TUGAS AKHIR

ANALISIS SISTEM KEAMANAN JARINGAN DENGAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) SNORT DAN HONEYPOT DENGAN MENGGUNAKAN QOS *(QUALITY OF SERVICE)*

FARAH AYU ASHARI HARIS

19102096

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS INFORMATIKA

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

2023

TUGAS AKHIR

ANALISIS SISTEM KEAMANAN JARINGAN DENGAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) SNORT DAN HONEYPOT DENGAN MENGGUNAKAN QOS *(QUALITY OF SERVICE)*

ANALYSIS OF NETWORK SECURITY SYSTEM USING SNORT AND HONEYPOT INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) METHOD USING QOS (QUALITY OF SERVICE)

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

FARAH AYU ASHARI HARIS

19102096

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS INFORMATIKA

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

2023

LEMBAR PERSETUJUAN PEMBIMBING

ANALISIS SISTEM KEAMANAN JARINGAN DENGAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) SNORT DAN HONEYPOT DENGAN MENGGUNAKAN QOS *(QUALITY OF SERVICE)*

ANALYSIS OF NETWORK SECURITY SYSTEM USING SNORT AND HONEYPOT INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) METHOD USING QOS (QUALITY OF SERVICE)

Dipersiapkan dan Disusun oleh

FARAH AYU ASHARI HARIS
19102096

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal 4 Juli 2023

Pembimbing I,	Pembimbing II,
Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom	Arif Wirawan Muhammad, S.Kom., M.Kom
NIDN. 0601098701	NIDN. 0613038503

LEMBAR PENGESAHAN

ANALISIS SISTEM KEAMANAN JARINGAN DENGAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) SNORT DAN HONEYPOT DENGAN MENGGUNAKAN QOS *(QUALITY OF SERVICE)*

Disusun Oleh

FARAH AYU ASHARI HARIS

19102096

Telah Diujikan dan Dipertahankan dalam Sidang Ujian TugasAkhir
Pada Tanggal:18 juli 2023

Penguji I,	Penguji II,	Penguji III,
(Cahyo Prihantoro, S.Kom., M.Eng)	(Alon Jala Tirta Segara, S.Kom., M.Kom)	(Agus Priyanto, S.Kom., M.Kom.)
NIDN. 0221019002	NIDN. 0607079301	NIDN. 0606118201

Pembimbing I,	Pembimbing II,
Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom	Arif Wirawan Muhammad, S.Kom., M.Kom
NIDN 0601098701	NIDN 0613038503

Dekan,

Auliya Burhanuddin, S.Si., M.Kom
NIK 19820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : **Farah Ayu Ashari Haris**
NIM : **19102096**
Program Studi : **S1 Teknik Informatika**

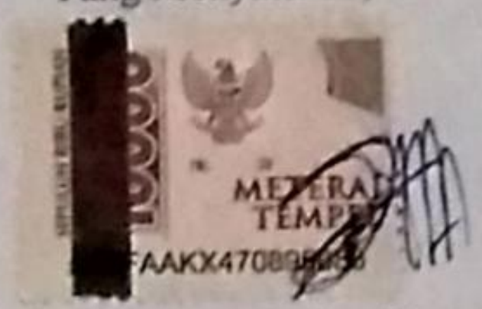
Menyatakan bahwa Tugas Akhir dengan judul berikut:
ANALISIS SISTEM KEAMANAN JARINGAN DENGAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) SNORT DAN HONEYPOT DENGAN MENGGUNAKAN QOS *(QUALITY OF SERVICE)*

Dosen Pembimbing : Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom
Dosen Pembimbing Pendamping : Arif Wirawan Muhammad, S.Kom.,M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing.
3. Dalam Karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima Sanksi Akademik dengan pencabutan gelar yang sudah diperoleh serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Purwokerto, 6 Juli 2023,

Yang Menyatakan,



(Farah Ayu Ashari Haris)

KATA PENGATAR

Puji syukur saya panjatkan kehadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan proposal penelitian ini dengan baik. Pada kesempatan ini penulis mengucapkan terima kasih kepada pihak yang telah membantu dalam penelitian ini, untuk itu penulis dalam kesempatan ini mengucapkan terima kasih kepada :

1. Allah SWT yang senantiasa melimpahkan rahmat dan karunia-Nya sehingga tugas akhir ini dapat terselesaikan dengan baik.
2. Dr. Tenia Wahyuningrum, S.Kom., M.T. selaku rektor Institut Teknologi Telom Purwokerto
3. Auliya Burhanuddin, S.Si., M. Kom selaku Dekan fakultas Informatika Institut Teknologi Telkom Purwokerto.
4. Amalia Belandina Arifa, S.Pd., M.Cs Selaku ketua program Studi S1 Informatika
5. Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom selaku dosen pembimbing pertama yang telah memberikan bimbingan dan pengarahan pada saat penyusunan penelitian tugas akhir.
6. Arif Wirawan Muhammad, S.Kom., M.Kom selaku dosen pembimbing kedua yang telah memberikan bimbingan dan pengarahan pada saat penyusunan tugas akhir penelitian.
7. Orang tua kakak, adik, mama aji dan bapak aji penulis yang selalu mendukung dalam do'a, suport dan material sehingga tugas akhir ini dapat berjalan dengan lancar dan baik.
8. Andi Muhardis yang selalu menemani hari-hari penulis dan senantiasa memberikan dukungan, motivasi dan do'a sehingga dapat menyelesaikan penelitian ini dengan baik dan lancar.
9. Rias Gauri, Chatrine, Arifah, Khusnul, Egidya, Ariesta, Mursyidah yang senantiasa memberikan dukungan dan motivasi dalam menyelesaikan tugas akhir ini.

Penulis menyadari bahwa masih banyak kekurangan dalam menyusun skripsi ini.Dalam penyusunan tugas akhir ini penulis berharap semoga tugas akhir ini dapat bermanfaat dan menambah wawasan bagi pembaca.

Purwokerto, 4 Juli 2023

Farah Ayu Ashari Haris

DAFTAR ISI

TUGAS AKHIR ii

LEMBAR PERSETUJUAN PEMBIMBING iii

LEMBAR PENGESAHAN iv

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR v

KATA PENGATAR vi

DAFTAR ISI viii

DAFTAR TABEL x

DAFTAR GAMBAR xiii

ABSTRAK xiv

ABSTRACT xv

BAB 1 PENDAHULUAN 1

1.1 LATAR BELAKANG 1

1.2 RUMUSAN MASALAH 3

1.3 PERTANYAAN PENELITIAN 4

1.4 BATASAN MASALAH 4

1.5 TUJUAN PENELITIAN 4

1.6 MANFAAT PENELITIAN 5

BAB II TINJAUAN PUSTAKA 6

2.1 TINJAUAN PUSTAKA 6

2.2 DASAR TEORI 12

2.2.1 JARINGAN INTERNET 12

2.2.2 FIREWALL 12

2.2.3 HONEYPOT 12

2.2.4 ZONA DEMILITERISASI (DMZ) 15

2.2.5 SNORT 15

2.2.6 INTRUSION DETECTION AND PREVENTION SYSTEMI (IDPS) 16

2.2.7 MAN IN THE MIDDLE (MiTM) 19

2.2.8 DISTRIBUTED DENIAL OF SERVICE (DDoS) 19

2.2.9 WIRESHARK.....20
2.2.10 QUALITY OF SERVICE (QOS).....21
BAB III METODOLOGI PENELITIAN.....24
3.1 OBJEK DAN SUBJEK PENELITIAN.....24
3.2 DIAGRAM DAN ALUR PENELITIAN.....24
3.2.1 IDENTIFIKASI MASALAH DAN STUDI LITERATUR.....25
3.2.2 PERANCANGAN SISTEM.....25
3.2.3 ANALISA KEBUTUHAN SISTEM.....27
3.2.4 INSTALASI DAN KONFIGURASI SISTEM.....28
3.2.5 SKENARIO PENGUJIAN SISTEM.....33
3.2.6 SKENARIO PENGUJIAN SERANGAN.....33
3.3 TEKNIK PENGUMPULAN DATA.....35
3.4 ANALISIS DATA.....35
BAB IV HASIL DAN PEMBAHASAN.....38
4.1 PENGUJIAN SERANGAN.....38
4.1.1 *Distributed Denial Of Service* (DDoS).....38
4.1.2 *Man in The Middle* (MiTM).....40
4.2 PENGUJIAN SISTEM.....40
4.3 PENGUKURAN QUALITY OF SERVICE).....42
4.3.1 *Throughput*.....43
4.3.2 *Delay*.....48
4.3.3 Jitter.....53
4.3.4 Packet Loss.....57
4.3.5 *Packet Delivery Ratio*.....60
BAB V KESIMPULAN DAN SARAN.....65
5.1 KESIMPULAN.....65
5.2 SARAN.....66
DAFTAR PUSTAKA.....67

DAFTAR TABEL

Tabel 2. 1 Tabel Penelitian Sebelumnya.....11

Tabel 3.1 Kebutuhan sistem.....28

Tabel 3.2 Standar Kualitas *Throughput*.....36

Tabel 3.3 Standar Quality Delay.....36

Tabel 3.4 Standar Kualitas *Jitter*.....37

Tabel 3.5 Standar Kualitas *Packet Loss*.....37

Tabel 4.1 Pengukuran *Quality of Service*.....43

Tabel 4.2 ICMP+Snort Throughput.....44

Tabel 4.3 ICMP tanpa Snort Throughput.....44

Tabel 4. 4 UDP tanpa Snort Throughput.....45

Tabel 4.5 UDP + Snort Throughput.....45

Tabel 4.6 MiTM tanpa Snort Throughput.....47

Tabel 4.7 MiTM + Snort Throughput.....47

Tabel 4.8 ICMP + Snort Delay.....48

Tabel 4. 9 ICMP tanpa Snort Delay.....49

Tabel 4.10 UDP tanpa Snort Delay.....50

Tabel 4.11 UDP + Snort Delay.....50

Tabel 4.12 MiTM Tanpa Snort Delay.....51

Tabel 4.13 MiTM + Snort Delay.....51

Tabel 4.14 ICMP + Snort JITTER.....53

Tabel 4.15 ICMP tanpa Snort JITTER.....53

Tabel 4.16 UDP tanpa Snort JITTER.....54

Tabel 4.17 UDP + Snort JITTER.....54

Tabel 4.18 MiTM tanpa Snort JITTER.....55

Tabel 4.19 MiTM + Snort JITTER.....56

Tabel 4.20 ICMP + Snort Packet Loss 57

Tabel 4.21 ICMP tanpa Snort Packet Loss 58

Tabel 4.22 UDP tanpa Snort Packet Loss 58

Tabel 4.23 UDP + Snort Packet Loss 59

Tabel 4.24 MiTM tanpa Snort Packet Loss 59

Tabel 4.25 MiTM + Snort Packet Loss 60

DAFTAR GAMBAR

Gambar 2.1 Penerapan IDS 17

Gambar 3.1 Alur Penelitian.....25

Gambar 3. 2 Topologi Perancangan Sistem 25

Gambar 3.3 Alur Kerja Sistem 26

Gambar 3.4 Penginstalan Snort Complete 29

Gambar 3.5 Konfigurasi Snort.conf 30

Gambar 3.6 Konfigurasi File Rules 31

Gambar 3.7 Penginstalan Depedensi Cowrie 31

Gambar 3.8 Mengambil cowrie di Github 32

Gambar 3.9 Menjalankan Python 32

Gambar 3.10 Mengaktifkan Lingkungan virtual python.....32

Gambar 3.11 Mengkonfigurasi cowrie 33

Gambar 3.12 Menjalankan cowrie 33

Gambar 3.13 skrnario pengujian serangan DDoS 34

Gambar 3.14 Skenario Pengujian Serangan Hping3 34

Gambar 3.15 Skenario Pengujian Serangan MiTM 34

Gambar 4.1 Proses Serangan DDoS Protokol UDP.....39

Gambar 4.2 Proses Serangan ARP *poisining* 40

Gambar 4.3 Sistem berhasil menjalankan IDPS untuk serangan ICMP flooding . 41

Gambar 4.4 Sistem berhasil menjalankan IDPS untuk serangan UDP flooding ...42

Gambar 4.5 Sistem berhasil menjalankan IDPS untuk serangan MiTM.....42

Gambar 4. 6 Grafik Pengukuran *Throughput* ICMP *Flooding* 44

Gambar 4.7 Grafik Pengukuran *Throughput* UDP *Flooding* 46

Gambar 4.8 Grafik Pengukuran *Throughput* MiTM 47

Gambar 4.9 Grafik Pengukuran *Delay* ICMP *Flooding* 49

Gambar 4. 10 Grafik Pengukuran *Delay* UDP *Flooding* 50

Gambar 4. 11 Grafik Pengukuran *Delay* MITM 52

Gambar 4.12 Grafik Pengukuran *Jitter* ICMP *Flooding* 53

Gambar 4.13 Grafik Pengukuran *Jitter* UDP *Flooding* 55

Gambar 4.14 Grafik Pengukuran *Jitter* MiTM 56

Gambar 4.15 Grafik pengukuran *Packet Loss* ICMP *Flooding* 58

Gambar 4.16 Grafik pengukuran *Packet Loss* UDP *Flooding* 59

Gambar 4.17 Grafik pengukuran *Packet Loss* MiTM 60

Gambar 4.18 Grafik pengukuran *Packet Delivery Ratio* ICMP 62

Gambar 4.19 Grafik pengukuran *Packet Delivery Ratio* UDP 63

Gambar 4.20 Grafik pengukuran *Packet Delivery Ratio* MiTM 64