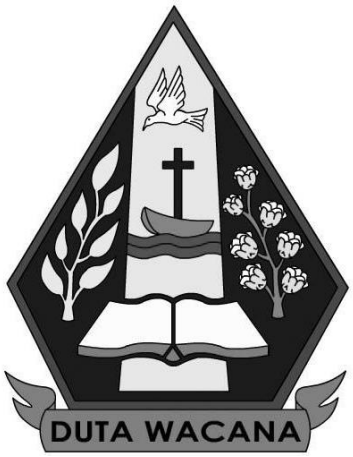
PROGRAM BANTU UNTUK MENCEGAH PENYUSUPAN MELALUI *SCAN PORT* PADA JARINGAN KOMPUTER

Tugas Akhir



Diajukan kepada Fakultas Teknologi Informasi Program Studi Teknik Informatika
Universitas Kristen Duta Wacana
Sebagai salah satu syarat dalam memperoleh gelar
Sarjana Komputer

Disusun oleh:

Orry Adrianus Mokola
NIM. 22043703

Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Tahun 2010

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul:

PROGRAM BANTU UNTUK MENCEGAH PENYUSUPAN MELALUI *SCAN PORT* PADA JARINGAN KOMPUTER

Yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan sarjana Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika di kemudian hari didapati bahwa skripsi ini adalah hasil dari plagiasi atau tiruan dari skripsi lain, saya bersedia menerima sanksi berupa pencabutan gelar kesarjanaan saya.

Yogyakarta, 11 Januari 2011

(Orry Adrianus Mokola.)

22043703

HALAMAN PERSETUJUAN

Judul	:	Program Bantu Untuk Mencegah Penyusupan Melalui *Scan Port* Pada Jaringan Komputer
Nama	:	Orry Adrianus Mokola
NIM	:	22043703
Mata Kuliah	:	Tugas Akhir
Kode	:	T12126
Semester	:	Genap
Tahun Akademik	:	2010/2011

Telah diperiksa dan disetujui
Di Yogyakarta,
Pada Tanggal 22 Desember 2010

Dosen Pembimbing I	Dosen Pembimbing II
(Junius K. Tampubolon, S.Si. M.T)	(Antonius Rachmat C, S.Kom. M.cs)

HALAMAN PENGESAHAN

SKRIPSI

Program Bantu Untuk Mencegah Penyusupan Melalui Scan Port Pada Jaringan Komputer

Oleh : Orry Adrianus Mokola / 22043703

Dipertahankan di depan dewan Penguji Tugas Akhir / Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh
Gelar Sarjana Komputer
Pada tanggal
7 - 1 - 2011

Yogyakarta, 12 - 1 - 2011
Mengesahkan,

Dewan Penguji :

1. Nugroho Agus Haryono, S.Si., M.Si
2. Antonius Rachmat C, S.Kom., M.Cs.
3. Hendro Setiadi, ST., MM., M.EngSc
4. _____

Dekan

(Drs. Wimmie Handiwidjojo, MIT)

Ketua Program studi

(Nugroho Agus Haryono,S.Si., M.Si)

Skripsi ini ku persembahkan buat...

Tuhan Yesus,
yang tak pernah tinggalkan ku walau sedetik pun...
Dia jadikan semua indah pada waktunya...

Bapa dan Mama,
Sabar dan selalu melimpahkan kasih Sayangnya...
Dan menjadi sumber semangatku...

Kakak-kakakku tersayang
Jhon, Max, Maya,
Atas semua dukungannya...

Sebab Tuhan, Dia Sendiri akan berjalan di depanmu, Dia sendiri akan menyertai engkau,
Dia tidak akan membiarkan engkau dan tidak akan meninggalkan engkau;
janganlah takut dan janganlah patah hati
(Ulangan 31 : 8)

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan kepada Tuhan Yesus Kristus yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Tugas akhir.

Tugas akhir ini ditulis dalam rangka pemenuhan salah satu syarat dalam memperoleh gelar Sarjana Komputer. Dalam kesempatan ini, penulis ingin mengucapkan terimakasih yang sebesar-besarnya kepada pihak-pihak yang secara langsung maupun tidak langsung turut membantu, mendorong, dan mendoakan penulis selama masa kuliah hingga saat diselesaikannya pembuatan program dan laporan tugas akhir ini, yaitu kepada:

1. Bapak **Junius K. Tampubolon, S.Si. M.T.,** selaku dosen pembimbing I. Terima kasih atas waktu yang disediakan untuk konsultasi penulis, bimbingan, petunjuk, masukan, kesabaran, ilmu maupun pengetahuan yang diberikan selama penulis mengerjakan tugas akhir hingga Tugas Akhir ini selesai.
2. Bapak **Antonius Rachmat C, S.Kom**, **M.cs.**, selaku dosen pembimbing II. Terima kasih atas waktu yang disediakan untuk konsultasi penulis, bimbingan, petunjuk, masukan, motivasi, kesabaran, ilmu maupun pengetahuan yang diberikan selama penulis mengerjakan Tugas Akhir.
3. Kedua Orang Tuaku, Bapa dan Mama tercinta atas dukungan doa yang tidak pernah berhenti kepadaku, atas kasih sayang yang berkelimpahan, atas motivasi di saat terasa lemah, atas perkataan - perkataan yang menguatkan penulis disaat terasa berat dan tidak mampu, dan bantuan moril dan materil yang penulis terima.
4. Buat Allmarhum Bapak ”Daud Mokola” dan Mama ”Sofia Saudale” selaku orang tua wali, yang selalu jadi Sumber inspirasi dan pemacuh semangat buat penulis untuk menyelesaikan Tugas Akhir ini,terima kasih atas dukungan doa, bantuannya.

5. Buat Kakak-Kakakku Tersayang Jhon, Max, Maya, terima kasih atas dukungan doa, bantuan, kesabaran, motivasi dan canda tawa selama penulis mengerjakan tugas akhir ini. Sukses selalu untuk kalian, semoga Tuhan selalu memberkati.
6. Buat Semua Keluarga terima kasih atas dukungan doa, bantuan, kesabaran, motivasi dan canda tawa selama penulis mengerjakan tugas akhir ini
7. Buat keluarga “Fareck Jogja” Pa Roby, Pa Chely, Pa Roni, K Mije, K Yedit, K Nona, Mas Yoga, Bang Robert, Mas Mbe, Hutri, Ernest, Boss, Willem, Redy, Epen, Antus, Joddy, Arpark, Reza, Juary, Yoan, Resta, Alda, Fitha, Ati, William, Aldy, Vhodalk, Jhoa, Erik, Mea, Shibe, Eppy, Noken, Qiqi. Terima kasih untuk kebersamaan rasa kekeluargaan dan secara tidak langsung memberikan dukungan semangat buat penulis.
8. Buat temen – temen kos “728”, Bang bertus, Bang Ayak, Daefan, Wendy, Yunes, Decky, Aun, Mortal, Eko, Hanes, Rano, Ricko, Andre, Mei-Mei, Tony, Bibir, Saut, Willy, Smith, Hunter. Terima kasih buat pengalaman indah bersama yang membuat penulis merasakan kehangatan keluarga selama ini.
9. Buat teman – teman keluarga besar “Gappala”, keluarga Besar “Perkuray”. Terima kasih untuk kebersamaan rasa kekeluargaan dan secara tidak langsung memberikan dukungan semangat buat penulis.
10. Buat teman – teman “UKDW 2004”, teman - teman “Informatika A”. Terima kasih untuk kebersamaan rasa kekeluargaan dan secara tidak langsung memberikan dukungan semangat buat penulis, Sukses Selalu Buat Kalian Semua.
11. Buat teman – teman yang secara tidak langsung memberi dukungan buat penulis. Terima kasih dukungan doa dan semangat kalian yang membuat penulis semangat dan tidak menyerah.
12. Seluruh staf dan dosen Universitas Kristen Duta Wacana yang telah banyak membantu dan mendidik penulis selama duduk dibangku kuliah.
13. Semua orang yang belum disebutkan dalam ucapan terima kasih tetapi sudah memberikan doa, semangat, dukungan, masukan, inspirasi, dan lain-lain.

Penulis menyadari bahwa Penulisan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca, sehingga suatu saat penulis dapat memberikan karya yang lebih baik lagi.

Akhir kata penulis ingin meminta maaf bila ada kesalahan selama pembuatan Tugas Akhir ini. Semoga ini dapat berguna bagi kita semua. Tuhan Yesus Memberkati.

Yogyakarta, Desember 2010

Penulis

DAFTAR ISI

DAFTAR GAMBAR

ABSTRAKSI

Dari sekian banyak tindakan kejahatan melalui teknologi jaringan, yang paling di takuti adalah *Port Scanning*, *port scanning* merupakan suatu aktivitas awal dari suatu tindak kejahatan pada teknologi jaringan untuk mendapatkan informasi target sebelum melakukan *intrusion* atau penyusupan.

Melalui *port scanning* seorang penyusup bisa melihat fungsi dan cara bertahan sebuah sistem dari berbagai macam *port*. Seorang penyusup bisa mendapatkan akses kedalam sistem melalui *port* yang tidak dilindungi, contohnya scaning bisa digunakan untuk menentukan dimana default SNMP string di buka untuk publik, yang artinya informasi bisa di *extract* untuk digunakan dalam *remote command attack*, oleh sebab itu diperlukan sebuah program *Intrusion Detection System* (IDS) yang dapat mengatasi terjadinya penyusupan tersebut.

Program *Intrusion Detection System* yang dibuat ini di rancang untuk mendeteksi adanya *port scanning* dan merespon secara aktif jika ada *port scanning* atau *intrusion*. Cara kerja program ini adalah dengan melihat komputer yang melakukan *scan* dan secara aktif akan memblokir mesin penyerang agar tidak dapat masuk dan melakukan transaksi dengan *Server* kita, juga dapat berfungsi untuk mengkonfigurasi *port-port* mana saja yang akan dibuka buat publik dan melindungi *port-port* yang dibuka tersebut.

Program *intrusion detection system* yang dibuat ini berbasis konsule, dan berjalan di atas soket *TCP* dan *UDP* untuk mendeteksi *scan port* ke sistem kita. Program ini juga akan bereaksi secara *real-time* (langsung) dengan cara memblokir *IP address* dari *intruder*, dan mencatat data atau informasi dari penyerang melalui syslog, seperti nama system, waktu serangan, IP mesin penyerang, TCP atau UDP *port* tempat serangan dilakukan, kendala yang dialami adalah program IDS yang dibuat ini hanya mampu secara efektif mendeteki adanya *intrusion* sesuai dengan pola atau *patern* dari program serta tools yang digunakan oleh *intruder*.

Bab 1

PENDAHULUAN

1.1 Latar Belakang

Pada dasarnya jaringan yang bebas dari penyusupan merupakan salah satu syarat sebuah jaringan dikatakan aman dan layak digunakan sebagai media pengiriman data. Seiring dengan meningkatnya jumlah pengguna teknologi jaringan, jumlah para penyusup yang ingin menginstrusi jaringan-jaringan tersebut juga meningkat.

Dari sekian banyak tindakan kejahatan melalui teknologi jaringan, yang paling di takuti adalah *Port Scanning*, *port scanning* merupakan suatu aktivitas awal dari suatu tindak kejahatan pada teknologi jaringan untuk mendapatkan informasi target sebelum melakukan *intrusion* atau penyusupan. Dalam melakukan *hacking* jarak jauh (*remote*), langkah paling awal yang harus dilakukan adalah melihat servis yang diberikan oleh *server* atau target di Internet. Dalam konsep jaringan komputer *client-server*, setiap program atau *service* akan menempati sebuah *port* dalam tatanan protokol TCP (*Transmission Control Protocol*). Melalui *port scanning* seorang penyusup bisa melihat fungsi dan cara bertahan sebuah system dari berbagai macam *port*. Seorang penyusup bisa mendapatkan akses kedalam sistem melalui *port* yang tidak dilindungi, contohnya scaning bisa digunakan untuk menentukan dimana default SNMP string di buka untuk public, yang artinya informasi bisa di extract untuk digunakan dalam *remote command attack*.

Port yang terbuka untuk publik mempunyai resiko terkait dengan *exploit* oleh karena itu perlu dikelola port mana yang perlu dibuka dan yang ditutup untuk mengurangi resiko terhadap *exploit*. Ada beberapa *utility* atau *tools* yang bisa dipakai untuk melakukan diagnosa terhadap sistem service dan *port* kita, *utility* atau *tools* 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. Untuk mendapatkan akses ke *host*, penyusup harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila penyusup sudah mengetahui bahwa host menjalankan proses ftp server, penyusup dapat menggunakan kelemahan-kelemahan yang ada pada ftp server untuk mendapatkan akses. Dari bagian ini kita dapat mengambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi.

Sehingga dibutuhkan peralatan keamanan komputer maupun software yang memonitor jaringan, aktifitas sistem, dari serangan atau keadaan yang tidak diinginkan berupa dan dapat bereaksi secara *real time* untuk menghentikan aktifitas tersebut.

1.2 Rumusan Masalah

Berdasarkan uraian pada Sub Bab 1. maka dapat dibuat suatu perumusan masalah, dibutuhkan suatu program bantu untuk mendeteksi adanya penyusupan melalui *scan port,* yang dapat menahan dan mendeteksi adanya serangan penyerangan dan penyusupan melalui *port* yang dibuka untuk publik, bahkan jika mungkin secara *real time* menangkal serangan atau aktifitas tersebut sesegera mungkin. Berdasarkan hal tersebut dapat dirumuskan permasalahan sebagai berikut:

a. Apakah program bantu yang dibuat penulis untuk mendeteksi serangan tersebut dapat bekerja secara efektif untuk mendeteksi penyusupan?
b. Bagaimana cara mendeteksi *intrusion* atau penyusupan yang masuk melalui *Port* dalam jaringan ?
c. Apakah program bantu yang dibuat penulis dapat memberikan solusi yang cepat bila terjadi *intrusion* atau penyusupan?

1.3 Batasan Masalah

Program yang dibuat mempunyai batasan masalah sebagai berikut :

1. Sistem ini bekerja pada *Port* TCP dan UDP.
2. Intrusi atau penyerangan pada jaringan terbatas pada *scanning port* pada port yang terbuka.
3. Sistem ini hanya digunakan untuk menganalisis beberapa jenis port scanning yaitu : *TCPconnect scan, TCP SYN scan, TCP FIN scan, TCP Xmas Tree scan, TCP Null scan, TCP ACK scan, TCP Windows scan, TCP RPC scan*.
4. Pembahasannya meliputi identifikasi paket data yang dikirim, tes konfigurasi dan kinerja jaringan, serta analisa sistem.

1.4 Tujuan Penulisan

Adapun Tujuan penelitian dalam tugas akhir ini adalah:

1. Mengerti dan memahami cara kerja dan dari sebuah *IDS (Intrusion Detection System) firewall* untuk pengamanan port pada sebuah jaringan.
2. Kostumisasi program aplikasi *IDS firewall* untuk pengamanan *port* pada *Server*.
3. Membantu administrator untuk mencegah terjadinya penyerangan.
4. Membuat konfigurasi utama dari aplikasi *IDS firewall,* dimana disini akan dilakukan pengesetan port mana saja yang perlu dimonitor, dan respond apa yang harus dilakukan ke mesin yang melakukan *port scanning*. Dan memasukan semua *IP address* di LAN (*Local Area Network*) yang selalu diabaikan oleh aplikasi ini.

1.5 Metode atau Pendekatan

Metode yang digunakan dalam melakukan penelitian adalah:

a) Studi Pustaka

Metode penelitian ini digunakan dalam pengumpulan informasi dari buku, jurnal, artikel maupun sumber dari internet yang terkait dengan penentuan kebijakan, pembangunan aplikasi *firewall*, pengkombinasian *firewall* dan *Intrusion Detection System*, serta jaringan komputer untuk mendukung penelitian.

b.) Diskusi dan Konsultasi

Metode ini dilakukan dengan dosen maupun orang yang kompeten di bidang jaringan agar dapat menjelaskan mengenai metode yang akan diteliti.

1.6 Sistematika Penulisan

Penulisan tugas akhir ini disusun dalam 5 (lima) bab dengan rincian sebagai berikut :

Bab I Pendahuluan, dalam Bab ini menguraikan latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, metodologi, dan sistematika penyusunan tugas akhir.

Bab II Tinjauan Pustaka, dalam Bab ini memperkuat gagasan-gagasan yang muncul dengan memberikan landasan teori akurat dari berbagai sumber dan konsep-konsep dasar dalam memecahkan masalah penyusupan melalui *Port*. Pembahasan dalam bab ini adalah teori yang berkaitan dengan konsep keamanan jaringan, penyusupan melalui *Port* dan cara mencegah penyusupan, dan rencana penelitian.

Bab III Perancangan Sistem, Pada Bab ini akan berisi Persiapan, perencanaan, perancangan dari pembuatan program bantu *Intrusion Detection System (IDS) firewall*, *hardware* dan *software* yang dibutuhkan untuk pembuatan

aplikasi *IDS Firewal* untuk membangun jaringan yang aman dan optimal. Dan Jalannya penelitian akan dijabarkan beserta skenario atau cara analisis yang diterapkan.

Bab IV Implementasi dan Analisis Sistem, Pada Bab ini h akan lebih banyak berisi implementasi *Intrusion detection system* pada jaringan, analisa intrusi yang masuk, cara kerja program bantu berupa *Intrusion Detection System (IDS) firewall* dalam penanggulangan intrusi, hasil penelitian serta kelebihan dan kekurangan dari program bantu *IDS Firewall* yang diterapkan.

Bab V Penutup, merupakan Bab terakhir dari Penulisan Tugas Akhir, pada Bab ini berisi Kesimpulan dan saran dari penulis.

Selain berisi bab-bab utama tersebut, skripsi ini juga dilengkapi dengan Intisari, Kata Pengantar, Daftar Isi, Daftar Tabel, Daftar Gambar, Daftar Pustaka dan Lampiran.

Bab 5
KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang dapat diambil dari pengerjaan Tugas Akhir. Selain itu juga dituliskan saran-saran yang dapat dipergunakan sebagai pertimbangan untuk pengembangan Tugas Akhir kedepanya .

5.1 Kesimpulan

Setelah melakukan analisis dan implementasi berdasarkan pembahasan dari bab-bab sebelumnya, dapat disimpulkan sebagai berikut :

1. *Patern* atau pola yang digunakan oleh program ini berfungsi dengan baik untuk melakukan deteksi *intrusion* bila *intruder* menggunakan *tools* Nmap untuk melakukan *intrusion*.
2. *Intrusion* atau penyusupan dapat terdeteksi dan dicegah secara *efektif* bila *packet data* yang dikirim sesuai dengan *patern* dari program yang dibuat, dan *tools* yang digunakan oleh *intruder*.
3. Program ini dapat bekerja dengan baik, bila instalasi *package – package* pada linux dan konfigurasi utama dari komponen pendeteksian *Port Scan* tidak ada *error* .

5.2 Saran

Penulis menyadari bahwa Program yang dibuat ini masih terdapat banyak kekurangan, karena keterbatasan waktu dan sarana. Saran-saran yang dapat diberikan bagi yang ingin mendalami lebih lanjut program ini antara lain:

1. Untuk menghasilkan sebuah program pendeteksian yang baik, sebaiknya disesuaikan dengan perkembangan tipe *intrusion* yang ada pada setiap *protokol*.
2. Untuk mempermudah adminstrator dalam menggunakan program ini disarankan untuk membuat sebuah sistem berbasis web sederhana, menggunakan PHP.
3. Perlunya dilakukan pengujian pada jaringan dengan *traffic* yang sangat tinggi sehingga kinerja dari program bisa dapat terukur, tidak hanya *fungsionalitasnya* saja yang mampu mendeteksi penyusupan.

DAFTAR PUSTAKA

Belovin, S. and Cheswick, W (1994). *Network Firewalls*. IEEE Communications Magazine.

Chapman , D. Brent. *Network (In)Security Through IP Packet Filtering* September, 1992.

Cukier, Michel: *Quantifying Computer Security;* University of Maryland. 2005

Defense Advanced Research Projects Agency (DARPA). RFC793 – Transmission Control Protocol. 1981: http://www.faqs.org/rfcs/rfc793.html.

Dony, A. (2007). *Intrusion Detection System, Sistem Pendeteksi Penyusup Pada Jaringan Komputer*, Penerbit Andi, Yogyakarta.

Gerhard, Mourani. *Securing and Optimizing Linux : Red Hat Edition,* june 2000

Gordon "Fyordor" Lyon. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, 3rd, Zero Day, Edition* . Insecure.com LLC. 2008.

Grennan, Mark. *Firewalling and Proxy Server HOWTO*.

Lee, C.Bailey. Roedel Chris. S, Elena : *Detection and Characterization of Port Scan Attacks* : Jurnal

Mann, Scott and L . Mitchell, Ellen. *Linux System Security.*

Postel, J. RFC768, User Datagram Protocol. http://www.faqs.org/rfcs/rfc768.html.

Postel, Jon. *Internet Protocol* , RFC 791, September 1981.

Postel, Jon. *Transmission control Protocol*, RFC 793, September 1981.

Purbo, Onno W., Wiharjito, Tony., Keamanan Jaringan Internet, Elex Media Komputindo, 2000.

Purbo, Onno W., TCP/IP : Standar, Desain, dan Implementasi., Elex Media Komputindo, 1998.

Rahardjo, Budi : *Intrusion detection System*. 2006.

Rebecca Bace, "*An Introduction To Instrussion Detection And Assesment*", http://www.SecurityFocus.com, 2004.

Roger Christopher "*Port Scanning, Techniques and the Defense Against Them*" (October 5, 2001)

Semeria, Chuck *: Internet Firewalls and Security.* (1996)

Stallings, William (1999). *CRYPTOGRAPHY AND NETWORK SECURITY, principle and practice*: *second edition*. Prentice-Hall,Inc., New Jersey.

S. Kent., R.Atkinson., *Security Architecture for the Internet Protocol*,RFC 2401, November 1998.

S. Kent., R. Atkinson., *IP Authentication Header*, RFC 2402, November 1998.

Wack, John. *Packet Filtering Firewall.*

Ziegler, L.Robert. *Linux Firewalls*, November, 1999.