



**ANALISIS PENINGKATAN KEAMANAN SERVER
MENGUNAKAN SNORT DAN PFSENSE PADA
JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER DI POLITEKNIK NEGERI JAKARTA**

LAPORAN SKRIPSI

SUCI RAHMADHANI

4817050415

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021**



RANCANG BANGUN KEAMANAN SISTEM SERVER

ANALISIS PENINGKATAN KEAMANAN SERVER MENGUNAKAN SNORT DAN PFSENSE PADA JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER DI POLITEKNIK NEGERI JAKARTA

LAPORAN SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk
Memperoleh Diploma Empat Politeknik**

**SUCI RAHMADHANI
4817050415**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021**



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Suci Rahmadhani

NIM : 4817050415

Tanggal : 23 juni 2021

Tanda Tangan :

**POLITEKNIK
NEGERI
JAKARTA**

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama : Suci Rahmadhani
NIM : 4817050415
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Peningkatan Keamanan Server Menggunakan Snort dan Pfsense pada Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta

Sudah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 30, Bulan Juni Tahun 2021 Dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Defiana Arnaldy, S.Tp., M.Si. ()

Penguji I : Maria Agustin, S.Kom., M.Kom. ()

Penguji II : Muhammad Yusuf Bagus Rasyiidin, S.Kom., M.TI. ()

Penguji III : Ariawan Andi Suhandana, S.Kom., M.T.I. ()

Mengetahui:

Ketua Jurusan Teknik Informatika dan Komputer

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

- a. Bapak Defiana Arnaldy, S.Tp., M.Si. selaku kepala program studi serta dosen pembimbing yang menyediakan waktu serta tenaga dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini.
- b. Bapak Fachroni Arbi Murad, S.Kom., M.Kom. Selaku dosen yang juga telah ikut membantu untuk mengarahkan penulis dalam penyusunan skripsi ini.
- c. Orang tua dan keluarga penulis yang sudah memberikan bantuan dukungan penuh secara moral dan material. Dalam mendukung penulis pembuatan skripsi.
- d. Febby Rahmi A. kakak saya tercinta yang memberikan dukungan moral serta mendengarkan segala keluh kesah penulis dan membantu penulis dalam penyelesaian skripsi.
- e. Dita Nurhayati, selaku teman satu tim, satu perjuangan dalam penyusunan laporan skripsi ini yang telah memberikan bantuan dukungan secara moral
- f. Sabrina Annisa A., Trisya Talia D. dan Laily Rachmi atas waktunya mendengarkan segala keluh kesah penulis dan menemani penulis begadang untuk mengerjakan skripsi hingga larut setiap harinya.
- g. Sahabat-sahabat saya, teman-teman Cahya Mulyadi, David Matius, Kevin K., Aji Trinio, Marta Surya dan teman “Bismillah” lainnya, teman kelas satu perjuangan dari awal hingga akhir masa perkuliahan yang tidak pernah putus memberi semangat.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Yolanda Wahyu R, Vina Rachmawaty dan Reni Afriyanti sahabat saya memberikan semangat serta mendengarkan segala dukungan dalam segi moral.

Egi Dita A. dan Norma Asyifa sahabat saya memberikan dukungan moral serta mendengarkan segala keluhan penulis. Serta membantu penulis dalam segala yang dibutuhkan penulis dalam pembuatan skripsi.

Akhir kata, penulis berharap Allah SWT. Membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini dapat bermanfaat bagi semua masyarakat.

Depok, 23 Juni 2021

Uci Rahmadhani





HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Suci Rahmadhani
NIM : 4817050415
Program Studi : Teknik Multimedia dan Jaringan
Jurusan : Teknik Informatika dan Komputer
Tesis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul:

Analisis Peningkatan Keamanan Server Menggunakan Snort dan Pfsense Pada Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta.

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : 30 juni 2021

Yang Menyatakan

(Suci Rahmadhani)



Analisis Peningkatan Keamanan Server Menggunakan Snort dan Pfsense pada Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta.

ABSTRAK

Kendala luar yang mengganggu keamanan pada sistem server jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta seperti serangan pada sistem server serangan DoS Attack. Dalam meningkatkan segi keamanan sistem server Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta. Oleh sebab itu dibutuhkan penanggulangan dari ancaman berupa penggunaan Intrusion Detection System (IDS) mengetahui adanya serangan yang masuk berupa peringatan pada sistem jaringan komputer. Serta penerapan Intrusion Prevention System (IPS) sebagai proteksi keamanan sistem server berupa penggunaan pfsense. Metode yang digunakan berupa alert atau monitoring server apabila adanya serangan yang masuk, Log snort membantu system administrator mencatat segala jenis aktivitas yang mencurigakan pada server dan penggunaan firewall sebagai hardening apabila terjadi serangan yang masuk dari jaringan local, serta dapat melakukan deny akses apabila serangan mencoba akses sistem server Jurusan TIK-PNJ. Firewall pada pfsense menghalau dan memproteksi serangan yang mencoba masuk menuju server. Dari hasil pengujian, snort mampu melakukan monitoring dan menyimpan log dan pfsense dapat melakukan blocking akses pada saat jaringan mencoba masuk pada sistem server serta pada serangan ping of death dan smurf attack berlangsung.

Kata Kunci: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Pfsense, Snort.

POLITEKNIK
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	i
HALAMAN PENGESAHAN.....	ii
KATA PENGANTAR	iii
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	xi
DAFTAR TABLE.....	xiv
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat	4
1.4.1 Tujuan.....	4
1.4.2 Manfaat.....	4
1.5 Metode Pelaksanaan.....	4
1.5.1 Fase Persiapan (<i>Prepare</i>).....	5
1.5.2 Fase Perencanaan (<i>Plan</i>)	5
1.5.3 Fase Desain (<i>Design</i>).....	5
1.5.4 Fase Implementasi (<i>Implement</i>)	5
1.5.5 Fase Operasi (<i>Operate</i>).....	5
1.5.6 Fase Optimasi (<i>Optimize</i>).....	5
BAB II.....	6
TINJAUAN PUSTAKA	6
2.1 Penelitian Sejenis	6
2.2 IDS (<i>Intrusion Detection System</i>)	8
2.3 IPS (<i>Intrusion Prevention System</i>).....	9
2.4 Cisco Packer Tracer	10
2.5 VirtualBox.....	11

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

3.6 Ubuntu Server 16.04 CLI.....	12
3.7 Kali Linux	12
3.8 PfSense.....	13
3.9 Snort.....	14
3.10 Nmap (Network Mapper).....	15
3.11 Wordpress	16
3.12 SSH (<i>Secure Shell</i>).....	17
3.13 PuTTY.....	18
3.14 LOIC	18
3.15 HPING3	19
3.16 <i>DoS Attack</i>	19
3.16.1 <i>Ping of Death</i>	21
3.16.2 <i>Smurf Attack</i>	21
3.17 BAB III	23
3.18 PERANCANGAN DAN REALISASI	23
3.19 3.1 Perancangan Sistem	23
3.19.1 Deskripsi Sistem.....	23
3.19.2 Alur Kerja Sistem.....	24
3.19.3 Desain Topologi Jaringan.....	26
3.19.4 Spesifikasi Perangkat dan <i>Software/Tools</i>	27
3.19.5 Skenario Pengujian.....	28
3.19.6 Blok Diagram	29
3.20 3.2 Realisasi Sistem	29
3.20.1 Konfigurasi <i>Scanning</i> Server JTIK-PNJ	30
3.20.1.1 Port Scanning Server JTIK-PNJ	30
3.20.1.2 Scanning Website JTIK-PNJ	31
3.20.2 Pembuatan Server <i>Dummy</i> JTIK-PNJ	33
3.20.2.1 Instalasi Server Virtual Ubuntu 16.04 CLI.....	34
3.20.2.2 Instalasi OpenSSH pada Sever <i>Dummy</i>	34
3.20.3 Pembuatan <i>Website Dummy</i> JTIK-PNJ	35
3.20.3.1 Instalasi Apache2.....	36
3.20.3.2 Instalasi PHP 5.6-40	37
3.20.3.3 Pembuatan Website Dummy WordPress JTIK-PNJ.....	38



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

3.2.4 Implementasi <i>Intrusion Detection System</i> (IDS).....	43
3.2.4.1 Instalasi Snort	43
3.2.4.2 Konfigurasi Snort.....	44
3.2.5 Implementasi <i>Intrusion Prevention System</i> (IPS).....	47
3.2.5.1 Instalasi Pfsense	47
3.2.5.2 Konfigurasi Pfsense pada <i>Virtual Machine</i>	48
3.2.5.3 Setting Pfsense	49
BAB IV	58
PEMBAHASAN	58
4.1 Pengujian.....	58
4.2 Deskripsi Pengujian	58
4.3 Prosedur Pengujian	59
4.3.1 Prosedur Waktu Penyerangan (<i>Real Time</i>).....	59
4.3.2 Prosedur Efektivitas	60
4.3.3 Prosedur Kualifikasi	60
4.4 Data Hasil Pengujian.....	60
4.4.1 Hasil Prosedur Waktu Penyerangan (<i>Real Time</i>).....	61
4.4.1.1 <i>Ping of Death</i>	61
4.4.1.2 <i>Smurf Attack</i>	66
4.4.2 Hasil Prosedur Efektivitas	69
4.4.2.1 <i>States</i>	70
4.4.2.2 <i>Traffic Graph</i>	73
4.4.3 Hasil Prosedur Kualifikasi.....	77
4.4.3.1 Pfsense dan Snort terhadap <i>Ping of Death</i>	78
4.4.3.2 Pfsense dan Snort terhadap <i>Smurf Attack</i>	79
4.5 Analisis Data / Evaluasi	82
4.5.1 Analisis Hasil Data Prosedur Waktu Penyerangan (<i>Real Time</i>)	82
4.5.2 Analisis Hasil Data Prosedur Efektifitas	83
4.5.3 Analisis Hasil Data Prosedur Kualifikasi	84
BAB V.....	85
PENUTUP.....	85
5.1 Simpulan	85
5.2 Saran.....	85



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





DAFTAR GAMBAR

Gambar 2. 1	Logo Packet Tracer	10
Gambar 2. 2	Logo Virtual Box	11
Gambar 2. 3	Logo Ubuntu	12
Gambar 2. 4	Logo kali linux	12
Gambar 2. 5	Logo Pfsense	13
Gambar 2. 6	Logo Snort.....	14
Gambar 2. 7	Logo Nmap.....	15
Gambar 2. 8	Logo Wordpress	16
Gambar 2. 9	SSH (Secure shell)	17
Gambar 2. 10	Logo PuTTY	18
Gambar 2. 11	Logo LOIC	18
Gambar 2. 12	Logo HPING3	199
Gambar 3. 1	Deskripsi Pengujian Sistem.....	23
Gambar 3. 2	Flowchart cara kerja sistem server.....	24
Gambar 3. 3	Flowchart cara kerja sistem penyerangan	25
Gambar 3. 4	Design Topologi Jaringan	26
Gambar 3. 5	Skenario Pengujian.....	28
Gambar 3. 6	Blok Diagram Sistem	29
Gambar 3. 7	Hasil Port <i>Scanning</i> Nmap	30
Gambar 3. 8	Hasil Port <i>Scanning</i> menggunakan NMAP.....	31
Gambar 3. 9	<i>Scanning</i> Website Jurusan TIK-PNJ	32
Gambar 3. 10	Penggunaan WordPress.....	32
Gambar 3. 11	Penggunaan Apache 2.4	33
Gambar 3. 12	Penggunaan Ubuntu server.....	33
Gambar 3. 13	Penulisan nama Server <i>dummy</i> JTIK	34
Gambar 3. 14	Penerapan instalasi Server <i>dummy</i> JTIK	34
Gambar 3. 15	Instalasi OpenSSH pada server <i>dummy</i>	35
Gambar 3. 16	Server <i>dummy</i> Ubuntu 16.04.....	35
Gambar 3. 17	Instalasi Apache2	36
Gambar 3. 18	Intalasi Apache2.....	36
Gambar 3. 19	Konfigurasi Network Interface.....	37
Gambar 3. 20	Login Wordpres JTIK-PNJ	38
Gambar 3. 21	Dashboard Website JTIK-PNJ	39
Gambar 3. 22	Dashboard Website JTIK-PNJ	39
Gambar 3. 23	Dashboard Website JTIK-PNJ	40
Gambar 3. 24	Dashboard Website JTIK-PNJ	40
Gambar 3. 25	Dashboard Website JTIK-PNJ	41
Gambar 3. 26	Dashboard Website JTIK-PNJ	41
Gambar 3. 27	Dashboard Website JTIK-PNJ	42
Gambar 3. 28	Dashboard Website JTIK-PNJ	42

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Gambar 3. 29 Dashboard Website JTIC-PNJ	43
Gambar 3. 30 Instalasi Snort.....	43
Gambar 3. 31 Konfigurasi Snort	44
Gambar 3. 32 Konfigurasi <i>Rules</i> Snort	45
Gambar 3. 33 <i>Rules</i> snort.....	45
Gambar 3. 34 Konfigurasi Snort	46
Gambar 3. 35 Router Pfsense JTIC-PNJ.....	47
Gambar 3. 36 <i>Setting</i> Pfsense	47
Gambar 3. 37 Konfigurasi Router Pfsense.....	48
Gambar 3. 38 <i>Setting</i> Pfsense	49
Gambar 3. 39 <i>Setting</i> Pfsense	49
Gambar 3. 40 <i>Setting</i> Pfsense	50
Gambar 3. 41 <i>Setting</i> Pfsense	50
Gambar 3. 42 <i>Setting</i> Pfsense	51
Gambar 3. 43 <i>Setting</i> Pfsense.....	51
Gambar 3. 44 <i>Setting</i> Pfsense <i>Interface</i>	52
Gambar 3. 45 <i>Setiing</i> Pfsense <i>Interface</i>	52
Gambar 3. 46 <i>Setting</i> Pfsense <i>Interface</i>	53
Gambar 3. 47 <i>Setting</i> Pfsense Firewall/NAT	53
Gambar 3. 48 <i>Setting</i> Pfsense Firewall	54
Gambar 3. 49 <i>Setting</i> Pfsense Firewall	54
Gambar 3. 50 <i>Setting</i> Pfsense Firewall	55
Gambar 3. 51 <i>Setting</i> Pfsense Firewall	55
Gambar 3. 52 <i>Setting</i> Pfsense Firewall	56
Gambar 3. 53 <i>Setting</i> Pfsense Firewall	56
Gambar 3. 54 <i>Setting</i> Pfsense Firewall <i>rules</i>	57
Gambar 3. 55 <i>Setting</i> Pfsense Firewall <i>blocking</i> Akses.....	57
Gambar 4. 1 Hasil Pengujian Pfsense	61
Gambar 4. 2 Serangan <i>Ping of Death</i> menggunakan <i>tools</i> LOIC	62
Gambar 4. 3 Serangan Selama 5 Menit.....	62
Gambar 4. 4 <i>Log</i> Snort	63
Gambar 4. 5 <i>Log</i> Snort	63
Gambar 4. 6 Serangan Ping of Death menggunakan tools LOIC	64
Gambar 4. 7 Serangan Yang Masuk	64
Gambar 4. 8 <i>Blocking</i> Akses pada Pfsense	64
Gambar 4. 9 Serangan Ping of Death menggunakan tools LOIC	65
Gambar 4. 10 Serangan sebelum blocking akses	65
Gambar 4. 11 Serangan Ping of Death menggunakan tools LOIC	66
Gambar 4. 12 <i>Monitoring</i> pada Snort	66
Gambar 4. 13 Serangan Smurf Attack	67
Gambar 4. 14 <i>Monitoring</i> Snort.....	67
Gambar 4. 15 Serangan Smurf Attack	67
Gambar 4. 16 serangan Smurf Attack	68



© Hak Cipta milik Jurusan Teknik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Gambar 4. 17 Serangan yang masuk pada snort	68
Gambar 4. 18 PuTTY tidak dapat diakses	69
Gambar 4. 19 Traffic Graph serangan Ping of Death	74
Gambar 4. 20 Traffic Graph serangan Ping of Death	74
Gambar 4. 21 Setting Firewall	74
Gambar 4. 22 Traffic Graph setelah serangan	75
Gambar 4. 23 Traffic Graph setelah serangan	75
Gambar 4. 24 Traffic Graph Sebelum serangan	76
Gambar 4. 25 Traffic Graph sebelum serangan	76
Gambar 4. 26 Traffic Graph setelah serangan	77
Gambar 4. 27 Traffic Graph setelah serangan	77
Gambar 4. 28 Alert Pada snort	78
Gambar 4. 29 Konfigurasi Snort	78
Gambar 4. 30 Konfigurasi log Snort	78
Gambar 4. 31 Blocking Akses pfsense	79
Gambar 4. 32 Log Snort.....	79
Gambar 4. 33 Log Snort.....	79
Gambar 4. 34 Log Snort.....	80
Gambar 4. 35 Website Jtik	81
Gambar 4. 36 Traffic Graph pada pfsense	81
Gambar 4. 37 Traffic Graph pada pfsense	82
Gambar 4. 38 Grafik Hasil Prosedur Waktu Penyerangan	82



DAFTAR TABLE

Tabel 2. 1 Penelitian Sejenis	6
Tabel 3. 1 Routing IP Address	26
Tabel 3. 2 Spesifikasi Perangkat server <i>dummy</i>	27
Tabel 3. 3 Spesifikasi Perangkat <i>Attacker</i>	27
Tabel 3. 4 Spesifikasi Perangkat/ <i>tools</i> serangan	27
Tabel 3. 5 Spesifikasi Perangkat Lunak	28
Tabel 3. 6 Spesifikasi Perangkat Lunak Serangan	48
Tabel 3. 7 Setting jaringan pada virtual box	47
Tabel 4. 1 Prosedur waktu Penyerangan	59
Tabel 4. 1 IP yang terdeteksi	70
Tabel 4. 2 Hasil Analisis Serangan prosedur Kualifikasi	84



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era global saat ini, pengelola server jaringan serta internet (*system administrator*) mempunyai kendala serta tanggung jawab terhadap keamanan sistem dari waktu ke waktu. *Administrator* yang bertugas dalam pengaksesan jaringan sebagai *monitoring* apabila terjadi adanya serangan dan penyalahgunaan jaringan. Berbagai macam kendala seperti serangan yang terjadi dari luar mengganggu keamanan jaringan sistem server serta koneksi internet. Penyalahgunaan atau penyusupan data maupun jaringan sistem menyebabkan administrator harus memastikan sistem dan pengelolaan jaringan berjalan dengan baik dari adanya ancaman penyalahgunaan jaringan tersebut.

Pemecahan masalah tersebut diperlukan keamanan sistem pada server dari ancaman luar seperti serangan *Ping of Death* dan *Smurf Attack* menggunakan *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* berupa metode keamanan jaringan sistem dapat melindungi server pada sebuah jaringan. *IDS* sebagai *alert* atau mendeteksi ketika terjadi adanya serangan. Serta *IPS* yang dapat *rules* menindaklanjuti dalam serangan dengan cara menindaklanjuti serangan yang terjadi dengan cara *block* akses server atau sistem jaringan pada komputer penyerang.

Pekerjaan utama sistem deteksi intrusi adalah mengumpulkan paket dari jaringan, memprosesnya dan jika serangan mengidentifikasi maka ini akan menghasilkan peringatan untuk kemungkinan serangan. Keamanan jaringan, sistem deteksi intrusi memiliki dua rasa untuk jaringan dan host berdasarkan kategori dan ragam itu yang dikenal sebagai tanda tangan atau basis aturan deteksi intrusi dan deteksi intrusi berbasis anomali. (Patel, S. K. & Sonker, A., 2016.).

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Suatu serangan dapat dideteksi atau tidak oleh Snort dikonfigurasi pada pengaturan aringan dan *rule* Snort yang ada. Pengujian Snort IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan Snort dalam mendeteksi sebuah serangan terhadap sistem keamanan. Berdasarkan hasil pengujian sistem Snort IDS dengan *ping*, *nmap*, eksploitasi, dan *Ping of Death*, Snort dapat memberikan peringatan adanya serangan keamanan terhadap sistem jaringan. Hasil peringatan tersebut dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan. (Pratama, I. P. A. E. & Handayani, N. K. M., 2019.)

Intrusion Detection and Prevention System (IDPS) merupakan salah satu pilihan untuk meningkatkan keamanan jaringan dalam sebuah jaringan baik intranet maupun internet. Penerapan *Intrusion Detection and Prevention System* (IDPS) digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu *administrator* dalam memantau dan menganalisa paket-paket berbahaya yang terdapat dalam sebuah jaringan. IDPS diterapkan karena mampu mendeteksi penyusup atau paket-paket berbahaya dalam jaringan dan memberikan laporan berupa *log* kepada *administrator* tentang aktivitas dan kondisi jaringan secara real-time sekaligus melakukan drop packet terhadap penyusup. Sehingga segera dapat diambil tindakan terhadap gangguan atau serangan yang terjadi. (Arsin, F., Yamin, M. & Surimi, L., 2017.)

Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran (*traffic*) paket-paket yang keluar dan masuk pada sistem, maka IDS akan merekam aktifitas tersebut. IDS merupakan software atau hardware yang melakukan otomatisasi proses *monitoring* kejadian yang muncul di sistem komputer atau jaringan, menganalisanya untuk menemukan permasalahan keamanan (Wijaya, B. & Pratama, A., 2020)

Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi yaitu dengan menggunakan aplikasi *Intrusion Detection System* (IDS) yaitu Snort dan PfSense (Router OS) sebagai penindak lanjut terhadap *alert* snort yang dihasilkan. (Sutarti, pancaro, A. P. &



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

aputra, F. I., 2018.). Meningkatkan keamanan server dengan Snort IDS melalui beberapa pengujian, sehingga, manfaat yang didapat dari hasil penelitian ini adalah meningkatnya keamanan dalam jaringan, dapat digunakan pada banyak sistem operasi, cepat dan mampu mendeteksi serangan pada jaringan, mudah dikonfigurasi dan open source. (Pratama, I. P. A. E. & Handayani, N. K. M., 2019.)

1.2 Perumusan Masalah

Perumusan masalah yang terdapat pada analisis keamanan jaringan IDS/IPS Snort dan Pfsense pada jurusan Teknik Informatika dan Komputer adalah:

- a. Bagaimana menguji serangan pada *Ping of Death* dan *Smurf Attack* pada sistem server ?
- b. Bagaimana cara penanggulangan sistem keamanan *Ping Of Death* dan *Smurf Attack* pada server menggunakan IDS/IPS ?
- c. Bagaimana penggunaan Snort dan Pfsense pada server?
- d. Bagaimana kelebihan dan kekurangan dari metode penggunaan *Snort* dan *Pfsense* pada server (untuk keamanan server)?
- e. Bagaimana implementasi efektivitas penggunaan Pfsense pada keamanan sistem server?
- f. Bagaimana meningkatkan keamanan server?

1.3 Batasan Masalah

Batasan masalah yang ditentukan dalam Analisis keamanan jaringan menggunakan IDS/IPS adalah sebagai berikut :

- a) Sistem keamanan pada server *dummy* jurusan TIK PNJ menggunakan sistem operasi Ubuntu 16.04 CLI yang dijalankan dengan *Virtual machine* (VirtualBox).
- b) Pengujian uji coba serangan *Denial of Service* (DoS) berupa serangan *Ping of Death* dan *Smurf Attack* dilakukan berupa *Intrusion Detection System* (IDS) *monitoring* server menggunakan snort dan *Intrusion Prevention System* (IPS) berupa *blocking* akses menggunakan pfsense



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

- c) Serangan disimulasikan secara *Local Area Network* (LAN), penyerang berada dalam satu jaringan internet dengan server.
- d) Serangan *Ping of Death* dan *Smurf Attack* menggunakan LOIC dan HPING3.
- e) Pengujian penelitian berupa prosedur waktu penyerangan (*Real Time*), prosedur Efektifitas dan prosedur kualifikasi.
- f) Hasil berupa *traffic* dan jumlah paket yang dihasilkan berupa dilakukan sebelum dan sesudah penyerangan dengan durasi waktu secara *real time* 5 dan 10 menit.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah Diantaranya adalah sebagai berikut :

- a. Meningkatkan penanggulangan sistem keamanan pada serangan *Ping of Death* dan *Smurf Attack* pada sistem server.
- b. Meningkatkan dalam pengamanan data penting seperti data jurusan Teknik Informatika dan Komputer.

1.4.2 Manfaat

Manfaat dari Implementasi *Intrusion Prevention System* menggunakan Snort dan Pfsense pada sistem server Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta adalah sebagai berikut :

- 1) Dihasilkan sistem server yang aman dari dari serangan *Ping of Death* dan *Smurf Attack* pada server jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.
- 2) Dihasilkan sistem keamanan server yang aman bagi Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

1.5 Metode Pelaksanaan

Penelitian menggunakan pendekatan metodologi penelitian berupa PPDIIO (*Prepare, Plan, Design, Implement, Operate dan Optimize*) sebagai berikut:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

1.5.1 Fase Persiapan (*Prepare*)

Pada langkah ini, penulis melakukan persiapan berupa jurnal, studi literatur dan referensi jurnal yang berhubungan dengan topik penelitian. Serta mempersiapkan perangkat lunak dan perangkat keras yang akan digunakan dalam realisasi sistem.

1.5.2 Fase Perencanaan (*Plan*)

Langkah ini dilakukan perencanaan berdasarkan tujuan dan kebutuhan. Peneliti akan melakukan implementasi IDS (*Intrusion Detection System*) dan IPS (*Intrusion Detection Prevention*) berupa snort dan pfsense. Serta melakukan pengujian serangan *Ping of Death* dan *Smurf Attack* menggunakan *tools* LOIC dan HPING3.

1.5.3 Fase Desain (*Design*)

Pada langkah ini peneliti menggunakan langkah design penelitian dalam merancang topologi jaringan, alur pengerjaan, alur pengujian, serta skenario pengujian.

1.5.4 Fase Implementasi (*Implement*)

Peneliti melakukan pengimplementasian IDS dan IPS yaitu berupa *snort* serta aplikasi penunjang lainnya yang mendukung sistem keamanan seperti Pfsense yang akan menindaklanjuti serangan yang terjadi pada server untuk diblock.

1.5.5 Fase Operasi (*Operate*)

Peneliti melakukan *monitoring* sistem yang bekerja pada snort dan pfsense. Berupa jumlah paket yang masuk, *traffic*, *States* dan *firewall* ketika terjadinya serangan.

1.5.6 Fase Optimasi (*Optimize*)

Setelah melakukan pengimplementasian selesai, apabila terjadi kesalahan yang ada pada sistem dapat dilakukan *optimize* seperti penambahan source, penambahan fitur atau lainnya yang menunjang penelitian lebih baik.



BAB V

PENUTUP

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

5.1 Simpulan

Berdasarkan penelitian ini bahwa yang dilakukan konfigurasi sistem keamanan berupa snort dan pfsense pada server *dummy* Jurusan TIK-PNJ, dapat disimpulkan bahwa:

- **Snort:**
 - a) Keamanan sistem *Intrusion Detection System* (IDS) dapat menangani adanya serangan yang masuk dengan penggunaan *Snort* yang mampu mengatasi adanya serangan atau jaringan yang masuk sebagai *alert* dan mencatat serangan yang masuk. Berupa jenis serangan *Ping of Death* dan *Smurf Attack* sukses.
 - b) Serta dalam rentang waktu yang telah dilakukan pengujian terbukti sistem dapat membaca jumlah paket data, waktu, dan protokol jaringan yang masuk pada sistem server.
- **Pfsense:**
 - a) Keamanan sistem sebagai *Intrusion Prevention System* (IPS) pfsense dapat menangani adanya serangan berupa *Ping of Death* berupa keamanan *blocking* akses sukses. Serta Pfsense melakukan *blocking* akses dari serangan berupa *Smurf Attack* terjadi kegagalan dalam *blocking* akses dari serangan luar.
 - b) Pfsense mampu membaca *traffic* yang berjalan saat adanya serangan yang masuk dari pfsense menuju server *dummy* Jurusan TIK-PNJ.

5.2 Saran

Adapun beberapa saran diataranya dalam penelitian keamanan sistem yang telah dilaksanakan pada jurusan TIK-PNJ yaitu:

- a) Penggunaan pfsense dapat melakukan percobaan serangan lainnya.

- b) Menambahkan fitur sistem keamanan lainnya pada sistem server Jurusan TIK-PNJ seperti Suricata atau *Honeypot*



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





DAFTAR PUSTAKA

- Williams. (2018). The best Linux distros of 2018. [Online], Available: <https://www.techradar.com/news/best-linux-distro>.
- Abdulloh, Y., Triyono, J., & Lestari, U. (2020). Pengaruh Penempatan Snort Terhadap Keamanan Jaringan. *Jurnal JARKOM*, 2338-6304.
- Ariyanto, Y., Firdaus, V. A., & Pramana, H. (2020). Klasifikasi Jenis serangan DOS dan Probing pada IDS menggunakan metode K-Nearest Neighbor.
- Arman, M., & Inayatullah. (2019, Vol. 11 No. 1, April 2019, 49-58). Rancang Bangun Owncloud dan Melindunginya Terhadap Serangan DDOS. *Jurnal Integrasi*, 49-58.
- Arman, M., & Rachmat, N. (2020). Implementasi Sistem Keamanan Web Server Menggunakan Pfsense. *Jurnal Sistem Komputer Musirawas*, Vol. 05, 13-23.
- Arsin, F., Yamin, M., & Surimi, L. (2017). IMPLEMENTASI SECURITY SYSTEM MENGGUNAKAN METODE IDPS (INTRUSION DETECTION AND PREVENTION SYSTEM) DENGAN LAYANAN REALTIME NOTIFICATION. *semanTIK*, Vol.3, pp. 39-48.
- Bella, M. R., Data, M., & Yahya, W. (2019). Implementasi Load Balancing Server Web Berbasis Docker Swarm Berdasarkan Penggunaan Sumber Daya Memory Host. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 3, 3478-3487.
- Cahyani, I. D. (2010). Sistem Keamanan Enkripsi SECURE SHELL (SSH) UNTUK Keamanan Data. *Majalah Ilmiah Universitas Pandanaran*, hal. 1-7.
- Deepa, M., & P, S. (2020). Detection of DOS and probe attacks based on snort with density clustering. *ScienceDirect Journal*, 2-5.
- Firdaus, B. P., & Suartana, I. M. (2020). Implementasi Keamanan Jaringan Intrusion Detection System Menggunakan Pfsense. *Jurnal Manajemen Informatika*, Vol. xx, 40-47.
- Gaddam, R., & Nandhini, D. M. (2017). An Analysis of Various Snort Based Techniques to Detect and Prevent Intrusions in Networks. *International Conference on Inventive Communication and Computational Technologies*, 10-15.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

- Hartawan, I. N., & Satwika, K. S. (t.thn.). Rancang Bangun Laboratorium Virtual Berbasis Cloud Computing di STMIK Stikom Indonesia. *Jurnal Ilmu Kompuer dan Sains Terapan*, 54=60.
- hsana, A. N., & Maslan, A. (2020). Analisis Keamanan Jaringan Dari Serangan Paket Data Sniffing Di PT Raden Syaid Kantor POS PIAYU KOTA BATAM. *Jurnal Comasie, VOL.03 NO.05*.
- Muhammad , A. R., Mochammad , F. R., & Tedi , G. (Vol.3, No.3 Desember 2017). IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER. *e-Proceeding of Applied Science , Vol.3*.
- ratel, S. K., & Sonker, A. (2016). Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort. *International Journal of Future Generation Communication and Networking, Vol. 9*, 339-350.
- ratama, I. P., & Handayani, N. K. (2019). Implementasi IDS Menggunakan Snort Pada Sistem Operasi Ubuntu. *Jurnal Mantik Penusa, Vol. 3*, 176-181.
- ratiwati, D., Santoso, G. B., Mardianto, I., Sedyono, A., & Rochman, A. (2020). Pengelolaan Konten Web Menggunakan Wordpress, Canva dan Photoshop untuk Guru-Guru Wilayah Jakarta. *ABDIHAZ: Jurnal Ilmiah Pengabdian pada Masyarakat*, 11-15.
- Putra, C. A., Munir, M. S., Via, Y. V., & Achmadipoetro, R. (2019). Deteksi Serangan Trojan Horse Dengan Memanfaatkan IDS Snort. *SEMINAR SANTIKA*, 203-206.
- Saleh, K. (2020). Implementasi InstrutionDetection System (IDS) Pada Server Web PT.XYZ Menggunakan Snort.
- Sharma, R., & Parekh, C. (2017). Firewalls: A Study and Its Classification. *International Journal of Advanced Research in Computer Science, Volume 8*, 1979-1983.
- Sutarti, pancaro, A. P., & Saputra, F. I. (2018). IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM) PADA SISTEM KEAMANAN JARINGAN SMAN 1 CIKEUSAL. *Jurnal PROSISKO, Vol. 5*, 2406-7733.
- Tohirin. (2020). Penerapan Keamanan Remote Server Melalui SSH Dengan Kombinasi Kriptografi Asimtris dan Autentikasi Dua Langkah. *Jurnal Teknologi Informasi*, 2580-7927.



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Vasconcelos, G., G. C., Miani, R., Souza, J., & Guizilini, V. (2016). The impact of DoS attacks on the AR.Drone 2.0. *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium*, DOI 10.1109/LARS-SBR.2016.28.

Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort. *Jurnal SISFOKOM (Sistem Informasi dan Komputer)*, Vol. 09, 97-101.

