RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN UNIVERSITAS AHMAD DAHLAN MELALUI APLIKASI MOBILE BERBASIS ANDROID DENGAN METODE *INTRUSION DETECTION SYSTEM*

SKRIPSI

Disusun Oleh:

HAMAS ARDYAN PRASETYO
1900018121

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS AHMAD DAHLAN

2024

LEMBAR PERSETUJUAN PEMBIMBING

SKRIPSI

RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN UNIVERSITAS AHMAD DAHLAN MELALUI APLIKASI MOBILE BERBASIS ANDROID DENGAN METODE *INTRUSION DETECTION SYSTEM*

Dipersiapkan dan disusun oleh:

HAMAS ARDYAN PRASETYO
1900018121

Program Studi S1 Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan

Telah disetujui oleh:

Pembimbing

Ir. Nuril Anwar, S.T., M.Kom.

NIPM : 19890409 201606 111 1228017

ii

LEMBAR PENGESAHAN

SKRIPSI

RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN UNIVERSITAS AHMAD DAHLAN MELALUI APLIKASI MOBILE BERBASIS ANDROID DENGAN METODE INTRUSION DETECTION SYSTEM

Dipersiapkan dan disusun oleh:

HAMAS ARDYAN PRASETYO
1900018121

Telah dipertahankan di depan Dewan Penguji
pada 20 Maret 2024
dan dinyatakan telah memenuhi syarat

Susunan Dewan Penguji

Ketua	**: Ir. Nuril Anwar, S.T., M.Kom.**	.....
Penguji 1	**: Bambang Robi'in, S.T., M.T.**	.....
Penguji 2	**: Guntur Maulana Zamroni, B.Sc., M.Kom.**	.....

Yogyakarta, 24 Maret 2024
Dekan Fakultas Teknologi Industri
Universitas Ahmad Dahlan

Prof. Dr. Ir. Siti Jamilatun, M.T.
NIPM : 19660812 199601 011 0784324

iii

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Hamas Ardyan Prasetyo
NIM	: 1900018121
Prodi	: Informatika
Judul TA/Skripsi	: Rancang Bangun Sistem Monitoring Keamanan Jaringan Universitas Ahmad Dahlan Melalui Aplikasi Mobile Berbasis Android dengan Metode *Intrusion Detection System*

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 Maret 2024

Mengetahui,
Dosen Pembimbing

Ir. Nuril Anwar, S.T., M.Kom.
NIPM : 19890409 201606 111 1228017

Yang menyatakan,

Hamas Ardyan Prasetyo
NIM. 1900018121

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan dibawah ini:

Nama : Hamas Ardyan Prasetyo

NIM : 1900018121

Email : hamas1900018121@webmail.uad.ac.id

Program Studi : Informatika

Fakultas : Teknologi Industri

Judul Tesis : RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN UNIVERSITAS AHMAD DAHLAN MELALUI APLIKASI MOBILE BERBASIS ANDROID DENGAN METODE *INTRUSION DETECTION SYSTEM*

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah mendapatkan gelar kesarjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian dan implementasi saya sendiri, tanpa bantuan pihak lain kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan di setujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 22 Maret 2024
Yang Menyatakan

(Hamas Ardyan Prasetyo)

v

Lampiran 2

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Hamas Ardyan Prasetyo

NIM : 1900018121 Email : hamas1900018121@webmail.uad.ac.id

Fakultas : Teknologi Industri Program Studi : Informatika

Judul tugas akhir : RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN UNIVERSITAS AHMAD DAHLAN MELALUI APLIKASI MOBILE BERBASIS ANDROID DENGAN METODE *INTRUSION DETECTION SYSTEM*

Dengan ini saya menyerahkan hak *sepenuhnya* kepada Perpustakaan Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut

Saya **(mengijinkan/~~tidak mengijinkan~~)*** karya tersebut diunggah ke dalam Repository Perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 22 Maret 2024

Hamas Ardyan Prasetyo

Mengetahui,
Pembimbing**

Ir. Nuril Anwar, S.T., M.Kom.

Ket:
*coret salah satu
**jika diijinkan TA dipublish maka ditandatangani dosen pembimbing dan mahasiswa

HALAMAN PERSEMBAHAN

Puji syukur yang mendalam dengan telah diselesaikannya skripsi atau tugas akhir ini, penulis persembahkan kepada:

1. Tuhan yang diyakini penulis, Allah SWT yang telah memberikan rahmatNya dan kesehatan sehingga saya masih diberikan kesempatan untuk menyelesaikan skripsi ini dengan lancar tanpa ada hambatan apapun dan saya selalu bersholawat kepada Nabi Muhammad SAW sebagai sosok panutan yang senantiasa memperhatikan umatnya.
2. Orang tua penulis, Ibu Murtasiyah dan Bapak Dwiyanto, Terimakasih (جزاك الله خيرا) atas kepercayaan, dukungan, doa yang selalu diberikan pada penulis agar selalu kuat dalam menghadapi segala tantangan yang ada.
3. Dosen Pembimbing Skripsi penulis, saya ucapkan terimakasih (جزاك الله خيرا) kepada bapak Ir. Nuril Anwar, S.T., M.Kom. yang telah memberikan saran, kritik dan arahan selama saya membuat laporan sejak Metodologi Penelitian hingga sampai pada Skripsi selesai.
4. Dosen Pembimbing Akademik penulis, saya ucapkan terimakasih (جزاك الله خيرا) kepada bapak Bambang Robi'in, S.T., M.T. yang telah memberikan masukan dan arahan selama saya 4 tahun berkuliah.
5. Teman satu angkatan, saya ucapkan terimakasih (جزاك الله خيرا) kepada Pradipa R. H. , Rahadewan R. , Muhid, Suprayogi B. P. dan Sulharjan F. yang telah memberikan semangat dan dukungan sampai saya dapat menyelesaikan skripsi ini.
6. Teman adik tingkat angkatan 20 penulis, saya ucapkan terimakasih (جزاك الله خيرا) atas dukungan selama saya menyusun laporan skripsi ini.
7. Teman seperjuangan TA Lab. Relata yang menemani disaat saya mengerjakan skripsi.

MOTTO

“Katakanlah: 'Dialah Allah Yang Maha Esa, Allah tempat bergantung (semata-mata).'"

(QS. Al-Ikhlas: 1-2)

“Dan sungguh Allah tidak akan mengubah nasib suatu kaum kecuali mereka mengubah keadaan yang ada pada diri mereka sendiri.”

(QS. Ar-Ra’d: 11)

"Dan katakanlah kepada hamba-hamba-Ku (wahai Muhammad), hendaklah mereka mengucapkan perkataan yang baik (yang bermanfaat)."

(QS. Al-Qalam: 4)

"Sesungguhnya Allah SWT menyukai orang-orang yang berlaku adil."

(QS. Al-Humaza: 8)

“Katakanlah: "Tidak ada yang terjadi kecuali dengan izin Allah." Dia Maha Mengetahui apa yang di hadapanmu dan apa yang di belakangmu. Dan kamu tidak kuasa sedikitpun melainkan dengan kehendak Allah."

(QS. Al-Hadid: 22)

Barang siapa bersungguh-sungguh pasti dia akan mendapatkan, barang siapa yang bersabar pasti dia akan menang, dan barang siapa yang meminta pasti dia akan diberi.

(HR. Ibnu Majah)

“Lebih baik terlambat daripada tidak sama sekali”

“Usaha tidak akan menghianati hasil”

“Jika orang lain bisa, maka aku juga harus bisa”

“Selesaikanlah apa yang sudah dimulai”

KATA PENGANTAR

Alhamdulillah, Segala puji dan syukur kehadirat Allah *Subhanahu wa ta'ala*, yang telah memberikan nikmat iman, nikmat sehat serta rahmad dan hidayahnya kepada kita semua, sehingga Penelitian Skripsi ini dapat terselesaikan dengan baik. Shalawat dan salam semoga senantiasa tercurah kepada junjungan kita Nabi Muhammad *Shalallahu 'Alaihi Wassalam* beserta keluarga dan para sahabat dan semoga kita semua sebagai umatnya bisa mendapatkan syafa'atnya di yaumul akhir**.**

Skripsi merupakan tugas akhir bagi mahasiswa untuk mendapatkan gelar sarjana dan lulus dari perguruan. Terselesaikannya skripsi ini, tidak terlepas dari dukungan dan bimbingan dari berbagai pihak dengan memberikan masukan dan kritik kepada penulis. Oleh sebab itu, penulis mengucapkan terimakasih kepada:

1. Prof. Dr. Muchlas, M.T. sebagai Rektor Universitas Ahmad Dahlan
2. Prof. Dr. Ir. Siti Jamilatun, M.T. sebagai Dekan Fakultas Teknologi Industri di Universitas Ahmad Dahlan
3. Dr. Murinto, S.Si., M.Kom. sebagai Kepala Prodi Informatika di Universitas Ahmda Dahlan
4. Ir. Nuril Anwar, S.T., M.Kom. sebagai Dosen Pembimbing Skripsi
5. Bambang Robi'in, S.T., M.T. sebagai Dosen Wali Akademik
6. Kedua orang tua yang selalu mendoakan dan memberikan dukungan.
7. Teman seperjuangan angkatan 2019 yang menemani, memberikan dukungan dan semangat
8. Adik Tingkat Angkatan 2020 yang selalu memberikan semangat dan dukungan.

Penulis menyadari perlunya saran dan kritik yang membangun untuk pengembangan yang lebih baik di masa yang akan datang. Akhir kata penulis mengucapkan banyak terima kasih dan semoga skripsi ini dapat bermanfaat bagi para pembaca.

Yogyakarta, 22 Maret 2024

Penulis

DAFTAR ISI

HALAMAN JUDUL i
LEMBAR PERSETUJUAN PEMBIMBING ii
LEMBAR PENGESAHAN iii
LEMBAR PERNYATAAN KEASLIAN iv
PERNYATAAN TIDAK PLAGIAT v
PERNYATAAN PERSETUJUAN AKSES vi
HALAMAN PERSEMBAHAN vii
MOTTO viii
KATA PENGANTAR ix
DAFTAR ISI x
DAFTAR GAMBAR xii
DAFTAR TABEL xiv
DAFTAR KODE PROGRAM xv
DAFTAR LAMPIRAN xvi
ABSTRAK xvii
BAB I Pendahuluan 1
1.1. Latar Belakang Masalah 1
1.2. Rumusan Masalah 3
1.3. Tujuan Penelitian 4
1.4. Batasan Masalah Penelitian 4
1.5. Manfaat Penelitian 5
BAB II Tinjauan Pustaka 6
2.1. Kajian Penelitian Terdahulu 6
2.2. Landasan Teori 11
BAB III Metodologi Penelitian 30
3.1. Metode Pengumpulan Data 30
3.2. Alat dan Bahan 31
3.3. Tahapan Penelitian 32
BAB IV Hasil dan Pembahasan 35
4.1. Analisis Kebutuhan 35
4.2. Perancangan 36
4.3. Implementasi 50
4.4. Pengujian 75
4.5. Analisis Hasil 112
BAB V Kesimpulan dan Saran 117
5.1 Kesimpulan 117
5.2 Saran 118
DAFTAR PUSTAKA 119
LAMPIRAN 122
Lampiran 1. Uji 1 *Rules* Snort IDS Deteksi Serangan DoS/DDoS 122

Lampiran 2. Uji 2 *Rules* Snort IDS Deteksi Serangan DoS/DDoS 126
Lampiran 3. Uji 3 *Rules* Snort IDS Deteksi Serangan DoS/DDoS 131
Lampiran 4. Uji 1 *Rules* Snort IDS Deteksi *Port Scanning* 135
Lampiran 5. Uji 2 *Rules* Snort IDS Deteksi *Port Scanning* 137
Lampiran 6. Uji 3 *Rules* Snort IDS Deteksi *Port Scanning* 139
Lampiran 7. Uji *Respon Time* Notifikasi *Alert* IDS dari Serangan DoS/DDoS 142
Lampiran 8. Uji *Respon Time* Notifikasi *Alert* IDS dari Serangan *Port Scanning* 146
Lampiran 9. *BlackBox Testing* Sistem Aplikasi 149

DAFTAR GAMBAR

Gambar 2.1 Model Pengembangan *Waterfall* 11
Gambar 2.2 *Local Area Network* (LAN) 14
Gambar 2.3 *Metropolitan Area Network* (MAN)..... 14
Gambar 2.4 *Wide Area Network* (WAN) 15
Gambar 2.5 Konsep Dasar *Network-based Intrusion Detection System* (NIDS)..... 19
Gambar 2.6 Konsep Dasar *Host-Based Intrusion Detection System* (HIDS) 20
Gambar 2.7 Skema Cara Kerja *Short Message Service* (SMS) 21
Gambar 2.8 Model Skema SMS *Gateway* 22
Gambar 2.9 Komponen Snort IDS 25
Gambar 2.10 Ilustrasi Serangan DoS/DDoS [23]. 27
Gambar 3.1 *Flowchart* Tahapan Penelitian. 32
Gambar 4.1 Topologi Jaringan IDS 36
Gambar 4.2 Fitur *Dashboard* Statistik..... 37
Gambar 4.3 Fitur *Update* Kontak Admin Jaringan 38
Gambar 4.4 *Entity Relationship Diagram* (ERD) Sistem Snort 39
Gambar 4.5 Proses Bisnis Sistem Monitoring keamanan Jaringan 45
Gambar 4.6 *Wireframe* Tampilan Selamat Datang 46
Gambar 4.7 *Wireframe* Tampilan Statistik..... 47
Gambar 4.8 *Wireframe* Tampilan Pengaturan..... 48
Gambar 4.9 *Wireframe* Tampilan Pengaturan Nomor Admin Jaringan..... 49
Gambar 4.10 Tampilan Ambil Data Statistik Serangan Pada Browser 60
Gambar 4.11 Tampilan SMS Notifikasi Serangan..... 63
Gambar 4.12 Tampilan *Push* Notifikasi pada Aplikasi..... 64
Gambar 4.13 Halaman *Welcome* Aplikasi 66
Gambar 4.14 Halaman Statistik..... 68
Gambar 4.15 Halaman Pengaturan..... 71
Gambar 4.16 Halaman Pengaturan Data Kontak Admin Jaringan 74
Gambar 4.17 Proses Serangan DoS SYN ke *Port* 80 Http dan 443 Https 75
Gambar 4.18 Proses Rule dalam Mendeteksi Serangan DoS SYN di Sisi Snort..... 76
Gambar 4.19 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS SYN..... 77
Gambar 4.20 Proses Serangan DoS ACK ke *Port* 80 Http dan 443 Https 78
Gambar 4.21 Proses Rule dalam Mendeteksi Serangan DoS ACK 78
Gambar 4.22 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoSACK..... 79
Gambar 4.23 Proses Serangan DoS FIN ke *Port* 80 Http dan 443 Https 80
Gambar 4.24 Proses Rule dalam Mendeteksi Serangan DoS FIN..... 81
Gambar 4.25 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS FIN..... 82
Gambar 4.26 Proses Serangan DoS RST ke *Port* 80 Http dan 443 Https..... 83
Gambar 4.27 Proses Rule dalam Mendeteksi Serangan DoS RST 83
Gambar 4.28 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS RST 84
Gambar 4.29 Proses Serangan DoS PSH ke *Port* 80 Http dan 443 Https 85

Gambar 4.30 Proses Rule dalam Mendeteksi Serangan DoS PSH..... 86
Gambar 4.31 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS PUSH 87
Gambar 4.32 Proses Serangan DoS tanpa *Flags* ke Alamat Server..... 88
Gambar 4.33 Proses Rule dalam Mendeteksi Serangan DoS tanpa *Flags* 88
Gambar 4.34 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS Tanpa *Flags* 89
Gambar 4.35 Proses Serangan DoS UDP ke Alamat Server..... 90
Gambar 4.36 Proses Rule dalam Mendeteksi Serangan DoS UDP..... 90
Gambar 4.37 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS UDP 91
Gambar 4.38 Proses Serangan DoS ICMP ke Alamat Server..... 92
Gambar 4.39 Proses Rule dalam Mendeteksi Serangan DoS ICMP 93
Gambar 4.40 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan DoS/DDoS ICMP..... 94
Gambar 4.41 Proses Serangan *PortScan* SYN ke Alamat Server dengan Tool nmap 95
Gambar 4.42 Proses Rule dalam Mendeteksi Serangan *PortScan* SYN..... 96
Gambar 4.43 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan *PortScan* SYN 97
Gambar 4.44 Proses Serangan *PortScan* ACK ke Alamat Server dengan Nmap..... 98
Gambar 4.45 Proses Rule dalam Mendeteksi Serangan *PortScan* ACK..... 99
Gambar 4.46 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan *PortScan* ACK 100
Gambar 4.47 Proses Serangan *PortScan* FIN ke Alamat Server dengan nmap 101
Gambar 4.48 Proses Rule dalam Mendeteksi Serangan *PortScan* FIN..... 102
Gambar 4.49 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan *PortScan* FIN 103
Gambar 4.50 Proses Serangan *PortScan* UDP ke Alamat Server dengan nmap 104
Gambar 4.51 Proses Rule dalam Mendeteksi Serangan *PortScan* UDP..... 105
Gambar 4.52 Notifikasi Aplikasi dan Notifikasi SMS dari Serangan *PortScan* UDP..... 106
Gambar 4.53 Sebelum dilakukan Uji Beban *Traffic*..... 107
Gambar 4.54 Proses Uji Beban *Traffic* Tinggi pada *Rule* DoS *SYN*..... 108
Gambar 4.55 Paket yang Tertangkap di *Tools* Wireshark Saat Uji Beban *Traffic* 109

DAFTAR TABEL

Tabel 2.1 Kajian Penelitian Terdahulu 9
Tabel 3.1 Spesifikasi *Hardware* yang akan digunakan pada Penelitian ini 31
Tabel 4.1 Kebutuhan Fungsional Sistem 35
Tabel 4.2 Kebutuhan Non-Fungsional Sistem 35
Tabel 4.3 Struktur Tabel Nomor Telepon Administrator 39
Tabel 4.4 Struktur Tabel Sensor Perangkat 40
Tabel 4.5 Struktur Tabel *Encoding Log* Serangan 41
Tabel 4.6 Struktur Tabel *Detail* Tipe *Log* Serangan 41
Tabel 4.7 Struktur Tabel *Signature* Serangan 41
Tabel 4.8 Struktur Tabel *Signature Class* 42
Tabel 4.9 Struktur Tabel *Event* Serangan 42
Tabel 4.10 Struktur Tabel *Header Internet Protocol* (IP) 42
Tabel 4.11 Struktur Tabel *Header* Protokol TCP 43
Tabel 4.12 Struktur Tabel *Header* Protokol UDP 43
Tabel 4.13 Struktur Tabel *Header* Protokol ICMP 44
Tabel 4.14 Skenario Pengujian Halaman Dashboard Statistik 110
Tabel 4.15 Skenario Pengujian Halaman Dashboard Statistik 2 110
Tabel 4.16 Skenario Pengujian Halaman Pengaturan Nomor Admin 111
Tabel 4.17 Persentase *Rules* IDS dalam Mendeteksi Serangan 112
Tabel 4.18 Waktu Respon Notifikasi *Alert* IDS 115

DAFTAR KODE PROGRAM

Kode Program 4.1 *Rule* Deteksi Serangan DoS SYN 50
Kode Program 4.2 *Rule* Deteksi serangan DoS ACK 50
Kode Program 4.3 *Rule* Deteksi serangan DoS RST 51
Kode Program 4.4 *Rule* Deteksi serangan DoS FIN 51
Kode Program 4.5 *Rule* Deteksi serangan DoS PSH 52
Kode Program 4.6 *Rule* Deteksi Serangan DoS tanpa *Flags* 52
Kode Program 4.7 *Rule* Deteksi Serangan DoS UDP 53
Kode Program 4.8 *Rule* Deteksi Serangan DoS ICMP 53
Kode Program 4.9 *Rule* Deteksi Serangan Port Scanning TCP SYN 54
Kode Program 4.10 *Rule* Deteksi Serangan Port Scanning TCP ACK 54
Kode Program 4.11 *Rule* Deteksi Serangan *Port Scanning* TCP FIN 55
Kode Program 4.12 *Rule* Deteksi Serangan *Port Scanning* UDP 55
Kode Program 4.13 Mengambil Data Statistik Dari Basis Data 59
Kode Program 4.14 *Update* Kontak Admin Jaringan 60
Kode Program 4.15 Kirim Notifikasi Peringatan *Via* SMS 62
Kode Program 4.16 Halaman Selamat Datang 65
Kode Program 4.17 Halaman Dashboard Statistik 68
Kode Program 4.18 Halaman Pengaturan 70
Kode Program 4.19 Halaman *Form* Pengaturan Nomor Kontak Admin 73

DAFTAR LAMPIRAN

Lampiran 1. Uji 1 *Rules* Snort IDS Deteksi Serangan DoS/DDoS 122
Lampiran 2. Uji 2 *Rules* Snort IDS Deteksi Serangan DoS/DDoS 126
Lampiran 3. Uji 3 *Rules* Snort IDS Deteksi Serangan DoS/DDoS 131
Lampiran 4. Uji 1 *Rules* Snort IDS Deteksi *Port Scanning* 135
Lampiran 5. Uji 2 *Rules* Snort IDS Deteksi *Port Scanning* 137
Lampiran 6. Uji 3 *Rules* Snort IDS Deteksi *Port Scanning* 139
Lampiran 7. Uji *Respon Time* Notifikasi *Alert* IDS dari Serangan DoS/DDoS 142
Lampiran 8. Uji *Respon Time* Notifikasi *Alert* IDS dari Serangan *Port Scanning* 146
Lampiran 9. *BlackBox Testing* Sistem Aplikasi 149

RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN UNIVERSITAS AHMAD DAHLAN MELALUI APLIKASI MOBILE BERBASIS ANDROID MENGGUNAKAN METODE *INTRUSION DETECTION SYSTEM*

Hamas Ardyan Prasetyo
1900018121

ABSTRAK

Keamanan jaringan merupakan salah satu faktor penting dalam mengamankan data pada sebuah server dalam jaringan komputer, sehingga sebuah server perlu untuk dijaga keamanannya dari hal-hal yang dapat mengancam validitas dan integritas data yang tersimpan didalam server tersebut. salah satu cara yang dapat digunakan untuk mendeteksi ancaman pada sebuah server yaitu mengimplementasikan sebuah *Intrusion detection system* Snort ke server. Studi literatur yang dilakukan pada penelitian yang mengimplementasi *intrusion detection system,* menemukan bahwa kurangnya penelitian *intrusion detection system* yang dapat mendeteksi satu jenis serangan keamanan jaringan dengan variasi variabel serangannya dan ditemukan juga pada penelitian yang sudah berhasil mengimplementasikan *intrusion detection system* untuk mendeteksi serangan keamanan jaringan namun masih salah dalam mengidentifikasi jenis serangan.

Penelitian ini menggunakan metode *intrusion detection system* Snort dengan model eksperimental sistem deteksi serangan dan aplikasi android yang diterapkan untuk memonitoring statistik serangan yang terdeteksi pada jaringan Universitas Ahmad Dahlan, pengumpulan data dilakukan dengan cara observasi, wawancara dan studi literatur. Alat yang digunakan dalam penelitian ini yaitu satu buah perangkat sebagai *IDS* Snort, satu buah perangkat sebagai *web* server yang menjadi target uji coba serangan, dua buah perangkat untuk membuat *traffic* lalu lintas, satu buah perangkat untuk membuat *traffic* serangan dan satu buah perangkat *smartphone* yang akan terinstal aplikasi untuk menampilkan grafik statistik serangan dan menerima notifikasi peringatan dari IDS Snort.

Berdasarkan hasil penelitian dapat diperoleh hasil *rules* yang dibuat pada snort IDS dapat mendeteksi serangan-serangan yang terjadi pada jaringan, khususnya pada penelitian ini serangan DoS/DDoS dan *Port Scanning*. Lalu telah dibuat sistem *Intrusion Detection System* yang dapat mengirimkan notifikasi peringatan *via* aplikasi dan *via* SMS dengan waktu respon yang masuk pada indikator cukup responsif berdasarkan acuan NIST *Cybersecurity Framework* dengan rata-rata 22 detik untuk serangan DoS/DDoS dan 21 detik untuk serangan *Port Scanning*, Untuk hasil persentase dari 3 kali pengujian *rule* dengan mengirimkan paket serangan DoS/DDoS sebanyak 309.462 hingga 1.459.548, mendapatkan tingkat akurasi yang tinggi dengan rata-rata sebesar 92,1% pada *test* pertama, 91,7% pada *test* kedua dan 91,5% pada *test* ketiga. Pada hasil pengujian *rule* dengan mengirimkan paket serangan *Port Scanning* sebanyak 1.001 hingga 10.564 paket didapat tingkat akurasi yang tinggi juga dengan hasil rata-rata sebesar 92,2% pada *test* pertama, 94,2% pada *test* kedua dan 93,4% pada *test* ketiga.

Kata Kunci: Aplikasi Android; *Intrusion Detection System (IDS)*; Keamanan Jaringan; Sistem Monitoring; Universitas Ahmad Dahlan