

SKRIPSI

***ANALISIS KINERJA KEAMANAN JARINGAN *HOST-BASED*
INTRUSION PREVENTION SYSTEM (HIPS) DENGAN METODE
ANOMALY-BASED DETECTION***

***NETWORK SECURITY PERFORMANCE ANALYSIS OF *HOST-*
BASED INTRUSION PREVENTION SYSTEM (HIPS) WITH
ANOMALY-BASED DETECTION METHOD***



Disusun oleh

**IMAM YULIANO SANTOSO
18101237**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2022

SKRIPSI

***ANALISIS KINERJA KEAMANAN JARINGAN *HOST-BASED*
INTRUSION PREVENTION SYSTEM (HIPS) DENGAN METODE
ANOMALY-BASED DETECTION***

***NETWORK SECURITY PERFORMANCE ANALYSIS OF *HOST-*
BASED INTRUSION PREVENTION SYSTEM (HIPS) WITH
ANOMALY-BASED DETECTION METHOD***



Disusun oleh

**IMAM YULIANO SANTOSO
18101237**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2022

**ANALISIS KINERJA KEAMANAN JARINGAN *HOST-BASED*
INTRUSION PREVENTION SYSTEM (HIPS) DENGAN METODE
*ANOMALY-BASED DETECTION***

***NETWORK SECURITY PERFORMANCE ANALYSIS OF HOST-
BASED INTRUSION PREVENTION SYSTEM (HIPS) WITH
ANOMALY-BASED DETECTION METHOD***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2022**

Disusun oleh
**IMAM YULIANO SANTOSO
18101237**

**DOSEN PEMBIMBING
Jafaruddin Gusti Amri Ginting, S.T., M.T.
M. Lukman Leksono, S.Pd., M.Pd.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2022**

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KINERJA KEAMANAN JARINGAN *HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS)* DENGAN METODE *ANOMALY-BASED DETECTION*

NETWORK SECURITY PERFORMANCE ANALYSIS OF HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) WITH ANOMALY-BASED DETECTION METHOD

Disusun Oleh
IMAM YULIANO SANTOSO
18101237

Telah dipertanggungjawabkan di hadapan Tim Penguji tanggal 2 September 2022

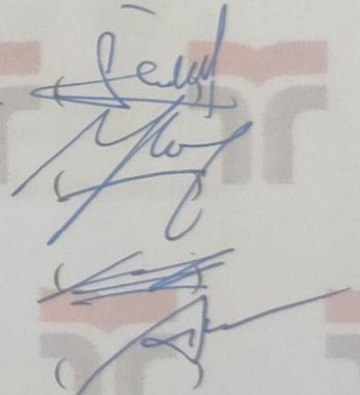
Susunan Tim Penguji

Pembimbing Utama : Jafaruddin Gusti Amri Ginting, S.T., M.T.
NIDN. 0620108901

Pembimbing Pendamping : M. Lukman Leksono, S.Pd., M.Pd.
NIDN. 0630108704


Penguji 1 : Eko Fajar Cahyadi, S.T., M.T., Ph.D.
NIDN. 0616098703

Penguji 2 : Bongga Arifwidodo, S.ST., M.T.
NIDN. 0603118901



Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto



Prasetyo Yuliantoro, S.T., M.T.
NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **IMAM YULIANO SANTOSO**, menyatakan bahwa skripsi dengan judul “**ANALISIS KINERJA KEAMANAN JARINGAN *HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) DENGAN METODE ANOMALY-BASED DETECTION***” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 18 Agustus 2022

Yang menyatakan,



(Imam Yuliano Santoso)

PRAKATA

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan berkah dan rahmat-Nya sehingga penulis dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak dari masa perkuliahan sampai proses penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, penulis menyampaikan rasa terima kasih kepada:

1. Kedua orang tua yang telah mendukung, menasehati, mendoakan dan melakukan segala yang terbaik untuk saya.
2. Bapak Dr. Arfianto Fahmi, S.T., M.T., IPM. selaku Rektor Institut Teknologi Telkom Purwokerto.
3. Ibu Dr. Anggun Fitriani Isnawati, S.T., M.Eng. selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro
4. Bapak Prasetyo Yuliantoro, S.T., M.T. Ketua Program Studi S1 Teknik Telekomunikasi.
5. Bapak Jafaruddin Gusti Amri Ginting, S.T., M.T. selaku pembimbing I.
6. Bapak M. Lukman Leksono, S.Pd., M.Pd. selaku pembimbing II.
7. Teman-teman dan seluruh pihak yang tidak dapat disebutkan satu persatu selama proses pembuatan skripsi ini.
8. *Last but not least, I wanna thank me. I wanna thank me for believing in me. I wanna thank me for all doing this hard work. I wanna thank me for having no days off. I wanna thank me for never quitting. I wanna thank me for just being me at all times.*

Purwokerto, 18 Agustus 2022



(Imam Yuliano Santoso)

DAFTAR ISI

| | |
|--|------|
| HALAMAN PENGESAHAN..... | iv |
| HALAMAN PERNYATAAN ORISINALITAS..... | v |
| PRAKATA..... | vi |
| ABSTRAK..... | vii |
| ABSTRACT..... | viii |
| DAFTAR ISI..... | ix |
| DAFTAR GAMBAR..... | xi |
| DAFTAR TABEL..... | xiii |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 2 |
| 1.3 Batasan Masalah..... | 2 |
| 1.4 Tujuan Penelitian..... | 3 |
| 1.5 Manfaat Penelitian..... | 3 |
| 1.6 Sistematika Penulisan..... | 3 |
| BAB II DASAR TEORI..... | 5 |
| 2.1. Kajian Pustaka..... | 5 |
| 2.2. Dasar Teori..... | 7 |
| 2.2.1. <i>Intrusion Detection System</i> | 7 |
| 2.2.2. <i>Firewall</i> | 9 |
| 2.2.3. <i>Intrusion Prevention System</i> | 9 |
| 2.2.4. <i>Host-Based Intrusion Prevention System</i> | 10 |
| 2.2.5. <i>Anomaly-Based Detection</i> | 11 |
| 2.2.6. <i>Denial of Service</i> | 11 |
| 2.2.7. <i>Distributed Denial of Service</i> | 11 |
| 2.2.8. <i>Ping of Death</i> | 13 |
| 2.2.9. <i>UDP Flood</i> | 13 |
| 2.2.10. <i>SYN Flood</i> | 13 |
| 2.2.11. <i>ICMP Flood</i> | 14 |

| | | |
|-----------------------------------|--|----|
| 2.2.12. | Bruteforce..... | 14 |
| 2.2.13. | Snort | 14 |
| 2.2.14. | Wireshark | 15 |
| 2.2.15. | Ethtool..... | 15 |
| 2.2.16. | Hping..... | 15 |
| 2.2.17. | Hydra..... | 16 |
| 2.2.18. | CUPP..... | 16 |
| 2.2.19. | <i>Quality of Service</i> | 16 |
| BAB III METODE PENELITIAN..... | | 20 |
| 3.1 | Alat dan Bahan Penelitian | 20 |
| 3.2 | Alur Penelitian..... | 21 |
| 3.2.1 | Studi Literatur dan Observasi..... | 21 |
| 3.2.2 | Analisis kebutuhan | 22 |
| 3.2.3 | Instalasi dan Konfigurasi..... | 22 |
| 3.2.4 | Pengujian..... | 41 |
| 3.2.5 | Hasil dan Kesimpulan | 45 |
| 3.3 | Alur Kerja <i>Host-Based Intrusion Prevention System</i> | 46 |
| 3.4 | Alur Kerja <i>Anomaly-Based</i> | 46 |
| BAB IV HASIL DAN PEMBAHASAN | | 48 |
| 4.1 | Hasil Pengujian <i>Baseline</i> | 48 |
| 4.2 | Hasil Pengujian <i>ICMP Flood</i> | 52 |
| 4.3 | Hasil Pengujian <i>UDP Flood</i> | 57 |
| 4.4 | Hasil Pengujian <i>SYN Flood</i> | 63 |
| 4.5 | Hasil Pengujian <i>FTP Bruteforce</i> | 67 |
| 4.6 | Analisis Hasil Pengujian | 72 |
| BAB V KESIMPULAN DAN SARAN..... | | 74 |
| 5.1 | Kesimpulan..... | 74 |
| 5.2 | Saran..... | 75 |
| DAFTAR PUSTAKA | | 76 |
| LAMPIRAN..... | | 79 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 3.1 Alur Penelitian..... | 21 |
| Gambar 3.2 Topologi Jaringan..... | 22 |
| Gambar 3.3 Pemasangan Snort | 23 |
| Gambar 3.4 Tampilan Versi Snort | 24 |
| Gambar 3.5 Ketersediaan DAQ | 25 |
| Gambar 3.6 Tampilan <i>File Snort.conf</i> | 26 |
| Gambar 3.7 Tampilan Folder <i>Rules</i> | 27 |
| Gambar 3.8 <i>File local.rules</i> | 28 |
| Gambar 3.9 Aturan ICMP | 28 |
| Gambar 3.10 Aturan UDP..... | 29 |
| Gambar 3.11 Aturan SYN..... | 30 |
| Gambar 3.12 Aturan FTP | 31 |
| Gambar 3.13 Pemasangan Wireshark | 35 |
| Gambar 3.14 Tampilan Folder <i>Log</i> | 35 |
| Gambar 3.15 Isi <i>File Log</i> | 36 |
| Gambar 3.16 Pemasangan Ethtool | 36 |
| Gambar 3.17 Pengaturan IP pada IPS | 37 |
| Gambar 3.18 Restart <i>interface</i> | 38 |
| Gambar 3.19 Pemasangan Hping..... | 39 |
| Gambar 3.20 Pemasangan Hydra..... | 39 |
| Gambar 3.21 Pemasangan CUPP..... | 40 |
| Gambar 3.22 Pembuatan <i>Wordlist</i> | 40 |
| Gambar 3.23 Pengaturan IP pada Penyerang | 41 |
| Gambar 3.24 Pengujian <i>Baseline</i> | 42 |
| Gambar 3.25 Pengujian <i>ICMP Flood</i> | 42 |
| Gambar 3.26 Perintah <i>ICMP Flood</i> | 43 |
| Gambar 3.27 Pengujian <i>UDP Flood</i> | 43 |
| Gambar 3.28 Perintah <i>UDP Flood</i> | 43 |

| | |
|--|----|
| Gambar 3.29 Pengujian <i>SYN Flood</i> | 44 |
| Gambar 3.30 Perintah <i>SYN Flood</i> | 44 |
| Gambar 3.31 Pengujian <i>FTP Bruteforce</i> | 44 |
| Gambar 3.32 Perintah <i>FTP Bruteforce</i> | 45 |
| Gambar 3.33 Alur Kerja HIPS | 46 |
| Gambar 3.34 Alur Kerja <i>Anomaly-Based</i> | 47 |
| Gambar 4.1 Hasil Pengujian <i>Baseline</i> | 48 |
| Gambar 4.2 Isi File <i>baseline.txt</i> | 48 |
| Gambar 4.3 Hasil <i>Monitoring Baseline</i> | 49 |
| Gambar 4.4 Grafik CPU <i>usage Baseline</i> | 50 |
| Gambar 4.5 Hasil Pengujian <i>ICMP Flood</i> | 53 |
| Gambar 4.6 Isi File <i>icmpflood30s.txt</i> | 53 |
| Gambar 4.7 Hasil <i>Monitoring ICMP Flood</i> | 54 |
| Gambar 4.8 Grafik CPU <i>Usage ICMP Flood</i> | 55 |
| Gambar 4.9 Hasil Pengujian <i>UDP Flood</i> | 58 |
| Gambar 4.10 Isi File <i>udpflood30s.txt</i> | 58 |
| Gambar 4.11 Hasil <i>Monitoring UDP Flood</i> | 59 |
| Gambar 4.12 Grafik CPU <i>Usage UDP Flood</i> | 60 |
| Gambar 4.13 Hasil Pengujian <i>SYN Flood</i> | 63 |
| Gambar 4.14 Isi File <i>SYNflood30s.txt</i> | 63 |
| Gambar 4.15 Hasil <i>Monitoring SYN Flood</i> | 64 |
| Gambar 4.16 Grafik CPU <i>Usage SYN Flood</i> | 65 |
| Gambar 4.17 Hasil Pengujian <i>FTP Bruteforce</i> | 68 |
| Gambar 4.18 Isi File <i>ftpbruteforce30s.txt</i> | 68 |
| Gambar 4.19 Hasil <i>Monitoring FTP Bruteforce</i> | 69 |
| Gambar 4.20 Grafik CPU <i>Usage FTP Bruteforce</i> | 70 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 2.1 Kategori <i>Throughput</i> Versi TIPHON | 17 |
| Tabel 2.2 Kategori <i>Packet Loss</i> Versi TIPHON | 17 |
| Tabel 2.3 Kategori <i>Delay</i> Versi TIPHON..... | 18 |
| Tabel 2.4 Kategori <i>Jitter</i> Versi TIPHON..... | 18 |
| Tabel 3.1 Spesifikasi Perangkat Keras..... | 20 |
| Tabel 3.2 Modul DAQ | 25 |
| Tabel 3.3 Tipe Kelas Aturan | 33 |
| Tabel 4.1 <i>Server</i> Keadaan Normal | 52 |
| Tabel 4.2 Hasil Pengujian <i>ICMP Flood</i> | 57 |
| Tabel 4.3 Hasil Pengujian <i>UDP Flood</i> | 62 |
| Tabel 4.4 Hasil Pengujian <i>SYN Flood</i> | 67 |
| Tabel 4.5 Hasil Pengujian <i>FTP Bruteforce</i> | 72 |
| Tabel 4.6 Perbandingan Hasil Pengujian | 73 |