Institut Teknologi Nasional Malang

SKRIPSI – KOMPUTER

ANILISIS KINERJA SISTEM PENCEGAHAN PENYUSUPAN JARINGAN MENGGUNAKAN SNORT IDS DAN HONEYD PADA WINDOWS

Usama
NIM 1512523

Dosen Pembimbing
Dr. F Yudi Limpraptono, ST., MT
Sotyohadi, ST., MT

PROGRAM STUDI TEKNIK ELEKTRO S-1
Fakultas Teknologi Industri
Institut Teknologi Nasional Malang
September 2019

Institut Teknologi Nasional Malang

SKRIPSI – TEKNIK KOMPUTER

ANALISIS KINERJA SISTEM PENCEGAHAN PENYUSUPAN JARINGAN MENGGUNAKAN SNORT IDS DAN HONEYD PADA WINDOWS

Usama
NIM 1512523

Dosen Pembimbing
Dr. F. Yudi Limpraptono, ST, MT
Sotyohadi, ST, MT

PROGRAM STUDI TEKNIK ELEKTRO S-1
Fakultas Teknologi Industri
Institut Teknologi Nasional Malang
September 2019

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCA SARJANA MAGISTER TEKNIK

PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG

Kampus I Jl. Bendungan Sigura-gura No 2 Telp. (0341) 551431 (Hunting) Fax. (0341) 553015 Malang 65145
Kampus II Jl. Raya Karanglo. Km 2 Telp. (0341) 417636. Fax. (0341) 417634 Malang

LEMBAR PERSETUJUAN PERBAIKAN SKRIPSI

Nama Mahasiswa	: Usama
NIM	: 1512523
Program Studi	: Teknik Elektro S-1
Peminatan	: Teknik Komputer
Masa Bimbingan	: Semester Genap 2018-2019
Judul Skripsi	: **Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd pada Windows**

Tanggal	Uraian	Paraf
Penguji I 22-07-2019		
Penguji II 22-07-2019	Analis Kinerja Sistem	

Disetujui,

Dosen Penguji I

M. Ibrahim Ashari, ST, MT
NIP.P. 1030100358

Dosen Penguji II

Dr. Eng. I Komang Somawirata, ST, MT
NIP.P. 1030100361

Mengetahui,

Dosen Pembimbing I

Dr. F Yudi Limpraptono. ST, MT
NIP.Y. 1039500274

Dosen Pembimbing II

Sotyohadi, ST, MT
NIP.Y. 1039700309

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

BERITA ACARA RAPAT PERSETUJUAN JUDUL/PROPOSAL SKRIPSI
PROGRAM STUDI TEKNIK ELEKTRO S-1
SEMESTER GENAP 2018/2019

Peminatan : T.

Tanggal :

1	NIM	15.17.523
2	Nama	Usamah
3	Judul yang diajukan	
	Disetujui/Ditolak*	
4	Catatan: Diskusi dg pembimbing.	
5	Pembimbing yang diusulkan: 1. F. Yudi 2. Satyo Hadi	

Menyetujui
Koordinator Bidang Keahlian

( )

* : Coret yang tidak perlu

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALAN
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

Nama : Usama
NIM : 1512523
Program Studi : Teknik Elektro S-1
Peminatan : Teknik Komputer
Masa Bimbingan : Semester Genap 2018/2019
Judul : ANALISIS KINERJA SISTEM PENCEGAHAN PENYUSUPAN JARINGAN MENGGUNAKAN SNORT IDS DAN HONEYD PADA WINDOWS

Dipertahankan dihadapan Majelis Penguji Skripsi Strata Satu (S-1) pada :
Hari : Senin
Tanggal : 22 juli 2019
Nilai : 80 (A)

Panitia Ujian Skripsi

Ketua Majelis Penguji

Dr. Irrine Budi Sulistiawati, ST, MT
NIP. 197706152005012002

Sekretaris Majelis Penguji

Dr. Eng. I Komang Somawirata, ST, MT
NIP.P. 1030100361

Anggota Penguji

Penguji I

M. Ibrahim Ashari, ST, MT
NIP.P. 1030100358

Penguji II

Dr. Eng. I Komang Somawirata, ST, MT
NIP.P. 1030100361

JURUSAN TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

BERITA ACARA SEMINAR HASIL SKRIPSI
PROGRAM STUDI TEKNIK ELEKTRO S-1
Semester Genap Tahun Akademik 2018/2019

PEMINATAN	Teknik Komputer

1.	Nama Mahasiswa	Usama		NIM	1512523
2.	Keterangan Pelaksanaan	Tanggal	Waktu		Tempat
3.	Judul Skripsi yang Diseminarkan Mahasiswa	Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan SNORT IDS dan HONEYD Pada Windows			

4. Nilai :

No	Keterangan	Nilai (dalam angka)
1)	Penampilan	
2)	Presentasi	
3)	Penguasaan Materi Skripsi	
4)	Penguasaan Materi Penunjang	
Rata-Rata		90

5. Berdasarkan Seminar Hasil hari ini maka skripsi ini:

Layak/Tidak Layak*)

untuk mengikuti Ujian Komprehensif

Mengetahui,	Disetujui,
Ketua Program Studi Teknik Elektro S-1	Dosen Pengamat
Dr. Irrine Budi Sulistiawati, ST., MT.	(.....)
NIP. 19770615 200501 2 002	

*) Coret salah satu

Form S-3c

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

BERITA ACARA SEMINAR PROGRESS SKRIPSI
PROGRAM STUDI TEKNIK ELEKTRO S-1
Semester Genap Tahun Akademik 2018/2019

PEMINATAN	Teknik Komputer

1.	Nama Mahasiswa	Usama		NIM	1512523
2.	Keterangan	Tanggal	Waktu		Tempat
	Pelaksanaan	6/4/2019	#.8.30		III. 1.3
3.	Judul Skripsi yang Diseminarkan Mahasiswa	Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan SNORT IDS dan HONEYD Pada Windows			
4.	Progress yang dilalui	- Konfig SNORT - Konfig RULES. - Rancangan Penyerangan (Attack).			
5.	Hambatan	- Mencari Konfig IDS di Windows.			
6.	Saran dari dosen: - Konfig IDS → segera - IDS + firewall → IPS. - Bagi jika hasilnya sudah dicetak satu pasar. segera dicoba utk attacker!				

Disetujui,
Dosen Pembimbing

Pembimbing I	Pembimbing II
Dr. F. Yudi Limpraptono, ST., MT.	Sotyohadi, ST., MT.

Mengetahui,
Ketua Program Studi Teknik Elektro S-1

Dr. Irrine Budi Sulistiawati, ST., MT.
NIP. 19770615 200501 2 002

Form S-3c

JURUSAN TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

BERITA ACARA SEMINAR PROPOSAL SKRIPSI
PROGRAM STUDI TEKNIK ELEKTRO S-1
Semester Genap Tahun Akademik 2018/2019

PEMINATAN	Teknik Komputer

1.	Nama Mahasiswa	Usama		NIM	1512523
2.	Keterangan	Tanggal	Waktu		Tempat
	Pelaksanaan	13/3/2019	13.00		III. 1. 3
3.	Judul Proposal yang Diseminarkan Mahasiswa	Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan SNORT IDS dan HONEYD Pada Lab. Jaringan Komputer			
4.	Perubahan Judul yang Disarankan (bila ada)	Analisis kinerja sistem Pencegahan Penyusupan Jaringan Menggunakan SNORT IDS dan HONEYD Pada Sistem Windows			
5.	Masukan yang harus ditambahkan dalan skripsi: – Latar belakang masalah lebih diperdalam utk mendukung judul. – Khususnya harus disertai kips tesis tentang sistem windows.				

Persetujuan Judul Skripsi

Disetujui, Dosen Keahlian I	Disetujui, Dosen Keahlian II
(.....)	(.....)

Disetujui,
Dosen Pembimbing

Pembimbing I	Pembimbing II
Dr. F. Yudi Limpraptono, ST., MT.	Sotyohadi, ST., MT.

Mengetahui,
Ketua Program Studi Teknik Elektro S-1

Dr. Irrine Budi Sulistiawati, ST., MT.
NIP. 19770615 200501 2 002

Form S-3c

LEMBAR PENGESAHAN

ANALISIS KINERJA SISTEM PENCEGAHAN PENYUSUPAN JARINGAN MENGGUNAKAN SNORT IDS DAN HONEYD PADA WINDOWS

SKRIPSI

Disusun dan diajukan untuk melengkapi dan memenuhi persyaratan guna mencapai gelar Sarjana Teknik

Disusun oleh:

USAMA
NIM : 1512523

Diperiksa dan disetujui:

Dosen Pembimbing I	Dosen Pembimbing II
Dr. F Yudi Limpraptono, ST. MT	**Sotyohadi, ST. MT**
NIP.Y. 1039500274	**NIP.Y. 1039700309**

Mengetahui,
Ketua Program Studi Teknik Elektro S-1

Dr. Eng. I Komang Somawirata, ST. MT
NIP. P. 1030100361

PROGRAM STUDI TEKNIK ELEKTRO S-1
PEMINATAN TEKNIK KOMPUTER
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2019

ANALISIS KINERJA SISTEM PENCEGAHAN PENYUSUPAN JARINGAN MENGGUNAKAN SNORT IDS DAN HONEYD PADA WINDOWS

Usama
YudiLimpraptono
Sotyohadi
usamaassegaf@gmail.com

ABSTRAK

Snort sebuah perangkat lunak yang open source yang mendukung semua sistem operasi seperti linux,window maupun solaris, snort merupakan sistem pendeteksi yang bisa dikembangkan menjadi sistem pencegahan dengan cara mengkombinasikan IDS dan firewall dengan menjalankan snort pada mode inline.. snort sangat membantu para administrator jaringan untuk meningkatkan sistem keamanan jaringan, karena bisa dikonfigurasi sesuai keinginan. Snort juga bisa dikonfigurasi untuk meyimpan outputnya ke database log snort, yang setiap saat bisa dilihat paket yang dianggap sebuah penyusupan. Pada skripsi ini penyusun akan mengkonfigurasi snort pada sistem operasi windows 7, kenapa memilih windows karena pada penelitian sebelumnya kebanyakan menggunakan sistem operasi linux. Disini penulis mengkonfigurasi snort sebagai sistem yang dapat mendeteksi dan mencegah paket yang di identifikasi sebuah serangan, jika terdeteksi sebagai sebuah serangan maka sistem akan mengirimkan alert untuk memblocking sehingga paket tersebut tidak terkirim ke alamat korban, namun snort akan mencatat disebuah log databasenya. Ketika Snort NIPS(Network Intrusion Prevention System) aktif, serangan seperti Ping Of death, seranga DOS dan Port Scanning bisa dicegah.

Kata Kunci : Intrusion Detection System, Windows,Snort dan Rules Snort

PERFORMANCE ANALYSIS OF NETWORK INTRUSION PREVENTION SYSTEM USING SNORT IDS AND HONEYD ON WINDOWS

Usama
YudiLimpraptono
Sotyohadi
usamaassegaf@gmail.com

ABSTRACT

Snort, an open source software that supports all operating systems such as Linux, Windows and Solaris, Snort is an Intrusion Detection System (IDS) detection system that can be developed into an Intrusion Prevention System (IPS) prevention system by combining IDS and a firewall by running snort in inline mode too. some network administrators use this software. snort is very useful for network administrators to improve the network security system because it can be configured as desired. Snort can be configured to save its output to the Snort log database which can be seen at any time which packages are considered an attack. In this thesis the author will configure the snort on the Windows 7 operating system, why choose Windows because in previous studies mostly use the Linux operating system. Here the author configures it as a prevention system that whenever a package is identified as an attack or suspicious it will be rejected. Snort works with its rules that will match the package in the snort's rules database. if it is in the form of an attack the system will send an alert to block it so that the packet is not forwarded to the victim but the snort will record it in its database log. When Snort NIPS is active, attacks like Ping of death, DOS attacks and Port Scanning are prevented

Keywords : Intrusion Detection System, Windows,Snort and Rules Snort.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL