ANALISA METODE ANOMALY DETECTION IDS MENGGUNAKAN ANOMALY BASELINE PADA SEBUAH JARINGAN KOMPUTER

Danang Prasetyo Nugroho

Teknik Informatika, Universitas Dian Nuswantoro Semarang

Email : danang_prasetyo18@rocketmail.com

Abstrak **-** Seiring dengan Perkembangan Teknologi Informasi menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi tidak diiringi dengan perkembangan pada sistem keamanan itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan harus ditingkatkan keamanannya. Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar.

Serangan tersebut berupa serangan *Hacker* yang bermaksud merusak Jaringan Komputer yang terkoneksi pada internet ataupun mencuri informasi penting yang ada pada jaringan tersebut. Metode *anomaly detection* merupakan salah satu cara yang dilakukan dalam menganalisa terhadap serangan pada sistem deteksi intrusi dengan bantuan alat Ethereal yang digunakan menangkap paket data yang ada. Hasil penelitan menunjukkan bahwa *anomaly detection* dapat digunakan untuk mengetahui bagian-bagian dalam jaringan yang akan dilakukan penyusupan.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat menjadikan keamanan sangat penting dan jika suatu jaringan komputer terhubung dengan internet. Dengan perkembangan ini yang cukup cepat ini maka banyak serangan yang dila kukan oleh para penyusup. Adanya firewall tidak semua dapat menjamin keamanan secara sepenuhnya, maka dari itu ada teknologi IDS yang dapat membantu pengamanan data pada jaringan komputer. Dari hasil latar belakang di atas penulis mencoba untuk menganalisa menggunakan

metode deteksi anomali yang digunakan cukup baik atau tdak untuk mengetahui serangan yang mungkin dilakukan penyusup.

1.2 Rumusan Masalah

Berdasarkan latar belakang seperti yang diuraikan sebelumnya, dapat dirumuskan suatu masalah yaitu :

1. Bagaimana cara kerja dari ethereal untuk mendapatkan paket data dan port pada jaringan komputer.
2. Bagaimana virus melakukan penyusupan pada port yang tertangkap.

1.3 Batasan Masalah

Untuk mendapatkan hasil penelitian seperti yang diharapkan dan penelitian yang terarah, maka permasalahan dalam penelitian ini akan dibatasi pada penerapan metode anomaly detection untuk mengetahui paket data serta port pada jaringan komputer yang memungkinkan terjadinya serangan.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang didapat di atas diketahui tujuan penelitian yaitu mengetahui hasil dari penggunaan metode anomali yang digunakan dalam penggunaannya untuk mengatasi serangan yang ada pada jaringan komputer.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat untuk membantu dan mengetahui akan terjadinya sebuah serangan yang akan merusak sebuah jaringan komputer yang ada. Diharapkan dapat memudahkan administrator jaringan mengetahui apabila akan adanya serangan ataupun penyusup yang mengancam sistem komputer dan jaringan komputer:

a. Bagi Akademik

1. Sebagai pelengkap literatur di perpustakaan yang dapat dijadikan refernsi dan evaluasi jika melakukan penelitian sejenis.

2. Sebagai tolak ukur keberhasilan suatu akademik dengan diterapkan ilmu yang diajarkan kedalam dunia kerja dan acuan akademik untuk menilai sejauh mana kemampuan mahasiswa menyerap ilmu yang telah diberi.

b. Bagi Penulis

1. Membantu dalam mengaplikasikan ilmu yang telah di dapat di perkuliahan dengan menunjang kesiapan untuk terjun di dunia kerja.

2. Memberi tambahan ilmu pengetahuan serta wawasan.

c. Bagi Masyarakat

1. Sebuah bahan referensi dan untuk menambah pengetahuan bagi pembaca.

BAB II

TINJAUAN PUSTAKA

2.1 Anomaly Baseline

Anomali baseline merupakan suatu acuan dasar yang di jadikan patokan sebelum melakukan perbandingan terhadap data yang nantinya akan di analisis. Baselin sendiri merupakan tindakan pengukuran dan penilaian nilai kerja dari jaringan berdasarkan kondisi *real-time*. Untuk membangun baseline dibutuhkan adanya uji cobaan pelaporan konektifitas secara fisik, penggunaan jaeingan yang normal, penggunaan protocol, puncak penggunaan jaringan dan rata-rata penggunaan *throughput* jaringan.

Sistem Deteksi Intrusi berdasarkan anomali adalah sistem keamanan jaringan yang

berfungsiuntuk mendeteksi adanya gangguan-gangguan pada jaringan komputer dengan cara mendeteksigangguan-gangguan tersebut berdasarkan pola-pola anomali yang ditimbulkan. Serangan Denialof Services (DoS) adalah salah satu contoh jenis serangan yang dapat mengganggu infrastrukturdari jaringan komputer, serangan jenis ini memiliki suatu pola khas, dimana dalam setiapserangannya akan mengirimkan sejumlah paket data secara terus-menerus kepada targetserangannya. Dengan menggunakan metode deteksi anomali, serangan DoS dapat dideteksidengan mengidentifikasi pola-pola anomali yang ditimbulkan.

BAB III

METODE PENELITIAN

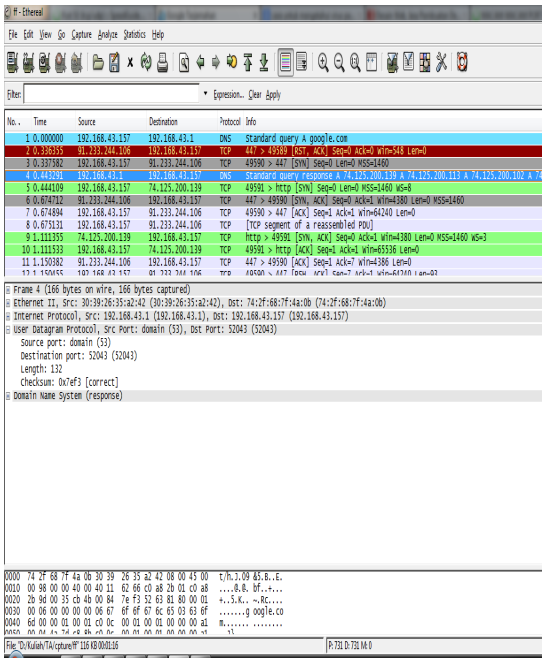
3.1 Ruang Lingkup Penelitian

Agar penelitian dapat terfokus dan terarah, maka perlu adanya ruang lingkup yang digunakan sebagai pedoman dalam melaksanakan penelitian. Ruang lingkup penelitian ini adalah analisa metode deteksi anomali dengan menggunakan *anomaly baseline* untuk mengetahui IP mana saja yang biasanya terjadi intrusi atau ancaman.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Analisa



Gambar 4.1 : Tampilan Capture port 53

Dalam hal ini terdapat beberapa virus yang melakukan serangan terhadap port ini antara lain :

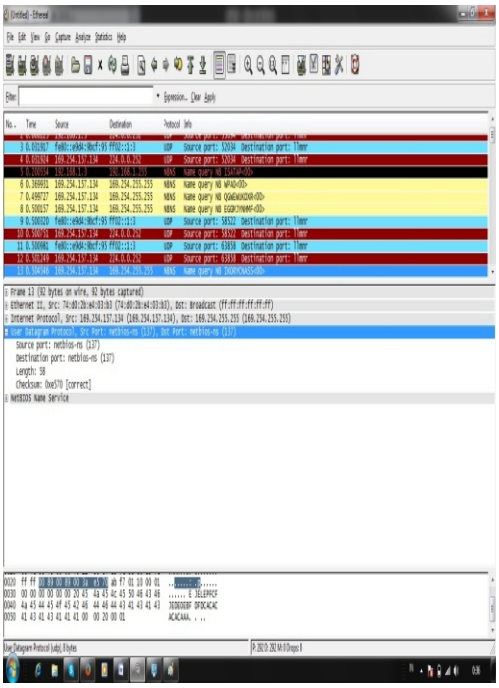
a. ADM worm

Sebuah sistem yang ditargetkan oleh Adm akan menerima paket khusus dibuat pada port tcp 53 . Paket ini memanfaatkan buffer overflow dalam server BIND DNS dan memungkinkan kode untuk dijalankan dengan hak akses root .

b. Lion (1i0n)

Lion adalah worm Linux yang menyebabkan beberapa kerusakan kecil pada awal tahun 2001. Varian ketiga agak mirip dengan Ramen. Beberapa ahli antivirus mencurigai kemungkinan adanya hubungan antara lion dan Slammer worm.

Pada sistem yang sudah terinfeksi dengan Lion, worm akan memindai acak jaringan IP kelas B pada port 53 untuk sistem dengan Signiture Transaksi (TSIG) kerentanan buffer overflow di Berkeley Internet Name Service Domain (BIND DNS).



Gambar 4.2 : Tampilan Capture port 137

Pada port ini merupakan NetBIOS yang di gunakan untuk melakukan *file and sharing.* Dalam port ini juga apabila di aktifkan untuk melakukan *file and sharing* yang termasuk TCP/IP (Internet Protocol) maka tidak hanya di jaringan lokal akan tetapi di sleluruh internet dapat membaca port ini sedang melakukan aktifitas jaringan.

Selain itu juga ada beberapa worm/virus yang bisa melakukan serangan yaitu :

a. W32.HLLW.Moega

Worm / cacing yang memiliki kemampuan backdoor. Ia mencoba untuk menyebar melalui jaringan area lokal. Worm ini menghubungkan ke server IRC untuk menerima instruksi lebih lanjut dari penciptanya.

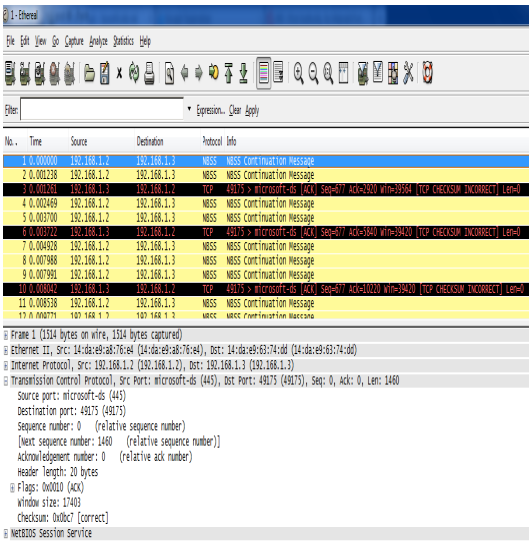
b. W32.Crowt.A

Worm atau virus ini telah sering digunakan dalam serangan penolakan layanan dan upaya lain untuk mengganggu djaringan komputasi dalam skala besar . Mereka dirancang untuk mereplikasi diri dan menyebar dengan cepat melalui lampiran email palsu, email spam, dan metode lainnya. Mereka juga dapat menyebarkan backdoors untuk memungkinkan akses remote dan kontrol dari komputer yang terinfeksi.

c. W32.Reidana.A

worm yang menyebar menggunakan kerentanan RPC DCOM MS. Worm ini

mencoba untuk men-download dan menjalankan file remote melalui FTP .



Gambar 4.3 : Tampilan Capture port 445

Sama halnya seperti prt 137 dimana pada port 445 ini juga digunakan untuk *file and sharing*. Selain itu port ini sering sekali digunakan para Hacker untuk mencoba melakukan penyusupan serangan melalui port ini, maka daripada itu salah satu kelemahan dari port ini mudahnya terinfeksi virus atau worm.

beberapa virus bisa menyusup port ini yaitu :

a. W32.Zotob.C

Worm atau cacing yang membuka backdoor dan memanfaatkan MS Plug and Play Buffer Overflow kerentanan pada port 445/tcp. Ini menghubungkan ke server IRC dan mendengarkan perintah remote pada port 8080/tcp. Ini juga membuka server FTP pada port 33333/tcp.

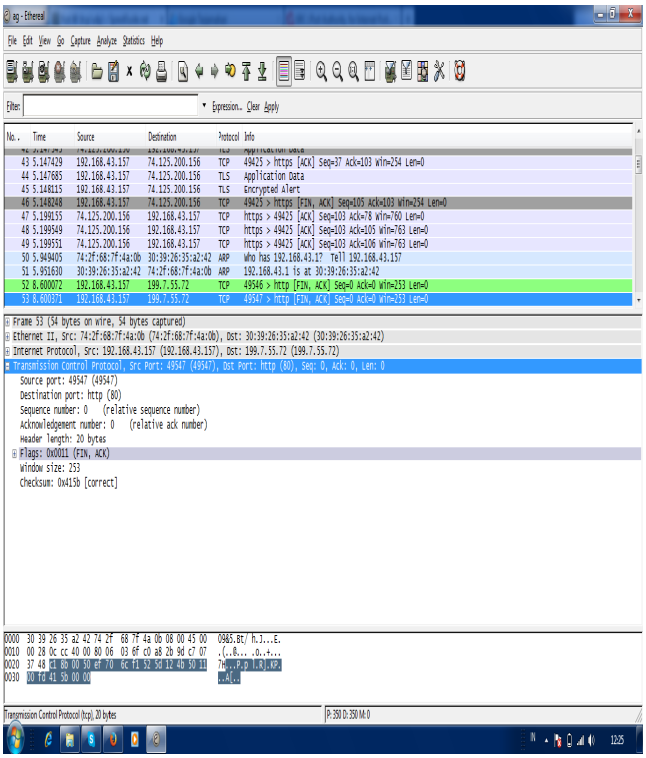
b. W32.Zotob.D

Worm atau cacing yang membuka backdoor dan memanfaatkan MS Plug and Play Buffer Overflow kerentanan pada port 445/tcp. Conects ke server IRC untuk mendengarkan perintah remote pada port 6667/tcp. Juga membuka server FTP pada port 1117/tcp.

c. W32.Zotob.E

Worm/cacing yang membuka backdoor dan memanfaatkan

MS Plug and Play Buffer Overflow kerentanan pada port 445/tcp. Ini berjalan dan menyebar menggunakan semua versi Windows saat ini, tetapi hanya menginfeksi Windows 2000. Worm ini menghubungkan ke server IRC dan mendengarkan perintah remote pada port 8080/tcp . Ini membuka port 69/udp untuk memulai transfer TFTP. Ini juga membuka backdoor pada komputer dikompromikan jarak jauh pada port 8594/tcp. Port 445/tcp juga digunakan oleh W32.Zotob.H varian dari worm.



Gambar 4.4 : Tampilan Capture port 80

Pada port 80 ini ternyata bisa sdisusupi oleh virus atau worm pada saat tidak menjalankan web salah satunya worm Code Red yang merambat melalui TCP port 80 ini.

Ada pula selain worm yng melakukan serangan melalui port ini yaitu virus 711 trojan (Seven Eleven), AckCmd, Back End, Executor, God Message, God Message Creator, Hooker,

IISworm, MTX, NCX, Nerte 7.8.1, RingZero, Seeker, dan lain-lain.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis jaringan pada Ethereal untuk mendapatkan port yang mungkin terjadinya serangan, maka dapat diambil kesimpulan sebagai berikut :

a. Dari beberapa port yang didapat dari hasil capture yang dilakukan menggunakan ethereal terdapat dua port yang sering muncul yaitu port 445 dengan jumlah paket data yang melebihi normal yaitu 50 kilobytes dan port 137 dengan paket data yang tdak terlalu besar akan tetapi dengan jumlah kemunculan yang sering dan ini menunjukkan bahwa kedua port tersebut telah terinfeksi virus.

b. Pada port 445 sangat rentan terhadap serangan virus atau worm dan memudahkan melakukan serangan.

5.2 Saran

Dari beberapa kesimpulan yang telah diambil, maka dapat dikemukakan saran -saran yang akan sangat membantu untuk pengembangan sistem ini selanjutnya yaitu :

a. Perlu dipertimbangkan untuk menambah jumlah port yang akan di analisis dikarenakan sangat banyak port yang nantinya akan di analisa sehingga untuk melakukan lebih banyak lagi diperlukan aplikasi tambahan yang lebih baik supaya port-port yang belum teridentfikasi dapat diketahui .

b. Analisa yang dilakukan pada jaringan komputer masih cukup sederhana sehingga

masih dapat dilakukan lagi analisa lebih lanjut dan dikembangkan lagi untuk mencapai hasil yang lebih akurat dan tepat.

DAFTAR PUSTAKA

[1] Nadhori,Izbat Uzzin dan Hariadi ,Moch. (2009). *Pendeteksi Anomali pada Jaringan didasarkan pada Analisa Payload Data Berbasis Metode Support Vector Machine.*

[2] Karima,Aisyatul. (2012). *Deteksi Anomali untuk Identifikasi Botnet Kraken dan Conficker menggunakan Pendekatan Rule Based.*

[3] Khosasi,Yohanes. (2010). *Sistem Pendeteksi Intrusi berdasarkan Anomali pada Packet Header* .

[4] http://www.mlarik.com/2013/07/pengertian-jaringan-komputer.html (diakses tanggal 22 Oktober 2013)

[5] http://www.mlarik.com/2013/07/pengertian-jaringan-komputer.html (diakses tanggal 22 Oktober 2013)

[6] Rudyanto,Muhammad. (2011). *Penggunaan Sistem IDS (Intrution Detection System) untuk Pengamanan Jaringan dan Komputer*.AMIKOM Jogjakarta

[7] Arya Sucipta, I Gusti Ngurah. (2012). *Analisa Kinerja Anomaly-Based Intrution Detection System (IDS) dalam Mendeteksi Serangan DoS (Denial of Services) pada Jaringan Komputer.* Bali: JELIKU Vol 1

[8] http://siipglobal.blogspot.com/2010/09/analisa-protokol-layer-2-dan-3.html (diakses tanggal 26 Oktober 2013)

[9]http://multi-centre.blogspot.com/2011/03/ethereal-network-

analyzersnifer.html (diakses tanggal 14 Januari 2014)

[10]http://rian-share4u.blogspot.com/2012/07/macam-macam-port-pada-jaringan.html (diakses tanggal 16 Januari 2014)