ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN MAIL REPORT

(Studi Kasus : PT. Wahana Lintas Nusa Persada)

SKRIPSI

disusun oleh

Duwi Haryanto

10.11.3719

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014

ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN EMAIL REPORT

(Studi Kasus : PT. Wahana Lintas Nusa Persada)

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Duwi Haryanto

10.11.3719

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2014

PERSETUJUAN

SKRIPSI

ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN MAIL REPORT

(Studi Kasus : PT. Wahana Lintas Nusa Persada)

yang dipersiapkan dan disusun oleh

Duwi Haryanto

10.11.3719

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 3 Agustus 2013

Dosen Pembimbing,

Sudarmawan, MT
NIK. 190302035

PENGESAHAN

SKRIPSI

ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN MAIL REPORT

(Studi Kasus : PT. Wahana Lintas Nusa Persada)

yang dipersiapkan dan disusun oleh

Duwi Haryanto

10.11.3719

telah dipertahankan di depan Dewan Penguji
pada tanggal 6 Maret 2014

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Sudarmawan, MT **NIK. 190302035**	
Andi Sunyoto, M.Kom **NIK. 190302052**	
Dony Ariyus, S.S, M.Kom **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 7 Maret 2014

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan hasil karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 7 Maret 2014

Duwi haryanto
10.11.3719

MOTTO

“KAU MENCIPTAKAN SEMESTAMU, DISETIAP LANGKAHMU”

“ORANG SUSKSES ADALAH ORANG YANG MELAKUKAN SESUATU KARENA MEMANG HARUS DILAKUKAN MESKIPUN ITU TIDAK DISUKAINYA”

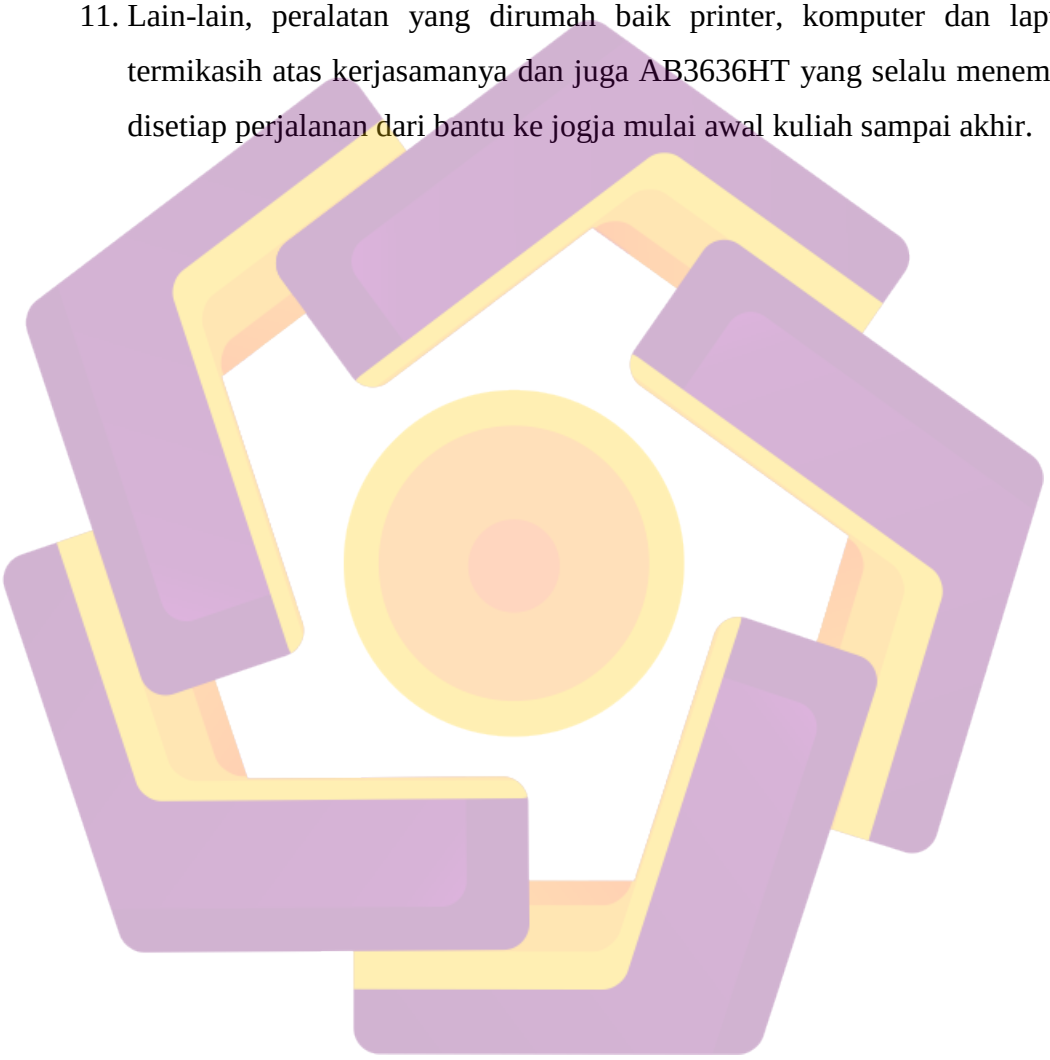
“INVESTASI YANG PALING MENGUNTUNGKAN ADALAH BELAJAR”

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Kedua orang tua saya, Bapak MURDIYONO dan Ibu SARJIYEM yang selalu mendidik, membimbing, melatih dan mengajarkan hal yang baik-baik kepada saya serta memberikan doa dan dukungan dalam menyelesaikan skripsi ini.
2. Kakakku ARIS WIDIYANTO yang telah memfasilitasi saya peralatan yang dibutuhkan serta semangat dan dukunganya untuk menyelesaikan skripsi ini sesuai dengan target yang telah saya tentukan.
3. Adikku TITIK WULANDARI yang telah memberikan semangat dan dukunganya untuk menyelesaikkan skripsi ini tepat waktu.
4. Teman kumpul sekaligus sahabat, WAHID HARTOMO,WYLDAN CANDRA A, NOVENTA PUNGKI R, RIDHO ARJI H, ARIFIN, MARZUQI DWI, BAMBANG JATI P, RUDI Y yang selalu kumpul dari semester 1 sampai 7, sehat dan sukses selalu buat kalian.
5. Teman seperjuangan ERWIN, ANGGI, ARDHA, CICI, PITI, TITA, RANDI, FIKRI,AYYAS, YUSRON,IQMAL,PARSIMIN, KOKO, ARIFIN, RIDHO, AZHARI dan GINA pengalaman membuat event bersama kalian tidak akan mudah terlupakan, sukses dan sehat selalu buat kalian.
6. Keluarga besar S1-TI-03, saya bangga menjadi penghuninya, yang membuat kuliah di STMIK AMIKOM Yogyakarta menjadi menyenangkan.
7. Keluarga besar HMJTI (Himpunan Mahasiswa Teknik Informatika) STMIK AMIKOM Yogyakarta, terimakasih atas pengalaman keorganisasiannya dan ilmu tambahannya selama ini, membuat kuliah di STMIK AMIKOM menjadi menantang dan tidak monoton.
8. Kampus tercinta STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmu dan pengalaman dalam menjalani kehidupan menjadi lebih baik dan baik lagi.

9. Warga FMI (Forum Mikrotik Indonesia) yang telah memberikan banyak referensi mengenai tutorial-tutorial mikrotiknya.
10. PT. Wahana Lintas Nusa Persada (WLAN) Yogyakarta yang telah memberikan izin kepada penulis untuk melakukan observasi dan penelitian.
11. Lain-lain, peralatan yang dirumah baik printer, komputer dan laptop termikasih atas kerjasamanya dan juga AB3636HT yang selalu menemani disetiap perjalanan dari bantu ke jogja mulai awal kuliah sampai akhir.



KATA PENGANTAR

Assalamualaikum Wr. Wb.

Segala puji syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan segala nikmat-Nya yang tiada terkira sehingga penulis mampu menyelesaikan skripsi yang berjudul "ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN EMAIL REPORT (Studi kasus: PT. Wahana Lintas Nusa Persada)." Dapat selesai sesuai dengan target yang telah direncanakan.

Skripsi ini disusun guna memenuhi salah satu persyaratan dalam rangka menyelesaikan pendidikan pada program Strata satu (S1) pada Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM " Yogyakarta.

Dalam menyusun skripsi ini penyusun banyak mendapatkan bantuan dari beberapa pihak. Untuk itu penyusun menyampaikan rasa hormat dan terima kasih kepada :

1 Prof. Dr. M. Suyanto, MM., selaku ketua STMIK AMIKOM Yogyakarta.
2 Sudarmawan, MT. Selaku Ketua Jurusan S1-TI dan sekaligus dosen pembimbing yang telah membimbing dan memberikan masukkan yang membangun.
3 Ir. Syafiq Iqbal selaku direktur PT.Wahana Lintas Nusa Persada (WLAN) yang telah memberikan izin untuk penelitian.
4 Dody, Yogi, Vani dan Kaka beserta seluruh karyawan PT.Wahana Lintas Nusa Persada Yogyakarta yang telah membantu memberi masukkan dan saran serta ilmunya dalam mengerjakan skripsi ini.
5 Tim pemguji dan dosen STMIK AMIKOM Yogyakarta yang selama masa study telah memberikan ilmu yang bermanfaat bagi penulis.
6 Keluarga Besar HMJTI STMIK AMIKOM Yogyakrta yang telah memberikan dukungannya selama ini.

7 Teman-teman S1-TI-03 angkatan 2010 dan semua pihak yang membantu kelancaran penyusunan skripsi yang tidak dapat penulis tulis satu persatu.

Penulis menyadari masih ada kekurangan dari penyusunan laporan skripsi ini karena keerbatasan penulis dalam hal pengetahuan. Kritik dan saran yang bersifat membangun guna mencapai kesempurnaan skripsi ini selalu penulis harapkan sehingga dapat bermanfaat bagi penulis serta pihak-pihak yang membutuhkan. Amin

Wassalamualaikum Wr. Wb.

Yogyakarta, 7 Maret 2014

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

PT. Wahana Lintas Persada yang merupakan salah satu *Internet Service Provider* (ISP) menyadari bahwa semakin bertambahnya pelanggan, semakin meningkatnya node pada jaringan wahana yang harus selalu dimonitoring guna meningkatkan layanan *technical support* yang selalu *stanby* 24 jam. Kebutuhan akan sistem keamanan jaringan menjadi salah satu aspek yang perlu diperhatikan untuk meningkatkan layanan kepada pelanggan.

Membangun sistem peringatan dini atau IDS (*Intrusion Detection System*) merupakan salah satu solusi pemecahan masalah tersebut. Sistem ini bekerja dengan cara mendeteksi adanya serangan dan memberikan peringatan (*alert*) kepada administrator jaringan apabila terjadi serangan pada jaringan, selain itu IDS juga dapat digunakan untuk melakukan monitoring jaringan. Reactive IDS adalah IDS yang dapat melakukan *auto respon* berupa tindakan pencegahan saat terjadi serangan dan menampilkan peringatan serta mengirim *report* email.

Sistem Reactive IDS ini menggunakan mikrotikOS dan tool winbox dan beberapa tools untuk melakukan percobaan penyerangan terhadap jaringan. Pengujian sistem ini dilakukan dengan menggunakan beberapa jenis serangan ke jaringan dan pengujian fungsionalitas sistem adalah dengan melakukan cek peringatan (*alert*) dan report berupa email yang berisi IP penyerang untuk dikirim ke email administrator, guna membantu administrator *mobile* dalam melakukan monitoring jaringan.

Kata Kunci : Reactive IDS, winbox, ftp bruteforce, ICMP Flood, SSH bruteforce.

ABSTRACT

PT. Wahana Lintas Nusa Persada which is one of the Internet Service Providers (ISPs) realize that the increasing customers, increasing network node on a vehicle that should always be monitored in order to improve technical support services are always standby 24 hours. The need for network security systems into one of the aspects that need to be considered to improve the service to customers.

Build an early warning system or IDS (Intrusion Detection System) is one of the problem-solving solutions. This system works by detecting the presence of attacks and provides a warning (alert) to the network administrator in case of an attack on the network, in addition to the IDS can also be used to perform network monitoring. IDS is a reactive IDS can perform auto response form precautions during the attack and displays a warning and sends an email report.

Reactive IDS system uses mikrotikOS and Winbox tool and some tools to conduct attacks against the network experiments. System test is performed using several types of attacks to the network and testing the functionality of the system is to do a check warning (alert) and a report in the form of an email containing the attacker's IP to be sent to the email administrator, to assist administrators in monitoring mobile networks.

***Keywords**: Reactive IDS, Winbox, ftp bruteforce, ICMP Flood, SSH bruteforce.*