

DAFTAR ISI

| | |
|--|------------|
| KATA PENGANTAR | i |
| ABSTRAK | ii |
| ABSTRACT | iii |
| DAFTAR ISI | iv |
| DAFTAR TABEL | vi |
| DAFTAR GAMBAR | vii |
| DAFTAR PERSAMAAN | ix |
| DAFTAR LAMPIRAN | x |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Batasan Masalah..... | 2 |
| 1.4 Tujuan..... | 3 |
| 1.5 Manfaat..... | 3 |
| 1.6 Sistematika Penulisan..... | 3 |
| BAB II KAJIAN TEORI | 5 |
| 2.1 Penelitian Terkait | 5 |
| 2.2 Apache Web Server..... | 6 |
| 2.3 Honeypot | 6 |
| 2.4 Mysql Database | 7 |
| 2.5 Brute-Force..... | 8 |
| 2.5.1 Definisi Brute Force..... | 8 |
| 2.5.2 Serangan Brute Force..... | 8 |
| 2.5.3 Karakter/ Indikator Brute Force..... | 10 |
| 2.6 Python Programming..... | 10 |
| 2.7 Definisi Login..... | 11 |
| 2.8 PHP..... | 11 |
| 2.9 Precision and Recall | 11 |
| 2.10 Socket | 13 |

| | |
|--|-----------|
| BAB III METODOLOGI PENELITIAN DAN PERANCANGAN | 15 |
| 3.1 Studi Literatur..... | 16 |
| 3.2 Analisis Kebutuhan | 16 |
| 3.3 Perancangan Sistem..... | 18 |
| 3.3.1 Perancangan Program Pendeteksi Brute-Force..... | 21 |
| 3.3.2 Perancangan Database Sistem | 22 |
| 3.4 Implementasi Sistem | 23 |
| 3.5 Pengujian Sistem | 24 |
| 3.5 Pengambilan Kesimpulan..... | 26 |
| BAB IV IMPLEMENTASI | 27 |
| 4.1 Lingkungan Jaringan Sistem | 27 |
| 4.2 Implementasi Honeypot Server | 29 |
| 4.2.1 Implementasi <i>True Web Server</i> | 29 |
| 4.2.2 Implementasi <i>Fake Web Server</i> | 33 |
| 4.3 Implementasi Server Pendeteksi Paket..... | 36 |
| 4.3.1 Implementasi Program Pendeteksi Paket <i>Brute-Force</i> | 36 |
| 4.3.1.1 Implementasi NewEgineServer.py | 39 |
| 4.3.1.2 Implementasi engineServer.conf | 49 |
| 4.3.2 Implementasi Database Program Server Pendeteksi Paket <i>Brute-Force</i> | 50 |
| BAB V PENGUJIAN DAN ANALISIS..... | 54 |
| 5.1 Pengujian | 54 |
| 5.1.1 Pengujian Pengiriman Paket <i>Non-Brute-Force</i> | 54 |
| 5.1.2 Pengujian Pengiriman Paket <i>Brute-Force</i> | 56 |
| 5.2 Hasil Pengujian dan Analisis..... | 58 |
| 5.2.1 Analisis Pengujian Pengiriman Paket <i>Non-Brute-Force</i> | 59 |
| 5.2.2 Analisis Pengujian Pengiriman Paket <i>Brute-Force</i> | 65 |
| BAB VI PENUTUP | 72 |
| 6.1 Kesimpulan..... | 72 |
| 6.2 Saran | 72 |
| DAFTAR PUSTAKA | 74 |
| LAMPIRAN..... | 75 |



DAFTAR TABEL

| | |
|---|----|
| Tabel 2.1 Tabel kelebihan dan kelemahan Brute-force | 9 |
| Tabel 2.2 Parameter indikator terjadinya serangan <i>brute-force</i> | 10 |
| Tabel 2.3 Tabel parameter kondisi dari variable hitung | 13 |
| Tabel 3.1 Kebutuhan Perangkat Keras | 17 |
| Tabel 3.2 Tabel Kebutuhan Perangkat Lunak | 17 |
| Tabel 3.3 Penjelasan kegunaan tiap-tiap tabel pada perancangan <i>database</i> sistem | 23 |
| Tabel 3.4 Pengujian Pengiriman Paket | 24 |
| Tabel 3.5 Skenario Pengujian Pengiriman Paket <i>Non-Brute-Force</i> | 25 |
| Tabel 3.6 Skenario Pengujian Pengiriman Paket <i>Brute-Force</i> | 25 |
| Tabel 4.1 Nama berkas dan deskripsi singkat | 39 |
| Tabel 4.2 Keterangan atribut tabel <i>tb_block</i> | 51 |
| Tabel 4.3 Keterangan atribut tabel <i>tb_host</i> | 51 |
| Tabel 4.4 Keterangan atribut tabel <i>tb_log</i> | 52 |
| Tabel 4.5 Keterangan atribut tabel <i>tb_normal_user</i> | 52 |
| Tabel 4.6 Keterangan atribut tabel <i>tb_request</i> | 53 |
| Tabel 5.1 Skenario pengujian pengiriman paket <i>non-brute-force</i> | 55 |
| Tabel 5.2 Data hasil pengujian pengiriman paket <i>non-brute-force</i> | 56 |
| Tabel 5.3 Skenario pengujian pengiriman paket <i>brute-force</i> | 57 |
| Tabel 5.4 Data hasil pengujian pengiriman paket <i>brute-force</i> | 58 |
| Tabel 5.5 Presentase tingkat keberhasilan sisem mendeteksi paket <i>non-brute-force</i> | 61 |
| Tabel 5.6 Presentase tingkat keberhasilan sisem mendeteksi paket <i>brute-force</i> ... | 69 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2.1 Diagram Konteks Honeypot..... | 6 |
| Gambar 2.2 Langkah operasi socket TCP..... | 14 |
| Gambar 3.1 Diagram Alir Keseluruhan Pelaksanaan Penelitian | 15 |
| Gambar 3.2 Topologi sistem..... | 19 |
| Gambar 3.3 Diagram alir algoritma program..... | 21 |
| Gambar 4.1 Lingkungan Jaringan Sistem | 28 |
| Gambar 4.2 Instalasi apache2 milik <i>true web server</i> | 29 |
| Gambar 4.3 Tampilan halaman web server apache2 milik <i>true web server</i> | 30 |
| Gambar 4.4 Instalasi php5 milik <i>true web server</i> | 31 |
| Gambar 4.5 Instalasi mysql milik <i>true web server</i> | 31 |
| Gambar 4.6 Proses pemberian password root MySQL..... | 32 |
| Gambar 4.7 Proses konfirmasi password root MySQL | 32 |
| Gambar 4.8 Konfigurasi IP address pada file <i>interfaces</i> milik <i>true web server</i> ... | 33 |
| Gambar 4.9 Instalasi apache2 milik <i>fake web server</i> | 34 |
| Gambar 4.10 Tampilan halaman web server apache2 milik <i>fake web server</i> | 34 |
| Gambar 4.11 Instalasi php5 milik <i>fake web server</i> | 35 |
| Gambar 4.12 Konfigurasi IP address pada file <i>interfaces</i> milik <i>fake web server</i> . 35 | |
| Gambar 4.13 Proses instalasi python pada komputer server pendeteksi paket..... | 36 |
| Gambar 4.14 Cek instalasi python | 37 |
| Gambar 4.15 Konfigurasi file <i>interfaces</i> pada PC 3 <i>brute-force detector</i> | 38 |
| Gambar 4.16 Source code fungsi def on_recv sebagai pembaca paket | 40 |
| Gambar 4.17 Source code fungsi def isBlocked | 41 |
| Gambar 4.18 Source code fungsi def insertReq..... | 42 |
| Gambar 4.19 Source code fungsi def attempCount | 43 |
| Gambar 4.20 Source code fungsi def blockUser..... | 46 |
| Gambar 4.21 Source code fungsi def on_accept..... | 47 |
| Gambar 4.22 Konfigurasi file <i>egineServer.conf</i> | 49 |
| Gambar 4.23 Tabel database <i>db_brute_log</i> | 50 |
| Gambar 5.1 Konfigurasi Syntax <i>Hydra</i> | 57 |

Gambar 5.2 Hasil log *server* untuk skenario pengujian pengiriman paket *non brute-force*..... 60

Gambar 5.3 Grafik Tingkat Akurasi Sistem Pada Percobaan Pengiriman Paket *non-brute-force* 63

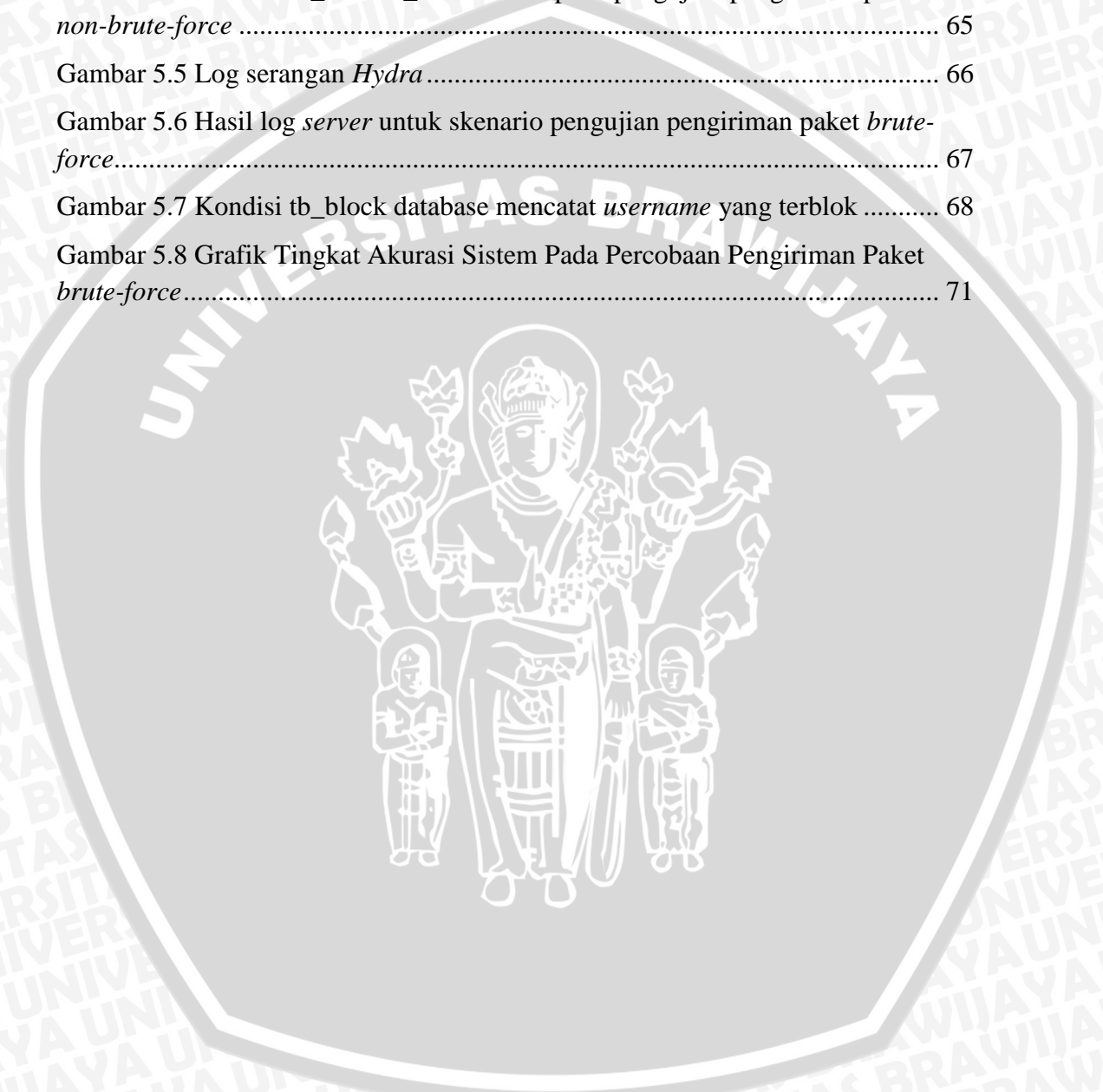
Gambar 5.4 Kondisi *tb_normal_user* setelah pada pengujian pengiriman paket *non-brute-force* 65

Gambar 5.5 Log serangan *Hydra*..... 66

Gambar 5.6 Hasil log *server* untuk skenario pengujian pengiriman paket *brute-force*..... 67

Gambar 5.7 Kondisi *tb_block* database mencatat *username* yang terblok 68

Gambar 5.8 Grafik Tingkat Akurasi Sistem Pada Percobaan Pengiriman Paket *brute-force*..... 71



DAFTAR PERSAMAAN

| | |
|---------------------|----|
| Persamaan 2.1 | 12 |
| Persamaan 2.2 | 12 |
| Persamaan 2.3 | 12 |



DAFTAR LAMPIRAN

| | |
|--|----|
| Lampiran 1. Diagram Alur Implementasi True Web Server..... | 75 |
| Lampiran 2. Diagram Alur Implementasi Fake Web Server | 76 |
| Lampiran 3. Diagram Alur Implementasi Server Pendeteksi Paket Brute-Force 77 | 77 |
| Lampiran 4. Konfigurasi IP <i>client</i> | 78 |
| Lampiran 5. Konfigurasi <i>egineServer.conf</i> | 79 |
| Lampiran 6. Source code program server pendeteksi paket brute-force “NewEgineServer.py” | 79 |
| Lampiran 7. Dump query database program server pendeteksi paket brute-force | 91 |
| Lampiran 8. Dump query simulasi database web admin pada true web server | 92 |

