

Pembuatan Sistem

**PEMBUATAN SISTEM KEAMANAN JARINGAN DENGAN
MENERAPKAN METODE IDPS PADA MULTIPLE SERVER**

(Studi kasus : Yayasan Pondok Pesantren Al-Fattah)

SKRIPSI



Oleh :

KRIS ANDRE PRASETYO

NPM : 1634010006

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL “ VETERAN ”

JAWA TIMUR

2020

**PEMBUATAN SISTEM KEAMANAN JARINGAN DENGAN
MENERAPKAN METODE IDPS PADA MULTIPLE SERVER**

(Studi kasus : Yayasan Pondok Pesantren Al-Fattah)

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan

Dalam Memperoleh Gelar Sarjana Komputer

Jurusan Informatika



Oleh :

KRIS ANDRE PRASETYO

NPM : 1634010006

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL " VETERAN "

JAWA TIMUR

2020

LEMBAR PENGESAHAN SKRIPSI

Judul : Sistem Informasi Penjualan Pakaian Berbasis *Web* pada DEFIRZA
Collection Surabaya

Oleh : Deny Alif Firmansyah

NPM : 1434010198

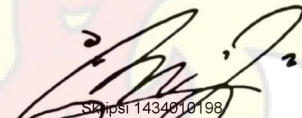
Telah Diseminarkan Dalam Ujian Skripsi
Pada Tanggal : 20 Juli 2020

Menyetujui:


Dosen Pembimbing

Dosen Penguji


1.


Budi Nugroho, S.Kom, M.Kom
NPT. 3 8009 050 205 1


1.


Henni Endah Wahanani, S.T, M.Kom
NPT. 3 7809 13 0342 1

2.


Firza Prima Aditiawan, S.Kom, MTI
NPT. 3 8605 13 03441

2.


Mohammad Idhom, S.P, S.Kom, M.T
NPT. 3 8303 10 0285 1

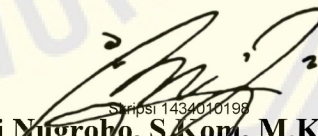
Mengetahui:

Dekan
Fakultas Ilmu Komputer,

Koordinator Program Studi
Informatika,




Ir. Ni Ketut Sari, MT
NIP. 19650731 199203 2 001


Budi Nugroho, S.Kom, M.Kom
NPT. 3 8009 050 205 1

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Informatika UPN “Veteran” Jawa Timur, yang bertandatangan di bawah ini:

Nama : Kris Andre Prasetyo

NPM : 1634010006

Menyatakan bahwa Judul Skripsi / Tugas Akhir yang saya ajukan dan akan dikerjakan, yang berjudul:

“Pembuatan Sistem Keamanan Jaringan Dengan Menerapkan Metode IDPS Pada Multiple Server (Studi kasus : Yayasan Pondok Pesantren Al-Fattah)”

Bukan merupakan plagiat dari Skripsi / Tugas Akhir / Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi / Tugas Akhir ini adalah pekerjaan saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN “Veteran” Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka saya siap menerima segala konsekuensinya.

Surabaya, Juli 2020

Hormat Saya,



Kris Andre Prasetyo

NPM. 1634010006

KATA PENGANTAR

Puji syukur penulis ucapkan kepada Tuhan Yang Maha Esa, karena berkat rahmat serta karunia-Nya penulis dapat menyelesaikan laporan skripsi. Adapun skripsi ini sebagai syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada fakultas ilmu komputer jurusan informatika UPN Veteran Jatim.

Laporan ini disusun berdasarkan hasil dari penelitian yang telah penulis lakukan dengan judul **“PEMBUATAN SISTEM KEAMANAN JARINGAN DENGAN MENERAPKAN METODE IDPS PADA MULTIPLE SERVER (Studi kasus : Yayasan Pondok Pesantren Al-Fattah)”**.

Penulis menyadari bahwa penulisan laporan skripsi ini masih belum sempurna. Oleh karena itu, saran dan kritik yang bersifat membangun kearah yang positif. Meskipun terdapat halangan dan kesulitan dalam pengerjaan skripsi ini, Alhamdulillah dapat penulis atasi dan selesaikan dengan baik.

Akhir kata, penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak dan dapat dikembangkan khususnya bagi pembaca.

Surabaya, Juli 2020

Penulis,

Kris Andre Prasetyo

UCAPAN TERIMA KASIH

Puji Syukur kehadiran Allah SWT. Berkat rahmat dan berkah-nya penulis dapat menyelesaikan skripsi ini. Dalam pengerjaan skripsi ini, selain doa dari kedua orang tua dan keluarga juga tidak lepas dari dukungan dan bantuan dari berbagai pihak, baik secara langsung maupun tidak langsung, Dengan segala kerendahan hati, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang turut membantu penulis, khususnya kepada :

1. Ibu Dr. Ir. Ni Ketut Sar, MT. selaku Dekan Fakultas Ilmu Komputer UPN “Veteran” Jawa Timur
2. Bapak Budi Nugroho, S.Kom, M.Kom. selaku kepala jurusan Informatika UPN “Veteran” Jawa Timur
3. Bapak Mohammad Idhom, SP, S.Kom, MT. dan Ibu Henni Endah Wahanani, ST, M.Kom. selaku dosen pembimbing skripsi yang telah bersedia meluangkan waktu, memberikan saran dan masukan selama proses pengerjaan skripsi penulis.

**PEMBUATAN SISTEM KEAMANAN JARINGAN DENGAN
MENERAPKAN METODE IDPS PADA MULTIPLE SERVER
(Studi kasus : Yayasan Pondok Pesantren Al-Fattah)**

Nama mahasiswa : Kris Andre Prasetyo
NPM : 1634010006
Program Studi : Informatika
Dosen Pembimbing : Mohammad Idhom, SP, S.Kom, MT
Henni Endah Wahanani, ST, M.Kom

ABSTRAK

Pada perkembangan internet yang semakin cepat dengan berbagai macam fungsi dan manfaat, menuntut meningkatnya kualitas keamanan jaringan, bocornya informasi ke pihak yang tidak berkepentingan dapat menimbulkan kerugian bagi pemilik informasi, terutama pada server yang menyimpan banyak informasi didalamnya, pada suatu tempat bisa terdapat lebih dari satu server, sehingga akan menyulitkan jika dilakukan monitoring serangan, oleh karena itu dibutuhkan suatu sistem keamanan jaringan yang dapat berjalan pada *multiple* server agar proses *monitoring* dan pencegahan serangan dapat dilakukan dengan cepat dan efektif.

IDPS (intrusion Detection and Prevention System) merupakan metode keamanan jaringan yang dapat melakukan deteksi dan pencegahan suatu serangan dengan melakukan pemblokiran terhadap alamat ip yang mencurigakan, *IDPS* sendiri merupakan pengembangan dari *IDS (intrusion Detection System)* yang dikombinasikan dengan ip tables sehingga dapat melakukan deteksi dan pencegahan terhadap aktifitas-aktifitas yang mencurigakan pada suatu jaringan,

Sehingga dengan adanya suatu sistem keamanan jaringan yang dapat berjalan pada *multiple* server proses pencegahan serangan dapat dilakukan lebih cepat dan efektif karena ketika salah satu server mendeteksi suatu serangan, server yang lain akan melakukan pencegahan dengan mengambil informasi yang telah masuk pada *database collector*, dengan melakukan sinkronisasi pada semua server, server lain dapat melakukan pencegahan serangan sebelum terjadi serangan pada server tersebut.

Kata kunci : *IDS, IDPS*

DAFTAR ISI

COVER	i
LEMBAR PENGESAHAN	ii
SURAT PERNYATAAN ANTI PLAGIAT	iii
KATA PENGANTAR	iv
UCAPAN TERIMA KASIH.....	v
ABSTRAK.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Penelitian Terdahulu.....	6
2.1.1 Arthur S. Petrosyan, dan Gurgun S. Petrosyan, 2016	6
2.1.2 Mike Ford, Cody Mallery, Frank Palmasani, Michael Rabb, Reid Turner, Lem Soles, dan Dallas Snider, 2016	7
2.1.3 Tilak Maharashtra Vidyapeeth, Pune, 2018.....	7
2.1.4 Iwan Kurniawan, Ferry Mulyanto, dan Fuad Nandiasa, 2016.....	8
2.1.5 Fadlin Arsin, Muhammad Yamin, dan La Surimi, 2017.....	9
2.2 Dasar Teori	9

2.2.1	Server	10
2.2.2	<i>Crontab</i>	11
2.2.3	Serangan <i>DDoS</i>	11
2.2.4	Serangan <i>Brute Force</i>	11
2.2.5	<i>Fail2ban</i>	12
2.2.6	<i>Firewall</i>	12
2.2.7	Topologi	13
2.2.8	Sistem Operasi	14
2.2.9	<i>Ubuntu</i>	15
2.2.10	<i>Web</i>	16
2.2.11	<i>IDS</i>	17
2.2.12	<i>IPS</i>	17
2.2.13	<i>PHP</i>	17
2.2.14	<i>CSS</i>	18
2.2.15	<i>SSH</i>	18
2.2.16	<i>Xerxes</i>	19
2.2.17	<i>DBeaver</i>	19
2.2.18	<i>Database</i>	19
BAB III METODOLOGI		21
3.1	Alur penelitian	21
3.2	Studi Literatur	23
3.3	Definisi Kebutuhan	23
3.3.1	Kebutuhan Perangkat Keras	23
3.3.2	Kebutuhan Perangkat Lunak	26
3.4	Desain dan perancangan	28

3.4.1	Topologi	29
3.4.2	Konfigurasi <i>Fail2ban</i>	29
3.4.3	Proses Pengiriman <i>Log</i>	32
3.4.4	Proses <i>ban</i> dari <i>database</i>	33
3.4.5	<i>Database</i>	34
3.4.6	Website Monitoring	35
3.5	Pembuatan sistem	41
3.6	Testing	43
BAB IV HASIL DAN PEMBAHASAN		46
4.1	Instalasi dan konfigurasi <i>fail2ban</i>	46
4.2	Konfigurasi <i>database fail2ban</i>	48
4.4	<i>Website</i>	56
4.4.1	Login Admin	56
4.4.2	Halaman beranda.....	57
4.4.3	Halaman grafik.....	60
4.5	Testing	60
4.5.1	Testing Tahap Pertama.....	60
4.5.2	Testing Tahap Kedua	63
BAB V KESIMPULAN DAN SARAN.....		70
5.1	Kesimpulan.....	70
5.2	Saran	70
DAFTAR PUSTAKA		72
BIODATA PENULIS		75
LAMPIRAN.....		76

DAFTAR GAMBAR

Gambar 3.1 Diagram alur penelitian.....	21
Gambar 3.2 Alur program dalam penelitian	28
Gambar 3.3 Topologi yang digunakan.....	29
Gambar 3.4 Alur konfigurasi <i>fail2ban</i> pada server.....	30
Gambar 3.5 Alur rule yang ditentukan.....	31
Gambar 3.6 Alur konfigurasi log ke database.....	32
Gambar 3.7 Alur pengiriman log serangan	33
Gambar 3.8 Alur konfigurasi ban dari database	33
Gambar 3.9 Alur proses <i>ban</i> dari database	34
Gambar 3.10 Conceptual Data Model.....	34
Gambar 3.11 Physical Data Model	35
Gambar 3.12 Use case diagram.....	36
Gambar 3.13 Activity diagram login	36
Gambar 3.14 Activity diagram menyimpan report	37
Gambar 3.15 Activity diagram mencari data	37
Gambar 3.16 Activity diagram halaman grafik.....	38
Gambar 3.17 Activity diagram logout	38
Gambar 3.18 Mockup halaman login.....	39
Gambar 3.19 Mockup halaman beranda	40
Gambar 3.20 Mockup halaman diagram.....	41

gambar 3.21 Alur pembuatan sistem.....	41
Gambar 3 22 Sekema serangan brute force dan DDoS.....	43
Gambar 3.23 Alur brute force	44
Gambar 3.24 Alur serangan DDoS	45
Gambar 4.1 Remote ssh server.....	46
Gambar 4.2 Instalasi fail2ban	47
Gambar 4.3 Konfigurasi ssh pada rule fail2ban.....	47
Gambar 4.4 Konfigurasi banaction fail2ban	48
Gambar 4.5 Halaman download DBEaver	49
Gambar 4.6 Tampilan tool DBEaver	49
Gambar 4.7 Tampilan tool DBEaver	50
Gambar 4.8 Tabel fail2ban.....	51
Gambar 4.9 Tabel user	52
Gambar 4.10 List cronjob pada server	55
Gambar 4.11 Isi <i>file</i> pada <i>directory</i> /usr/local/fail2db	56
Gambar 4.12 Halaman login website	57
Gambar 4.13 Halaman beranda.....	57
Gambar 4.14 <i>Widget</i> jumlah serangan	58
Gambar 4.15 <i>Log</i> serangan	59
Gambar 4.16 Output cetak log serangan.....	59
Gambar 4.17 Halaman grafik.....	60

Gambar 4.18 Isi tabel fail2ban pada database.....	61
Gambar 4.19 Status ssh client pada service fail2ban	62
Gambar 4.20 Remote ssh pada server	64
Gambar 4.21 List ban sshd pada server	64
Gambar 4.22 List ban sshd-ddos pada server.....	65
Gambar 4.23 Serangan brute force dengan tool hydra.....	65
Gambar 4.24 List ban pada server.....	66
Gambar 4.25 Tampilan website	66
Gambar 4.26 List ban pada server lain.....	67
Gambar 4.27 List ban pada server.....	68
Gambar 4.28 Tampilan website monitoring.....	68

DAFTAR TABEL

Tabel 3.1 Spesifikasi laptop penyerang	24
Tabel 3.2 Spesifikasi komputer server satu	24
Tabel 3.3 Spesifikasi komputer server dua	25
Tabel 3.4 Spesifikasi komputer server tiga.....	25
Tabel 3.5 Spesifikasi komputer server empat	25
Tabel 4.1 Uji coba file pada server	63
Tabel 4.2 Ip pada server	63
Tabel 4.3 Uji coba serangan.....	69