

ABSTRAKSI

Perkembangan dunia teknologi yang semakin memudahkan para penggunanya mengakses informasi, seringkali menimbulkan dampak negatif bagi sistem keamanan. Keinginan seseorang semisal *hacker/cracker* untuk merusak atau bahkan mendapatkan informasi ilegal dari sebuah sistem, menuntut sistem keamanan untuk siap menanganinya. Keberadaan *malware, spyware, virus*, atau program lain yang berbahaya seringkali membuat seorang admin sistem kesulitan untuk sekedar menganalisa dan mendapatkan cukup informasi mengenai *file* tersebut.

Sistem ini dibuat untuk menjawab kebutuhan admin sistem dalam memonitor *malware* pada VPS. Sistem diintegrasikan dengan *honeypot* sebagai penangkap *malware* yang terinstall pada VPS, berguna untuk memberikan cukup informasi mengenai *file* berbahaya yang berhasil ditangkap oleh *honeypot*. Hasil *analysis* didapat dari integrasi dengan www.virustotal.com sebagai media analisator *file binary*.

Setelah dilakukan pengujian dan implementasi, didapatkan kesimpulan bahwa aplikasi *reporting* untuk *honeypot* berbasis *website* dapat meningkatkan keamanan pada VPS dari serangan *malware*. Selain itu, aplikasi ini juga mudah dimengerti, dipelajari, dan digunakan. Aplikasi ini memudahkan para *admin system* dalam memonitor VPS. Fitur pada aplikasi dapat di maksimalkan sebagai media *report* yang lengkap (*addressed RPC/DCE calls, attacked port, attacks offer a day, attacker country information, popular malware download, popular download location, dionaea statistik*). Aplikasi ini memberikan cukup informasi mengenai *detail malware* berdasarkan *analysis* dari beberapa *Antivirus*.

Kata kunci : *Malware, Honeypot, Report, Analysis*

ABSTRACT

The development of technology that make it easier for users to access information, sometimes have negative impact to security system. The urge of a person (hacker, cracker, etc) to retrieve private information from a system has to be anticipated by developing a security system. Malwares, spywares, virus or other dangerous software could initiate lots of problem for system administrator to handle and analyze information about those.

This system is built to answer the needs of a system administrator, to monitor the conditions of the server (VPS). This system is integrated with honeypot as a malware catcher installed in VPS, it is usefull to display various informations about the malicious file captured by honeypot. Analysis of the report is based on www.virustotal.com as a media to analyze binary files.

After thorough testing and implementation of this application, the main conclusions is this application are this web-based application for honeypot is capable to increase security level of the VPS in terms of malware attack. This application also is easy to understand, easy to learn, and easy to use. Beside that, this application allows administrator to monitor their VPS server. The feature of honeypot application can be maximized as a complete media report (addressed RPC/DCE calls, attacked port, attacks offer a day, attacker country information, popular malware download, popular download location, *dionaea* statistik). This application also provides sufficient malware details based on multiple antivirus analysis.

Keywords : *Malware, Dionaea, Report, Analysis*

DAFTAR ISI

| | |
|---|-------------|
| ABSTRAKSI | vi |
| ABSTRACT | vii |
| LEMBAR PENGESAHAN | ii |
| PERANCANGAN APLIKASI WEB-BASED REPORTING | ii |
| UNTUK HONEYPOT DIONAEA | ii |
| PERNYATAAN ORISINALITAS LAPORAN PENELITIAN | iii |
| PERNYATAAN PUBLIKASI LAPORAN PENELITIAN | iv |
| PRAKATA | v |
| DAFTAR ISI | vi |
| DAFTAR GAMBAR | xii |
| DAFTAR TABEL | xiv |
| DAFTAR SIMBOL | xv |
| DAFTAR LAMPIRAN | xvii |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Tujuan Pembahasan..... | 2 |
| 1.4 Ruang Lingkup Penelitian | 2 |
| 1.5 Metodologi Penelitian | 2 |
| 1.5.1 Studi Literature | 3 |
| 1.5.2 Wawancara | 3 |
| 1.5.3 Pengembangan Aplikasi | 3 |
| 1.6 Sistematika Pembahasan | 4 |
| BAB 2 LANDASAN TEORI | 5 |
| 2.1 Definisi <i>Honeypot</i> | 5 |
| 2.2 Klasifikasi <i>Honeypot</i> | 6 |
| 2.2.1 <i>Low Interaction Honeypot</i> | 6 |

| | | |
|--------------|---|-----------|
| 2.2.2 | <i>Medium Interaction Honeypot</i> | 6 |
| 2.2.3 | <i>High Interaction Honeypot</i> | 7 |
| 2.3 | <i>Malware</i> | 7 |
| 2.4 | <i>VPS (Virtual Private Server)</i> | 8 |
| 2.5 | <i>PHP</i> | 8 |
| 2.6 | <i>MySQL</i> | 9 |
| 2.7 | <i>Virus Total</i> | 11 |
| 2.8 | <i>UML</i> | 12 |
| 2.8.1 | <i>Use-case Diagram</i> | 13 |
| 2.8.2 | <i>Crow's Foot Notation</i> | 14 |
| 2.8.3 | <i>Flowchart</i> | 15 |
| 2.8.4 | <i>Activity Diagram</i> | 16 |
| 2.9 | <i>Pseudocode</i> | 17 |
| 2.10 | <i>Nephentes</i> | 18 |
| 2.11 | <i>Dionaea</i> | 18 |
| 2.12 | <i>DCE/RPC</i> | 19 |
| BAB 3 | ANALISA DAN PERANCANGAN | 20 |
| 3.1. | <i>Analisis Kebutuhan</i> | 20 |
| 3.1.1. | <i>Kebutuhan Perangkat Keras</i> | 20 |
| 3.1.2. | <i>Kebutuhan Perangkat Lunak</i> | 21 |
| 3.2. | <i>Gambaran Pengimplementasian Honeypot</i> | 22 |
| 3.3. | <i>Flowchart Pembuatan Report Malware Detection</i> | 23 |
| 3.4. | <i>Use case Diagram</i> | 24 |
| 3.5. | <i>Activity Diagram</i> | 30 |
| 3.5.1. | <i>Proses Login</i> | 30 |
| 3.5.2. | <i>Melihat Report</i> | 31 |
| 3.5.3. | <i>Melihat Detail Malware</i> | 32 |
| 3.5.4. | <i>Melihat Analysis Malware</i> | 33 |
| 3.5.5. | <i>Mengunduh Details Malware via PDF</i> | 34 |
| 3.5.6. | <i>Melihat Chart</i> | 35 |
| 3.5.7. | <i>Mengirim Report via Email</i> | 36 |
| 3.5.8. | <i>Mengganti Password</i> | 37 |

| | | |
|--------|---|----|
| 3.6. | ERD (<i>Entity Relationship Diagram – Crow’s Foot Notation</i>) | 38 |
| 3.7. | Rancangan <i>User Interface</i> | 39 |
| 3.7.1. | Halaman <i>Login</i> | 39 |
| 3.7.2. | Halaman <i>Utama</i> | 40 |
| 3.7.3. | Halaman <i>View Chart</i> | 41 |
| 3.7.4. | Halaman <i>Change Password</i> | 42 |
| 3.7.5. | Halaman <i>Detail Malware</i> | 43 |
| 3.7.6. | Halaman <i>Analysis Malware(AntiVirus)</i> | 44 |
| 3.7.7. | Halaman <i>Report</i> | 45 |

BAB 4 HASIL IMPLEMENTASI 47

| | | |
|---------|--|----|
| 4.1. | Implementasi <i>Honeypot</i> | 47 |
| 4.2. | <i>Table Implementation</i> Aplikasi untuk <i>Honeypot</i> | 48 |
| 4.3. | Implementasi Aplikasi untuk <i>Honeypot</i> | 49 |
| 4.3.1. | Halaman <i>Login</i> | 50 |
| 4.3.2. | Halaman <i>Utama</i> | 51 |
| 4.3.3. | Halaman <i>View Chart</i> | 52 |
| 4.3.4. | Halaman <i>Change Password</i> | 53 |
| 4.3.5. | Halaman <i>Analysis</i> | 54 |
| 4.3.6. | Halaman <i>Analysis (Antivirus)</i> | 56 |
| 4.3.7. | Halaman <i>Analisis Malware (www.virustotal.com)</i> | 58 |
| 4.3.8. | Halaman <i>Report</i> | 59 |
| 4.3.9. | <i>Attacked Port Pop Up</i> | 61 |
| 4.3.10. | <i>Attack Over a Day Pop Up</i> | 62 |
| 4.3.11. | <i>Popular Malware Download Pop Up</i> | 64 |
| 4.3.12. | <i>Busy Attacker Pop Up</i> | 66 |
| 4.3.13. | <i>Attacker Ask to Download Pop Up</i> | 68 |
| 4.3.14. | <i>Popular Download Location Pop Up</i> | 70 |
| 4.3.15. | <i>Addressed DCE/RPC Calls Pop Up</i> | 72 |
| 4.3.16. | <i>Most Recent Download Pop Up</i> | 74 |
| 4.3.17. | <i>Dionaea Statistik Pop Up</i> | 76 |
| 4.3.18. | <i>Attacker Country Information Pop Up</i> | 78 |
| 4.3.19. | <i>Email Notification</i> | 80 |

| | |
|--|-----------|
| 4.3.20. PDF Attachment <i>Report</i> Summary | 81 |
| BAB 5 PENGUJIAN | 84 |
| 5.1. Pengujian <i>Black Box</i> | 84 |
| 5.1.1. Rencana Pengujian..... | 84 |
| 5.1.2. Kasus dan Hasil Pengujian Alpha..... | 84 |
| 5.1.3. Kesimpulan Hasil Pengujian Alpha..... | 88 |
| 5.1.4. Kasus dan Hasil Pengujian Beta..... | 88 |
| 5.1.5. Kesimpulan Hasil Pengujian Beta..... | 93 |
| BAB 6 KESIMPULAN DAN SARAN | 95 |
| 6.1. Kesimpulan..... | 95 |
| 6.2. Saran..... | 95 |
| DAFTAR REFERENSI | 96 |
| LAMPIRAN | 97 |
| A. Instalasi <i>Honeypot</i> | 97 |
| B. Deskripsi Quesioner..... | 107 |

DAFTAR GAMBAR


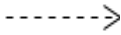



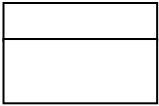
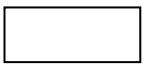
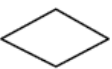
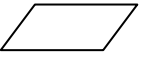
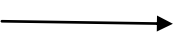

| | |
|--|----|
| Gambar 3. 1 Topologi Jaringan | 22 |
| Gambar 3. 2 Proses Pembuatan <i>Report Malware Detection</i> | 23 |
| Gambar 3. 3 <i>Use case</i> Diagram | 24 |
| Gambar 3. 4 Proses Login | 30 |
| Gambar 3. 5 Melihat Report | 31 |
| Gambar 3. 6 Melihat <i>Detail Malware</i> | 32 |
| Gambar 3. 7 Melihat <i>Analysis Malware</i> | 33 |
| Gambar 3. 8 Mengunduh Details Malware via PDF | 34 |
| Gambar 3. 9 Melihat Chart | 35 |
| Gambar 3. 10 Mengirim <i>Report via Email</i> | 36 |
| Gambar 3. 11 Mengganti <i>Password</i> | 37 |
| Gambar 3. 12 <i>Entity Relationship diagram – Crow’s Foot Notation</i> | 38 |
| Gambar 3. 13 Tampilan Halaman <i>Login</i> | 39 |
| Gambar 3. 14 Tampilan Halaman Utama | 40 |
| Gambar 3. 15 Halaman <i>View Chart</i> | 41 |
| Gambar 3. 16 Halaman <i>Change Password</i> | 42 |
| Gambar 3. 17 Halaman Detail Malware | 43 |
| Gambar 3. 18 Halaman <i>Analysis Malware (Antivirus)</i> | 44 |
| Gambar 3. 19 Tampilan Halaman <i>Report</i> | 45 |
| Gambar 3. 20 <i>Pop Up Report</i> | 46 |
| Gambar 4. 1 Port Dionaea | 47 |
| Gambar 4. 2 <i>Malware</i> di Folder Binaries | 48 |
| Gambar 4. 3 <i>Table Implementation</i> | 49 |
| Gambar 4. 4 Halaman Login | 50 |
| Gambar 4. 5 <i>Pseudocode</i> Halaman Login | 50 |
| Gambar 4. 6 Tampilan Halaman Utama | 51 |
| Gambar 4. 7 <i>Pseudocode</i> Halaman utama | 51 |
| Gambar 4. 8 Halaman <i>View Chart</i> | 52 |
| Gambar 4. 9 <i>Pseudocode View Chart</i> | 52 |
| Gambar 4. 10 Halaman <i>Change Password</i> | 53 |
| Gambar 4. 11 <i>Pseudocode</i> Mengganti <i>Password</i> | 53 |
| Gambar 4. 12 <i>Halaman Analysis</i> | 54 |
| Gambar 4. 13 <i>Pseudocode</i> Halaman <i>Analysis</i> | 55 |
| Gambar 4. 14 <i>Halaman Analysis (Antivirus)</i> | 56 |
| Gambar 4. 15 <i>Pseudocode</i> Halaman <i>Analysis (Antivirus)</i> | 57 |
| Gambar 4. 16 Halaman Analisis <i>Malware</i> | 58 |
| Gambar 4. 17 Halaman <i>Report</i> | 59 |
| Gambar 4. 18 <i>Pseudocode</i> halaman <i>Report</i> | 60 |
| Gambar 4. 19 <i>Attacked Port Pop Up</i> | 61 |
| Gambar 4. 20 <i>Pseudocode Attacked Report</i> | 62 |





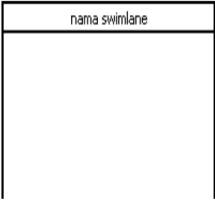
| | |
|--|----|
| Gambar 4. 21 Attack Over a Day Pop Up | 63 |
| Gambar 4. 22 Pseudocode Attack Over a Day | 63 |
| Gambar 4. 23 Popular Malware Download | 64 |
| Gambar 4. 24 Pesudocode Popular Malware Download | 65 |
| Gambar 4. 25 Busy Attacker | 66 |
| Gambar 4. 26 Pseudocode Busy Attacker | 67 |
| Gambar 4. 27 Attacker Ask to Download..... | 68 |
| Gambar 4. 28 Pseudocode Attacker Ask to Download | 69 |
| Gambar 4. 29 Popular Download Location | 70 |
| Gambar 4. 30 Pseudocode Popular Download Location | 71 |
| Gambar 4. 31 Addressed DCE/RPC Calls | 72 |
| Gambar 4. 32 Pseudocode Addressed DCE/RPC Calls | 73 |
| Gambar 4. 33 Most Recent Download | 74 |
| Gambar 4. 34 Pseudocode Most Recent Download | 75 |
| Gambar 4. 35 Dionaea Statistik Pop Up..... | 76 |
| Gambar 4. 36 Pseudocode Dionaea Statistik | 77 |
| Gambar 4. 37 Attacker Country Information | 78 |
| Gambar 4. 38 Pseudocode Attacker Country Information | 79 |
| Gambar 4. 39 Report malware via Email | 80 |
| Gambar 4. 40 PDF Attachment Report Summary Page 1 | 81 |
| Gambar 4. 41 PDF Attachment Report Summary Page 2 | 82 |
| Gambar 4. 42 PDF Attachment Report Summary Page 3 | 83 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 2. 1 Simbol – simbol diagram <i>Use case</i> | 14 |
| Tabel 2. 2 Simbol - simbol <i>Crow's Foot Notation</i> | 15 |
| Tabel 2. 3 Simbol - simbol pada <i>flowchart</i> | 15 |
| Tabel 2. 4 Simbol – simbol <i>Activity Diagram</i> | 17 |
| Tabel 3. 1 Skenario <i>Use Case</i> melakukan <i>login</i> | 25 |
| Tabel 3. 2 Skenario <i>Use Case</i> melihat <i>detail malware</i> | 25 |
| Tabel 3. 3 Skenario <i>Use Case</i> mengunduh <i>detail malware via PDF</i> | 26 |
| Tabel 3. 4 Skenario <i>use case</i> melihat analisis <i>malware</i> | 27 |
| Tabel 3. 5 Skenario <i>Use Case</i> melihat <i>chart</i> | 27 |
| Tabel 3. 6 Skenario <i>use case</i> melihat <i>report</i> | 28 |
| Tabel 3. 7 Skenario <i>use case</i> mengirim <i>report malware via email</i> | 28 |
| Tabel 3. 8 Skenario <i>use case</i> mengganti <i>password</i> | 29 |
| Tabel 3. 9 Skenario <i>use case</i> melakukan <i>logout</i> | 29 |
| Tabel 5. 1 Rencana pengujian aplikasi reporting untuk honeypot..... | 84 |
| Tabel 5. 2 Pengujian login admin | 85 |
| Tabel 5. 3 Pengujian <i>change password</i> | 86 |
| Tabel 5. 4 Pengujian <i>custom report date range</i> | 86 |
| Tabel 5. 5 Pengujian <i>input email address</i> | 87 |
| Tabel 5. 6 Kuesioner..... | 89 |
| Tabel 5. 7 Nilai Persentase Pernyataan ke-1..... | 90 |
| Tabel 5. 8 Nilai Persentase Pernyataan ke-2..... | 90 |
| Tabel 5. 9 Nilai Persentase Pernyataan ke-3..... | 90 |
| Tabel 5. 10 Nilai Persentase Pernyataan ke-4..... | 91 |
| Tabel 5. 11 Nilai Persentase Pernyataan ke-5..... | 91 |
| Tabel 5. 12 Nilai Persentase Pernyataan ke-6..... | 91 |
| Tabel 5. 13 Nilai Persentase Pernyataan ke-7..... | 92 |
| Tabel 5. 14 Nilai Persentase Pernyataan ke-8..... | 92 |
| Tabel 5. 15 Nilai Persentase Pernyataan ke-9..... | 92 |
| Tabel 5. 16 Nilai Persentase Keseluruhan Pernyataan | 93 |
| Tabel 5. 17 Nilai Persentase Tujuan 1 | 93 |
| Tabel 5. 18 Nilai Persentase Tujuan 2 | 94 |

DAFTAR SIMBOL

| USE CASE DIAGRAM | | |
|----------------------|---|---------------------------|
| NO | SIMBOL | ISTILAH |
| 1 |  | <i>Actor</i> |
| 2 |  | <i>Include</i> |
| 3 |  | <i>Extend</i> |
| 4 |  | <i>Association</i> |
| 5 |  | <i>Use Case</i> |
| CROW'S FOOT NOTATION | | |
| 6 |  | Entitas |
| FLOWCHART DIAGRAM | | |
| 7 |  | Proses / langkah |
| 8 |  | Titik keputusan |
| 9 |  | <i>Masukan / Keluaran</i> |
| 10 |  | Garis Alir |
| 11 |  | Terminasi |

| ACTIVITY DIAGRAM | | |
|------------------|--|-------------------------------|
| NO | SIMBOL | ISTILAH |
| 12 |  | <i>Actifity</i> |
| 13 |  | <i>Decission/ percabangan</i> |
| 14 |  | <i>Initial Node</i> |
| 15 |  | <i>Actifity Final Node</i> |
| 16 |  | <i>Swimlane</i> |

DAFTAR LAMPIRAN

| | |
|------------------------------------|-----|
| A. Instalasi <i>Honeypot</i> | 97 |
| B. Deskripsi Quesioner..... | 107 |