

## DAFTAR ISI

|   |      |
|---|------|
| HALAMAN PENGESAHAN.....   | ii   |
| PERNYATAAN BEBAS PLAGIASI.....                                    | iii  |
| KATA PENGANTAR.....   | iv   |
| DAFTAR ISI .....  | vi   |
| DAFTAR GAMBAR .....   | ix   |
| DAFTAR TABEL .....  | xi   |
| INTISARI.....   | xii  |
| <i>ABSTRACT</i> .....   | xiii |
| BAB I PENDAHULUAN .....   | 1    |
| 1.1 Latar Belakang .....  | 1    |
| 1.2 Rumusan Masalah .....   | 3    |
| 1.3 Batasan Masalah.....  | 3    |
| 1.4 Tujuan Penelitian.....  | 3    |
| 1.5 Manfaat Penelitian.....                                       | 4    |
| 1.6 Metodologi Penelitian .....                                   | 4    |
| 1.7 Sistematika Penulisan.....                                    | 5    |
| BAB II TINJAUAN PUSTAKA .....                                     | 7    |
| BAB III LANDASAN TEORI.....                                       | 13   |
| 3.1 <i>Supervisory Control and Data Acquisition (SCADA)</i> ..... | 13   |
| 3.2 Protokol Jaringan.....  | 14   |
| 3.2.1 Serangan protokol jaringan .....                            | 15   |
| 3.3 <i>Intrusion Detection System (IDS)</i> .....                 | 16   |
| 3.3.1 <i>Anomaly-based detection</i> .....                        | 16   |
| 3.3.2 <i>Signature-based detection</i> .....                      | 17   |
| 3.3.3 <i>Hybrid detection</i> .....                               | 17   |
| 3.4 <i>Machine Learning</i> .....                                 | 17   |
| 3.4.1 <i>Random forest</i> .....                                  | 20   |
| 3.4.2 <i>Oversampling</i> .....                                   | 22   |
| 3.4.3 <i>Feature selection</i> .....                              | 22   |

|                                    |  |    |
|------------------------------------|--|----|
| 3.5                                | Suricata. ....   | 22 |
| 3.6                                | <i>Port Mirroring</i> .....  | 24 |
| 3.7                                | <i>Firewall</i> ... ..   | 24 |
| BAB IV METODOLOGI PENELITIAN ..... |  | 25 |
| 4.1                                | Alat dan Bahan .....   | 25 |
| 4.2                                | Tahapan Penelitian.....  | 29 |
| 4.3                                | Analisis Sistem .....  | 31 |
| 4.4                                | Rancangan Topologi Jaringan .....  | 33 |
| 4.5                                | Rancangan <i>Hardware</i> .....  | 34 |
| 4.6                                | Rancangan <i>Software</i> .....  | 35 |
| 4.7                                | Rancangan Simulasi Penyerangan.....  | 35 |
| 4.8                                | Rancangan Sistem <i>Anomaly-based Detection</i> .....                          | 35 |
| 4.9                                | Rancangan Sistem <i>Signature-based Detection</i> .....                        | 37 |
| 4.10                               | Rancangan Visualisasi .....  | 38 |
| 4.11                               | Rancangan <i>Alerting</i> .....  | 38 |
| 4.12                               | Penilaian Sistem .....   | 39 |
| BAB V IMPLEMENTASI .....           |  | 40 |
| 5.1                                | Implementasi Topologi Jaringan .....   | 40 |
| 5.2                                | Implementasi <i>Hardware</i> .....   | 43 |
| 5.3                                | Implementasi <i>Software</i> .....   | 44 |
| 5.4                                | Implementasi Simulasi Penyerangan.....   | 45 |
| 5.5                                | Implementasi Sistem <i>Anomaly-based Detection</i> .....                       | 47 |
| 5.6                                | Implementasi Sistem <i>Signature-based Detection</i> .....                     | 53 |
| 5.7                                | Implementasi Visualisasi .....   | 55 |
| 5.8                                | Implementasi <i>Alerting</i> .....   | 58 |
| 5.9                                | Tahap Pengujian Sistem .....   | 60 |
| 5.9.1                              | Pengujian <i>port mirroring</i> .....  | 60 |
| 5.9.2                              | Pengujian <i>hybrid detection</i> pada <i>attacking SCADA web server</i> ..... | 60 |
| 5.9.3                              | Pengujian pemblokiran <i>attacker</i> dengan <i>firewall</i> .....             | 62 |
| BAB VI HASIL DAN PEMBAHASAN .....  |  | 63 |
| 6.1                                | Hasil Pengujian <i>Port Mirroring</i> .....                                    | 63 |

|                                    |  |    |
|------------------------------------|--|----|
| 6.2                                | Hasil Pengujian <i>Hybrid Detection</i> pada <i>Attacking SCADA Web Server</i> | 63 |
| 6.3                                | Hasil Pengujian Pemblokiran <i>Attacker</i> dengan <i>Firewall</i> .....       | 69 |
| BAB VII KESIMPULAN DAN SARAN ..... |  | 71 |
| 7.1                                | Kesimpulan.....  | 71 |
| 7.2                                | Saran.....   | 72 |
| DAFTAR PUSTAKA .....               |  | 73 |
| LAMPIRAN.....                      |  | 76 |