



**ANALISIS DAMPAK PENERAPAN INTRUSION PREVENTION SYSTEM (IPS)  
TERHADAP KEAMANAN JARINGAN PADA SISTEM LINUX UBUNTU DAN  
LINUX CENTOS**

**SKRIPSI**

**DUWI GANDA PUTRA**

**161420181**

**Skripsi ini diajukan sebagai syarat untuk memperoleh gelar  
sarjana komputer**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS BINA DARMA**

**PALEMBANG**

**2022**

**HALAMAN PENGESAHAN**

**ANALISIS DAMPAK PENERAPAN *INTRUSION PREVENTION SYSTEM (IPS)* TERHADAP KEAMANAN JARINGAN PADA SISTEM LINUX UBUNTU DAN LINUX CENTOS**

**DUWI GANDA PUTRA**

**161420181**

**Telah diterima sebagai salah satu syarat untuk memperoleh gelar  
Sarjana Komputer pada Program Studi Teknik Informatika**

**Palembang, 31 Maret 2022  
Fakultas Ilmu Komputer  
Universitas Bina Darma  
Dekan,**

**Dosen Pembimbing,**



**Dedy Syamsuar, S.Kom., M.I.T., Ph.D**



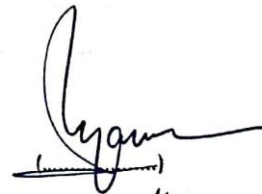
**Dedy Syamsuar, S.Kom., M.I.T., Ph.D**

## HALAMAN PERSETUJUAN

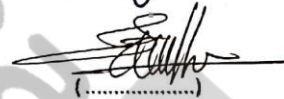
Skripsi Berjudul "ANALISIS DAMPAK PENERAPAN INTRUSION PREVENTION SYSTEM (IPS) TERHADAP KEAMANAN JARINGAN PADA SISTEM LINUX UBUNTU DAN LINUX CENTOS" Oleh "Duwi Ganda Putra", telah dipertahankan di depan komisi penguji pada hari Kamis tanggal 31 Maret 2022.

### Komisi Penguji

1. Ketua : Dedy Syamsuar, S.Kom., M.I.T., Ph.D.



2. Anggota : Zaid Amin, M.Kom., Ph.D.



3. Anggota : Maria Ulfa, M.Kom.



**Mengetahui,**

Program Studi Teknik Informatika  
Fakultas Ilmu Komputer Universitas  
Bina Darma  
Ketua,

Universita Bina  
Darma  
Fakultas Ilmu Komputer

**Alex Wijaya, S.Kom., M.I.T**

## SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Duwi Ganda Putra

Nim : 161420181

Dengan ini menyatakan bahwa :

1. Karya tulis saya (skripsi) adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana) di Universitas Bina Darma atau perguruan tinggi lainnya ;
2. Karya tulis ini murni gagasan, rumusan dan penelitian saya dengan arah dari tim pembimbing ;
3. Didalam karya tulis ini tidak terdapat karya ataupun pendapat yang telah ditulis atau di publikasikan orang lain, kecuali secara tertulis dengan jelas dandiikuti dengan mencantumkan nama pengarang dan memasukan kedalam rujukan ;
4. Saya bersedia tugas skripsi, di cek ke asliannya menggunakan plagiarism checker serta diunggah ke internet, sehingga dapat diakses secara daring ;
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila diperbaiki melakukan penyimpangan atau ketidak benaran dalam pernyataan ini maka saya bersedia menerima sanksi dengan peraturan perundang- undangan yang berlaku ;

Demikian surat ini saya buat agar dapat dipergunakan sebagai mestinya.

Palembang , 14 April 2022

Yang Membuat Pernyataan



Duwi Ganda Putra  
Nim : 161420181

## MOTTO DAN PERSEMBAHAN

### **MOTTO**

*Kerjakan apa yang semestinya menjadi tanggung jawab kamu, jangan sekali-kali kamu menunda dan melalaikannya, sekali saja kamu melalaikannya atau menunda-nunda waktu maka penyeselan lah yang akan kamu dapatkan di kemudian hari.*

### **PERSEMBAHAN**

Alhamdulillah atas rahmat dan hidayah-Nya saya dapat menyelesaikan skripsi ini dengan baik karya ini ku persembahkan untuk :

- ❖ Ibu dan Bapakku, yang telah mendukungku, memotivasi dan mendoakan ku dalam segala hal serta memberikan kasih sayang yang teramat besar yang tak akan mungkin bisa ku balas dengan apapun.
- ❖ Keluarga besarku, kakaku, dan adik-adikku tercinta yang selalu mendukungku.
- ❖ Untuk kekasih ku yang selalu menemaniku berjuang.
- ❖ Teman-teman satu angkatan Teknik Informatika terkhusus kelas IF6D yang selalu saling memberi support dan semangat.

## ABSTRAK

*Peran teknologi dewasa ini semakin meningkat dan dapat ditemukan dalam segala aspek kehidupan. Hal ini menyebabkan banyak kegiatan semakin tergantung dengan teknologi tersebut. Tetapi disisi lain, keamanan teknologi menjadi permasalahan tersendiri dimana dengan berkembangnya ilmu pengetahuan, perangkat hacking dan cracking semakin tersedia dan mudah dioperasikan. Oleh karena itu, pengelola teknologi informasi harus lebih waspada untuk mencegah dan meminimalisir ancaman terhadap jaringan yang kita gunakan. Adapun penelitian ini bertujuan untuk membandingkan tingkat keamanan jaringan dengan penerapan IPS di system Linux Ubutu dan Centos guna melihat tingkat keamanan jaringan mana yang kompetitif terhadap aktifitas yang mengancam pengguna dengan melakukan pelacakan dini terhadap kegiatan-kegiatan yang dapat mengancam keamanan pengguna yang mencurigakan. Untuk itu, penelitian ini menerapkan sebuah metode keamanan yang bernama Intrusion Prevention Sytem (IPS), Dalam metode IPS sendiri untuk memperoleh hasil yang diinginkan peneliti menggabungkan dengan menggunakan teknik firewall sekaligus untuk mengetahui seberapa tinggi tingkat keamaman suatu jaringan ketika dilakukan simulasi penyerangan. Setelah dilakukan pengujian didapatlah hasil bahwa penggunaan sistem keamanan Linux Ubuntu dan CentOS setelah di terapkan IPS ialah, tingkat keamanan Linux Centos lebih efisien dan cepat terhadap pendeteksian dari sebuah ancaman serangan ketimbang system Linux Ubuntu, hasil ini didapat dari setelah melakukakn simulasi penyerangan LinuxCentOS lebih aman di bandingkan Linux Ubuntu, dikarnakan CentOS lebih cepat mendeteksi dan memblock ip attacker ketika terjadi serangan.*

**Kata Kunci :** *Keamanan jaringan, IPS, firewall, sistem operasi linux Ubntu dan CentOS, brute force.*

## ABSTRACT

*The role of technology today is increasing and can be found in all aspects of life. This causes many activities to become increasingly dependent on this technology. But on the other hand, technology security is a problem in itself where with the development of science, hacking and cracking tools are increasingly available and easy to operate. Therefore, information technology managers must be more vigilant to prevent and minimize threats to the network that we use. This study aims to compare the level of network security with the application of IPS on Linux Ubutu and Centos systems in order to see which network security level is competitive against activities that threaten users by conducting early tracking of activities that can threaten the security of suspicious users. For this reason, this study applies a security method called the Intrusion Prevention System (IPS). In the IPS method itself, to obtain the desired results the researchers combine using a firewall technique at the same time to find out how high the security level of a network is when an attack simulation is carried out. After testing, the results showed that the use of the Linux Ubuntu and CentOs security systems after IPS was applied, the security level of Linux Centos was more efficient and faster in detecting an attack threat than the Linux Ubuntu system. compared to Linux Ubuntu, because CentOS is faster at detecting and blocking the attacker's IP when an attack occurs.*

*Keywords : Network security, IPS, firewall, Ubuntu and CentOs linux operating systems, brute force.*

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Segala puji bagi Allah SWT, atas limpahan rahmat serta hidayah-Nya sehingga penulis mampu mengerjakan dan menyelesaikan proses penyusunan skripsi yang merupakan salah satu syarat untuk meraih gelar sarjana komputer di Universitas Bina Darma Palembang.

Penulis menyadari bahwa dalam penyusunan skripsi ini tidak lepas dari adanya kerjasama dan bantuan dari berbagai pihak. Oleh karena itu dengan segenap kerendahan hati pada kesempatan ini penulis mengucapkan banyak terima kasih kepada pihak-pihak berikut :

1. Allah SWT.
2. Kedua Orang Tua saya yang selalu mendoakan saya tanpa henti disetiap sujudnya.
3. Dr. Sunda Ariana, M.Pd., MM., selaku Rektor Universitas Bina Darma
4. Dedy Syamsuar, Ph.D, selaku Dekan sekaligus menjadi sosok pembimbing yang senantiasa selalu peduli dengan penyelesaian skripsi ini.
5. Alex Wijaya, S.Kom, M.I.T, selaku Ketua Program Studi Teknik Informatika.
6. Bapak/Ibu Dosen penguji.
7. Seluruh Dosen serta staff Universitas Bina Darma Palembang.
8. Kakaku Debi Irawan, dan adik-adiku Dika Akbar, Lidia Sari, serta keluargaku yang telah mendoakan dan membantu baik moral maupun materi.



9. Teman – teman dari kelas IFD 2016 terkhusus untuk Qodri Harun Adriyanto, S.Kom terimakasih telah membantu sampai ke tahap ini.
10. Serta kekasihku Riska Aristantia, Amd. Adm Bisnis, yang selalu menemani dan rela mengundurkan wisuda demi tercapai impian bersama untuk wisuda bareng, Terimakasih.

Palembang, 14 April 2022

Penulis,



## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PENGESAHAN .....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PERNYATAAN.....	iv
HALAMAN MOTTO DAN PERSEMBAHAN .....	v
ABSTRAK .....	iii
KATA PENGANTAR.....	vi
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xii
<b>1 BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Perumasan Masalah.....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan dan MafaatPenelitian .....	4
1.4.1 Tujuan Penelitian.....	4
1.4.2 Manfaat Penelitian .....	5
1.5 Waktu Penelitian.....	5
1.6 Sistematika Penulisan .....	5
<b>2 BAB II LANDASAN TEORI .....</b>	<b>8</b>
2.1 Analisis Perbandingan.....	8
2.2 Metode Perbandingan (Studi Komparatif).....	8
2.3 Keamanan Jaringan.....	9
2.3.1 Aspek – aspek Keamanan Jaringan Komputer .....	10
2.3.2 Jenis Ancaman Keamanan Jaringan Komputer .....	12
2.4 <i>Intrusion Prevention System (IPS)</i> .....	14
2.4.1 Jenis – jenis Intrusion Prevention System (IPS).....	15
2.5 Firewall .....	17
2.5.1 Firewall Berbasi Hardware .....	17
2.5.2 Firewall Berbasis Software.....	18
2.5.3 Jenis – jenis firewall.....	18
2.5.4 Cara Kerja Firewall.....	20
2.6 Sistem Operasi Linux.....	22
2.6.1 Linux Ubuntu .....	23
2.6.2 Linux CentOs.....	23
2.6.3 RedHat .....	24
2.6.4 Debian .....	24
2.6.5 Slackware .....	24
2.6.6 SuSE .....	24
2.6.7 Mandrake.....	25

2.6.8	WinLinux .....	25
2.7	IPTables .....	25
2.7.1	Aturan Table yang ada pada IPTables.....	25
<b>3</b>	<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>27</b>
3.1	Metodologi .....	27
3.1.1	Metodologi Penelitian .....	27
3.1.2	Melakukan Diagnosa ( <i>Diagnosing</i> ).....	27
3.1.3	Membuat rencana tindakan ( <i>Action Planning</i> ) .....	28
3.1.4	Melakukan Tindakan ( <i>Action Taking</i> ) .....	28
3.1.5	Melakukan Evaluasi ( <i>Evaluating</i> ).....	28
3.1.6	Melakukan Pembelajaran ( <i>Specifying Learning</i> ) .....	28
3.2	Metode Pengumpulan Data .....	28
3.2.1	Studi Kepustakaan ( <i>Literature</i> ).....	29
3.2.2	Metode Observasi.....	29
3.3	Waktu Penelitian.....	29
3.4	Metode Penelitian.....	29
3.4.1	Melakukan Diagnosa ( <i>Diagnosing</i> ).....	30
3.4.2	Membuat Rencana Tindakan ( <i>Action Taking</i> ).....	33
3.4.3	Melakukan tindakan ( <i>action taking</i> ) .....	36
<b>4</b>	<b>BAB IV HASIL DAN PEMBAHASAN TEORI.....</b>	<b>48</b>
4.1	Hasil.....	48
4.1.1	Hasil pengujian serangan <i>Brute Force</i> pada <i>Ubuntu server</i> .....	49
4.1.2	Hasil pengujian serangan <i>Brute Force Linux CentOS</i> .....	50
4.2	Pembahasan.....	50
4.2.1	Uji serangan <i>Brute Force</i> di <i>Linux Ubuntu</i> .....	52
4.2.2	Uji serangan <i>Brute Force</i> di <i>Linux CentOS</i> .....	56
4.3	Analisis Perbandingan.....	60
4.4	Hasil Perbandingan.....	62
<b>5</b>	<b>BAB V KESIMPULAN &amp; SARAN.....</b>	<b>63</b>
5.1	Kesimpulan.....	63
5.2	Saran .....	65
	<b>DAFTAR PUSTAKA.....</b>	<b>66</b>
	<b>LAMPIRAN .....</b>	<b>67</b>

## DAFTAR GAMBAR

Gambar 2.1	Siklus <i>action research</i> .....	28
Gambar 2.2	Server.....	30
Gambar 2.3	Laptop <i>Attacker</i> .....	31
Gambar 2.4	Rancangan tahapan-tahapan yang akan dilakukan.....	33
Gambar 2.5	Topologi peer to peer .....	34
Gambar 2.6	Tampilan Sebelum Instalasi.....	35
Gambar 2.7	Select your location. ....	35
Gambar 2.8	Kemudian pilih <i>Configure the keyboard</i> .....	36
Gambar 2.9	Membuat <i>user</i> baru.....	37
Gambar 2.10	<i>Setup user and password</i> .....	37
Gambar 2.11	<i>Configure the clock</i> .....	38
Gambar 2.12	Membuat partisi baru .....	38
Gambar 2.13	GRUB <i>boot loader</i> .....	39
Gambar 2.14	Proses Instalasi <i>IPTables</i> .....	40
Gambar 2.15	Tampilan sebelum instalasi .....	41
Gambar 2.16	Menu instalasi .....	41
Gambar 2.17	Membuat partisi .....	42
Gambar 2.18	Memilih lokasi .....	43
Gambar 2.19	Proses instalasi .....	43
Gambar 2.20	Pengaturan <i>User dan Password</i> .....	44
Gambar 2.21	Log Linux Ubuntu .....	47
Gambar 2.22	Log Linux CentOS .....	48
Gambar 2.23	serangan SSH sebelum diterapkan IPS pada <i>Ubuntu Server</i> .....	50
Gambar 2.24	serangan menggunakan <i>SSH</i> gagal karna sudah diterapkan IPS pada <i>Ubuntu</i> .....	51
Gambar 2.25	Serangan menggunakan <i>FTP</i> gagal karna sudah diterapkan IPS pada <i>Ubuntu</i> .....	52
Gambar 2.26	Serangan menggunakan <i>TELNET</i> gagal karna sudah diterapkan IPS pada <i>Ubuntu</i> .....	53

Gambar 2.27 Serangan menggunakan *SSH* gagal karna suda diterapkan IPS pada *CentOs* ..... 54

Gambar 2.1 Serangan menggunakan *FTP* gagal karna sudah diterapkan IPS pada *CentOS*.....56

Gambar 2.1 Serangan menggunakan *TELNET* gagal karna sudah diterapkan IPS pada *CentOs* .....57



## DAFTAR TABEL

<b>Tabel 3.2 Spesifikasi Server.....</b>	<b>31</b>
<b>Tabel 3.3 Spesifikasi Laptop Attacker .....</b>	<b>32</b>
<b>Tabel 3.4 IPAddress yang akan digunakan pada Linux Ubuntu / CentOS.....</b>	<b>34</b>
<b>Tabel 3.5 Perbandingan pengujian Intrusion Prevention System .....</b>	<b>58</b>
<b>Tabel 3.10 Hasil Perbandingan Intrusion Prevention System .....</b>	<b>59</b>



## Daftar Lampiran

- [1] Lembar Pengajuan Judul
- [2] Lembar Konsultasi Proposal
- [3] Lembar Perbaikan Proposal
- [4] Surat Keterangan Lulus Proposal
- [5] Lembar Konsultasi Skripsi
- [6] Formulir Perbaikan Komprehensif
- [7] Surat Keterangan Lulus Komprehensif
- [8] Hasil Turnitin
- [9] Check List Kesesuaian Format Penulisan
- [10] SK Pembimbing
- [11] Sertifikat Toefl
- [12] Sertifikat Psikotes
- [13] Sertifikat Magang, dan Sertifikat lainnya

Universitas Bina  
Dharma

