.

6. Daftar Pusaka

Agus, I., Destiawati, F., & Dhika, H. (2019). *Perbandingan Cloud Computing Microsoft Onedrive , Dropbox, dan Google drive*. *12*(58), 20–27.

Ben-Eid, N. A. (2015). Ethical Network Monitoring Using Wireshark and Colasoft Capsa as Sniffing Tools. *International Journal of Advanced Research in Computer and Communication Engineering*. https://doi.org/10.17148/IJARCCE.2015.43113

Bogdanoski, M., Shuminoski, T., & Risteski, A. (2013). Analysis of the SYN Flood DoS Attack. *International Journal of Computer Network and Information Security*. https://doi.org/10.5815/ijcnis.2013.08.01

Chen, X. (2010). Distributed Denial of Service Attack and Defense. *ICEIT 2010 - 2010 International Conference on Educational and Information Technology, Proceedings*. https://doi.org/10.1109/ICEIT.2010.5608362

Dhody. (2014). Keamanan komputer. *Igarss 2014*. https://doi.org/10.1007/s13398-014-0173-7.2

Eddy, W. (2007). *TCP SYN Flooding Attacks and Common Mitigations*. RFC4987. https://doi.org/10.1007/s13398-014-

0173-7.2

Hasibuan, M. S. (2016). Keylogger pada Aspek Keamanan Komputer. *Teknovasi*.

Held, G. (2010). Understanding TCP/IP. In *A Practical Guide to Content Delivery Networks, Second Edition*. https://doi.org/10.1201/ebk1439835883-4

Hidayatulloh, S. (2014). Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSEC. *Jurnal Informatika*. https://doi.org/10.31311/ji.v1i2.47

Melnik, S., Garcia-Molina, H., & Rahm, E. (2002). Similarity Flooding: A Versatile Graph Matching Algorithm and Its Application To Schema Matching. *Proceedings - International Conference on Data Engineering*. https://doi.org/10.1109/ICDE.2002.994702

Mohammadi, R., Javidan, R., & Conti, M. (2017). SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks. *IEEE Transactions on Network and Service Management*. https://doi.org/10.1109/TNSM.2017.2701549

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity Security in The Internet Of Things. *Computer*, *46*(4), 46–53. https://doi.org/10.1109/MC.2013.74

Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of Known and Unknown DDoS Attacks Using Artificial Neural Networks. *Neurocomputing*. https://doi.org/10.1016/j.neucom.2015.04.101

Simanjuntak, P., Suharyanto, C. E., Jamilah, Teknologi, P. C. S., Simamora, S. N. M. P., Hendrarini, N., Lya, E., Sitepu, U., Riyana Rahadjeng, I., & Puspitasari, R. (2019). Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan. *Jurnal Teknologi Informasi Politeknik Telkom*. https://doi.org/.1037//0033-2909.I26.1.78

Sonny, M., & Dhika, H. (2017). Architecture as well as ISPs to review the Inter-connectivity Crossing IPv6 Internet. *Prosiding Seminar Nasional Inovasi Teknologi (Semnasinotek) 2017*, 1–6.

Sutarti, Pancaro, Adi, P., & Saputra, Fembi, I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*.

Zhang, Y., He, J., & Pathan, M. S. (2017). An Asymmetric Transport Protocol for Internet of Things. *Procedia Computer Science*, *107*(Icict), 636–641. https://doi.org/10.1016/j.procs.2017.03.171