

DAFTAR ISI

| | |
|---|------|
| ABSTRAK | ii |
| <i>ABSTRACT</i> | iii |
| LEMBAR PENGESAHAN | v |
| LEMBAR PERNYATAAN ORISINALITAS | vi |
| Kata Pengantar | i |
| Daftar Isi..... | ii |
| Daftar Gambar..... | v |
| Daftar Tabel | xiv |
| Daftar Lampiran | xv |
| Daftar Istilah..... | xvii |
| Bab I PENDAHULUAN..... | 21 |
| I.1 Latar Belakang | 21 |
| I.2 Perumusan Masalah..... | 25 |
| I.3 Tujuan Penelitian..... | 25 |
| I.4 Batasan Penelitian | 26 |
| I.5 Manfaat Penelitian..... | 27 |
| I.6 Metodologi Penelitian | 27 |
| Bab II TINJAUAN PUSTAKA..... | 30 |
| II.1 Penelitian Sebelumnya | 30 |
| II.2 Dasar Teori | 44 |
| II.2.1 Sistem Informasi | 45 |
| II.2.2 Keamanan Sistem Informasi | 45 |
| II.2.3 <i>Information System Security Assessment Framework (ISSAF)</i> | 47 |
| II.2.4 Keamanan Siber (<i>Cyber Security</i>)..... | 51 |

| | | |
|---------|--|----|
| II.2.5 | Serangan Keamanan Siber (<i>Cyber Security Attack</i>)..... | 51 |
| II.2.6 | Uji Penetrasi (<i>Penetration Testing</i>)..... | 54 |
| II.2.7 | Pengujian <i>Black Box</i> (<i>Black Box Testing</i>)..... | 55 |
| II.2.8 | Alat Pengujian Penetrasi (<i>Penetration Testing Tools</i>)..... | 55 |
| Bab III | Metodologi Penelitian..... | 67 |
| III.1.1 | Metode yang Digunakan | 68 |
| III.2 | Fase <i>Planning and Preparation</i> | 69 |
| III.2.1 | Observasi dan Wawancara | 69 |
| III.3 | <i>Assessment</i> | 69 |
| III.3.1 | Tahapan <i>Information Gathering</i> | 69 |
| III.3.2 | Tahapan <i>Network Mapping</i> | 70 |
| III.3.3 | Tahapan <i>Vulnerability Identification</i> | 71 |
| III.3.4 | Tahapan <i>Penetration</i> | 71 |
| III.3.5 | Tahapan <i>Gaining Access & Privilege Escalation</i> | 73 |
| III.3.6 | Tahapan <i>Enumerating Further</i> | 73 |
| III.3.7 | Tahapan <i>Compromise Remote User or Sites</i> | 74 |
| III.3.8 | Tahapan <i>Maintaining Access</i> | 74 |
| III.3.9 | Tahapan <i>Covering Tracks</i> | 74 |
| III.4 | Fase <i>Report, Clean Up and Destroy The Artifacts</i> | 75 |
| III.4.1 | <i>Result and Analysis</i> | 75 |
| III.4.2 | <i>Clean Up and Destroy The Artifact</i> | 75 |
| Bab IV | Analisis dan Perancangan | 76 |
| IV.1 | Alat dan Bahan Penelitian | 77 |
| IV.2 | Jadwal Pelaksanaan | 79 |
| Bab V | HASIL dan PEMBAHASAN..... | 81 |
| V.1 | <i>Planning and Preparation</i> | 81 |

| | | |
|---------|--|-----|
| V.1.1 | Observasi..... | 81 |
| V.1.2 | Wawancara Awal | 82 |
| V.2 | <i>Assessment</i> | 83 |
| V.2.1 | <i>Information Gathering</i> | 84 |
| V.2.2 | <i>Network Mapping</i> | 102 |
| V.2.3 | <i>Vulnerabilities Identification</i> | 108 |
| V.2.4 | Penetration..... | 125 |
| V.2.5 | <i>Gaining Access & Privilege Escalation</i> | 145 |
| V.2.6 | <i>Enumerating Further</i> | 156 |
| V.2.7 | <i>Compromise Remote Users or Sites</i> | 164 |
| V.2.8 | <i>Maintaining Access</i> | 182 |
| V.2.9 | <i>Covering Tracks</i> | 183 |
| V.3 | <i>Reporting, Clean-up and Destroy Artifacts</i> | 191 |
| V.3.1 | <i>Verbal Reporting</i> | 192 |
| V.3.2 | <i>Final Reporting (Result and Analysis)</i> | 192 |
| V.3.3 | Wawancara Hasil | 216 |
| V.3.4 | <i>Clean-up and Destroy Artifacts</i> | 216 |
| Bab VI | Kesimpulan dan Saran | 218 |
| VI.1 | Kesimpulan..... | 218 |
| VI.2 | Saran | 219 |
| Bab VII | Daftar Pustaka..... | 220 |