



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 (Punting) Fax. (0341) 553015 Malang 65145
Kampus II Jl. Raya Karanglo Km 2 Telp. (0341) 471636 Fax. (0341) 471634 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	Analisis Kinerja Sistem	

Disetujui,

Dosen Penguji I

M. Ibrahim Ashari, ST, MT
NIPP. 1030100358

Dosen Penguji II

Dr. Eng. I Komang Somawirata, ST, MT
NIPP. 1030100361

Mengetahui,

Dosen Pembimbing I

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

Dosen Pembimbing II

Sotyohadi, ST, MT
NIP.Y. 1039700309






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

Peminatan : T.

Tanggal :

1	NIM	15172523
2	Nama	Uhamy
3	Judul yang diajukan	
Disetujui/Ditolak*		
4	Catatan:	Drs kea dg pembahj.
5	Pembimbing yang diusulkan:	1. F. Yuda 2. Satyo Hadi
Menyetujui Koordinator Bidang Keahlian 		

*: Coret yang tidak perlu



PT BNI (PERSERO) MALANG
BANK NIAGA MALANG

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG

FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK

Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 651431 (Hunting), Fax. (0341) 653015 Malang 65145
Kampus II : Jl. Raya Kerangle, 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
MENGUNAKAN 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





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 :	<table border="1"><thead><tr><th>No</th><th>Keterangan</th><th>Nilai (dalam angka)</th></tr></thead><tbody><tr><td>1)</td><td>Penampilan</td><td></td></tr><tr><td>2)</td><td>Presentasi</td><td></td></tr><tr><td>3)</td><td>Penguasaan Materi Skripsi</td><td></td></tr><tr><td>4)</td><td>Penguasaan Materi Penunjang</td><td></td></tr><tr><td colspan="2">Rata-Rata</td><td>90</td></tr></tbody></table>			No	Keterangan	Nilai (dalam angka)	1)	Penampilan		2)	Presentasi		3)	Penguasaan Materi Skripsi		4)	Penguasaan Materi Penunjang		Rata-Rata		90
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, Ketua Program Studi Teknik Elektro S-1  Dr. Irine Budi Sulistiawati, ST., MT. NIP. 19770615 200501 2 002		Disetujui, Dosen Pengamat 																				

*) 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
	Keterangan	Tanggal	Waktu	Tempat
2.	Pelaksanaan	6/4/2019	# 8.30	11.1.3
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 Perancangan (Attach)		
5.	Hambatan	- Mencari Konfig IDS di windows		
6.	Saran dari dosen:	- Konfig IDS → segera - IDS + Firewall → IPS - Jika sudah hasil dicatat satu place segera dicoba utlu attacker		
Disetujui, Dosen Pembimbing				
Pembimbing I		Pembimbing II		
 Dr. F. Yudi Limpraptono, ST., MT.		 Sotyo Hadi, ST., MT.		
Mengetahui, Ketua Program Studi Teknik Elektro S-1				
 Dr. Irme Budi Sulistiawati, ST., MT. NIP. 19770615 200501 2 002				

Form S-3c



**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 Pelaksanaan	Tanggal	Waktu	Tempat
		13/3/2019	12.00	111.1.3
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		
Masukan yang harus ditambahkan dalam skripsi:				
5.	<p>latar belakang masalah lebih dipertajam dan mendetail judul khususnya harus disertai hipotesis tentang sistem windows.</p>			
Persetujuan Judul Skripsi				
Disetujui, Dosen Keahlian I		Disetujui, Dosen Keahlian II		
Disetujui, Dosen Pembimbing				
Pembimbing I		Pembimbing II		
 Dr. F. Yudi Limpraptono, ST., MT.		 Sotyoahadi, ST., MT.		
Mengetahui, Ketua Program Studi Teknik Elektro S-1				
 Dr. Irma Budi Sulistiawati, ST., MT. NIP. 19770615 200501 2 002				

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
NIP.Y. 1039500274


Sotvohadi, ST, MT
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 menyimpan 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 diidentifikasi sebuah serangan, jika terdeteksi sebagai sebuah serangan maka sistem akan mengirimkan alert untuk memblockng 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

LEMBAR PENGESAHAN	i
ABSTRAK	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR	16
DAFTAR TABEL.....	16
BAB I	
PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	2
1.3 Tujuan.....	2
1.4 Manfaat.....	3
1.5 Batasan	3
1.6 Sistematika Penulisan.....	3
BAB II.....	
KAJIAN PUSTAKA.....	5
2.1 Pengenalan Jaringan Komputer	5
2.1.1 Definisi Jaringan	5
2.1.2 Jenis - Jenis Jaringan.....	5
2.1.3 Komponen Dasar Jaringan	6
2.1.4 Topologi Jaringan	7
2.2 Protokol	10
2.3 Model Referensi OSI	10
2.3.1 layer pada OSI	10
2.3.2 Konsep dan Kegunaan pada Layer	12

2.4	Media Acces Control (MAC) Address	12
2.5	Address Resolution Protocol (ARP)	13
2.6	Ancaman Keamanan Jaringan	13
2.6.1	Prinsip Keamanan Jaringan.....	13
2.6.2	Jenis-Jenis Serangan Terhadap Jaringan.....	14
2.6.2.1	Danial Of Services.....	14
2.6.2.2	ARP Spoofing.....	15
2.6.2.3	Man-in-the-Midle Attacking	16
2.6.2.4	Sniffer.....	16
2.6.2.5	Spamming.....	16
2.6.2.6	Scanning.....	16
2.7	Intrusion Detection System (IDS).....	16
2.7.1	Host Intrusion Detection System	17
2.7.2	Network Intrusion Detection System	17
2.8	Intrusion Prevention System.....	17
2.8.1	Host Intrusion Prevention System (HIPS)	18
2.8.2	Network Intrusion Prevention System (NIPS).....	18
2.9	Sistem Operasi.....	20
2.9.1	Disk Operating System	20
2.9.2	Sistem Operasi Windows 7.....	20
2.10	Snort	21
2.10.1	Paket Sniffer Mode	23
2.10.2	Paket Logger Mode.....	23
2.10.3	Intrusion Detection System.....	23
2.11	Firewall	23
BAB III		

PERANCANGAN SISTEM	25
3.1 Diagram Secara Umum	25
3.1.1 Client Melakukan Penyerangan	25
3.1.2 Sistem Melakukan Penyerangan	25
3.2 Flowchart Sistem	27
3.3 Pemilihan Komponen yang Digunakan oleh Sistem	28
3.4 Konfigurasi Sistem	28
3.5 Konfigurasi Database Snort	28
3.6 Mengkonfigurasi Snort dan Rule Snort	29
3.7 Analisa Sistem Snort Intrusion Detection System	30
3.8 Analisa Sistem Snort Intrusion Prevention System	30
3.9 Perangkat Keras dan Perangkat Lunak yang akan digunakan	31
 BAB IV	
PERANCANGAN SISTEM	33
4.1 Implementasi Sistem.....	33
4.1.1 Batasan Implementasi	34
4.1.2 Hasil Implementasi	34
4.2 Pengujian Intrusion Detection System (IDS).....	34
4.2.1 identifikasi dan Rencana Pengujian Snort Network Intrusion Detection System (NIDS).....	34
4.2.2 Pengujian Ping of Death	34
4.2.3 Pengujian Ping Flood.....	36
4.2.4 Pengujian Port Scanning	38
 BAB V	
PENUTUP.....	41
5.1 Kesimpulan.....	41

5.2	Saran.....	41
-----	------------	----

DAFTAR GAMBAR

Gambar 2.1 Jaringan Client Server	6
Gambar 2.2 Jaringan Peer to Peer	6
Gambar 2.3 Topologi Bus	7
Gambar 2.4 Topologi Ring	8
Gambar 2.5 Topologi Star	9
Gambar 2.6 Cara Kerja Protokol ARP	13
Gambar 2.7 Aplikasi Snort.....	21
Gambar 3.1 Skema Network Intrusion Detection System.....	26
Gambar 3.2 Flowchart Sistem.....	27
Gambar 4.1 Serangan Ping Of Death	35
Gambar 4.2 Snort Mendeteksi Ping Of Death.....	35
Gambar 4.3 Serangan Ping Flood	37
Gambar 4.4 Snort Mendeteksi Ping Flood	37
Gambar 4.5 Serangan Port Scanning.....	39
Gambar 4.6 Snort Mendeteksi Port Scanning	39

DAFTAR TABEL

Tabel 2.1 Karakteristik Topologi Bus	8
Tabel 2.2 Karakteristik Topologi Token Ring	9
Tabel 2.3 Karakteristik Topologi Star	10
Tabel 2.4 Model Referensi OSI	11
Tabel 4.1 Rencana Pengujian Snort Intrusion Detection System	34
Tabel 4.2 Pengujian Ping of Death	36
Tabel 4.3 Pengujian Ping Flood	38
Tabel 4.4 Pengujian Port Scanning	40