

## DAFTAR ISI

|                                                    |      |
|----------------------------------------------------|------|
| ABSTRAK .....                                      | i    |
| <i>ABSTRACT</i> .....                              | ii   |
| LEMBAR PENGESAHAN .....                            | iii  |
| LEMBAR PERNYATAAN ORISINALITAS .....               | iv   |
| KATA PENGANTAR .....                               | v    |
| LEMBAR PERSEMBAHAN .....                           | vi   |
| DAFTAR ISI .....                                   | vi   |
| DAFTAR GAMBAR .....                                | ix   |
| DAFTAR TABEL .....                                 | x    |
| DAFTAR LAMPIRAN .....                              | xi   |
| DAFTAR SINGKATAN .....                             | xii  |
| DAFTAR ISTILAH .....                               | xiii |
| BAB I PENDAHULUAN .....                            | 1    |
| I.1 Latar Belakang .....                           | 1    |
| I.2 Perumusan Masalah .....                        | 2    |
| I.3 Tujuan Penelitian .....                        | 2    |
| I.4 Batasan Penelitian .....                       | 3    |
| I.5 Manfaat Penelitian .....                       | 3    |
| I.6 Sistematika Penulisan .....                    | 3    |
| BAB II TINJAUAN PUSTAKA .....                      | 7    |
| II.1 Data Publik .....                             | 7    |
| II.2 Ancaman Siber .....                           | 7    |
| II.3 <i>Open-Source Intelligence</i> (OSINT) ..... | 8    |
| II.4 <i>Profiling</i> Risiko .....                 | 8    |
| II.5 Aset IT .....                                 | 9    |
| II.6 <i>Preliminary Surveillance</i> .....         | 9    |
| II.7 <i>Threat Modelling</i> .....                 | 10   |
| II.8 <i>Data Flow Diagram</i> (DFD) .....          | 10   |
| II.9 <i>Attack Tree</i> .....                      | 11   |
| II.10 Penelitian Terdahulu .....                   | 12   |

|                                                                                     |           |
|-------------------------------------------------------------------------------------|-----------|
| II.11 Alasan Pemilihan Kerangka Kerja .....                                         | 14        |
| <b>BAB III METODOLOGI PENELITIAN.....</b>                                           | <b>16</b> |
| III.1 Model Konseptual .....                                                        | 16        |
| III.2 Sistematika Penyelesaian Masalah .....                                        | 18        |
| III.2.1 Tahap Awal .....                                                            | 19        |
| III.2.2 Tahap Hipotesis.....                                                        | 20        |
| III.2.3 Tahap Desain .....                                                          | 20        |
| III.2.4 Tahap Eksperimen.....                                                       | 21        |
| III.2.5 Tahap Analisis.....                                                         | 21        |
| III.2.6 Tahap Akhir .....                                                           | 22        |
| III.3 Pengumpulan Data.....                                                         | 22        |
| III.4 Pengolahan Data .....                                                         | 22        |
| III.5 Metode Evaluasi .....                                                         | 23        |
| <b>BAB IV PERCANCANGAN DAN ALUR EKSPERIMEN.....</b>                                 | <b>25</b> |
| IV.1 Data Berdasarkan <i>Review</i> Literatur .....                                 | 25        |
| IV.2 Perencanaan dan Persiapan Eksperimen.....                                      | 26        |
| IV.2.1 Spesifikasi Perangkat Keras.....                                             | 26        |
| IV.2.2 Spesifikasi Perangkat Lunak.....                                             | 27        |
| IV.2.3 Daftar Target <i>Domain</i> .....                                            | 30        |
| IV.3 Alur Eksperimen.....                                                           | 31        |
| IV.3.1 Alur Eksperimen Menggunakan <i>Tool</i> OSINT Berbasis CLI.....              | 31        |
| IV.3.2 Alur Eksperimen Menggunakan <i>Tools</i> OSINT Berbasis <i>Website</i> ..... | 33        |
| IV.3.3 Alur Eksperimen Menggunakan <i>Tool</i> OSINT <i>Extension</i> .....         | 35        |
| IV.4 Implementasi Eksperimen.....                                                   | 36        |
| IV.4.1 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> nslookup .....         | 36        |
| IV.4.2 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> whois .....            | 38        |
| IV.4.3 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> curl.....              | 40        |
| IV.4.4 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Shodan.....            | 44        |
| IV.4.5 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Wappalyzer .....       | 46        |
| IV.4.6 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> REDbot.....            | 48        |
| IV.4.7 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> nmap.....              | 50        |
| IV.4.8 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> Traceroute .....       | 52        |
| IV.4.9 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> sslscan .....          | 53        |
| IV.4.10 Implementasi Eksperimen Menggunakan OSINT <i>Tool</i> whatweb .....         | 55        |

|                                                            |            |
|------------------------------------------------------------|------------|
| IV.5 Data Hasil Eksperimen .....                           | 57         |
| <b>BAB V ANALISIS .....</b>                                | <b>66</b>  |
| V.1 Perumusan Definisi Aset Teknologi Informasi (TI) ..... | 66         |
| V.2 Perumusan Nilai <i>Aset IT</i> (A).....                | 67         |
| V.3 Perumusan Nilai <i>Vulnerability</i> (V) .....         | 69         |
| V.4 Perumusan Nilai <i>Threat</i> Potensial (T).....       | 74         |
| V.5 Pemetaan Skenario Ancaman.....                         | 84         |
| V.5.1 Model Serangan <i>Man-in-the-Middle</i> (MitM).....  | 84         |
| V.5.2 Model Serangan DNS <i>Hijacking</i> .....            | 91         |
| V.5.3 Model Serangan <i>Brute Force Login</i> .....        | 97         |
| V.6 Perhitungan Nilai Risiko (R).....                      | 102        |
| V.7 Analisis Perbandingan Nilai Risiko .....               | 106        |
| V.8 Ringkasan Hasil Analisis .....                         | 109        |
| <b>BAB VI KESIMPULAN DAN SARAN .....</b>                   | <b>112</b> |
| VI.1 Kesimpulan.....                                       | 112        |
| VI.2 Saran .....                                           | 113        |
| <b>DAFTAR PUSTAKA .....</b>                                | <b>105</b> |