ANALISA PENDETEKSIAN *WORM* dan *TROJAN* PADA JARINGAN INTERNET UNIVERSITAS SEMARANG MENGGUNAKAN METODE KALSIFIKASI PADA DATA MINING C45 dan *BAYESIAN NETWORK*

Rastri Prathivi
Fakultas Teknologi Informasi dan Komunikasi
Universitas Semarang
Email: vivi@usm.ac.id

Vensy Vydia
Fakultas Teknologi Informasi dan Komunikasi
Universitas Semarang
Email: vesy@usm.ac.id

***Abstract*— Worm attacks become a dangerous threat and cause damage in the Internet network. If the Internet network worms and trojan attacks the very disruption of traffic data as well as create bandwidth capacity has increased and wasted making the Internet connection is slow. Detecting worms and trojan on the Internet network, especially new variants of worms and trojans and worms and trojans hidden is still a challenging problem. Worm and trojan attacks generally occur in computer networks or the Internet which has a low level of security and vulnerable to infection. The detection and analysis of the worm and trojan attacks in the Internet network can be done by looking at the anomalies in Internet traffic and internet protocol addresses are accessed.**

This research used experimental research applying C4.5 and Bayesian Network methods to accurately classify anomalies in network traffic internet. Analysis of classification is applied to an internet address, internet protocol and internet bandwidth that allegedly attacked and trojan worm attacks.

The results of this research is a result of analysis and classification of internet addresses, internet protocol and internet bandwidth to get the attack worms and trojans.

Keywords - Worm, Trojan, C45, Bayesian Network

I. PENDAHULUAN

Universitas Semarang memiliki jaringan internet yang belum mempunyai keamanan jaringan yang baik. Jaringan internet di Universitas Semarang memiliki peluang yang sangat besar terkena serangan malware yang berbahaya. Serangan malware dapat mengakibatkan berbagai kerugian diantaranya adalah hilangnya data-data, bandwidth internet menjadi penuh akibat penggandaan diri yang dilakukan oleh malware, kerusakan sistem hingga kehancuran sistem. Serangan malware dapat dikategorikan menjadi beberapa jenis serangan dengan perilaku yang berbeda-beda, seperti serangan worm, virus, trojan dan spyware .

Worm bekerja dengan cara menggandakan dan merambatkan dirinya dalam jaringan internet dan menginfeksi komputer dalam jarak jauh. Adanya serangan worm sangat mengganggu kelancaran lalu lintas data dalam internet serta membuat kapasitas bandwidth menjadi bertambah dan terbuang sehingga menjadikan koneksi internet menjadi lambat.

Trojan mempunyai kemampuan mereplikasi dirinya sendiri dalam jaringan internet jika ada interaksi dari pengguna, seperti mengklik. Dengan adanya interaksi dari pengguna jaringan internet, maka trojan menjadi aktif.

Mendeteksi worm dan trojan pada jaringan internet terutama varian worm dan trojan baru serta worm dan trojan yang tersembunyi masih merupakan masalah yang menantang. Serangan worm dan trojan pada umumnya terjadi dalam jaringan-jaringan komputer atau internet yang memiliki tingkat keamanan yang rendah dan rentan terinfeksi. Pendeteksian dan analisa terhadap adanya serangan worm dan trojan dalam jaringan internet dapat dilakukan dengan cara memperhatikan dan menganalisa anomali yang terjadi pada lalu lintas alamat internet dan protokol internet yang diakses. Semakin besar anomali yang muncul dalam lalu lintas alamat internet dan protokol internet yang diakses maka semakin besar serangan worm dan trojan dalam jaringan internet tersebut.

II. STUDI PUSTAKA

Serangan Melalui Internet dan Jaringan

Menurut Shelly (2007), informasi yang ditransmisikan melalui jaringan memiliki tingkatan resiko keamanan yang lebih tinggi dibandingkan informasi yang berada dalam lokai perusahaan. Dalam sebuah perusahaan , administrator jaringan biasanya harus melindungi jaringan dari resiko keamanan. Pada internet, yang tidak memiliki administrator, resiko keamanan menjadi lebih tinggi.Serangan internet dan jaringan yang membahayakan keamanan meliputi virus komputer, worm dan Trojan, selain adanya penipuan (spoofing).

Pengertian Worm

Worm merupakan program yang menggadakan dirinya secara berulang – ulang, misalnya di memori atau jaringan, menghabiskan sumber daya dan mungkin mematikan komputer atau jaringan.

Sebuah worm dapat menggandakan dirinya dengan memanfaatkan jaringan LAN/WAN/Internet) tanpa perlu campur tangan dari user itu sendiri. Worm tidak seperti virus komputer biasa, yang menggandakan dirinya dengan cara menyisipkan program dirinya pada program yang ada dalam komputer tersebut, tapi worm memanfaatkan celah keamanaan yang memang terbuka atau lebih dikenal dengan sebutan vulnerability. Beberapa worm juga menghabiskan bandwidth yang tersedia. Worm merupakan evolusi dari virus komputer. Hanya ada satu cara untuk mengatasi worm yaitu dengan menutup celah keamanan yang terbuka tersebut, dengan cara meng-update patch atau Service Pack dari operating sistem

yang digunakan dengan patch atau Service Pack yang paling terbaru.

Virus komputer memang dapat menginfeksi berkas-berkas dalam sebuah sistem komputer, tapi worm dapat melakukannya dengan lebih baik. Selain dapat menyebar dalam sebuah sistem, worm juga dapat menyebar ke banyak sistem melalui jaringan yang terhubung dengan sistem yang terinfeksi. Beberapa worm, juga dapat mencakup kode-kode virus yang dapat merusak berkas, mencuri dokumen, e-mail, atau melakukan hal lainnya yang merusak, atau hanya menjadikan sistem terinfeksi tidak berguna.

Beberapa contoh dari worm adalah sebagai berikut:

1. ADMw0rm: Worm yang dapat melakukan ekspolitasi terhadap layanan jaringan Berkeley Internet Name Domain (BIND), dengan melakukan buffer-overflow.
2. Code Red: Worm yang dapat melakukan eksploitasi terhadap layanan Internet Information Services (IIS) versi 4 dan versi 5, dengan melakukan serangan buffer-overflow.
3. LoveLetter: Worm yang menyebar dengan cara mengirimkan dirinya melalui e-mailkepada semua akun yang terdaftar dalam Address Book Microsoft Outlook Express/daftar kontak dalam Microsoft Outlook dengan cara menggunakan kode Visual Basic Script (VBScript).
4. Nimda
5. SQL-Slammer

Pengertian Trojan

Trojan merupakan program yang bersembunyi di dalam atau tampak seperti program sah atau legal. Kondisi atau tindakan tertentu biasanya memicu aktifnya Trojan. Tidak seperti Worm, Trojan tidak menggandakan dirinya ke komputer lain. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

Trojan berbeda dengan jenis perangkat lunak mencurigakan lainnya seperti virus komputer atau Worm karena dua hal berikut:

1. Trojan bersifat "stealth" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau Worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash.
2. Trojan dikendalikan dari komputer lain (komputer attacker). Kebanyakan Trojan saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM dalam sistem operasi Windows dan DOSatau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti ls, cat, dan lain-lain) yang dimasukkan ke dalam sistem yang ditembus oleh seorang cracker untuk mencuri data yang penting bagi pengguna (password, data kartu kredit, dan lain-lain). Trojan juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi (seringnya berupa game komputer) dari sumber yang tidak dapat dipercayai dalam jaringan Internet. Aplikasi-aplikasi tersebut dapat memiliki kode Trojan yang diintegrasikan di dalam dirinya dan mengizinkan seorang cracker untuk dapat mengacak-acak sistem yang bersangkutan.

Beberapa jenis Trojan yang beredar antara lain adalah:

1. Pencuri password: Jenis Trojan ini dapat mencari password yang disimpan di dalam sistem operasi (/etc/passwd atau /etc/shadow dalam keluarga sistem operasi UNIX atau berkas Security Account Manager (SAM) dalam keluarga sistem operasi Windows NT) dan akan mengirimkannya kepada si penyerang yang asli. Selain itu, jenis Trojan ini juga dapat menipu pengguna dengan membuat tampilan seolah-olah dirinya adalah layar login (/sbin/login dalam sistem operasi UNIX atau Winlogon.exe dalam sistem operasi Windows NT) serta menunggu pengguna untuk memasukkan passwordnya dan mengirimkannya kepada penyerang. Contoh dari jenis ini adalah Passfilt Trojan yang bertindak seolah-olah dirinya adalah berkas Passfilt.dll yang aslinya digunakan untuk menambah keamanan password dalam sistem operasi Windows NT, tapi disalahgunakan menjadi sebuah program pencuri password.
2. Pencatat penekanan tombol (keystroke logger/keylogger): Jenis Trojan ini akan memantau semua yang diketikkan oleh pengguna dan akan mengirimkannya kepada penyerang. Jenis ini berbeda dengan spyware, meski dua hal tersebut melakukan hal yang serupa (memata-matai pengguna).
3. Tool administrasi jarak jauh (Remote Administration Tools/RAT): Jenis Trojan ini mengizinkan para penyerang untuk mengambil alih kontrol secara penuh terhadap sistem dan melakukan apapun yang mereka mau dari jarak jauh, seperti memformat hard disk, mencuri atau menghapus data dan lain-lain. Contoh dari Trojan ini adalah Back Orifice, Back Orifice 2000, dan SubSeven.
4. DDoS Trojan atau Zombie Trojan: Jenis Trojan ini digunakan untuk menjadikan sistem yang terinfeksi agar dapat melakukan serangan penolakan layanan secara terdistribusi terhadap host target.
5. Ada lagi sebuah jenis Trojan yang mengimbuhkan dirinya sendiri ke sebuah program untuk memodifikasi cara kerja program yang diimbuhinya. Jenis Trojan ini disebut sebagai Trojan virus.
6. Cookies Stuffing, ini adalah script yang termasuk dalam metode blackhat, gunanya untuk membajak tracking code penjualan suatu produk, sehingga komisi penjualan diterima oleh pemasang cookies stuffing, bukan oleh orang yang terlebih dahulu mereferensikan penjualan produk tersebut di internet.

Mendeteksi keberadaan Trojan merupakan sebuah tindakan yang agak sulit dilakukan. Cara termudah adalah dengan melihat port-port mana yang terbuka dan sedang berada dalam keadaan "listening", dengan menggunakan utilitas tertentu semacam Netstat. Hal ini dikarenakan banyak Trojan berjalan sebagai sebuah layanan sistem, dan bekerja di latar belakang (background), sehingga Trojan- Trojan tersebut dapat menerima perintah dari penyerang dari jarak jauh. Ketika sebuah transmisi UDP atau TCP dilakukan, tapi transmisi

tersebut dari port (yang berada dalam keadaan "listening") atau alamat yang tidak dikenali, maka hal tersebut bisa dijadikan pedoman bahwa sistem yang bersangkutan telah terinfeksi oleh Trojan Horse.

Komputer Yang Terserang Worm dan Trojan

Worm dan Trojan diklasifikasikan sebagai malware, yaitu singkatan dari malicious software. Malware adalah program yang bertindak tanpa sepengetahuan pengguna dan bias merubah operasi – operasi computer. Malware ini bekerja dengan mengirimkan playload, yaitu kejadian atau trik destruktif yang ingin dikirimkan oleh program. Menurut Shelly (2007) , Komputer yang terserang Worm atauTrojan sering mengalami satu atau beberapa indikasi sebagai berikut :

1.Layar menampilkan pesan atau gambar yang tidak biasanaya muncul.
2. Musik atau suara yang tidak lazim terdengar secara acak.
3. Memori yang tersedia lebih kecil dari sebenarnya.
4. Program – program atau file – file menjadi hilang.
5. File menjadi rusak.
6. Program atau file tidak bekerja normal.
7. Program atau file yang tidak dikenal muncul secara misterius.
8. Perubahan properti sistem.

Pengertian Worm and Trojan Detection Analysis

Worm and Trojan DetectionAnalysis adalah sebuah aktivitas untuk mendeteksi dan menganalisa adanya serangan Worm dan Trojan, menggunakan metode dan tool tertentu. Tujuannya untuk mengetahui darimana Worm dan Trojan berasal, untuk kemudian menjadi dasar dalam pengambilan keputusan strategis dalam hal akses internet, sehingga aman dari serangan.

III. METODE PENELITIAN

Identifikasi Variabel Penelitian

Variabel penelitian di dalam penelitian ini adalah:

1. Time menunjukkan waktu pengaksesan alamat dan protokol jaringan internet.
2. Source menunjukkan data sumber dari pengaksesan trafik internet.
3. Destination menunjukkan data tujuan dari pemakaian trafik internet.
4. Protocol menunjukkan data protokol yang sering diakses.
5. Length
6. Info protokol yang diakses.

Metode Pengumpulan Data

a. Data Primer

Data primer dalam penelitian ini berasal dari data trafik jaringan internet Universitas Semarang. Pengumpulan data primer dilaksanakan selama enam bulan. Di dalam data trafik tersebut ada informasi mengenai alamat internet, protokol internet, jumlah bandwidth yang terpakai.

b. Data Sekunder

Data sekunder dalam penelitian ini adalah data – data yang berasal dari studi pustaka yang berkaitan dengan judul penelitian.menunjukkan data lebar bandwidth yang digunakan.

Metode Pengolahan Awal Data

Pengolahan awal data dilakukan dengan cara sebagai berikut:

1. Data penelitian diambil melalui software Wireshark, format file data adalah .csv
2. Pada software Weka masuk ke applications explorer
3. Pada menu preprocess, pilih tab Open file.
4. Buka file .csv

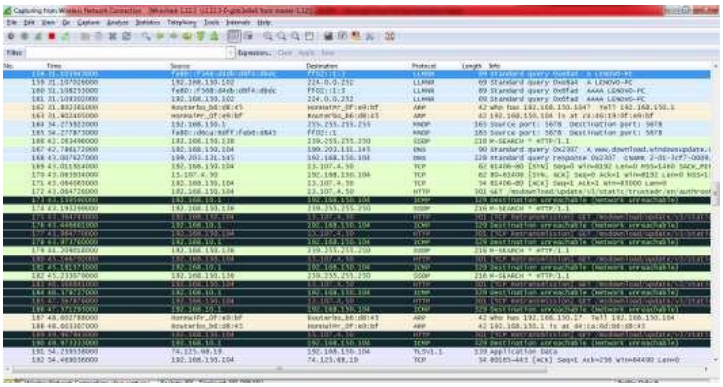
Desain eksperimental dalam penelitian ini dibagi menjadi beberapa tahap proses sebagai berikut:

1. Proses Pengumpulan Data
   Proses pengumpulan data dalam penelitian ini dibagi menjadi tiga proses yaitu:
2. Proses menampilkan trafik jaringan internet USM sebagai sumber data.
3. Data trafik jaringan internet dicapture dengan software wireshark.
4. Hasil capture dari trafik jaringan internet berupa file dengan format .csv.

IV. HASIL DAN PEMBAHASAN

Pengumpulan Data

Proses pengumpulan data menggunakan software wireshark.

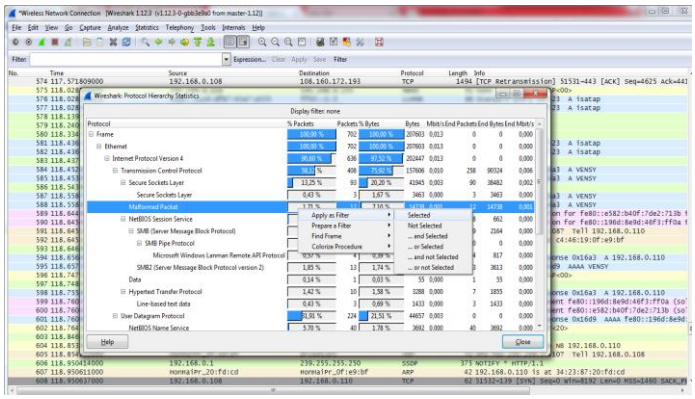


Gambar 1 Capture Data dengan Wireshark

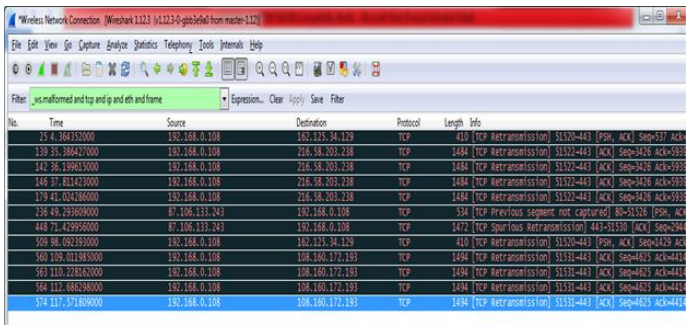
Dari hasil capture pada gambar 1, terlihat baris data yang di blok warna hitam. Data tersebut memperlihatkan adanya kejanggalan yang terjadi pada penggunaan jaringan internet. Warna hitam memperlihatkan adanya bad TCP yang mengindikasikan jaringan terinfeksi worm atau trojan. Keterangan tentang warna hitam pada jaringan yang dicapture dijelaskan di dalam perangkat lunak Wireshark dapat dilihat pada gambar 2.

Gambar 2 Keterangan Warna pada Capture Data dengan Wireshark

Untuk memisahkan data yang terinfeksi worm dan trojan dengan data yang tidak terinfeksi maka perlu dilakukan proses filtering melalui proses Protocol Hierarchy Statistics. Proses ini dilakukan melalui software wireshark. Proses tersebut ditunjukkan pada gambar 5.3. Filtering yang dilakukan adalah filtering pada bagian Malformed Packet yang merupakan paket jaringan yang terinfeksi.

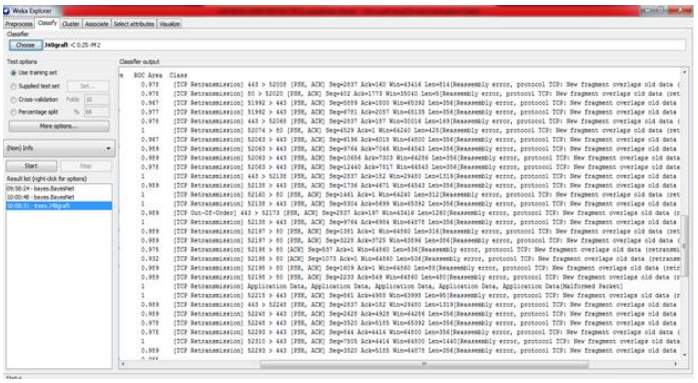


Gambar 3 Proses Protocol Hierarchy Statistics

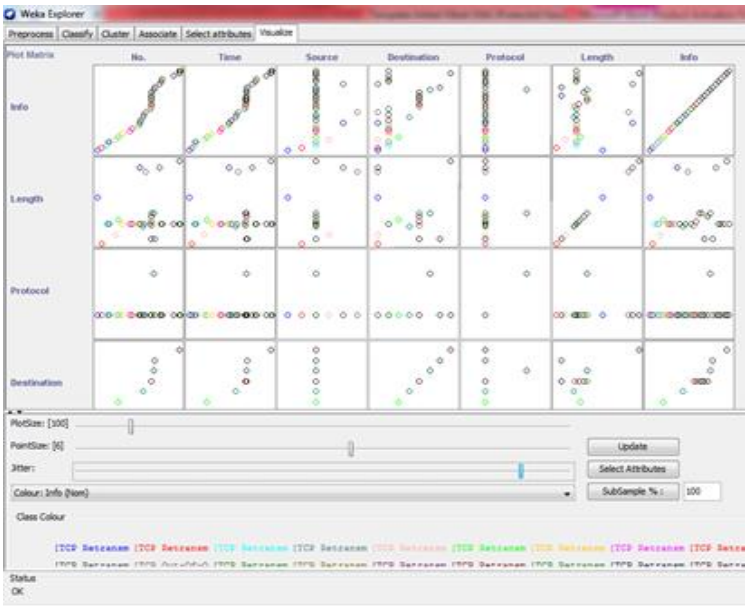


Gambar 4. Hasil *Filtering* Data Jaringan Terinfeksi *Worm* dan *Trojan*

Analisa Data



Gambar 5. Hasil Analisa Data



Gambar 6. Hasil Klasifikasi Data Metode C.45

Gambar 7. Hasil Klasifikasi Data Metode Bayessian Network

V. KESIMPULAN DAN SARAN

Kesimpulan

Dari hasil analisa penggunaan jaringan internet di Universitas Semarang diperoleh kesimpulan sebagai berikut:

1. Hasil filtering data pada preprocessing data jaringan internet menggunakan metode filter Supervised Attribut AddClasisfication memperlihatkan banyaknya data yang terinfeksi trojan dan worm sebanyak 46 data dari 500.000 data yang diakses
2. Dari analisa data jaringan internet menggunakan metode C.45 dan Bayessian Network memperlihatkan hasil adanya infeksi pada jaringan internet Universitas Semarang.

Saran

Dari hasil penelitian ini maka bisa disampaikan beberapa saran sebagai berikut:

1. Hasil analisa penelitian ini dapat memberikan evaluasi untuk keamanan jaringan internet di Universitas Semarang.
2. Setelah mengatahui hasil analisa jaringan internet yang terinfeksi trojan dan worm maka perlu adanya sistem untuk meningkatkan keamanan jaringan internet di Universitas Semarang.

DAFTAR PUSTAKA

[1] Abdul Kadir. 2013. *Pengantar Teknologi Informasi*. Penerbit Andi

[2] Aji Supriyanto. 2005. *Pengantar Teknologi Informasi*. Penerbit Salemba Infotek

[3] Dony Ariyus. 2007. *Intrusion Detection System*, Penerbit Andi

[4] Eko Prasetyo. 2012. *Data Mining*, Penerbit Andi

[5] Gupta, Momtora. 2012. *Intrusion Detection System Using Wireshark*. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 2, Issue 11, November.

[6] Jonathan Palmer. 2011. *Naive Bayes Classification for Intrusion Detection Using Live Packet Capture*. Data Mining in Bioinformatics, Spring.

[7] P. Szor. 2005. *The Art of Computer Virus Research and Defense*. Addison Wesley for Symantec Press, New Jersey.

[8] Rastri Prathivi. 2015. *Klasifikasi Data Trafik Internet Menggunakan Metode Bayes Network (Studi Kasus Jaringan Internet Universitas Semarang.*, Jurnal Transformatika Volume 12 Nomor 2 – ISSN 1693 – 3656

[9] Shelly, 2007. *Disovering Computers*. Penerbit Salemba Infotek