MikroTik

Intrusion Detection & Prevention System

dan Keamanan Jaringan Pada Mikrotik Router

(Teori dan Praktek)

Rifki Indra Perwira, S.Kom., M.Eng.
Bagus Muhammad Akbar, S.ST., M.Kom.
Hari Prapcoyo, S.Kom., M.ICT.

Lembaga Penelitian & Pengabdian Kepada Masyarakat
Universitas Pembangunan Nasional "Veteran" Yogyakarta

Intrusion Detection and Prevention System dan Keamanan Jaringan Pada Mikrotik Router (Teori dan Praktek)

Lembaga Penelitian & Pengabdian Kepada Masyarakat

Universitas Pembangunan Nasional "Veteran" Yogyakarta

Intrusion Detection and Prevention System dan Keamanan Jaringan Pada Mikrotik Router (Teori dan Praktek)

Rifki Indra Perwira, S.Kom., M.Eng.
Bagus Muhammad Akbar, S.ST., M.Kom
Hari Prapcoyo, S.Kom., M.ICT

ISBN **: 978-623-7840-60-2**

Diterbitkan oleh :
Lembaga Penelitian & Pengabdian Kepada Masyarakat
UPN "Veteran" Yogyakarta
Jln. SWK 104 (Lingkar Utara) Condong Catur, Yogyakarta 55283
Telp. 0274 486188, 486733, Fax : 0274 486400

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Yang Maha Kuasa yang senantiasa selalu mencurahkan rahmat dan hidayah-Nya sehingga kami dapat menyelesaikan buku ajar dengan judul Intrusion Detection and Prevention System dan Keamanan Jaringan Pada Mikrotik Router (Teori dan Praktek).

Buku ini berisi tentang Firewall,Implementasi Firewall Filter dalam Mikrotik, Contoh penerapan Firewall Filter, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Intrusion Detection and Prevention System (IDPS), Sniffing Dan Scanning Network. Buku ajar ini merupakan salah satu luaran dari penelitian yang di danai oleh LPPM UPN ”Veteran” Yogyakarta. Tentu saja buku ini masih jauh dari sempurna, maka masukan dan saran senantiasa kami harapkan.

Atas perhatian dari semua pihak yang membantu dalam pembuatan buku saku ini, kami ucapkan banyak terima kasih. Semoga buku ini dapat dipergunakan seperlunya.

Yogyakarta, September 2020

Tim penulis

DAFTAR ISI

BAB I
KEAMANAN JARINGAN PADA MIKROTIK ROUTER MENGGUNAKAN FILTERING FIREWALL

1.1 Firewall

1.1.1 Pengertian Firewall

Dalam membuat sebuh jaringan yang dapat saling terhubung ke beberapa komputer atau *device*, perlu adanya sebuah sistem keamanan untuk menjamin supaya di dalam jaringan tersebut tidak terjadi kejahatan yang dapat merugikan bagi pengguna yang ada di dalam jaringan tersebut, ataupun dapat merusak sistem jaringan tersebut. Salah satu cara yang dapat kita gunakan untuk mencegah terjaidinya sebuah kejahatan di dalam jaringan atau internet adalah menggunakan *firewall*. Di dalam jurnal (Sembiring et al., 2011), disebutkan bahwa dalam membuat sebuah jaringan komputer, komponen yang wajib digunakan adalah sebuah *firewall*, dengan menggunakan *firewall* tersebut, nantinya *firewall* akan melindungi computer kita dari berbagai serangan yang masuk ke dalam port-port yang ada pada hardware jaringan kita. Karena di dalam komputer kita, kita sering melakukan instalasi aplikasi seperti aplikasi pengolah dokumen, aplikasi email klien, aplikasi antivirus, aplikasi server klien, dan aplikasi lainnya. Aplikasi tersebut memungkinkan komputer kita untuk membuka port-port yang terhubung ke jaringan kita, port tersebut adalah port komunikasi yang digunakan agar kita saling terhubung dengan computer atau device laiinya di satu jaringan yang sama. Port tersebut berupa port yang berada di dalam protocol TCP atau UDP yang merupakan suatu bagian dari layer pada standar OSI.

Di dunia jaringan komputer, kita mengenal beberapa macam jaringan komputer seperti yang disebutkan dalam jurnal berikut (Sujito & Roji, 2010), dalam jurnal tersebut jaringan komputer yang biasa kita kenal adalah jaringan komputer seperti LAN dan WAN. Penjelasan LAN menurut (Wongkar et al., 2015), dalam jurnal tersebut dijelaskan pengertian LAN adalah singkatan dari *local area network* yang berarti jaringan komputer yang terdapat atau terhubung dengan sesame pengguna atau decive dalam lingkup local atau lingkup yang kecil. Biasanya LAN tersebut sering kita jumpai pada jaringan sekolah-sekolah, perkantoran, ataupun sebuah perusahaan yang membutuhkan jaringan dengan skala yang kecil. Sedangkan pengertian dari WAN menurut (Yudianto, 2014), pengertian WAN yang merupakan singkatan dari wide area network, merupakan sebuah jaringan komputer yang mencakup area yang lebih luas daripada yang menggunakan jaringan LAN, biasanya area yang mencakup WAN adalah perkotaan atau bahkan negara. Jaringan WAN digunakan untuk menghubungkan jaringan local yang satu dengan jaringan local yang lain. Sehingga pengguna computer di lokasi tertentu dapat berkomunikasi dengan pengguna computer di lokasi lain.

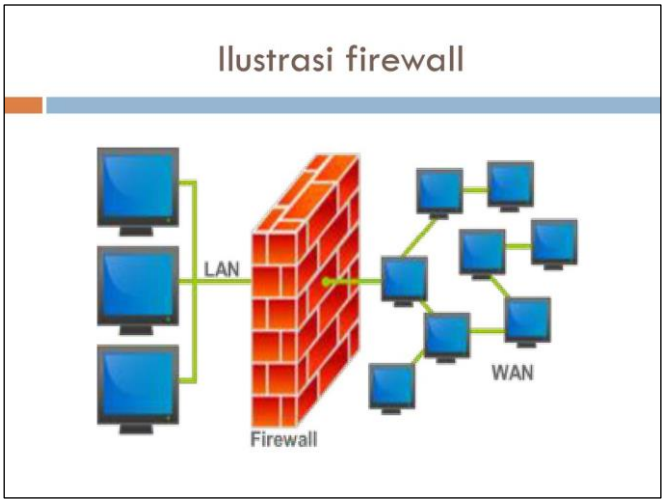
Setiap menggunakan jaringan komputer, entah itu LAN atau WAN, kita harus dapat menjaga keamanan dari jaringan komputer tersebut, sehingga kita dapat dengan tenang menggunakan jaringan komputer tersebut untuk komunikasi dan merasa lebih terjamin tidak akan terjadi hal-hal yang tidak diinginkan apabila sewaktu-waktu dapat terjadi.

Salah satu cara yang dapat digunakan untuk membuat jaringan adalah menggunaak router mikrotik, berdasarkan jurnal (Riadi, 2011), mikrotik adalah

sebuah sistem operasi yang dapat digunakan sebagai router jaringan yang handal. Router mikrotik dapat mencakup beberapa fitur yang dibutuhkan dalam suatu jaringan diantaranya adalah Mikrotik dapat menyediakan fitur sebagai *firewall* yang dapat menjamin kemanan bagi pengguna jaringan tersebut. Dalam sumber lain, berdasarkan jurnal (Pamungkas, 2016), disebutkan bahwa mikrotik routerboard adalah sebuah perangkat jaringan komputer yang menggunakan mikrotik routerOS yang berbasis Linux dan diperuntukan bagi network router. Selain itu mikrotik router juga memiliki beberapa fitur seperti *bandwith management*, *firewall*, *hotspot fot plug and play access*, *remote winbox*, dan *routing*. Admininstrasi untuk mikrotik routerboard dapat dilakukan menggunakan sistem operasi windows dengan aplikasi bernama WinBox. Dan, pada saat ini aplikasi tersebut sudah memiliki GUI sehingga lebih mudah digunakan untuk mengkonfigurasi router sesuai kebutuhan dengan mudah dan efisien.

Pengertian *firewall* menurut (Doni, 2015), dalam jurnalnya disebutkan bahwa *firewall* adalah sebuah sistem atau perangkat keamanan khususnya yang memiliki tugas untuk menjaga lalu lintas data yang berjalan atau saling bertukar informasi di dalam jaringan tersebut dan dalam waktu bersamaan juga bertugas untuk mencegah lalu lintas data yang tidak aman yang masuk ke dalam jaringan tersebut. *Firewall* biasanya di implementasikan pada sebuah *gateway* atau pintu gerbang pada sebuah jaringan komputer. Pengertian *firewall* dalam sumber lain, menurut (Pribadi, 2013), definisi *firewall* menurut jurnal tersebut adalah suatu cara yang baik diterapkan dalam sebuah hardware, software, ataupun sistem itu sendiri yang bertujuan untuk melindungi,

menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya.



Gambar 1.1 *Ilustrasi firewall*

Dalam jurnal sebelumnya disebutkan bahwa implementasi firewall biasanya ditempatkan pada sebuah *gateway*. Penjelasan *gateway* menurut (Fatriawan, 2016), dalam jurnalnya disebutkan bahwa pengertian *gateway* adalah sebuah perangkat dalam computer yang difungsikan untuk menghubungkan sebuah jaringan komputer dengan jaringan komputer yang laiinya, atau lebih menggunakan protocol informasi yang tidak sama. Salah satu aplikasi atau contoh dari penggunaan gateway adalah pada email, seperti kita tahu bahwa pertukaran email dapat dilakukan meskipun tidak menggunakan sistem yang sama. Kini, seiring dengan semakin merebaknya penggunaan internet, pengertian Gateway pun sering melakukan pergeseran atau mengalami salah arti. Banyak orang yang menyamakan *Gateway* dengan Router, tapi sebenarnya *Gateway* dan router adalah sesuatu yang berbeda.

Jika dilihat dari pengertiannya, maka kita mungkin dapat mengatakan bahwa secara umum *Gateway* berfungsi untuk menghubungkan sebuah

jaringan komputer dengan jaringan komputer yang lain dengan protocol yang berbeda. *Gateway* dapat digunakan dalam menghubungkan IBM SNA dengan digital SNA, Local Area Network atau LAN dengan Wide Area Network atau WAN.

1.1.2 Jenis Firewall

Jenis-jenis firewall menurut (Adhi Purwaningrum et al., 2018), dalam jurnal tersebut dijelaskan bahwa terdapat 3 jenis komfigurasi firewall diantaranya adalah sebagai berikut. *Screened host firewall system* (*single-homed bastion*), *screened host firewall system* (*Dual-homed bastion*), dan *screened subnet firewall*. Dan juga mengkonfigurasikan *firewall* dengan membuka port-port yang tepat untuk melakukan hubungan koneksi ke internet, karena dengan mengkonfigurasi port-port tersebut suatu *firewall* dapat menyaring paket-paket data yang masuk yang sesuai dengan policy atau kebijakannya. Arsitektur *firewall* ini yang akan digunakan untuk mengoptimalkan suatu firewall pada jaringan

Konfigrasi suatu *firewall* yang pertama adalah penentuan policy atau kebijakan *firewall* tersebut tentang apa saja yang akan dikenai kebijakan tersebut, siapa saja yang akan dikenai kebijakan tersebut dan layananlayanan yang dibutuhkan tiap individu tersebut. Kemudian menentukan port-port yang digunakan oleh berbagai protokol dan membuka port-port tersebut kedalam *firewall*, dan juga membuka port yang digunakan untuk *file sharing* dan *request ping*. Selanjutnya adalah menentukan suatu konfigurasi yang tepat dan sesuai dengan keadaan jaringannya. *Screened subnet* merupakan konfigurasi yang

paling tinggi tingkat keamanannya. Dengan konfigurasi tersebut memungkinkan *firewall* kita dapat menigkatkan keamanan yang jauh lebih baik dari ancaman-ancaman internet. Namun tidak menutup kemungkinan bahwa jaringan kita tetap dapat diserang oleh *hacker* yang serangannya sangat terarah. Namun lebih baik sedikit terlindungi daripada tidak sama sekali.

Sedangkan dalam sumber lain, menurut (Sutoyo & Wahyudi, 2009), dijelaskan bahwa firewall memiliki beberapa jenis diantaranya adalah sebagai berikut.

1. *Packet Filterring Firewall*

   Sesuai dengan namanya, prinsip kerja *firewall* jenis ini adalah melaksanakan penyaringan terhadap setiap paket data. Dari hasil penyaringan tersebut selanjutnya dapat diputuskan, apakah paket data tersebut dapat diproses lebih lanjut atau ditolak. *Firewall* jenis ini umumnya diimplementasikan pada perangkat router. Router adalah perangkat jaringan yang bekerja pada lapisan jaringan (network layer) pada model Open System Interconnection (OSI). Dengan demikian, penyaringan paket data oleh packet filtering firewall setidaknya didasarkan pada informasi yang diolah pada lapisan tersebut, yaitu Alamat IP.

   Kelebihan *firewall* jenis ini, antara lain : sifatnya independen, mudah disesuaikan dengan kebutuhan sistem, memiliki transparansi yang tinggi, dan unjuk kerjanya pun tinggi. Sebaliknya, kelemahan *firewall* jenis ini, antara lain pengamanan yang berfungsi untuk menyaring (filtering) lalu lintas data yang melewati titik-titik akses pada jaringan atau pintu-pintu keluar masuk lalu lintas data, baik yang ingin masuk ke dalam jaringan

internal (*inbound*) maupun yang ingin keluar ke jaringan eksternal (outbound). dilaksanakan masih sangat rendah dibandingkan dengan banyaknya ancaman yang mengintai jaringan komputer yang dijaga, sangat rentan terhadap IP Spoofing, tidak memiliki metode untuk memeriksa aktivitas yang dilakukan oleh koneksi-koneksi yang aktif (*stateless*), tidak memiliki metode otentikasi, dan kemampuannya sangat terbatas karen hanya bekerja pada lapisan jaringan (*network layer*).

2. *Application Level Gateway*

   Firewall jenis ini biasa dikenal sebagai proxy. Prinsip kerjanya adalah sebagai perantara antara host pada jaringan internal dengan sumber daya eksternal yang diakses oleh host tersebut. Nama yang umum dikenal untuk *firewall* jenis ini adalah *proxy server*. Dengan menggunakan *proxy server*, *host* pada jaringan internal tidak pernah berhubungan lansung dengan sumber daya jaringan di luar jaringan lokal tempat ia berada. Setiap ada permintaan koneksi untuk mengakses sumber daya jaringan di luar jaringan lokal harus selalu diarahkan ke proxy server terlebih dahulu. Proxy server inilah yang nantinya akan memutuskan, apakah koneksi boleh dilaksanakan atau tidak.

   Kelebihan *firewall* jenis ini, antara lain pengamanan yang dilaksanakan lebih bagus dibandingkan packet filter, memiliki metode otentikasi, memiliki metode kendali akses (*access control*), memiliki fasilitas *logging*, dan memiliki fasilitas caching untuk membantu menghemat bandwith. Sebaliknya, kelemahan *firewall* jenis ini, antara lain. kurangnya transparansi terhadap pengguna dimana aplikasi pengguna

harus dikonfigurasi untuk mendukung fungsi proxy, aplikasi yang digunakan harus mendukung fasilitas proxy, dan unjuk kerja yang lebih rendah dibandingkan packet filter.

3. *Circuit Level Gateway*

   Firewall jenis ini merupakan pengembangan dari Application Level Gateway. Prinsip kerja Circuit Level Gateway serupa dengan Application Level Gateway, yakni sebagai perantara antara host pada jaringan internal dengan sumber daya eksternal yang diakses oleh host tersebut. Perbedaaannya adalah pada tingkatan atau lokasi pelaksanaan fungsi perantaraan (proxy) tersebut dilaksanakan. Kelebihan firewall jenis ini kurang lebih sama dengan Application Level Gateway, namun ia menutupi kelemahan kurangnya transparansi dari Application Level Gateway, dimana setiap aplikasi tidak perlu dikonfigurasi untuk mendukung fungsi proxy, bahkan aplikasi yang tidak memiliki dukungan terhadap fungsi proxy pun masih dapat berjalan. Sebaliknya, kelemahan Firewall jenis ini pun kurang lebih sama, bedanya adalah aplikasi harus kompatibel dengan platform yang digunakan, misalnya harus kompatibel dengan *Application Programming Interface* (API).

4. *Statefull Inspection*

   Firewall jenis ini adalah *firewall* yang paling canggih dibandingkan dengan tiga jenis *firewall* sebelumnya. Prinsip kerja dari Statefull Inspection adalah selalu aktif mengawasi setiap koneksi yang terjadi, sehingga selalu dapat diketahui status dari koneksi-koneksi tersebut

(statefull) dan dapat dilaksanakan tindakan yang semestinya jika ditemukan adanya penyimpangan-penyimpangan dari koneksi yang ada.

Kelebihan *firewall* jenis ini, antara lain tingkat pengamanannya paling tinggi, pengamanannya paling lengkap karena mendukung dan dapat melaksanakan pengawasan pada seluruh lapisan OSI, memiliki unjuk kerja yang tinggi, memiliki skalabilitas yang bagus, dan memiliki transparansi yang tinggi. Sebaliknya, kelemahan *firewall* jenis ini adalah diperlukannya sumber daya yang sangat besar untuk menjalankannya, apalagi saat jumlah koneksi makin bertambah banyak.

1.1.3 Fungsi Firewall

Fungsi *firewall* pada dasaranya adalah untuk memberikan Batasan akses atau filter dari paket-paket data yang masuk ke dalam jaringan kita, dan mengatur lalu lintas dari jaringan yang keluar masuk atau saling berukuran paket data, sehingga dipastikan lalu lintas jaringan kita dilalui oleh paket-paket data yang aman dan sudah terpercaya. Fungsi firewall yang dijelaskan menurut (Mulyana & Purbo, 2000), dalam jurnalnya mengatakan bahwa fungsi *firewall* untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan, lebih khusus lagi, antara jaringan internal dengan jaringan global Internet. *Firewall* mempunyai beberapa tugas, diantaranya adalah sebagai berikut.

1. Pertama dan yang terpenting adalah: harus dapat mengimplementasikan kebijakan security di jaringan (site security policy). Jika aksi tertentu tidak diperbolehkan oleh kebijakan ini, maka firewall harus meyakinkan bahwa semua usaha yang mewakili operasi tersebut harus gagal atau digagalkan.

Dengan demikian, semua akses illegal antar jaringan (tidak diotorisasikan) akan ditolak.

2. Melakukan filtering: mewajibkan semua traffik yang ada untuk dilewatkan melalui firewall bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam konteks ini, aliran paket data dari/menuju firewall, diseleksi berdasarkan IP-address, nomor port, atau arahnya, dan disesuaikan dengan kebijakan security.
3. Firewall juga harus dapat merekam/mencatat even-even mencurigakan serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan security.

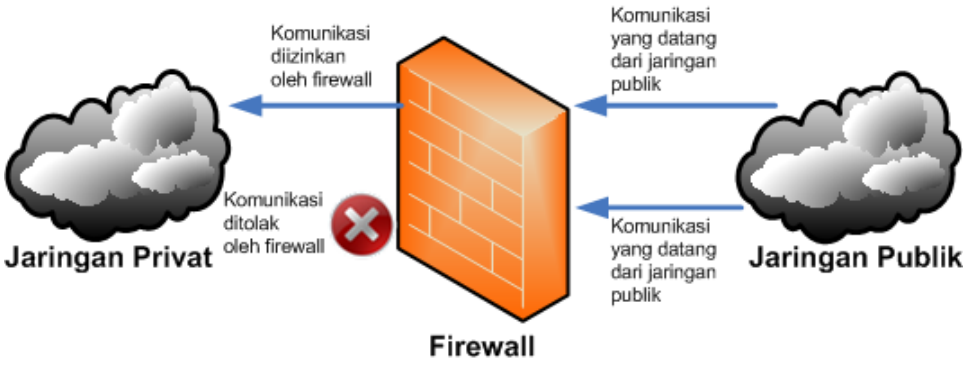
1.1.4 Cara Kerja Firewall

Cara kerja dari *firewall* secara umum adalah memberikan filter atau menyaring paket-paket data yang masuk, dan hanya memperbolehkan paket-paket data yang sudah dikenal oleh jaringan tersebut, dapat juga melarang paket yang masuk ke jaringan kita apabila kita sudah memberikan konfigurasi situs-situs yang tidak boleh diakses menggunakan jaringan tersebut.Cara kerja *firewall* disebutkan dalam (Dewaweb, 2019), dijelaskan beberapa cara kerja *firewall*, diantaranya adalah sebagai berikut.

1. Penyaringan paket. Paket (potongan kecil data) dianalisis terhadap satu set filter. Paket yang lolos melalui filter dikirim ke sistem yang diminta, sementara paket lainnya dibuang.
2. Layanan proxy. Informasi dari Internet diambil oleh firewall dan kemudian dikirim ke sistem yang diminta dan sebaliknya.

3. Inspeksi stateful. Metode lebih baru yang tidak memeriksa konten setiap paket tetapi membandingkan bagian-bagian kunci tertentu dari paket dengan database informasi tepercaya. Informasi dari dalam firewall ke luar dimonitor untuk menentukan karakteristik spesifik, kemudian informasi yang masuk dibandingkan dengan karakteristik ini. Jika perbandingan menghasilkan kecocokan yang masuk akal, informasi tersebut diizinkan masuk. Kalau tidak, dibuang.

Sedangkan cara kerja *firewall* yang dijelaskan menurut (Khadafi et al., 2019), dalam jurlanya mengatakah bahwa , *firewall* diberikan sebuah konfigurasi khusus disebut *the rule-set*, kemudian *the rule-set* dirancang sedemikian rupa sehingga *firewall* harus memeriksa dan menganalisa setiap *traffic* data yang masuk melalui *rule-set*. Filter *firewall* mempunyai kebijakan yang dibuat (*rule-set*) untuk mengontrol traffic data yang masuk sebelum mengizinkan traffic data tersebut masuk. *Firewall* juga dapat memblokir traffic data serta melakukan pencatatan bilamana traffic data yang masuk berisikan paket data yang mencurigakan. *The Rule-set* untuk *firewall* tersebut kemudian dikonversi menjadi sintaks khusus untuk mesin *firewall* yang digunakan oleh perangkat komputer.



Gambar 1.2 *Cara kerja Firewall*

1.2 Implementasi Firewall Filter dalam Mikrotik

1.2.1 Pengertian Firewall Filter

Firewall Filter ini berfungsi menyaring (*filter*) paket data yang masuk dan keluar dari jaringan dalam (local) atau dari jaringan luar (internet). Jadi, nantinya router akan menyaring data apa saja yang boleh masuk / keluar. Firewall filtering biasanya dilakukan dengan cara mendefinisikan IP address, baik itu src-address maupun dst-address. Misalnya Anda ingin blok komputer client yang memiliki ip tertentu atau ketika melakukan blok terhadap web tertentu berdasarkan ip web tersebut. Firewall tidak hanya digunakan untuk melakukan blok client agar tidak dapat mengakses resource tertentu, namun juga digunakan untuk melindungi jaringan local dari ancaman luar, misalnya virus atau serangan hacker. Biasanya serangan dari internet ini dilakukan dari banyak IP sehingga akan sulit bagi kita untuk melakukan perlindungan hanya dengan berdasarkan IP. Sebenarnya ada banyak cara filtering selain berdasar IP Address, misalnya berdasar protocol dan port.

1.2.2 Fitur Firewall Filter

1. Filter Rules

   Filter Rules merupakan salah satu firewall pada mikrotik yang digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak kedalam sistem Router MikroTik, paket data yang akan ditangani fitur filter ini adalah paket data yang ditunjukan pada salah satu interface router.

2. NAT

   NAT (Network Address Translation) fitur ini digunakan untuk melakukan pengubahan terhadap sumber maupun tujuan dari alamat IP Address. NAT akan mengubah paket data yang berasal dari komputer user seolah-olah berasal dari router tersebut.

3. Mangle

   Mangle merupakan fitur Firewall MikroTik yang berfungsi untuk menandai paket data dan koneksi tertentu yang dapat diterapkan pada fitur mikrotik lainnya, sepeti pada routes, pemisahan bandwidth pada queues, NAT dan filter rules. Tanda mangle yang ada pada router mikrotik hanya bisa digunakan pada router itu sendiri. Dan kita harus mengetahui bahwa proses pembacaan rule mangle ini dilakukan dari urutan pertama sampai ke bawah.

4. Service Ports

   Service Ports merupakan fitur yang digunakan untuk menonaktifkan atau merubah port-port yang aktif. Biasanya digunakan untuk menonaktifkan port aktif yang tidak dibutuhkan oleh Router MikroTik kita.

5. Connections

   Connections merupakan sebuah fitur yang digunakan untuk melihat atau memantau informasi koneksi yang pernah terhubung atau keluar dari Router MikroTik.

6. Address List

   Address Lists merupakan fitur Firewal MikroTik juga yang berfungsi untuk memudahkan kita dalam mengelompokan IP Address. Sehingga dengan address list ini, kita bisa membuat daftar IP Address yang ingin di tandai tanpa harus menggangu konfigurasi penting di fitur lainnya.

7. Layer 7 Protocols

   Layer 7 Protocols merupakan fitur yang digunakan untuk menentukan metode pencarian pola terhadap paket data yang melewati jalur ICMP, TCP, dan UDP Atau istilah lainnya regex pattern. Biasanya digunakan untuk melakukan blocking terhadap situs web dengan SSL https://

1.2.3 Jenis Chain dalam Firewall Filter

1. Chain pada Filter Rules

   a. Forward :

      Digunakan untuk memproses trafik paket data yang hanya melewati router. Misalnya trafik dari jaringan public ke local atau sebaliknya dari jaringan local ke public, contoh kasus seperti pada saat kita melakukan browsing. Trafik laptop browsing ke internet dapat dimanage oleh firewall dengan menggunakan chain forward.

b. Input :

Digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router. Jenis trafik ini bisa berasal dari jaringan public maupun dari jaringan lokal dengan tujuan router itu sendiri. Contoh: Mengakses router menggunakan winbox, webfig, telnet baik dari Public maupun Local.

c. Output :

Digunakan untuk memproses trafik paket data yang keluar dari router. Dengan kata lain merupakan kebalikan dari 'Input'. Jadi trafik yang berasal dari dalam router itu sendiri dengan tujuan jaringan Public maupun jaringan Local.Misal dari new terminal winbox, kita ping ke ip google. Maka trafik ini bisa ditangkap dichain output.

2. Chain pada NAT

a. Dstnat :

Memiliki fungsi untuk mengubah destination address pada sebuah paket data. Biasa digunakan untuk membuat host dalam jaringan lokal dapat diakses dari luar jaringan (internet) dengan cara NAT akan mengganti alamat IP tujuan paket dengan alamat IP lokal. Jadi kesimpulan fungsi dari chain ini adalah untuk mengubah/mengganti IP Address tujuan pada sebuah paket data.

b. Srcnat :

Memiliki fungsi untuk mengubah source address dari sebuah paket data. Sebagai contoh kasus fungsi dari chain ini banyak digunakan

ketika kita melakukan akses website dari jaringan LAN. Secara aturan untuk IP Address local tidak diperbolehkan untuk masuk ke jaringan WAN, maka diperlukan konfigurasi 'srcnat' ini. Sehingga IP Address lokal akan disembunyikan dan diganti dengan IP Address public yang terpasang pada router.

3. Chain pada Mangle

a. Forward, Input, Output :

Untuk penjelasan mengenai Forward, Input, dan Output sebenarnya tidak jauh berbeda dengan apa yang telah diuraikan pada Filter rules diatas. Namun pada Mangle, semua jenis trafik paket data forward, input, dan output bisa ditandai berdasarkan koneksi atau paket atau paket data.

b. Prerouting :

Merupakan sebuah koneksi yang akan masuk kedalam router dan melewati router. Berbeda dengan input yang mana hanya akan menangkap trafik yang masuk ke router. Trafik yang melewat router dan trafik yang masuk kedalam router dapat ditangkap di chain prerouting.

c. Postrouting :

Kebalikan dari prerouting, postrouting merupakan koneksi yang akan keluar dari router, baik untuk trafik yang melewati router ataupun yang keluar dari router.

4. Custom Chain

Biasanya custom chain digunakan untuk menghemat resource router dan mempermudah admin jaringan dalam membaca rule firewall. By default router akan membaca rule firewall secara berurutan sesuai nomor urut rule firewall. Namun dengan fitur jump ini, admin jaringan dapat menentukan pembacaan rule firewall yang lebih efisien.

Untuk membuat *custom chain* tersebut kita memerlukan sebuah 'Action' yaitu Jump. Jump sendiri berfungsi untuk melompat ke chain lain yang telah didefiniskan pada paramater *jump-target*. Sehingga kita bisa menempatkan rule dari *custom chain* yang telah kita buat pada urutan paling bawah. Ini dimaksudkan untuk mempermudah dalam pengelolaan rule-rule firewall, terlebih lagi jika kita memiliki rule-rule yang banyak.

1.2.4 Connection Tracking dan Connection State

Connection Tracking adalah “jantung” dari firewall, mengumpulkan informasi tentang active connections. Dengan mendisable connection tracking router akan kehilangan fungsi NAT, filter rule dan mangle. Setiap connection tracking membaca pertukaran traffic 2 arah (src dan dst address). Connection tracking membutuhkan CPU resources (disable saja jika kita tidak menggunakan firewall).

Connection tracking mempunyai kemampuan untuk melihat informasi koneksi yang melewati router, seperti source dan destination IP dan Port yang sedang di gunakan, status koneksi,tipe protocol dan lain-lain.

Setiap paket data itu memiliki status koneksi (connection state) yang dapat dilihat pada connection tracking, status koneksinya sebagai berikut :

- Invalid : paket tidak dimiliki oleh koneksi apapun, tidak berguna.
- New : paket yang merupakan pembuka sebuah koneksi/paket pertama dari sebuah koneksi.
- Established : merupakan paket kelanjutan dari paket dengan status new.
- Related : paket pembuka sebuah koneksi baru, tetapi masih berhubungan denga koneksi sebelumnya.

1.3 Contoh Penerapan Firewall Filter

1.3.1 Port Scan Detection (PSD)

Port Scanner merupakan aplikasi yang digunakan untuk melihat informasi atau status dari protocol dan port yang terbuka (open) dari sebuah perangkat. Dengan aplikasi ini bisa jadi merupakan sebuah awal dari dimulainya serangan terhadap sebuah resource di jaringan. Ketika informasi protocol/port sudah didapat maka 'Hacker' bisa memanfaatkan untuk melakukan eksploitasi dari protocol/port tersebut. Misal, salah satu contoh untuk serangan Distributed Denial of Service (DDoS). Banyak aplikasi yang bisa digunakan untuk melakukan port scanner yang umumnya seperti nmap, netcut, unicornscan.

Kali ini kita akan mencoba bagaimana mengamankan perangkat jaringan khususnya router dari port scanner. Di Mikrtoik sendiri sudah disediakan fitur untuk hal tersebut yaitu dengan Port Scan Detetction (PSD). Konfigurasinya bisa dilakukan pada menu firewall filter di Tab 'Extra'.

Pada parameter PSD terdapat beberapa konfigurasi yang perlu di setting:

1. Weight Threshold : Nilai total dari 'LowPortWeight' dan 'HighPortWeight' untuk paket-paket TCP/UDP dengan tujuan port yang berbeda ynag berasal dari host/Source IP Address yang sama. Rule PSD akan berjalan ketika sudah mencapai nilai Weight Threshold ini. (Secara default nilainya adalah 21).
2. Delay Threshold : Merupakan nilai waktu jeda (delay) dari trafik/paket yang dikirimkan oleh aplikasi port sacnner dari sebuah host/Source IP Address yang sama dengan tujuan berbeda port. (Default adalah 00:00:03)
3. Low Port Weight : Sebuah nilai yang diberikan oleh system ketika terdapat trafik/paket dari Port Scanner yang memiliki destinasi ke 'Low Port'. Disini yang dimaksud dari low port adalah port dibawah 1024 atau yang masuk dalam kategori System/Well-Known Port. Seperti port 80 (HTTP), 443 (HTTPS), 53 (DNS), 22 (SSH), 23 (Telnet), 110 (POP3), SMTP (25), dll.
4. High Port Weight : Sebuah nilai yang diberikan oleh system ketika terdapat trafik/paket dari Port Scanner yang memiliki destinasi ke 'High Port'. Disini yang dimaksud dari high port adalah port yang diatas 1024 atau yang masuk dalam kategori registered port dan dynamic/private port. Seperti 3128 (Squid web-Proxy), 1080 (SOCKS Proxy), 1701 (L2TP), 1723 (PPTP), dll.

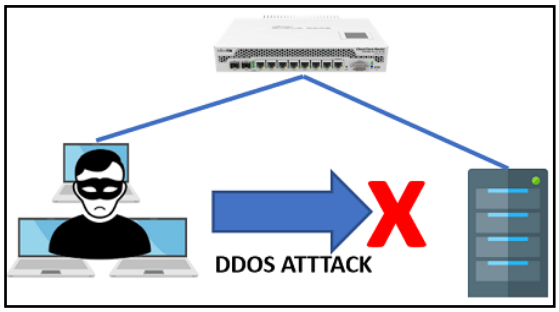
Secara garis besar mekanismenya adalah rule akan membaca trafik dari port scanner dan memberikan nilai dari port yang di-scan

sesuai dengan nilai LOW PORT atau HIGH PORT WEIGHT. Setelah total 'WEIGHT'' mencapai nilai sesuai yang didefinisikan pada 'Weight Threshold' maka rule PSD akan dijalankan.

1.3.2 Mengamankan Server dari Serangan DDOS

Memberikan keamanan kepada Router adalah salah satu kewajiban yang harus dilakukan oleh admin jaringan. Sebagai Admin jaringan, selain bisa melakukan konfigurasi, troubleshooting, dll maka seorang Admin jaringan juga diwajibkan untuk memberikan keamanan terhadap perangkat jaringan seperti Router, Server, dll. Sebelum memberikan konfigurasi Router ke Internet, maka sebaiknya kita bisa memberikan keamanan terlebih dahulu kepada Router. Bisa dimulai dari hal yang paling simple yaitu mengganti username dan password Router, kemudian menutup service yang tidak terpakai, dan mendisable Neighboor discovery. DDOS merupakan kependekan dari Distributed Denial of Service dimana DDOS ini adalah jenis serangan yang dilakukan dengan membanjiri lalu lintas traffic pada jaringan. Dengan adanya DDOS ini maka traffic di jaringan akan penuh dan menyebabkan resource dari perangkat naik.

Contoh Proteksi dari DDOS sebagai berikut :



Gambar 1.3 DDoS Attack

Langkah dalam konfigurasinya sebagi berikut :

1. Langkah pertama, kita bisa membuat rule firewall filter dengan action drop terhadap alamat ip asal "ddoser" dengan tujuan alamat ip "ddosed".

```
/ip firewall filter
add chain=forward connection-state=new src-address-list=ddoser dst-address-list=ddosed action=drop
```

2. Kemudian kita akan menangkap semua koneksi "new" dan membuat chain baru yaitu "detect-ddos".

```
/ip firewall filter
add chain=forward connection-state=new action=jump jump-target=detect-ddos
```

3. Kemudian kita akan membuat rule firewall.

```
/ip firewall filter
add chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/1s action=return
add chain=detect-ddos src-address=192.168.0.1 action=return
```

4. Dengan rule firewall diatas, maka ketika terdapat paket new yang tidak wajar, misalnya diatas 32 paket selama satu detik, maka firewall akan melakukan penandaan terhadap alamat asal dan alamat tujuan menggunakan address list.

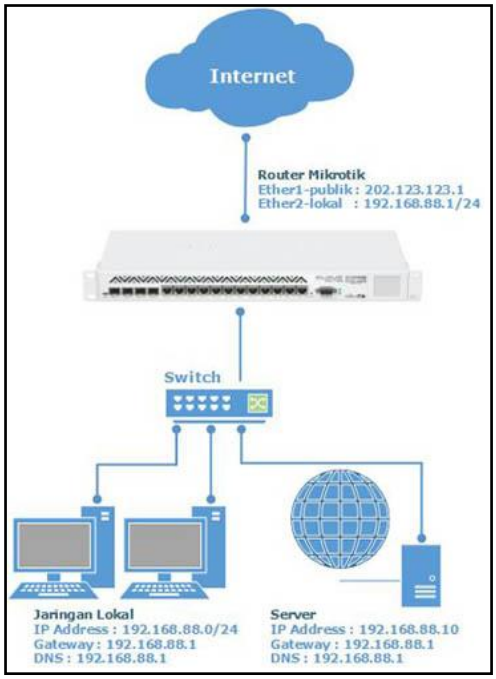
```
/ip firewall filter
add chain=detect-ddos action=add-dst-to-address-list address-list=ddosed address-list-timeout=10m
add chain=detect-ddos action=add-src-to-address-list address-list=ddoser address-list-timeout=10m
```

Dengan rule diatas maka ketika terdapat paket new yang tidak wajar akan dilakukan grouping menggunakan address list dengan nama "ddosed" dan "ddoser", setelah alamat IP penyerang dan alamat IP tujuan berhasil

ditangkap menggunakan address-list maka alamat IP tersebut akan di drop oleh firewall filter yang kita buat di awal tadi. Dengan begitu perangkat client seperti Server dapat terhindar dari serangan DDOS oleh orang yang tidak dikenal.

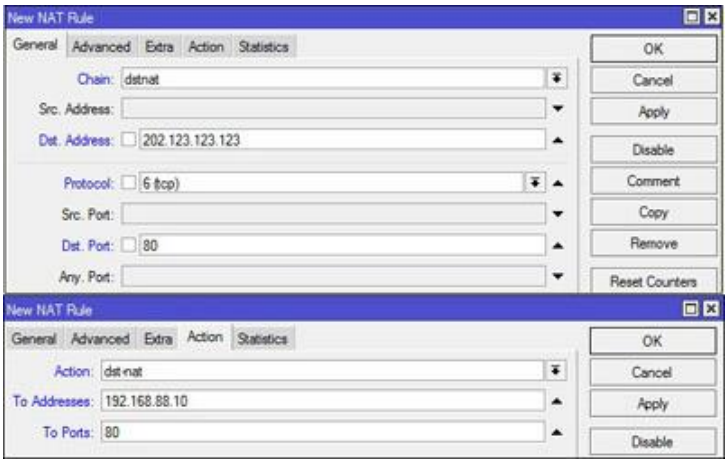
1.3.3 Forwarding dengan Fitur NAT

Ada kalanya server yang ada di jaringan kita perlu bisa diakses dari jaringan publik. Misalnya karena ada karyawan yang bersifat mobile dan harus bisa mengakses data yang ada di server tersebut. Yang kita butuhkan adalah IP publik. Ip publik statis lebih direkomandasikan. Kita bisa saja langsung memasang ip publik ke server kita, maka server tersebut sudah bisa diakses dari internet. Pada mikrotik, kebutuhan tersebut bisa diatasi dengan cara port forwading menggunakan fitur NAT. Agar bandiwidth bisa di manage dan firewall filtering bisa dilakukan, kita tempatkan server dibawah router mikrotik. Artinya, server berada di jaringan lokal, contoh topologi :



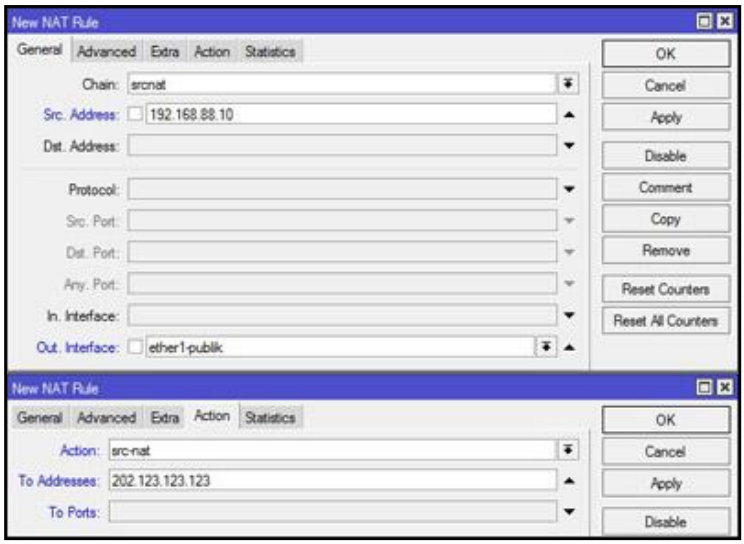
Gambar 1.4 NAT

Agar Server bisa diakses dari internet, set fowarding di router mikrotik dengan fitur firewall NAT. Fowarding ini akan membalokkan traffic yang menuju ke IP publik yang terpasang di router menuju ke IP lokal server. Dengan begitu, seolah-olah client dari internet berkomunikasi dengan server meminjam IP public router mikrotik. Langkah pembuatan rule, masuk ke menu IP --> Firewall --> klik tab "NAT", tambahkan rule baru dengan menekan tombol "add" atau tanda "+" berwarna merah.



Gambar 1.5 NAT

Jika NAT sudah berhasil, baru kemudian kita tentukan protokol dan port yang harus di foward ke server. Dengan konfigurasi diatas, rule fowarding sudah selesai. Akan tetapi jika kita memiliki lebih dari satu ip public, kita butuh satu rule lagi. Rule yang difungsikan untuk mengarahkan traffic respon dari server ke jalur yang sama dengan traffic request. Jika ternyata traffic respon keluar dari IP Public B, maka traffic tersebut tidak dikenali oleh cilent yang mencoba mengakses server. Rule yang harus dibuat seperti berikut :



Gambar 1.6 Rule

Rule NAT untuk fowarding sudah selesai, jika kita memiliki lebih dari satu server sedangkan kita hanya memiliki satu IP public, kita bisa foward berdasarkan port. Misal untuk server A dapat diakses melalui port 5678, kemudian server B melalui port 8910. Dengan logika tersebut, ketika router menerima koneksi dari port 5678, maka koneksi tadi akan diteruskan ke Server A, begitu juga ketika router menerima koneksi dari port 8910, maka akan diteruskan ke server B.

1.3.4 Pencegahan Penyebaran Malware WannaCry

Seluruh dunia lagi terguncang dengan kehadiran Malware Ransomware Wannacrypt yang sangat membahayakan khususnya bagi pengguna Sistem Operasi Windows. Malware ini menginfeksi pengguna PC berbasis Windows yang memiliki kelemahan terkait fungsi SMB yang dijalankan pada komputer tersebut. Malware Ransomware Wannacrypt dilaporkan sudah menginfeksi banyak pengguna di seluruh belahan dunia dan dikhawatirkan Indonesia akan mendapatkan malware yang lebih besar.

Berikut ini adalah beberapa tindakan pencegahan untuk meminimalisir terinveksi Malware Ransomware Wannacrypt :

1. Jangan terkoneksi di LAN/WIFI, Lakukan Back Up Data

   LAN DAN WIFI merupakan jaringan yang bisa saling bertukaran data anta komputer yang terhubung pada jaringan tersebut. Pencegahan yang terdini untuk menyelamatkan file Anda adalah melakukan backup terlebih dahulu, pastikan saat Anda melakukan backup jangan terkoneksi dengan LAN dan WIFI terlebih dahulu. Hal ini untuk mencegah malware masuk ke sistem komputer Anda

2. Lakukan Update AntiVirus

   Dengan adanya serangan ini, tentunya berbagai Anti Virus melakukan update untuk menanggulangi terjadinya serangan Malware Ransomware Wannacrypt. Pastikan Anda menggunakan Antivirus yang terpercaya untuk meningkatkan keamanan PC Anda yang menggunakan OS Windows.

3. Lakukan Update Patch MS17-010 pada OS Windows

Patch keamanan MS17-010 yang dirilis Microsoft sejatinya sudah diumumkan sejak bulan Maret lalu. Namun sepertinya sebagian besar komputer yang ada di dunia belum menginstalnya. Sehingga kelengahan ini pun dimanfaatkan secara masif oleh penyebar WannaCrypt.Update security pada windows anda dengan install Patch MS17-010 yang dikeluarkan oleh microsoft.

4. Non Aktifkan Fungsi SMB v1

Microsoft mengambil langkah yang tidak biasa untuk melindungi pelanggannya dengan versi Windows yang tidak didukung – termasuk Windows XP, Vista, Windows 8, Server 2003 dan 2008 – dengan merilis patch keamanan yang memperbaiki cacat SMB yang saat ini dieksploitasi oleh WannaCry ransomware.Setelah melakukan update patch MS17-010 terbaru pada OS Windows Anda, lakukan Disable pada fitur SMBv1 Komputer Anda. Ikuti Langkah-Langkah Berikut :

Update :

- *Cara Mematikan fitur SMB V1 untuk windows 7*
    1. Jalankan windows power shell (run as administrator)
    2. Masukan script berikut di perintahnya

       Set-ItemProperty-Path

       “HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\

       Parameters” SMB1 -Type DWORD -Value 0 –Force
- *Cara Mematikan fitur SMB V1 untuk windows 8*
    1. Jalankan windows power shell (run as administrator)

2. Masukan script berikut di perintahnya

   Set-SmbServerConfiguration -EnableSMB1Protocol $false

5. Jangan Mengaktifkan Fungsi Macros

   Windows Scripting Host (sering disingkat menjadi WSH) adalah sebuah aplikasi yang mendukung fungsi-fungsi skripting di dalam sistem operasi Windows 2000, Windows NT Option Pack, Windows 98, Windows XP, dan Windows Vista yang mengizinkan para administrator untuk mengeksekusi skrip-skirp untuk beberapa tugas administratif, baik itu menggunakan cscript.exe maupun wscript.exe.Perlu Anda ketahui Bahwa Fungsi macros digunakan untuk menghindari file dari aplikasi Ms. Office, atau WScript terkena dampak penyebaran Malware Ransomware Wannacrypt.Berikut ini adalah langkah untuk mengetahui status Windows Script & Macro ON / OFF :

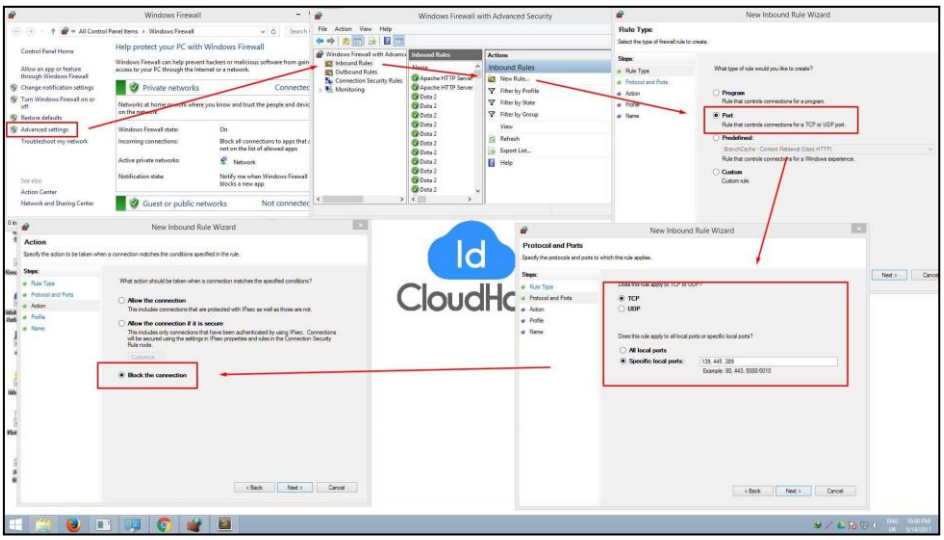
   1. Klik Start -> Run , kemudian ketik: “wscript” tanpa tanda kutip
   2. Jika muncul pesan: “Windows Script Host access is disabled on this machine. Contact your administrator for details.”, itu artinya WSH (Windows Script Host) dalam posisi OFF

6. Blokir port 139/445 dan 3389

   Port 139/445 dan 3389 merupakan jalur yang bisa saja dilewati oleh Malware Ransomware Wannacrypt, Anda perlu melakukan blokir untuk mencegah penyebaran Malware Ransomware Wannacrypt ke PC Anda.

Cara pertama Tutorial Cara Blokir port 139/445 dan 3389 :

1. Buka windows firewall atau windows run cmd : (ketik “wf.msc” , tanpa tanda petik)
2. Pilih advance setting
3. Inbound rules -> pilih New Rules
4. Pilih Port -> next
5. Pilih tcp dan isi port 139,445,3389 -> next
6. Centang public,home,private -> next
7. Name (isi terserah contoh : Block Wannacry) -> next



Gambar 1.7 Blocking Port

Cara kedua untuk melakukan Block port via windows firewall:

1. Navigate to Control Panel, System and Security and Windows Firewall.
2. Select Advanced settings and highlight Inbound Rules in the left pane.
3. Right click Inbound Rules and select New Rule.
4. Add the port you need to open and click Next.
5. Add the protocol (TCP or UDP) Port 139 and Port 445 and port 3389 (optional) the port number into the next window and click Next.
6. Select Block the connection in the next window and hit Next.

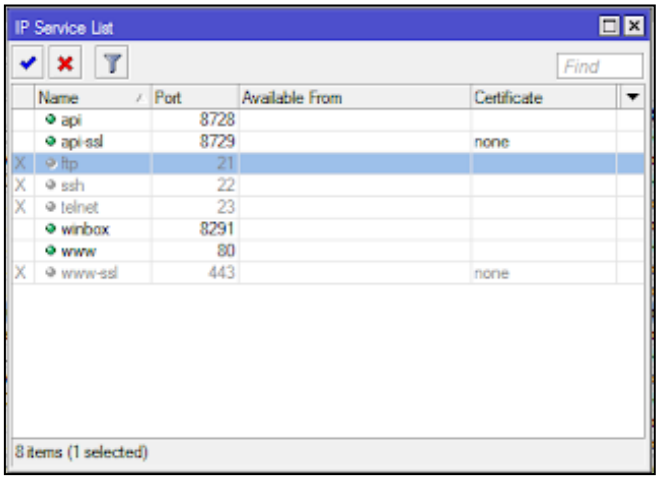
7. Select the network type as you see fit and click Next.
8. Name the rule something meaningful and click Finish.

1.3.5 Mengamankan Router dari serangan Bruteforce

Menjaga kemanan Router adalah salah satu kewajiban yang harus dilakukan oleh admin jaringan. Router bisa kita ibaratkan seperti sebuah rumah, Router adalah area privasi yang tidak bisa di akses oleh sembarang orang.

Sebelum melakukan konfigurasi Router ke Internet, sebaiknya memberi keamanan terlebih dahulu kepada Router. Kami sudah pernah membahas mengenai langkah pertama untuk menjaga Router, mulai dari mengganti username dan password default dari Router, menutup Service yang tidak terpakai, dan mendisable Neighboor discovery. Berikut ini adalah cara-cara mencegah Brute force login Mikrotik.

1. Matikan Service yang Tidak Digunakan
   - Silahkan masuk ke IP>Services->Disable pada service FTP, SSH, dan Telnet.



Gambar 1.8 IP Service List

2. Menandai & Memblokir FTP Attacker

- Silahkan Copy Paste script berikut pada NEW Terminal di winbox.

```
/ip firewall filter
add chain=output comment="Drop FTP Brute Forcers" content=\
    "530 Login incorrect" dst-limit=1/1m,9,dst-address/1m protocol=tcp
add action=add-dst-to-address-list address-list=FTP_BlackList \
    address-list-timeout=1d chain=output content="530 Login incorrect" \
    protocol=tcp
add action=drop chain=input dst-port=21 protocol=tcp src-address-list=\
```

3. Menandai dan Memblok SSH & Telnet Attacker

```
/ip firewall filter
add action=add-src-to-address-list address-list=ssh_blacklist_1 \
    address-list-timeout=1m chain=input comment=\
    "Drop SSH dan TELNET" connection-state=new dst-port=22-23 \
    protocol=tcp
add action=add-src-to-address-list address-list=ssh_blacklist_2 \
    address-list-timeout=1m chain=input connection-state=new dst-port= 22-23 protocol=tcp src-
address-list=ssh_blacklist_1
add action=add-src-to-address-list address-list=ssh_blacklist_3 \
    address-list-timeout=1m chain=input connection-state=new dst-port=\
    22-23 protocol=tcp src-address-list=ssh_blacklist_2
add action=add-src-to-address-list address-list=IP_BlackList \
    address-list-timeout=1d chain=input connection-state=new dst-port=\
    22-23 protocol=tcp src-address-list=ssh_blacklist_3
add action=drop chain=input dst-port=22-23 protocol=tcp \
    src-address-list=IP_BlackList
```

Dengan memasang script diatas kita dapat mencegah IP Attacker yang mencoba masuk ke router kita.

1.3.6 Simple Port Knocking

Port Knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupuan ICMP. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule knocking yang diterapkan, maka secara dinamis firewall akan memberikan akses ke port yang sudah diblock.

Dengan cara ini, perangkat jaringan seperti Router akan lebih aman, sebab admin jaringan bisa melakukan blocking terhadap port-port yang rentan terhadap serangan seperti Winbox (tcp 8291), SSH (tcp 22), Telnet (tcp 23) atau webfig (tcp 80). Jika dilakukan port scanning port-port tersebut terlihat tertutup. Dari sisi admin jaringan tetap bisa melakukan konfigurasi dan monitoring akan tetapi dengan langkah-langkah khusus (knocking) agar bisa diijinkan oleh firewall untuk akses port Winbox, SSH,dsb.

Dalam contoh setting Simple Port Knocking inilah, akan digunakan dynamic Address-List tersebut.

- Konsep

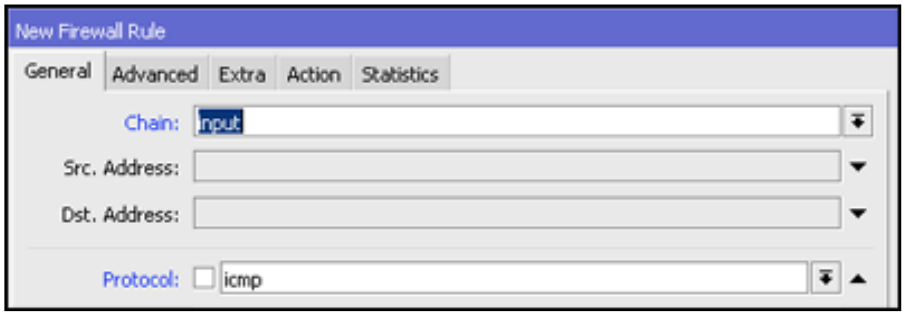
  Contoh kasus port knocking yang akan dibahas kali ini adalah bagaimana host dapat melakukan Winbox (tcp 8291) ke Router hanya jika host tersebut sudah melakukan knock ICMP (ping) terlebih dahulu.

  Cara kerja nya yaitu dengan memasukkan IP Address Host yang mengirimkan paket ICMP (ping) ke Router ke dalam sebuah Address-List

secara otomatis. Setelahnya, hanya IP yang sudah terdaftar pada Address-List yang bisa akses Winbox ke Router.

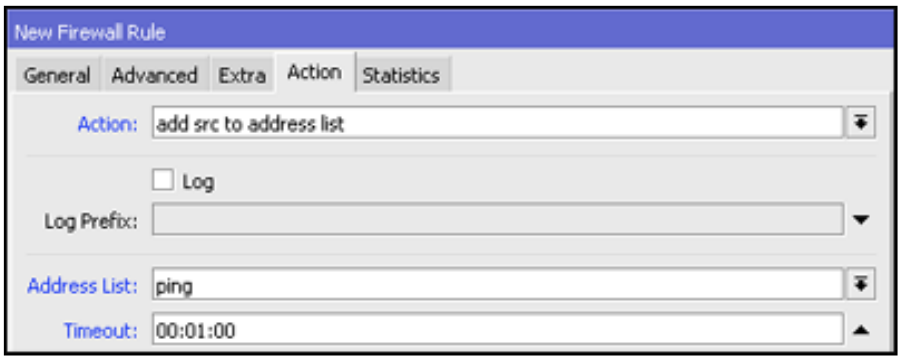
- Konfigurasi

Untuk melakukan grouping IP secara otomatis kita bisa menggunakan fitur Firewall Filter. Pertama, lakukan konfigurasi matcher Firewall. Spesifikan hanya traffic ping (icmp) ke Router yang akan ditangkap



Gambar 1.9 Chain Input

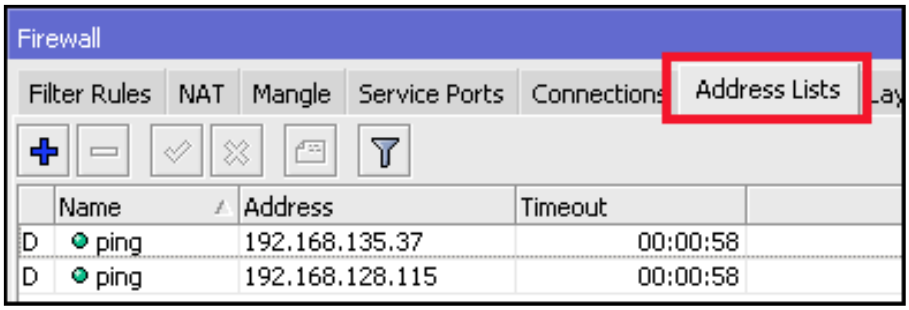
Setelah itu, gunakan action=add-src-to-address-list untuk memasukkan IP Address user yang melakukan ping ke Router ke dalam sebuah group.



Gambar 1.10 Add Address

Nama group dapat didefinisikan pada parameter Address List. Jika menghendaki IP tersebut tidak selamanya ada di dalam daftar group, maka bisa definisikan parameter Timeout.

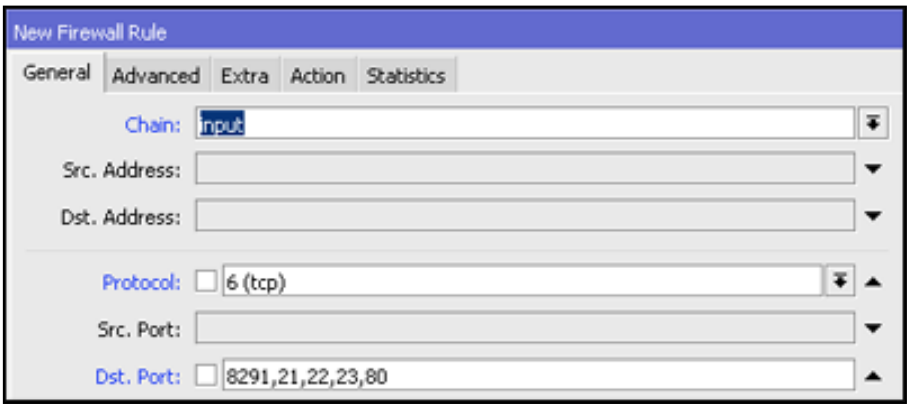
Sampai langkah ini, jika ada host yang melakukan ping ke Router maka ip user tersebut akan dimasukkan ke dalam Address-List dengan nama=ping.



Gambar 1.11 Address List

Perbedaan Address-List yang ditambahkan secara otomatis terletak pada flag "D" di depan nya. Karena sebelumnya TimeOut ditentukan maka IP Address tersebut akan dihapus otomatis dari daftar pada saat TimeOut habis.

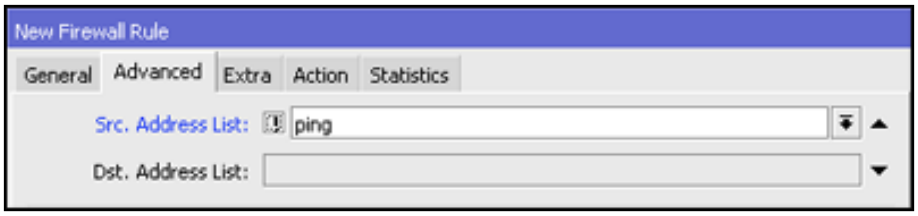
Langkah selanjutnya yang harus dilakukan adalah membuat rule Firewall Filter untuk melakukan blocking akses Winbox ke Router dari sumber (src-address) selain dari IP Address yang sudah masuk dalam Address-List.



Gambar 1.12 Chain Input Dst Port

Tentu saja tidak hanya Winbox saja yang bisa kita definisikan pada matcher, tetapi bisa juga Telnet ,SSH,FTP dan webfig agar lebih aman.

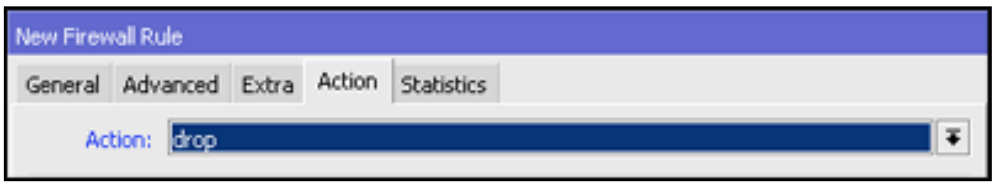
Selanjutnya spesifikan src-address dari paket data yang akan ditangkap. Untuk kasus ini kita bisa menggunakan nama address-list yang sebelumnya ditambahkan secara otomatis.



Gambar 1.13 Sources Address List

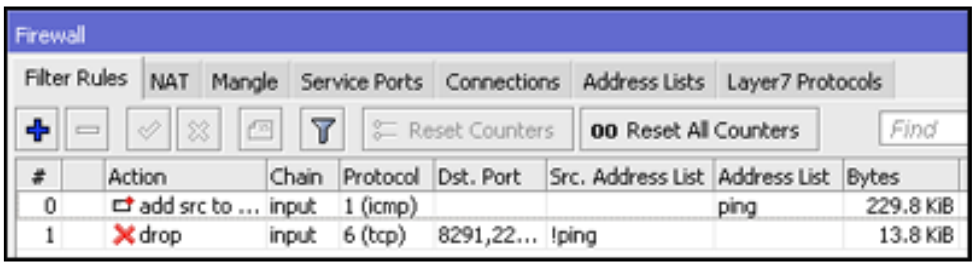
Karena yang akan kita tangkap adalah traffic data dari selain IP yang sudah terdaftar maka kita bisa menggunakan logika NOT (!).

Langkah terakhir adalah penentuan action. Untuk tujuan blocking gunakan action=drop.



Gambar 1.14 Action Drop

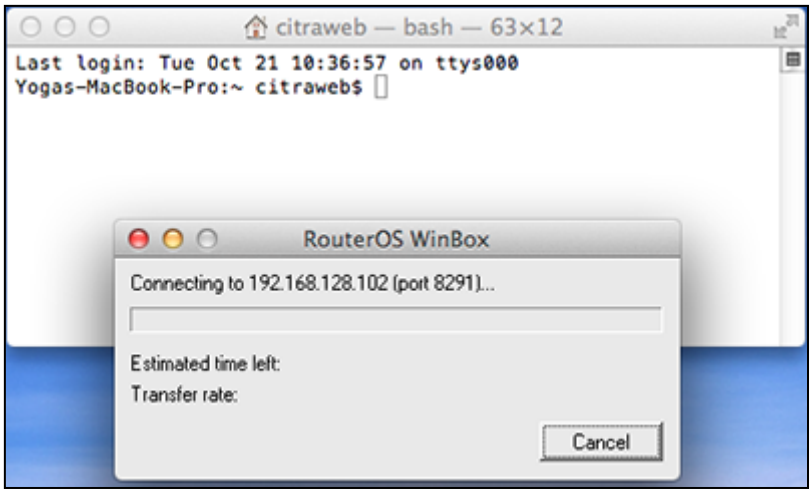
Jika dilihat keseluruhan rule Firewall Filter yang dibuat menjadi seperti berikut



Gambar 1.15 Firewall List

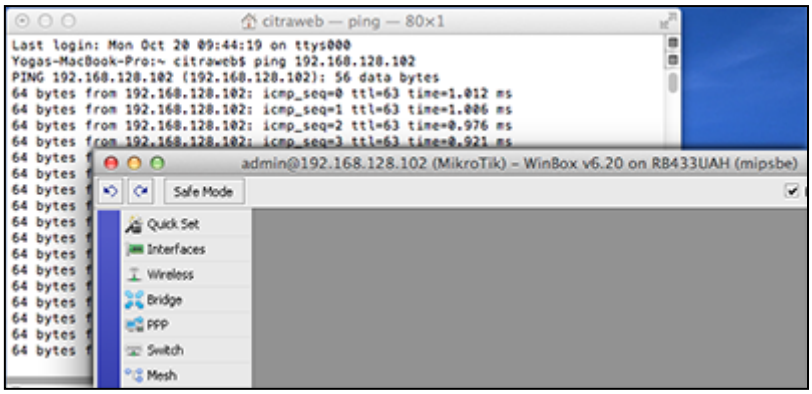
- Pengetesan

Setelah semua langkah selesai, lakukan pengetesan dengan akses winbox ke Router tanpa melakukan ping terlebih dahulu, maka akses akan diblock



Gambar 1.16 Connnecting IP

Akan tetapi jika lakukan ping terlebih dahulu, baru akses winbox ke Router, maka akses winbox akan sukses dilakukan.



Gambar 1.17 Winbox

Port knocking akan berlaku pada semua interface Router, karena tidak ada rule untuk menspesifikan in-interface. Untuk implementasi di lapangan bisa sesuaikan dengan kebutuhan.

1.3.7 Malware Security

Malware (Malicious Software) adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware dapat menginfeksi banyak komputer dengan masuk melalui email, download internet, atau program yang terinfeksi.

Malware bisa menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data / informasi. Hal yang pada umumnya terjadi penyebab malware adalah mendownload software dari tempat ilegal yang disisipan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, adware yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.

Security adalah proses menjaga resiko yang dirasakan, agar berada pada tingkatan yang dapat diterima. Dr. Mitch Kabay, seseorang yang pernah menjadi direktur pendidikan dari International Computer Security Asociation, pada tahun 1998 menulis, "security is a process, not an end state", yang artinya, security adalah sebuah proses, bukan sebuah hasil akhir.

Jadi malware security adalah proses menjaga resiko atau menjaga keamanan suatu komputer dari suatu aplikasi yang dapat merusak sistem komputer. Sudah banyak aplikasi malware security yang sering digunakan khalayak umum, contohnya saja di Indonesia sendiri sudah ada suatu tool anti-malware yang berkualitas untuk melindungi website Anda yaitu Dewaguard. Bagaimana cara kerja Dewaguard? Tool satu ini akan menghilangkan malware yang menginfeksi website Anda secara aman dan memberikan notifikasi secara tanggap bila ada potensi ancaman. Dewaguard juga mampu melakukan backup secara rutin dan otomatis sehingga Anda tak perlu lagi mengkhawatirkan data loss yang mungkin saja terjadi ketika perbaikan dilaksanakan. Bahkan semua spam yang terdapat pada link atau keyword di website Anda akan dibersihkan agar tidak memengaruhi ranking Anda di mesin penelusuran semacam Google.

1.4 PENUTUP

1.4.1 Latihan Soal

1. Jelaskan pengertian firewall?
2. Firewall biasanya diimplementasikan pada gateway. Apa itu gateway?
3. Terdapat jenis-jenis firewall, apa jenis firewall yang paling canggih?
4. Sebutkan fungsi firewall secara umum!
5. Jelaskan singkat cara kerja firewall dalam melakukan control terhadap traffic jarngan kita !
6. Apa fungsi dari firewall filter? Jelaskan!
7. Sebutkan fitur-fitur dari firewall filter!
8. Apa fungsi dari Address List?
9. Sebutkan dan jelaskan chain yang terdapat pada NAT!
10. Mengapa connection tracking merupakan jantung dari firewall?
11. Apa fungsi port scanner? Jelaskan!
12. Sebutkan parameter dari PSD!
13. Apa pengertian DDoS?
14. Sebutkan dan jelaskan langkah konfigurasi pengaman server daro DDoS!
15. Bagaimana cara membuat IP agar statis ?
16. Bagaimana cara pencegahan untuk meminimalisir terinveksi Malware Ransomware Wannacryp?
17. Bagaimana cara Blokir port 139/445 dan 3389?
18. Apa itu malware?
19. Dibagian router terdapat beberapa port, port apa saja yg rentan terhadap serangan?

BAB II
INTRUSION DETECTION AND PREVENTION SYSTEM

2.1 Pengantar IDPS

Keamanan jaringan komputer merupakan hal yang tidak terpisahkan dalam jaringan komputer, kemanan jaringan yang tidak dirancang dengan baik dapat menyebabkan kebocoran data, pelanggaran privasi, hingga kerugian finansial (Ramadhan T, M. Teguh, 2015), keamanan komputer (security) merupakan salah satu kunci yang dapat mempengaruhi tingkat Reliability (termasuk performance dan availability) suatu internetwork (Deris S., A. Hanan, M. Yazid, 2010). Pentingnya nilai sebuah informasi menyebabkan penyajian informasi tersebut dibatasi kepada orang-orang tertentu untuk mengakses informasi yang diinginkan (Arsin, Yamin dan Surimi, 2017).

Intrusion Detection and Prevention System, atau disingkat dengan IDPS ini dapat dibagi dua, yaitu sistem yang menggunakan metode IDS dan IPS (Shah K, Budanis D, Samsul A, 2017). IDS atau Intrusion Detection System adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan (Ariyus, Doni, 2007). IDS digunakan hanya untuk memantau trafik jaringan atau paket data bila terdapat intrusi.

2.2 Intrusion Detection System (IDS)

2.2.1 Pengertian

Intrusion Detection System mempunyai beberapa pengertian yaitu:

a Sistem untuk mendeteksi adanya intrusion yang dilakukan oleh intruder (pengganggu atau penyusup) dalam jaringan. Pada awal serangan, intruder biasanya hanya mengexplore data. Namun, pada tingkat yang lebih serius intruder berusaha untuk mendapat akses ke sistem seperti membaca data rahasia, memodifikasi data tanpa permisi, mengurangi hak akses ke sistem sampai menghentikan sistem.

b Sistem keamanan yang bekerja bersama Firewall untuk mengatasi Intrusion. Intrusion itu sendiri didefinisikan sebagai kegiatan yang bersifat anomaly, incorrect, inappropite yang terjadi di jaringan atau di host tersebut. Intrusion tersebut kemudian akan diubah menjadi rules ke dalam IDS (Intrusion Detection System).

c Sebuah metode pengamanan jaringan dengan melakukan pendeteksian terhadap gangguan – gangguan atau intrusion yang mengganggu.

d Sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

2.2.2 Arsitektur IDS

IDS umumnya berdasar pada arsitektur multi-tier dari:

1. Teknologi deteksi, yang bergantung pada:
    a. Sensor: biasanya disebut engine/probe, merupakan teknologi yang memungkinkan IDS untuk memantau sejumlah besar traffic.
    b. Agents: software yang di install pada suatu PC untuk memantau file atau fungsi tertentu. Dan melakukan pelaporan jika terjadi sesuatu.

c. Collector: seperti agent, tetapi lebih kecil, dan tidak membuat keputusan, tetapi hanya menyampaikan ke manager pusat.

2. Analisis data: Proses analisis data dan data mining sejumlah besar data dilakukan oleh lapisan (layer), kadang diletakkan pada pusat data/server.
3. Manajemen konfigurasi/GUI: Biasa disebut juga console merupakan antarmuka operator dengan IDS

2.2.3 Sifat – sifat IDS

Pada umumnya, IDS mempunyai sifat-sifat sebagai berikut:

a Suitability Aplikasi IDS yang cenderung fokuspada skema manajemen dan arsitektur jaringan yang dihadapkannya.

b Flexibility Aplikasi IDS yang mampu beradaptasi dengan spesifikasi jaringan yang akan dideteksi oleh aplikasi tersebut.

c Protection Aplikasi IDS yang secara ketat memproteksi gangguan yang sifatnya utama dan berbahaya.

d Interoperability Aplikasi IDS yang secara umum mampu beroperasi secara baik dengan perangkat-perangkat keamanan jaringan serta manajemen jaringan lainnya.

e Comprehensiveness Kelengkapan yang dimiliki oleh aplikasi IDS ini mampu melakukan sistem pendeteksian secara menyeluruh seperti pemblokiran semua yang berbentuk Java Applet, memonitor isi dari suatu email.

f Event Management Konsep IDS yang mampu melakukan proses manajemen suatu jaringan serta proses pelaporan pada saat dilakukan setiap pelacakan, bahkan aplikasi ini mampu melakukan updating pada sistem basis data pola suatu gangguan.

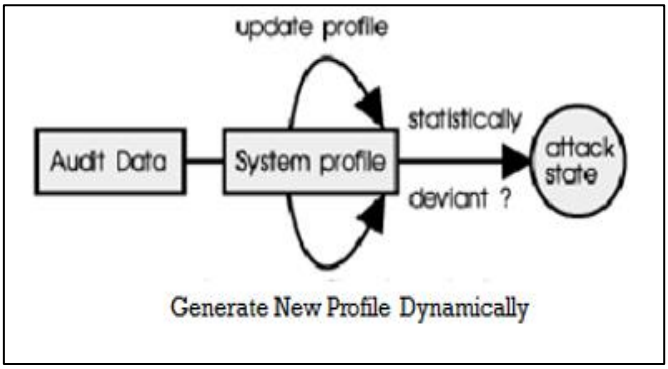
g Active Response Pendeteksi gangguan ini mampu secara cepat untuk mengkonfigurasi saat munculnya suatu gangguan, biasanya aplikasi ini berintegrasi dengan aplikasi lainnya seperti aplikasi Firewall serta aplikasi IDS ini dapat mengkonfigurasi ulang spesifikasi router pada jaringannya.

h Support Lebih bersifat mendukung pada suatu jenis produk apabila diintegrasikan dengan aplikasi lain.

2.2.4 Teknik dalam IDS

Ada beberapa teknik deteksi yang digunakan dalam IDS:

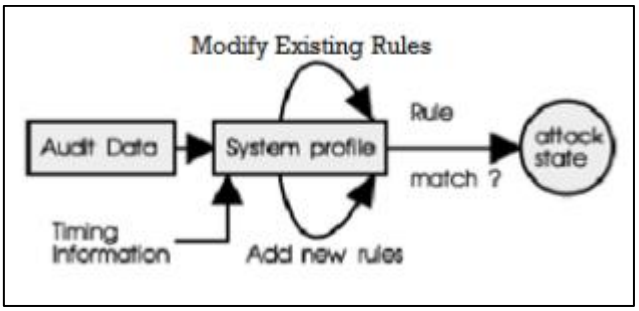
a Teknik Deteksi Anomali (Anomaly Detection/Behavior Based) Behavior Base adalah cara kerja IDS (Intrusion Detection System) dengan mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan – kejanggalan pada sistem, yaitu adanya keanehan dan kejanggalan dari kondisi pada saat sistem normal, sebagai contoh : adanya penggunaan memory yang melonjak secara terus menerus atau terdapatnya koneksi secara paralel dari satu IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi tersebut dianggap kejanggalan yang selanjutnya oleh IDS Anomaly Based ini dianggap sebagai serangan.



Gambar 2.1 Teknik Deteksi Anomali

b Teknik Deteksi Penyalahgunaan (Misuse Detection/ Knowledge Based) Knowledge Based adalah IDS mengenali adanya penyusupan dengan cara

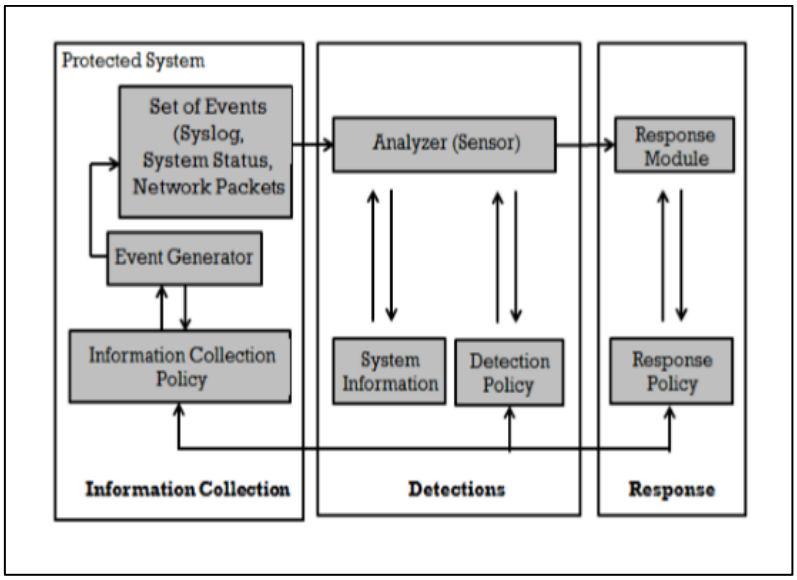
menyadap paket data kemudian membandingkannya dengan database rule pada IDS tersebut. Database rule tersebut dapat berisi signature – signature paket serangan. Jika pattern atau pola paket data tersebut terdapat kesamaan dengan rule pada database rule pada IDS maka paket data tersebut dianggap sebagai serangan.



Gambar 2.2 Teknik Deteksi Penyalahgunaan

2.2.5 Cara kerja IDS

IDS melindungi sistem komputer dengan mendeteksi serangan dan menghentikannya. Awalnya, IDS melakukan pencegahan intrusi. Untuk itu, IDS mengidentifikasi penyebab intrusi dengan cara membandingkan antara event yang dicurigai sebagai intrusi dengan signature yang ada. Saat sebuah intrusi telah terdeteksi, maka IDS akan mengirim sejenis peringatan ke administrator. Langkah selanjutnya dimulai dengan melakukan policy terhadap administrator dan IDS itu sendiri Komponen yang menyusun kerja sebuah IDS bisa dilihat pada diagram



Gambar 2.3 Diagram Kerja IDS

Ada beberapa cara bagaimana IDS bekerja, cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan. Cara lainnya adalah dengan mendeteksi adanya anomali, teknik yang lainnya adalah dengan memantau berkasberkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

2.2.6 Jenis – jenis IDS

IDS dapat dikategorikan sebagai berikut,

a Network-based Intrusion Detection System (NIDS) Memantau Anomali di Jaringan dan mampu mendeteksi seluruh host yang berada dalam satu

jaringan. Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Contoh: melihat adanya network scanning.

b Host-based Intrusion Detection System (HIDS) Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet. Contoh: memonitor logfile, process dan file ownership.

2.2.7 Kelebihan dan Kelemahan IDS

IDS memiliki beberapa kelebihan diantaranya sebagai berikut,

a Memiliki Akurasi keamanan yang baik IDS telah memiliki ketelitian tinggi, yaitu mampu secara realtime mendeteksi dan melakukan blocking terhadap tindakan yang mencurigakan. IDS juga mampu memeriksa dan menganalisa pattern objek secara menyeluruh yang dipergunakan serta membedakan paket data yang keluar masuk dalam lalu lintas jaringan sehingga dapat mengenal benar karakteristik trafic penyerang.

b Mampu Mendeteksi dan Mencegah Serangan. IDS dapat mendeteksi serangan dan juga mampu untuk melakukan pencegahan terhadap serangan tersebut.

c Memiliki cakupan yang Luas dalam Mengenal Proses Attacking. IDS memiliki pengetahuan yang luas, dapat mengenal serangan apa yang belum dikenalnya dan mampu mendeteksi segala sesuatu yang mencurigakan.

Sedangkan kelemahan IDS sendiri adalah,

a Alarm palsu, sering terjadinya alarm ataupun gangguan yang bersifat palsu, yaitu paket data yang datang terdeteksi sebagai intrusion karena tidak sesuai dengan rule–rule yang dibuat. Setelah diteliti ternyata hanya paket data biasa dan tidak berbahaya.

b Variants mengetahui sukses atau tidaknya, sebuah set signature harus cukup unik untuk memberikan peringatan atau alert pada saat yang memang berbahaya. Kesulitannya adalah kode-kode untuk exploit itu dengan mudahnya dimodifikasi oleh penyerangnya, jadi sangat memungkinkan sekali banyak terjadi variasi pada kodenya.

c False positives, merupakan alert yang memberitahu adanya aktifitas yang berpotensi berupa serangan, tetapi masih ada kemungkinan bahwa ternyata aktifitas tersebut bukan sebuah serangan. Kesulitannya adalah apabila jumlah alert banyak dan sulit untuk menyaring mana yang memang benar-benar serangan atau bukan.

2.3 Intrusion Prevention System (IPS)

2.3.1 Pengertian IPS

IPS (Intrusion Prevention System) adalah sebuah perangkat jaringan atau perangkat lunak yang berjalan di belakang firewall untuk mengidentifikasi dan memblokir ancaman terhadap jaringan dengan menilai setiap paket yang melintas berdasarkan protokol jaringan dalam aplikasi dan melakukan pelacakan ancaman terhadap keamanan jaringan. IPS membuat akses kontrol dengan cara melihat konten aplikasi, daripada melihat IP address atau ports yang biasanya digunakan oleh firewall. Sistem IPS sama dengan sistem setup IDS, IPS mampu mencegah serangan yang datang dengan sedikit bantuan dari

administrator atau bahkan tidak sama sekali. Serangan biasanya datang dalam bentuk input data berbahaya ke aplikasi target atau melalui layanan yang digunakan penyerang untuk mengganggu dan menguasai aplikasi atau jaringan target, setelah penyerang atau penyusup berhasil masuk dan menguasai jaringan maka penyerang dapat menonaktifkan jaringan target atau bahkan bisa mengakses semua izin dari aplikasi atau jaringan target. Oleh karena itu IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori dan IPS akan membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga menginterupsi sistem call.

2.3.2 Cara kerja IPS

Intrusion Prevention System dianggap sebagai solusi yang cukup aman dibandingkan dengan Intrusion Detection System kemampuan deteksi ancaman dan pencegahannya yang proaktif. Intrusion Prevention System bekerja dengan bergiliran, yang berisi sensor yang terletak langsung pada network traffic-nya langsung sehingga memeriksa dengan teliti semua network traffic dimana paket data berada. Cara bekerja bergiliran ini memungkinan sensor untuk melakukan pencegahan saat real-time packet inspection berlangsung. Dengan begitu, setiap paket mencurigakan atau berbahaya yang teridentifikasi segera dihapus.

Intrusion Prevention System dapat melakukan tindakan berikut yang mendeteksi aktifitas yang mencurigakan pada jaringan,

a Mengakhiri sesi TCP yang dieksploitasi oleh orang luar pada serangan yang diberikan. tindakan berikut memblokir akun pengguna yang

bersangkutan atau sumber alamat IP yang mencoba mengakses host target, aplikasi, atau sumber daya lainnya secara tidak etis.

b Begitu IPS mendeteksi aktifitas intrusi, IPS juga dapat mengkonfigurasi ulang atau memprogram ulang firewall untuk mencegah serangan serupa di masa mendatang.

c Teknologi IPS juga cukup pintar untuk mengganti atau menghapus konten berbahaya dari serangan yang dilakukan orang luar. Ketika digunakan sebagai proksi, IPS mengatur permintaan yang masuk. Untuk melakukan tindakan ini, IPS mengemas ulang muatan, dan menghapus informasi header yang berisi permintaan masuk. IPS juga memiliki kemampuan untuk menghapus lampiran yang terinfeksi dari email sebelum dikirim ke penerimanya di jaringan internal

2.3.3 Teknik pada IPS

Ada beberapa teknik pada IPS,

a Sniping, memungkinkan IPS untuk menterminasi serangan yang dicurigai melalui penggunaan paket TCP RST atau pesan ICMP Unreachable.

b Shunning, memungkinkan IPS mengkonfigurasi secara otomatis firewall untuk drop traffic berdasar apa yang dideteksi oleh IPS. Untuk kemudian melakukan prevention terhadap koneksi tertentu

2.4 Intrusion Detection and Prevention System (IDPS)

2.4.1 Pengertian IDPS

Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun system keamanan komputer, IPS mengkombinasikan teknik firewall dan metode Intrusion Detection System (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat attack telah teridentifikasi, IPS akan menolak akses (block) dan mencatat (log) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya Firewall yang akan melakukan allow dan block yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan signatures untuk mendeteksi di aktivitas traffic di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (inbound-outbound) dapat di cegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi early detection dan prevention menjadi penekanan pada IPS ini. Tujuan utama dari Intrusion Detection and Prevention System (IDPS) adalah untuk melindungi ketersediaan, kerahasiaan dan integritas sistem informasi kritis dan sistem komputer dengan mengidentifikasi aktivitas berbahaya, intrusi dan serangan dari orang dalam dan orang luar dan untuk berhenti semua kemungkinan insiden - penyalahgunaan sumber daya komputer dan sistem .

2.4.2 Penggunaan Teknologi IDPS

IDPS difokuskan untuk dapat mendeteksi intrusi yang terjadi. Contohnya IDPS dapat mendeteksi ketika penyerang sukses membahayakan sistem dengan cara menyerang kelemahan sistem tersebut. IDPS tersebut kemudian akan

melaporkannya ke Administrator keamanan, dimana Administrator keamanan ini dapat memberi tindakan dengan cepat sehingga dapat meminimalisasi kerusakan akibat intrusi tadi. IDPS juga dapat memotong informasi yang akan di dapatkan oleh penyerang dan dapat mendeteksi kegiatan pengintaian dari luar yang dapat mengindikasikan akan melakukan penyerangan. Contohnya ketika penyerang sedang melakukan pengintaian, IDPS apat membloknya dan melaporkannya ke Administrator keamanan. Kemampuan IDPS antara lain:

a Mengidentifikasi masalah policy keamanan.

b Melaporkan ancaman yang sering muncul.

c Mencegah pelanggaran policy keamanan.

2.4.3 Metode Deteksi

IDPS memiliki 3 metode dalam melakukan deteksi, yakni signatured-based, anomaly-based, dan stateful protocol analysis. Beberapa teknologi IDPS menggunakan ketiga metode tersebut untuk mendapatkan keakuratan dalam pendeteksian, tapi ada juga yang menggunakan sebagian saja.

a. Signatured-Based Detection

Metode ini dilakukan dengan membandingkan signature pada kejadian yang di pantau untuk mengidentifikasi kemungkinan terjadinya intrusi. Metode ini sangat efektif bila mendeteksi ancaman yang sudah di kenal, tetapi sangat tidak efektif ketika ancaman di sini tidak di kenal. Maksud dikenal disini adalah sudah pernah terjadi sebelumnya. Kejadian ini bisa saja terjadi ketika si penyerang mengubah nama intrusinya. Metode ini merupakan metode yang paling simpel, karena hanya membandingkan kegiatan yang sedang terjadi, lalu di daftarkan menggunakan operasi perbandingan. Tetapi kelemahannya adalah metode ini tidak dapat

melacak dan mamahami kejadian yang terjadi pada komunikasi yang lebih kompleks.

b. Anomaly-Based Detection

Metode ini digunakan dengan membandingkan ketentuan pada kegiatan yang di anggap normal dengan kegiatan yang sedang di pantau untuk mendeteksi penyimpangan yang lebih signifikan. Pada metode ini,IDPS memiliki profil yang mewakili perilaku yang normal dari user, host, koneksi jaringan dan aplikasi. Profil tersebut dibangun dengan memonitor karakteristik dari suatu kegiatan dalam selang waktu tertentu. Kelebihan dari metode ini adalah sangat efektif dalam mendeteksi ancaman yang tidak dikenal, contohnya ketika komputer diserang oleh tipe intrupsi yang baru. Sedangkan kekurangan dari metode ini adalah dalam beberapa kasus, akan sulit untuk mendapatkan deteksi yang akurat dalam komunikasi yang lebih kompleks.

c. Stateful Protocol Analysis

Metode ini membandingkan profil yang sudah ada dengan kegiatan yang sedang berlangsung untuk mengidentifikasi penyimpangan. Tidak seperti Anomaly-Based Detection yang menggunakan profil host, Stateful Protocol Analysis menggunakan profil yang lebih luas yang dapat merinci bagaimana sebuah protokol yang istimewa dapat digunakan atau tidak. Arti “Stateful” disini adalah sistem di IDPS ini bisa memahami dan melacak situasi pada protokol network, transport dan application. Kelebihan dari metode ini adalah bisa mengidentifikasi rangkaian perintah yang tidak terduga seperti mengeluarkan perintah yang sama berulang – ulang. Sedangkan kekurangannya adalah kemungkinan terjadinya

bentrokan antara protokol yang digunakan oleh IDPS dengan protokol umum yang digunakan oleh sistem operasi, atau bahasa mudahnya sulit membedakan pengimplementasian client dan server pada interaksi protokol.

2.4.4 Tipe Teknologi IDPS

Ada beberapa tipe dari teknologi IDPS ini dan di bagi menjadi empat jenis berdasarkan kejadian yang dapat di monitor dan dimana mereka di tempatkan, yakni Network-Based, Wireless, Network Behavior Analysis dan Host-Based.

a. Network-Based

Teknologi ini memonitor lalu lintas jaringan dan menganalisisnya untuk mengidentifikasi kegiatan yang mencurigakan, juga dapat mengidentifikasi beberapa jenis kejadian. Network-Based biasanya dibangun di perbatasan antara jaringan, seperti dekat perbatasan firewall atau router, VPN server, remote access server dan wireless network.

b. Wireless

Teknologi ini memonitor lalu lintas jaringan tanpa kabel (wireless) dan menganalisisnya untuk mengidentifikasi kejadian yang mencurigakan yang menyangkut protokol jaringan tersebut. Teknologi ini tidak dapat mengidentifikasi kejadian yang mencurigakan pada lapis yang lebih tinggi pada protokol jaringan (seperti TCP dan UDP). Wireless biasanya dibangun pada jangkauan jaringan wireless, atau dapat juga di bangun di daerah yang tidak memiliki izin tapi ada jaringan wireless.

c. Network Behavior Analysis (NBA)

Teknologi ini memeriksa lalu lintas jaringan untuk mengidentifikasi ancaman yang menghasilkan aliran lalu lintas yang tidak biasa, seperti suatu

bentuk dari intrusi (seperti virus, worm) dan pelanggaran policy (seperti sistem pada client yang menyediakan servis jaringan ke sistem yang lain). NBA biasanya di bangun di tempat yang dapat memonitor suatu aliran pada sebuah jaringan lokal. Tetapi biasanya juga di bangun di daerah yang dapat memonitor aliran antara jaringan internal dan jaringan eksternal.

d. Host-Based

Teknologi ini memonitor karakteristik dari single host dan kegiatan yang berlangsung antara host tersebut dengan kejadian yang mencurigakan. Atau lebih tepatnya ditanam pada sebuah spesifik computer. Contoh karakteristik yang bisa di monitor adalah lalu-lintas jaringan, system logs, running proccess, file access and modification, serta system and aplication configuration changes. Host-Based Biasanya di bangun di dalam host yang kritis seperti publicly accesible server dan server yang memuat informasi yang sensitif.

2.5 PENUTUP

2.5.1 Latihan Soal

1. Apa perbedaan antara IPS dan IDS ?
2. Apa fungsi dari IPS dan IDS ?
3. Sebutkan teknik - teknik yang digunakan pada IPS dan IDS !
4. Jelaskan secara singkat cara kerja dari IPS dan IDS ?
5. Jelaskan secara singkat apa itu IDPS !
6. Sebutkan teknologi yang ada pada IDPS
7. Apa perbedaan host-based dan network-based pada IDS
8. Sebutkan teknik-teknik yang ada pada IPS
9. Tuliskan kelebihan dari IDS

BAB 3
SNIFFING DAN SCANNING NETWORK

3.1 Sniffing and scanning network

Untuk istilah bidang informatika, sniffing adalah pekerjaan menyadap paket data yang ada disebuah jaringan. Paket data ini bisa berisi informasi mengenai apa saja, baik itu username, apa yang dilakukan pengguna melalui jaringan, termasuk mengidentifikasi komputer yang terinfeksi virus sekaligus melihat apa yang membuat komputer menjadi lambat dalam jaringan (Fito, 2011). Bisa juga untuk menganalisa apa yang menyebabkan jaringan macet. Jadi bukan sekedar untuk kejahatan, karena semuanya tergantung penggunanya. Sniffing bisa dilakukan tidak berarti karena masalah komputer atau sistem operasi, tapi sistem dari jaringan sendirilah yang bermasalah. Misalnya pada sistem jaringan yang menggunakan HUB, komputer sebab permintaan data maupun pengiriman data diproses dan dikirimkan ke seluruh komputer dalam jaringan, dan hanya komputer yang membutuhkan saja yang mengambil data yang ditujukan padanya sedangkan komputer lain akan mengacuhkannya. Tetapi semua itu akan berbeda jika salah satu komputer tersebut menggunakan sniffer. Semua data yang disiarkan termasuk ke komputer tersebut akan ditangkap, terlepas dari data tersebut adalah permintaan dari komputer tersebut atau tidak, seperti itulah sifat-sifat jaringan yang menggunakan hub(Akbar Fajrin, 2011). Berbeda dengan Scanning network, yaitu sebuah program atau alat yang mampu mendeteksi kelemahan sebuah komputer dijaringan lokal atau jaringan dengan lokasi lain(Anindhita, 2015).

3.2 Keterkaitan dengan Mata Kuliah

Mata kuliah yang kami ambil adalah mata kuliah Pengamanan Sistem Jaringan dimana pastinya akan membahas tentang dasar-dasar keamanan jaringan, macam-macam teknik penyerangan jaringan, dan yang terakhir tentu saja bagaimana cara untuk mengamankan jaringan dari berbagai macam serangan. Materi yang dibahas dalam buku ini

adalah Sniffing dan Scanning Network yang merupakan salah satu bentuk penyerangan melalui jaringan internet yang bersifat illegal sehingga materi ini termasuk dalam salah satu pokok bahasan dalam perkuliahan.

3.3 Manfaat Bahan Pembelajaran

Tujuan pembuatan makalah ini adalah untuk memenuhi tugas matakuliah Pengamanan Sistem Jaringan, serta untuk memberikan informasi kepada pembaca agar mengetahui lebih lanjut tentang detail pembahasan lengkap mengenai penjelasan *sniffing* dan *scanning*, penyebab dilakukannya *sniffing* yang berguna sebagai bahan analisa terkait jenis-jenis *sniffing* dan cara menghadapinya apabila hal itu membawa dampak negatif bagi perangkat terkait, maupun hal yang akan diperoleh dari *sniffing* bagi jaringan komputer dan sistem operasi yang berjalan di dalam komputer tersebut.

Diharapkan manfaat dari pembahasan yang telah dipaparkan dalam makalah ini dapat menambah pengetahuan lengkap tentang *sniffing* dan *scanning*, sehingga kita tidak hanya bisa mengetahui teori mengenai *sniffing* dan *scanning* tanpa tahu hal terperinci tentang *snifffing* dan *scanning* itu sebenarnya dan tentunya bisa dijadikan bahan referensi pembelajaran.

3.4 Petunjuk Pembelajaran

1. Mencari referensi e-book mengenai *sniffing* dan *scanning network*, majalah/tabloid mengenai komputer dan jaringan edisi online, dan jurnal-jurnal ilmiah mengenai *sniffing* dan *scanning network* untuk mengetahui pengertian dan beberapa hal mengenai *sniffing* dan *scanning network.*

   Misalkan saja pada jurnal thesis berjudul *Network Scanning dan Vulnerability Assessment with Report Generation* oleh Nikita Y Jhala, kami hanya mengambil pada halaman 10-12 untuk referensi dimana pada halaman itu membahas mengenai pengertian dan penjelasan dari *host scanning, port scanner*, Nslookup, dan Traceroute

karena membahas yang berhubungan dengan network scanning dimana hal-hal tersebut merupakan modul dari *Network Security Scanner*.

Jurnal dengan judul *A Review of Port Scanning Techniques*, kami mengambil pada seluruh halaman untuk acuan penulisan.

Pada makalah Tugas Keamanan Komputer dengan judul *Sniffer & Scanning/Port Scanning* yang disusun oleh Ahmad Fauzan dan kawan-kawan, kami mengambil beberapa bagian seperti pada bagaimana cara melakukan pencegahan dari *sniffing*. Begitupun juga pada bagian penjelasan mengenai *scanning*, kami mengambil bebereapa pada bagian yang dimana menjelaskan mengenai pencegahan dari aktifitas *scanning*.

Untuk jurnal dengan judul Analisa Sniffing Paket ICMP Menggunakan Wireshark oleh Inung Bagus Prasetyo, kami hanya mengambil pada halaman 221 dimana menjelaskan mengenai bagaimana cara kerja *sniffing* secara singkat.

2. Memahami tentang *sniffing* dan *scanning network* melalui beberapa contoh yang sudah terjadi dalam kehidupan nyata.

   Contoh kasus *sniffing* yang pernah terjadi yaitu pada tahun 1999 yang dilakukan oleh seorang remaja berusia 16 tahun bernama Joseph Jonathan James kelahian Miami florida yang saaat itu merupakan seorang hacker muda. Dia menginstal backdoor untuk membobol server Badan Pengurangan Ancaman Pertamanan yang merupakan lembaga Departemen Pertahanan. James juga masuk ke computer NASA dan mencuri software senilai $ 1,7 juta.

   Contoh kasus dari port scanning yaitu kasus yang dilakukan oleh seroang mahasiswa sebuah perguruan tinggi di Bandung yang bernama Buy alias Sam dimana apa yang dilakukannya selama setahun menyebabkan beberapa pihak di Jerman merufi sebesar 15.000 DM (sekitar Rp 70 juta). Pelaku melakukan pencurian nomor kartu kredit dan digunakan dalam transaksi jual beli di internet.

3. Memahami bagaimana *sniffing* dan *scanning* dilakukan dan bagaimana cara mencegah agar tidak terkena *sniffing* dan *scanning.*

Salah satu penerapan bagaimana *sniffing* dilakukan akan dibahas pada Bab selanjutnya dimana pada penerapan proses *sniffing* tersebut menggunakan aplikasi *Cain and Abel*. Untuk penerapan *scanning* juga akan dibahas dan dijelaskan pada bab selanjutnya dengan program *Port Scanner*.

Pencegahan yang dapat dilakukan untuk menghindari *sniffing* yaitu dengan cara ketika akan mengirimkan suatu data yang penting bisa dilakukan terlebih dahulu enkripsi data sebelum informasi atau data akan dikirimkan. Hal ini akan menyebabkan data atau informasi yang dikirimkan tersebut tidak dapat secara langsung dikenali dan dibaca oleh *sniffer*. Kita juga tidak boleh asal melakukan aktifitas yang bersifat rahasia misalkan saja yang ada hubunggannya dengan hal-hal pribadi yang privasi seperti email, e-banking, chatting rahasia, dan lain-lainnya pada suatu jaringan komputer yang belum kita kenal.

Dalam melakukan pendeteksian *sniffer* juga dapat dilakukan meskipun susah, salah satunya dengan cara menggunakan beberapa trik yang digunakan untuk mendeteksi *sniffer* berbasis jaringan dan juga berbasis host. Untuk berbasis host dapat menggunakan utilitas kecil untuk mendeteksi jika Lan Card berjalan dalam modus promiscuous pada semua host yang berada di jaringan. Untuk deteksi yang berbasis jaringan bisa dilakukan dengan perangkat lunak *anti-sniffer* yang dijalankan untuk mendeteksi keberadaan paket tanda tangan khusus untuk memeriksa setiap host jaringan untuk kehadiran *sniffer* diketahui. Pencegahan yang dapat dilakukan untuk menghindari *scanning* salah satunya dengan cara memasang sebuah aplikasi bernama PostSentry dimana aplikasi ini unuk mendeteksi adanya port *scanning* dan meresponds secara aktif jika ada port *scanning*. Cara kerja aplikasi ini yaitu dengan melakukan pemblokiran terhadap mesin penyerang.

3.5 Sniffing Networks

Sniffing adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer. Contohnya, User adalah pemakai komputer yang terhubung dengan suatu jaringan lokal dikampus. Saat user mengirimkan email ke teman yang berada di luar kota, email tersebut akan dikirimkan dari komputer user melewati gateway internet pada jaringan lokal kampus, kemudian dari jaringan lokal kampus diteruskan ke jaringan internet. Lalu masuk ke inbox email. Pada jaringan lokal kampus dapat terjadi aktifitas sniffing yang dapat dilakukan baik administrator jaringan yang mengendalikan server atau oleh pemakai komputer lain yang terhubung pada jaringan lokal kampus.. Dengan aktifitas sniffing, email user dapat ditangkap/dicapture sehingga isinya bisa dibaca oleh orang yang melakukan Sniffing. Bukan hanya email, tetapi seluruh aktifitas yang melalui jaringan lokal TCP/IP.

Aktivitas menyadap atau sniffing ini bisa dibagi menjadi 2 (dua) yaitu sniffing pasif dan sniffing aktif. Sniffing pasif melakukan penyadapan tanpa mengubah data atau paket apapun di jaringan, sedangkan sniffing aktif melakukan tindakan-tindakan atau perubahan paket data di jaringan. Sniffing pasif dapat ditanggulangi dengan cara menggunakan switch (S'to, 2007). Melihat kondisi saat ini bahwa harga switch hampir sama dengan hub, maka seiring waktu jaringan komputer akan beralih menggunakan switch sebagai penghubung antar komputer. Namun ada satu hal yang berbahaya, yaitu sniffing aktif. Sniffing aktif adalah metode sniffing dalam jaringan yang lebih canggih dari sniffing pasif. Sniffing aktif ini pada dasarnya memodifikasi Address Resolution Protocol (ARP) cache sehingga membelokkan data dari komputer korban ke komputer hacker. ARP adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address).

ARP didefinisikan di dalam RFC 826. Dua jenis sniffing ini sangat merugikan jika terjadi di dalam jaringan karena bisa saja data-data pribadi kita atau account-account

pribadi kita semacam e-mail yang bersifat sensitif dapat tercuri. Sniffing sendiri merupakan suatu tindakan yang sangat sulit untuk di cegah. Tidak ada solusi yang mudah, cepat, dan aman, yang bisa kita lakukan untuk mencecegah serangan semacam ini. Namun tentunya, kita bisa meminimalisir kerugian yang mungkin terjadi di kemudian hari. Hal yang paling cepat di gunakan dan tidak memakan biaya besar adalah penggunaan enkripsi sehingga data-data yang lalu lalang di dalam jaringan kita sangat sulit untuk di baca.

3.6 Network Scanning

Scanning adalah suatu prosedur yang dilakukan untuk mengidentifikasi hosts, ports, dan services pada network. Scanning networks bisa juga dikatakan sebagai Network Security Scanner, adalah bundel utilitas jaringan yang lengkap yang menggabungkan beragam alat untuk pemantauan jaringan, keamanan jaringan audit, audit kerentanan dan banyak lagi. Scanning networks sangat penting untuk mengumpulkan informasi tentang keadaan sebenarnya dari sistem komputer atau jaringan. Scanning networks dapat menghasilkan anomali lalu lintas jika pemindai menargetkan seluruh rentang alamat IP saat mencari host dan layanan yang rentan.

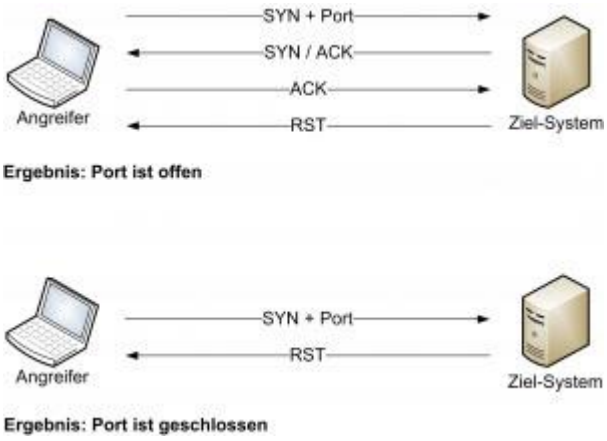
3.6.1 Tipe-tipe Network Scanning

a. Port scanning : serangkaian pesan yang dikirimkan pada sebuah computer untuk mempelajari service pada jaringan komputer.
b. Vulnerability scanning : proses yang terjadi secara ototmatis ketika mengidentifikasi kelemahan sistem computer pada sebuah jaringan.
c. Network scanning : sebuah prosedur untuk mengidentifikasi host mana yang sedanga aktif dalam sebuah jaringan.

3.6.2 Jenis Jenis Network Scanning

a. Connect scan (-sT)

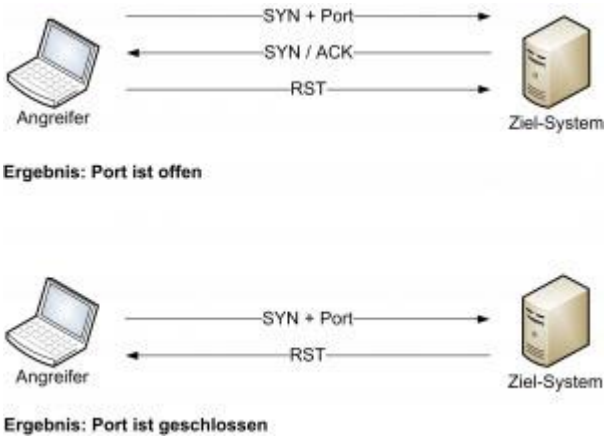
Jenis scan ini connect ke port sasaran dan menyelesaikan three-way handshake (SYN, SYN/ACK, dan ACK). Scan ini mudah terdeteksi oleh sistem sasaran.



Gambar 3.1 Jenis Connect scan (-sT)

b. TCP SYN Scan (-sS)

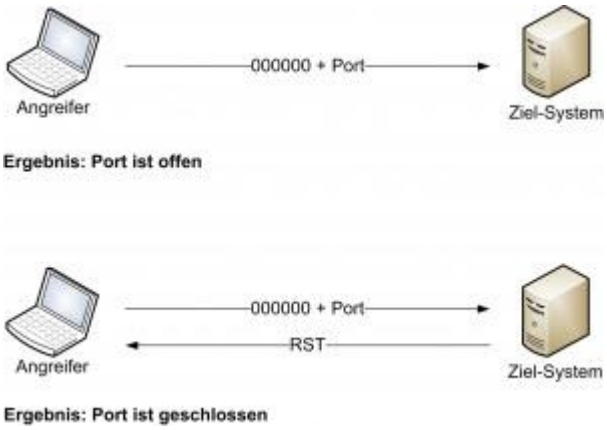
TCP SYN Scan merupakan scan default nmap. SYN scan juga sulit terdeteksi karena tidak menggunakan 3 *way handshke* secara lengkap, yang disebut dengan teknik *Half Open Scanning*. SYN scan juga efektif karena dapat membedakan 3 state port yaitu *open, filterd* ataupun *close*. Teknik ini dikenal sebagai *half open scanning* karena suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya suatu paket SYN dikirimkan ke port sasaran. Jika SYN/ACK diterima port sasaran maka dapat mengambil kesimpulan bahwa port itu berada dalam status LISTENING. Suatu RST/ACT akan dikirim oleh mesin yang melakukan *scanning* sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat tidak terlihat dibandingkan TCP connect penuh, dan tidak tercatat pada log sistem sasaran.



Gambar 3.2 Jenis TCP SYN Scan (-sS)

c. TCP Xmas Tree Scan (-sX)

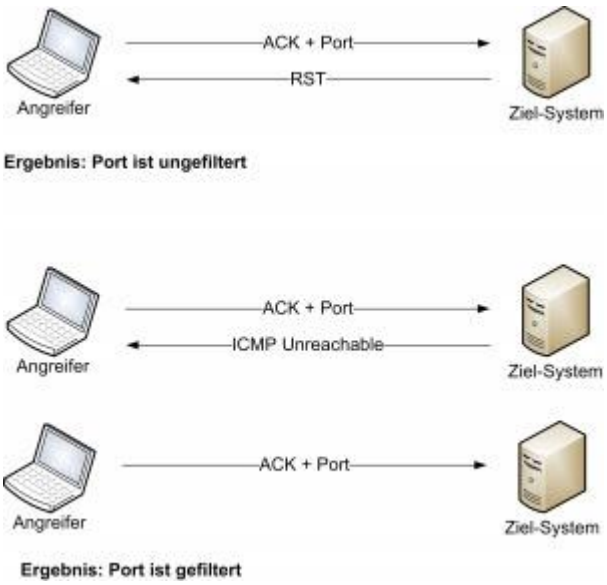
Teknik ini mematikan semua flag. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk semua port yang tertutup.



Gambar 3.3 Jenis TCP Xmas Tree Scan (-sX)

d. TCP ACK scan (-sA)

Teknik ini digunakan untuk memetakan set aturan firewall. Dapat membantu menentukan apakah firewall itu merupakan suatu simple packet filter yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan bit set ACK) atau suatu firewall yang menjalankan advance packet filtering.



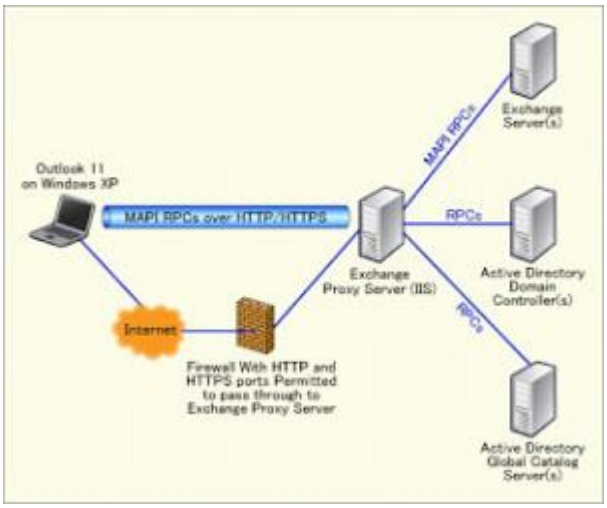
Gambar 3.4 Jenis TCP ACK scan (-sA)

e. TCP Windows Scan (-sW)

Teknik ini dapat mendeteksi port-port terbuka maupun terfilter atau tidak pada sistem-sistem tertentu (sebagai contoh : AIX dan FreeBSD) sehubungan dengan anomali dari ukuran windows TCP yang dilaporkan.

f. TCP RPC Scan (-sR)

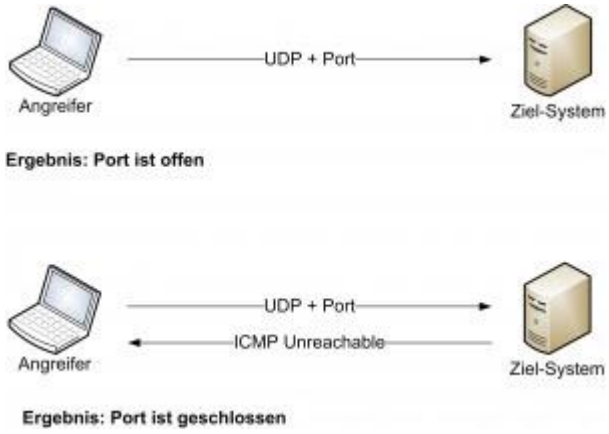
Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC (Remote Procedure Call) dan program serta nomor versi yang berhubungan dengannya.



Gambar 3.5 Jenis TCP RPC Scan (-sR)

g. UDP Scan (-sU)

Teknik ini mengirimkan suatu paket UDP ke port sasaran. Bila port sasaran memberikan respon berupa pesan (ICMP port unreachable) artinya port ini tertutup. Sebaliknya bila tidak menerima pesan, dapat disimpulkan bahwa port itu terbuka. Karena UDP dikenal sebagai *connectionless protocol*, akursai teknik ini sangat bergantung pada banyak hal sehubungan dengan penggunaan jaringan dan sistem *resource.*



Gambar 3.6 Jenis UDP Scan (-sU)

3.6.3 Metode Teknik Network Scanning

a. Random Scanning

Dalam metode ini, penyerang memindai jaringan secara terus menerus untuk mengetahui host dan layanan yang rentan. Namun, ia tidak mengetahui IP mana yang aktif atau layanan apa yang berjalan pada setiap host yang berjalan. Di sisi lain, penargetan host atau layanan yang tidak aktif akan sering menghasilkan pesan kegagalan koneksi. Jadi kegagalan koneksi yang sering dihasilkan oleh pemindaian jaringan mungkin menunjukkan keberadaan worm jaringan jika sedang dianalisis dengan benar (de Vivo, et al., 1999; Northcutt & Novak, 2002). Kegagalan koneksi dapat terjadi karena hal berikut:

1. Worm jaringan mencoba memindai beberapa layanan tetapi port ditutup; dalam hal ini port ICMP tidak dapat dijangkau atau paket TCP-Rest akan dihasilkan.

2. Worm mencoba memindai host yang tidak aktif; dalam hal ini host ICMP juga tidak dapat dijangkau dan sebuah paket akan dihasilkan.

b. Sequential Scanning

Dalam metode ini, penyerang bertujuan untuk memindai blok / kisaran alamat IP secara berurutan. Setelah worm secara acak memilih IP awal, pemindai akan terus memindai s + 1 atau s-1 (G. Gu et al., 2007). Sequential Scanning dapat dengan mudah dilihat oleh alat penghirup lalu lintas apa pun seperti Wireshark. Ini karena IP yang diambil yang sedang melakukan pemindaian berurutan terdaftar secara berurutan.

c. Hit List Scanning

Dalam metode ini, penyerang mendefinisikan daftar host dan layanan yang rentan untuk dipindai setelah worm dilepaskan. Daftar ini dapat dihasilkan dengan secara diam-diam memonitor jaringan atau dari tempat lain. Keakuratan metode ini tinggi karena penyerang memiliki pengetahuan sebelumnya tentang target dan layanan. Karena akurasinya yang tinggi, probabilitas perilaku anomali yang mungkin muncul sangat rendah, sehingga sulit bagi sistem deteksi anomali untuk mendeteksi pemindaian semacam itu.

d. Topological Scanning

Dalam metode ini, worm berdasarkan informasi lokal disimpan ke host. Informasi lokal mencakup alamat email dalam daftar kontak pengguna, file host (mis., / Etc / hosts) dan URL dalam riwayat penelusuran pengguna. Penyerang akan menggunakan informasi ini untuk mengidentifikasi target dan jalur infeksi dengan menggunakan saluran kedua seperti layanan yang disediakan oleh Google atau dengan menanyakan jaringan peer-to-peer atau server pesan instan untuk rekan-rekan yang rentan. Topologi worms dapat menyebar dengan sangat cepat, terutama

pada jaringan dengan aplikasi yang sangat terhubung (Weaver, Paxson, Staniford, & Cunningham, 2003).

e. Passive scanning

Dalam metode ini, informasi tentang host dan layanan yang rentan diperoleh dengan memonitor jaringan target secara pasif (Kato, Nitou, Ohta, Mansfield, & Nemoto, 1999). Bentuk pemindaian ini jauh lebih lambat daripada teknik-teknik sebelumnya tetapi bisa lebih sulit untuk dideteksi oleh *Intrusion Detection Systems* (IDS) karena tampaknya tidak menunjukkan perilaku anomali.

3.7 Contoh Penerapan

3.7.1 Penerapan Scanning Network

Server memiliki tugas untuk melayani *client* dengan menyediakan *service* yang dibutuhkan dengan bermacam-macam kemampuan, baik untuk lokal maupun remote. *Server listening* pada suatu *port* dan menunggu *incomming connection* ke *port*. Koneksi bisa berupa lokal maupuan remote.

Port adalah suatu alamat pada stack jaringan kernel, sebagai cara dimana transport layer mengelola koneksi dan melakukan pertukaran data antar komputer. *Port* yang terbuka mempunyai resiko terhadap serangan dari luar.

Aplikasi layanan sendiri mungkin mempunyai beberapa kelemahan seperti kesalahan pemrograman, penggunaan autentikasi/password yang lemah, *sensitive* data tidak terenkripsi atau mengijinkan koneksi dari berbagai alamat IP dan lain sebagainya. Kelemahan-kelemahan tersebut memungkinkan host yang menyediakan layanan tersebut rentan terhadap serangan. Oleh karena itu sebaiknya host hanya menyediakan layanan yang diperlukan saja, atau dengan kata lain meminimalkan *port* yang terbuka untuk mengurangi resiko tersebut.

Salah satu jenis serangan seperti yang telah dipaparkan dalam penjelasan di awal yakni *network scanning*. *Network scanning* merupakan salah satu bentuk aktivitas yang dilakukan oleh seseorang atau sekelompok orang terhadap IP/Network suatu jaringan komputer dengan tujuan untuk mendapatkan data informasi sebanyak-banyaknya dari komputer target sasaran *network scanning*. *Network scanning* digunakan untuk melakukan *scanning* pada mesin jaringan, baik itu untuk mendapatkan IP, *Port*, *Packet data* yang keluar masuk melalui jaringan, termasuk merekam aktivitas browsing, yang tentunya terdapat *username* dan *password*.

Cara kerja *Network Scanner*:

- Untuk mendapatkan akses ke *host*, *cracker* harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila *cracker* sudah mengetahui bahwa *host* menjalankan proses ftp *server*, ia dapat menggunakan kelemahan-kelemahan yang ada pada ftp *server* untuk mendapatkan akses.
- Biasanya "*scanning*" dijalankan secara otomatis mengingat "*scanning*" pada "*multiple-host*" sangat menyita waktu. "*Hackers*" biasanya mengumpulkan informasi dari hasil "*scanning*" ini. Dengan mengumpulkan informasi yang dibutuhkan maka "*hackers*" dapat menyiapkan serangan yang akan dilancarkannya.
- *Scanner* biasanya bekerja dengan men-scan port TCP /IP dan servis-servisnya dan mencatat respon dari komputer target. Dari *scanner* ini dapat diperoleh informasi mengenai *port-port* mana saja yang terbuka. Kemudian yang dilakukan adalah mencari tahu kelemahan-kelemahan yang mungkin bisa dimanfaatkan berdasar *port* yang terbuka dan aplikasi serta versi aplikasi yang digunakan.

Aplikasi *Network Scanner*

Ada beberapa *utility* yang bisa dipakai untuk melakukan diagnosa terhadap sistem *service* dan *port*. *Utility* ini melakukan *scanning* terhadap sistem untuk mencari

port mana saja yang terbuka, ada juga sekaligus memberikan laporan kelemahan sistem jika *port* ini terbuka.

Port Scanner merupakan program yang didesain untuk menemukan layanan (*service*) apa saja yang dijalankan pada *host* jaringan.

Cara kerjanya adalah para *hackers* biasanya menggunakan sebuah program yang secara otomatis akan mendeteksi kelemahan sistem keamanan sebuah jaringan komputer, misal *port-port* yang sedang aktif yang dapat dijadikan sebagai pintu masuk bagi *hacker* untuk melakukan aksinya. Kegiatan *Scanning* ini lebih bersifat aktif terhadap sistem-sistem sasaran. Di sini diibaratkan *hacker* sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya.

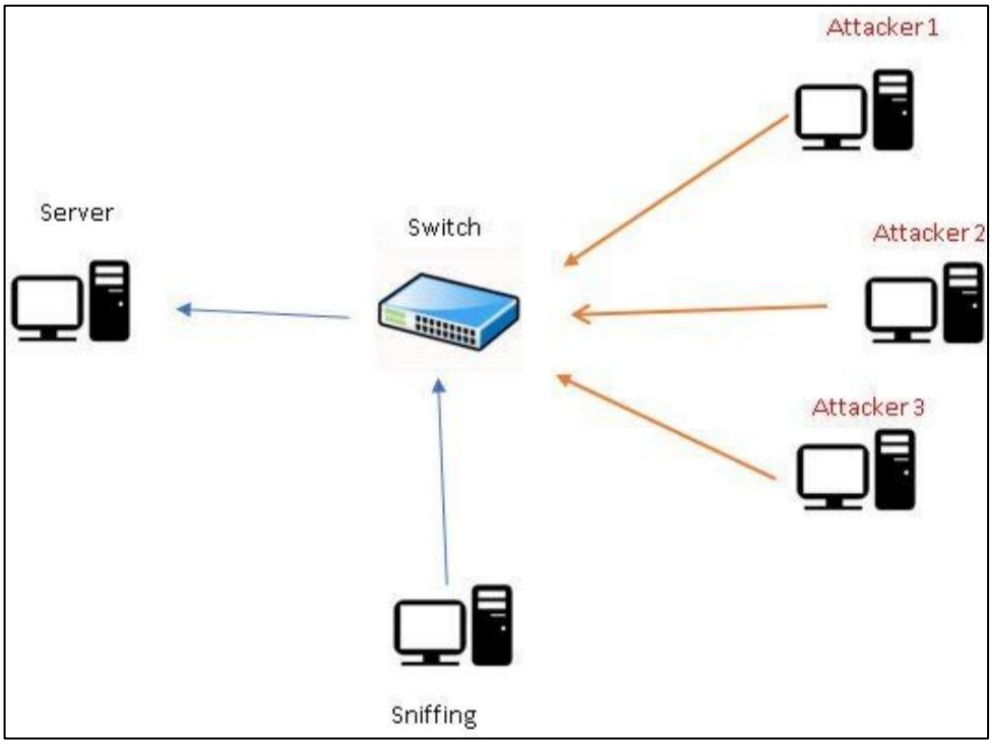
Dari bagian ini dapat diambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi.

Penelitian terkait penerapan pendeteksi serangan *port scanning* yang menggunakan algoritma *Naive Bayes* pernah digunakan oleh Julius Chandra, dkk. pada tahun 2017 dengan judul 'Deteksi Serangan *Port Scanning* Menggunakan Algoritma *Naive Bayes*' Program Studi Teknik Informatika, STMIK GI MDP, Palembang. Penelitian tersebut didasarkan pada sebuah permasalahan serangan *Port Scanning* yang dapat menjadi masalah untuk kedepannya bagi jaringan jika tidak diatasi karena dapat merusak sistem dengan melakukan serangan lanjutan.

Terdapat dua tipe serangan *port scanning* yaitu non *stealth scan* dan *stealth scan*. Peneliti mengklasifikasi serangan *stealth scan* berdasarkan tiga jenis yaitu FIN *scan,* NULL *scan* dan XMAS *scan*. Untuk mengenali ciri dari serangan tersebut dibutuhkan klasifikasi dari pola serangan dari tiga jenis tersebut. Peneliti

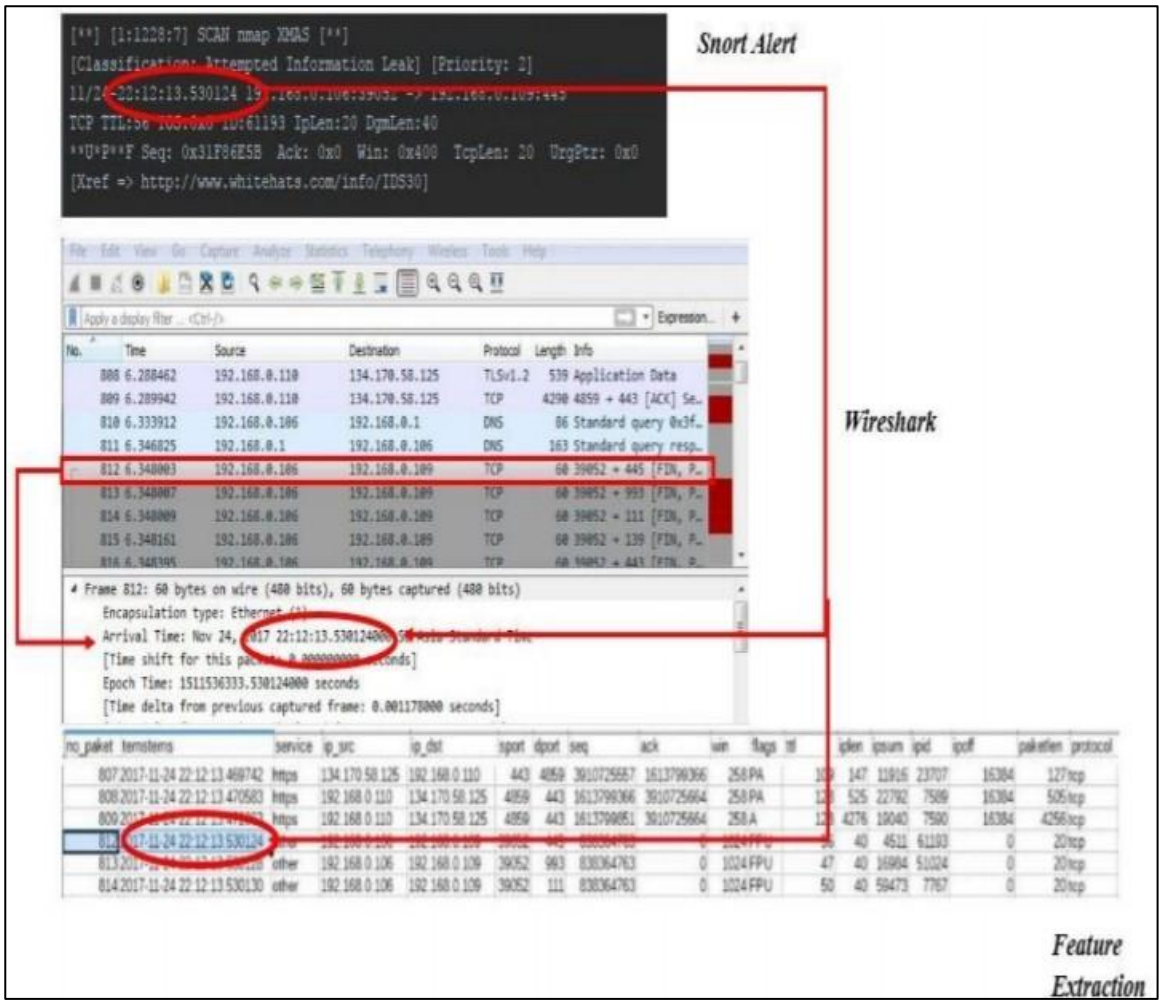
menggunakan algoritma *naive bayes* untuk mengklasifikasikan ketiga jenis tersebut berdasarkan pola serangan.

Dataset yang digunakan pada penelitian adalah paket-paket dari tiga jenis serangan *stealth scan* dari *port scanning* yaitu *fin scan*, *null scan* dan *xmas scan*. Paket-paket tersebut sebelumnya ditangkap terlebih dahulu melalui proses *sniffing*, topologi untuk skenario pengumpulan *dataset* dapat dilihat pada **Gambar ..**



Gambar 3.7. Topologi Skenario Pengumpulan *Dataset*

Dalam penelitian tersebut, peneliti menggunakan *dataset* yang akan diubah *file* nya melalui proses *feature extraction*. Tujuan dari *feature extraction* untuk mengubah file .pcap menjadi .csv, yang berguna untuk mempermudah dalam mengenali pola dari serangan *stealth scan*. Setelah dilakukan *feature extraction* pada paket .pcap yang didapat, *file* yang menjadi .csv tersebut dianalisis untuk dicari pola dari paket. Pencarian paket yang berupa serangan, dengan cara memvalidasi serangan dari *alert snort* adalah melihat waktu yang sama pada *alert* dan hasil *capture*.



Gambar 3.8. Proses Validasi Serangan

Setelah didapat pola serangan dari informasi paket yang berasal dari tcp *header* dan ip *header*, pola tersebut diamati dan dicari nilai probabilitasnya. Setelah didapat nilai probabilitasnya sistem IDS dirancang menggunakan bahasa *python* dan mengimplementasikan algoritma *naive* bayes. Hasil penelitian deteksi dan pengklasifikasian berdasarkan jenis serangan dengan rata-rata akurasi FIN *scan* 99.04%, NULL scan 98.94%, XMAS *scan* 99.13% dan *all out attack* sebesar 99.10%.

	FIN Scan	*NULL Scan*	*XMAS Scan*	*All Out Attack*
Pengujian 1	98.82%	98.59%	98.70%	99.32%
Pengujian 2	98.81%	98.81%	99.93%	99.17%
Pengujian 3	99.12%	98.93%	98.92%	99.10%
Pengujian 4	99.33%	99.14%	98.64%	99.16%
Pengujian 5	99.51%	99.00%	98.98%	99.22%
Pengujian 6	98.95%	99.08%	99.96%	99.18%
Pengujian 7	98.79%	99.06%	99.07%	98.79%
Pengujian 8	99.10%	98.61%	99.09%	99.28%
Pengujian 9	99.12%	99.04%	99.05%	99.19%
Pengujian 10	98.89%	99.23%	98.98%	98.99%

Gambar 3.9. Tabel Hasil Keseluruhan Akurasi Tiap Serangan

3.7.2 Penerapan Sniffing

Ada beberapa tools yang bisa digunakan untuk melakukan proses sniffing, salah satunya adalah aplikasi *Cain and Abel*. Berikut adalah contoh sniffing password wifi dengan aplikasi *Cain and Abel* terhadap salah satu Universitas di Semarang.

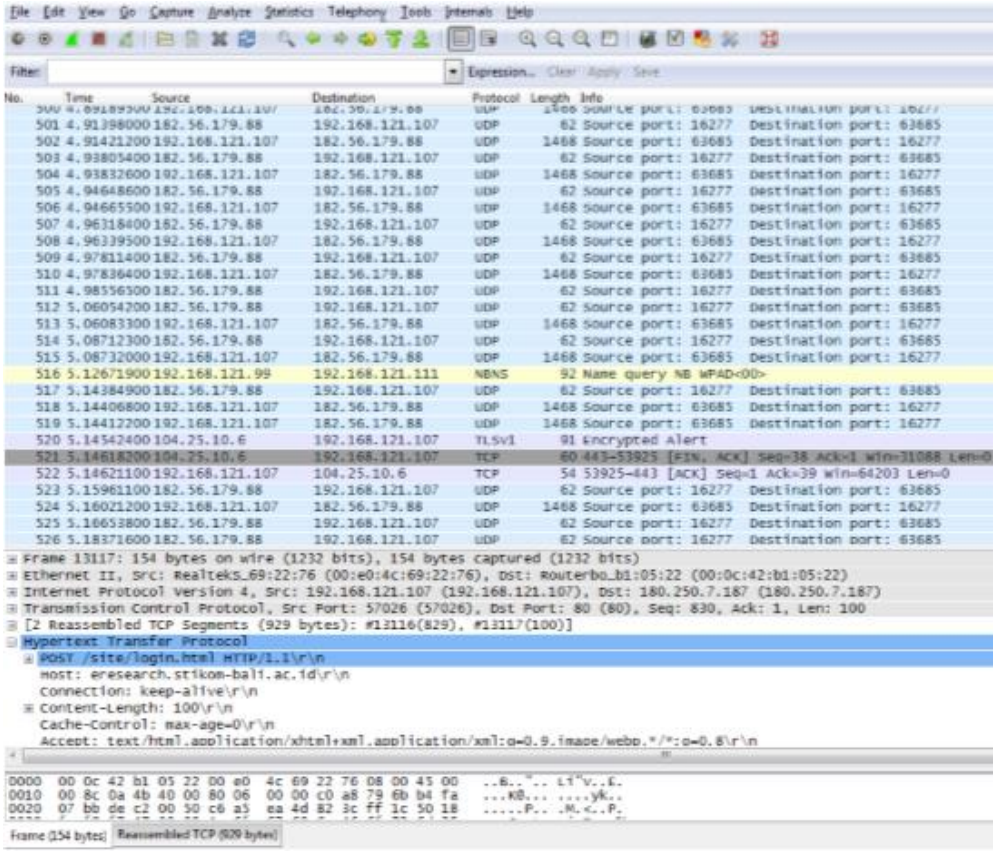
1. Install aplikasi *Cain and Abel*.
2. Setelah diinstall, buka aplikasi Cain and Abel maka akan muncul tampilan seperti dibawah ini.
3. Lalu pilih dan Klik Start/Stop Sniffer.
4. Klik kanan pada Scan Mac Address seperti gambar dibawah ini:
5. Setelah itu klik APR .
6. Dibawah ini sedang melakukan proses sniffing dapat dilihat beberapa terdeteksi sedang membuka website diantaranya facebook,instagram,google dan yahoo.
7. Klik start/stop APR,pastikan status di bawah berwarna hijau (full routing) hal ini memungkinkan untuk proses sniffing berhasil.
8. Berikut hasil sniffing yang didapatkan

Contoh aplikasi lainnya adalah Wireshark. Berikut akan dijelaskan mengenai bussiness impact analysis menggunakan teknik sniffing. Proses paket sniffing dimulai dengan menjalankan proses capture packet di perangkat jaringan. Dengan memilih interface card yang akan digunakan untuk memonitoring traffic.

Gambar 3.10. Tampilan Wireshark

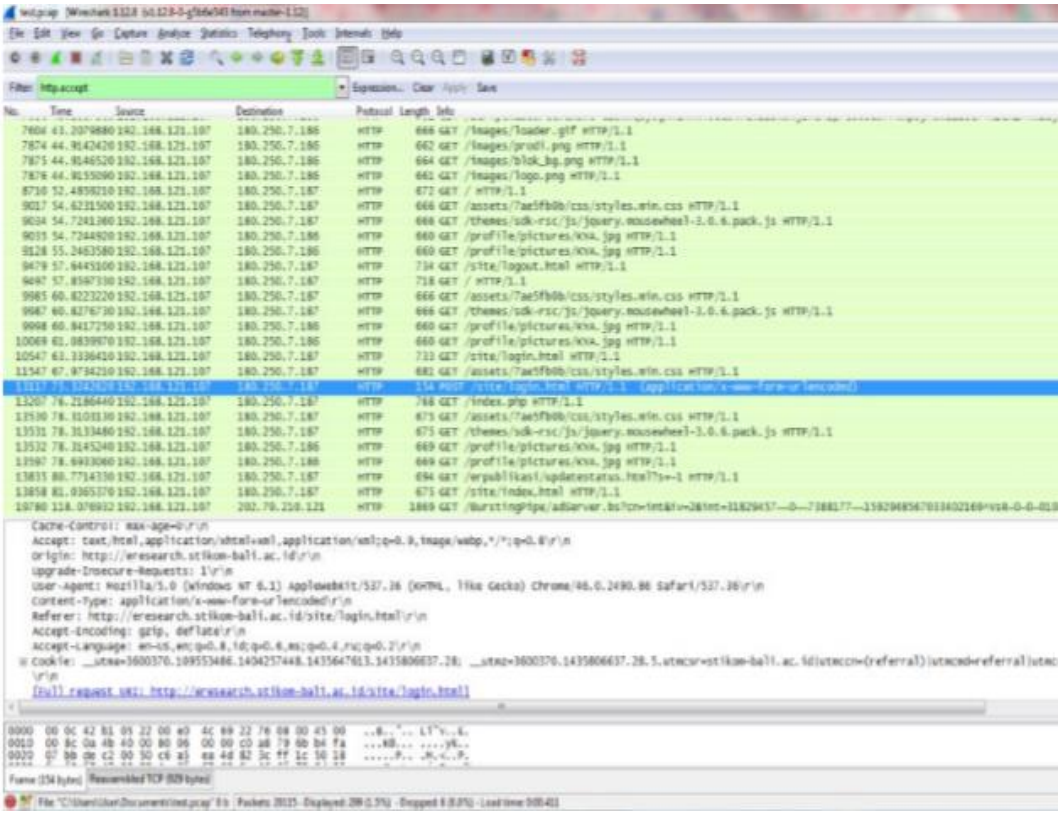
Proses pemilihan interface memperlihatkan perangkat kartu jaringan mana yang akan dijadikan sebagai media untuk memonitoring jaringan. Dalam proses percobaan ini terdapat dua kartu jaringan yang digunakan untuk melaukan proses capture traffic.

Selanjutnya dilakukan proses untuk melakukan sniffing pada jaringan lokal. Proses sniffing dilakukan selama 1 jam di dalam jaringan lokal. Semua data yang lewat akan ditangkap oleh wireshark dan akan diolah dengan menggunakan fasilitas filter. Dalam proses sniffing yang terlihat pada gambar di bawah selama satu jam didapatkan ribuan paket yang melewati jaringan lokal area network dan berbagai protokol seperti, TCP, UDP, ICMP, dan protokol yang lainnya. Dapat dilihat pada gambar traffic banyak menuju ke jaringan luar ataupun menuju ke jaringan internal. Paket yang dapat diambil atau di tangkap oleh wireshark berupa no, source ip address, destination IP address, protocol, panjang paket, dan yang terakhir info dari paket yang berhasil ditangkap.

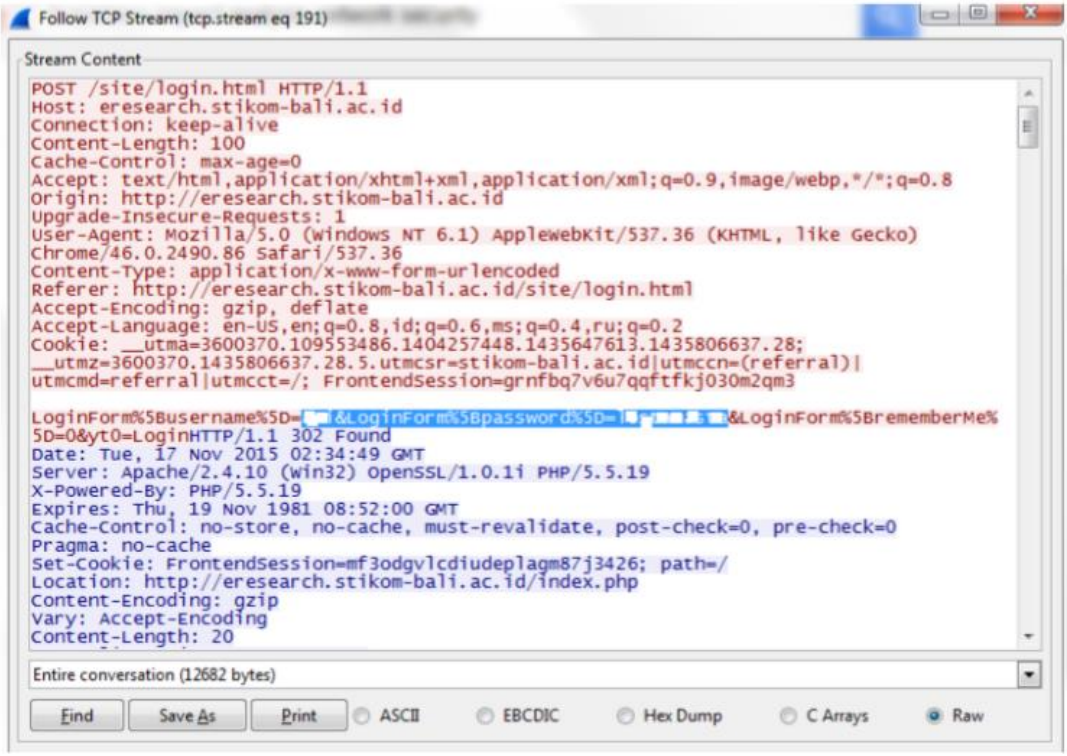


Gambar 3.11. Sniffing menggunakan Wireshark

Dari proses sniffing didapatkan ribuan paket yang melintasi layer 2 dari jaringan lokal area network sehingga dibutuhkan teknik filtering utuk mengetahui kerentanan yang ada di jaringan yang digunakan. Penggunaan filter di wireshark menunjukkan salah satu filter untuk mengetahui kualitas jaringan. Beberapa filter yang digunakan adalah tujuannya untuk mengetahui resiko dari komunikasi yang menggunakan protokol HTTP. Dalam proses komunikasi di internet protocol ini adalah protokol yang sangat sering memiliki resiko yang besar, disamping protokol yang lain seperti TCP dan UDP.

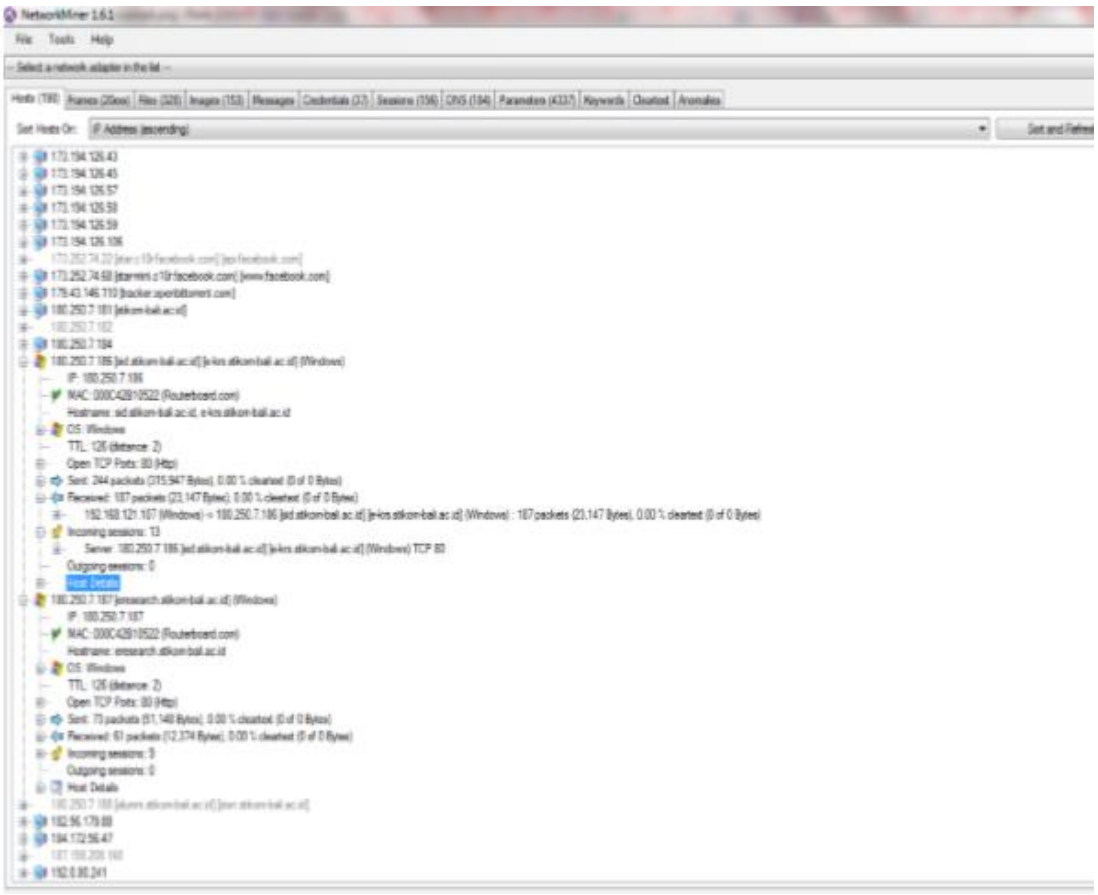


Gambar 3.12. Penggunaan filter di Wireshark



Gambar 3.13. Hasil penerapan filter

Salah satu hasil yang tampak dari penerapan filter dapat dilihat pada gambar diatas. Hasil dari penerapan filter. Traffic yang menggunakan protokol HTTP memiliki resiko terhadap bocornya data username dan password dari pengguna sehingga dapat menimbulkan dampak terhadap institusi jika sampai data account tersebut disalah gunakan oleh pihak yang tidak bertanggung jawab.



Gambar 3.14. Mining IP Address jaringan Local Area Network

Proses selanjutnya setelah resiko dan dampak sudah mulai terlihat adalah melakukan proses pengumpulan IP address yang melakukan transaksi. Dengan menggunakan aplikasi network miner maka akan terkumpul IP address berapa saja yang sedang melakukan komunikasi pada saat proses sniffing dan mengetahui bagaimana pola komunikasinya. Setelah mendapatkan IP adress yang berkomunikasi, proses selanjutnya adalah memperhitungkan bussiness impact analysis berdasarkan kerentanan yang didapat dengan menggunakan perhitungan Commond Vulnerability Scoring System (CVSS) Version 2 untuk mengukur tingkat dampak dari manajemen jaringan yang diterapkan. Dilihat pada gambar 7. Banyak IP address yang terlihat pada aplikasi network miner, namun dalam penelitian ini hanya mengambil ip address yang memiliki nilai High, Medium, dan low dalam proses komunikasi data. Didapatkan hasil bussiness impact analysis sebagai berikut :

NO	*IP Adress*	AV	AC	Au	C	I	A	IS	ES	SC	LEVEL	PROTOKOL
1	192.168.121.97	1.0	0.71	0.704	0.0	0.0	0.660	6.9	10	7.8	*High*	HTTP, TCP, UDP
2	192.168.121.99	1.0	0.71	0.704	0.0	0.0	0.660	6.9	10	7.8	*High*	HTTP, TCP, UDP
3	192.168.121.102	1.0	0.71	0.704	0.275	0.275	0.275	6.4	10	7.5	*High*	HTTP, TCP, UDP
4	192.168.121.104	1.0	0.71	0.704	0.275	0.275	0.275	6.4	10	7.5	*High*	HTTP, TCP, UDP
5	192.168.121.105	1.0	0.71	0.704	0.275	0.275	0.0	4.9	10	6.4	*High*	HTTP, TCP, UDP
6	192.168.121.107	1.0	0.71	0.704	0.275	0.275	0.0	4.9	10	6.4	*High*	HTTP, TCP, UDP
7	202.79.210.121	1.0	0.71	0.704	0.0	0.275	0.0	2.9	10	5	*Medium*	HTTP, TCP, UDP
8	203.190.241.2	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*	HTTP, TCP, UDP
9	203.190.241.6	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*	HTTP, TCP, UDP
10	203.190.241.9	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*	HTTP, TCP, UDP
11	180.250.7.184	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*	HTTP, TCP, UDP
12	180.250.7.186	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*	HTTP, TCP, UDP
13	180.250.7.187	1.0	0.61	0.704	0.0	0.275	0.0	2.9	8.6	4.3	*Medium*	HTTP, TCP, UDP
14	182.56.179.88	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*	HTTP, TCP, UDP
15	1876.158.208.160	1.0	0.35	0.704	0.275	0.275	0.0	4.9	4.9	4	*Medium*	HTTP, TCP, UDP

Gambar 3.15. analisis *bussiness impact*

PENUTUP

3.8 Latihan Soal

1. Jelaskan pengertian dari sniffing!
2. Bagaimanakah cara kerja dari sniffing?
3. Protocol apa yang digunakan untuk sniffing?
4. Jelaskan sniffing active!
5. Jelaskan sniffing pasif!
6. Berikan contoh dari serangan sniffing!
7. Bagimana cara mendeteksi sniffing?
8. Apa yang bisa dilakukan sebagai perlindungan dari sniffing?
9. Apa itu wireshark?
10. Apa itu Reconnaissance?
11. Jelaskan pengertian dari scanning!
12. Jelaskan teknik-teknik dalam scanning!
13. Berikan contoh dari serangan scanning!
14. Apa yang dimaksud scaning live system dan open port?
15. Apa yang dimaksud dengan bannergrabing dan os fingerprinting?
16. Apa yang dimaksud dengan vulnerability?
17. Apa yang dimaksud dengan proxy didalam proses network scanning?
18. Apa yang dimaksud dengan anonymizer dalam network scanning?
19. Apa yang dimaksud dengan drawing network diagram?
20. Apa yang dimaksud dengan scaning coutermasture?

DAFTAR PUSTAKA

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

Dewaweb. (2019). *Pengertian dan Cara Kerja Firewall*. Dewaweb.Com. https://www.dewaweb.com/blog/pengertian-firewall-dan-cara-kerjanya/

Doni, F. (2015). Optimalisasi Jaringan Wireless Dengan Router Mikrotik Studi Kasus Kampus Bsi Tangerang. *Evolusi*, *2*(1), 37–45. https://doi.org/10.2311/evo.v2i1.185

Fatriawan, R. (2016). *Pengertian dan fungsi getway*. 1–5.

Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. (2019). *Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server*. *4*(3), 181–188.

Mulyana, E., & Purbo, O. W. (2000). Firewall: Sekuriti Internet. *Computer Network Research Group ITB*, 1–6. http://4sucktie.tripod.com/firewall1.pdf

Pamungkas, C. A. (2016). Manajemen bandwith menggunakan mikrotik routerboard di politeknik indonusa surakarta. *INFORMA Politeknik Indonusa Surakarta*, *1*, 3–8.

Pribadi, Z. A. (2013). *Analisis dan Implementasi Firewall dengan Metode Stateful Multilayer Inspection Pada Mikrotik Router OS*. *1*, 1–9.

Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori. *JUSI, Universitas Ahmad Dahlan Yogyakarta*, *1*(1), 71–80.

Sembiring, I., Widiasari, I., & Prasetyo, S. D. (2011). Analisa dan Implementasi Sistem

Keamanan Jaringan Komputer dengan Iptables sebagai Firewall Menggunakan Metode Port Knocking. *Jurnal Informatika*, *5*(2). https://doi.org/10.21460/inf.2009.52.74

Sujito, & Roji, M. F. (2010). *Sistem Keamanan Internet dengan Menggunakan Iptables sebagai Firewall*. 58–70.

Sutoyo, I., & Wahyudi, M. (2009). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *Paradigma*, *XI*(2), 110–121. http://ejournal.bsi.ac.id/ejurnal/index.php/paradigma/article/view/4732

Wongkar, S., Sinsuw, A., Najoan, X., Studi, P., Informatika, T., Teknik, F., & Ratulangi, U. S. (2015). Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan Lan Dan Wlan Di Desa Kawangkoan Bawah Wilayah Amurang Ii. *E-Journal Teknik Elektro Dan Komputer*, *4*(6), 62–68. https://doi.org/10.35793/jtek.4.6.2015.10400

Yudianto, M. J. N. (2014). Jaringan Komputer dan Pengertiannya. *Ilmukomputer.Com*, *Vol.1*, 1–10.

https://idcloudhost.com/tips-cara-mengatasi-malware-ransomware-wannacrypt/

https://bepala.blogspot.com/2019/12/mengamankan-router-dari-serangan-bruteforce.html

http://ijongku.blogspot.com/2018/01/mencegah-brute-force-login-mikrotik.html

http://mikrotik.co.id/artikel_lihat.php?id=105

https://idcloudhost.com/mengenal-apa-itu-malware-penyebab-dan-mengatasinya/

http://sudutpandangpupil.blogspot.com/2013/02/apa-itu-security.html

https://www.dewaweb.com/blog/pengertian-malware-pentingnya-dewaguard

http://www.mikrotik.co.id/artikel_lihat.php?id=57

http://www.mikrotik.co.id/artikel_lihat.php?id=146

https://www.monitorteknologi.com/fungsi-fitur-fitur-firewall-mikrotik/#1_Filter_Rules

http://shibyansae.blogspot.com/p/modul-belajar.html

Arsin, F., Yamin, M., & Surimi, L. (2017). semanTIK. IMPLEMENTASI SECURITY SYSTEM MENGGUNAKAN METODE IDPS (INTRUSION DETECTION ANDPREVENTION SYSTEM) DENGAN LAYANAN REALTIME NOTIFICATION, 3(2), 39–48.

Gondohanindijo, J. (2012). Majalah Ilmiah INFORMATIKA . IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan / Intrusi, 3(3), 38–59.

Khadafi, S., Meilani, B. D., & Arifin, S. (2017). Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System). Jurnal IPTEK, 21(2), 67. doi: 10.31284/j.iptek.2017.v21i2.207

Gondohanindijo, J. (2011). Sistem Untuk Mendeteksi Adanya Penyusup (IDS: Intrusion Detection System). Majalah Ilmiah INFORMATIKA, 2(2).

Putri, L. (2011). Implementasi intrusion detection system (IDS) menggunakan snort pada jaringan wireless (studi kasus: SMK Triguna Ciputat).

McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: The role of intrusion detection systems. IEEE software, 17(5), 42-51.

Erza, M. (n.d.). Network Based IDPS (IDPS Berbasis Jaringan). Retrieved from https://keamanan-informasi.stei.itb.ac.id/2013/10/30/network-based-idps-idps-berbasis-jaringan/

James P. Anderson. (1980). Computer Security Threat Monitoring and Surveillance. Technical report Co, Fort Washington

Kopelu Letou , Dhruwajita Devi, Y. Jayatan Singh (2013). Host-based Intrusion Detection and Prevention System (HIDPS) . International Journal of Computer Applications (0975 – 8887)

Deris Stiawan. (2012) Intrusion Prevention System (IPS) dan Tantangan dalam pengembanganya.

Jhala, N. Y. (2014). *Network Scanning & Vulnerability Assessment with Report Generation*. *1*(5), 10–12.

M. de Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, "A review of port scanning techniques," ACM SIGCOMM Computer Communication Review, vol. 29, pp. 41-48, 1999.

G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "Bothunter: Detecting malware infection through ids-driven dialog correlation," 2007, pp. 1-16.

D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," IEEE Security & Privacy, vol. 1, pp. 33-39, 2003.

N. Kato, H. Nitou, K. Ohta, G. Mansfield, and Y. Nemoto, "A real-time intrusion detection system (IDS) for large scale networks and its evaluations," IEICE Transactions on Communications, vol. 82, pp. 1817-1825, 1999.

Anbar, M., Manasrah, A., Ramadass, S., & Altaher, A. (2013). Investigating Study on Network Scanning Techniques. *International Journal of Digital Content Technology and Its Applications (JDCTA)*, *7*(9), 312–320. https://doi.org/10.4156/jdcta.vol7.issue9.37.

Bhuyan, H. M, Bhattacharyya, D. K, Kalita. K, J. (2011). *Surveying Port Scans and Their Detection Metodologies*. The Computer Journal. Vol. 54 No. 10.

C. Julius, H. Hansen, R. Abdu. (2017). *Deteksi Serangan Port Scanning Menggunakan Algoritma Naive Bayes*. Program Studi Teknik Informatika, STMIK GI MDP, Palembang.

1-12.

Ahmad Fauzan dkk.2018.Sniffer & Scanning/Port Scanning.Makalah.Dikutip dari https://www.academia.edu/34554651/Makalah_Kejahatan_Komputer_Sniffer_Dan_Scanning_.docx.27 April 2020.

Prasetyo, Inung Bagus.(2019).Analisa Sniffing Paket ICMP Menggunakan Wireshark.Jurnal SISTEMASI,8(1),221.

https://sandylesmana21blog.wordpress.com/2016/09/10/network-scanning/

https://almaspens.wordpress.com/2016/03/19/teknik-scanning-jaringan/

http://bsickgkelompokenam.blogspot.com/2013/06/httpkumpulankisahnyataterbaru.html

https://etikaprofesikelompok14.wordpress.com/2015/04/10/probingport-scanning/amp/