

DAFTAR ISI

LEMBAR PENGESAHAN	iii
PERNYATAAN BEBAS PLAGIASI	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
INTISARI	xiii
<i>ABSTRACT</i>	xiv
BAB I PENDAHULUAN	1
1.1. Latar belakang	1
1.2. Rumusan masalah	2
1.3. Tujuan Proyek Akhir	3
1.4. Manfaat Proyek Akhir	3
1.5. Batasan penelitian	4
1.6. Sistematika penulisan	5
BAB II KAJIAN PUSTAKA	6
2.1. Tinjauan Pustaka	6
2.2. Dasar Teori	10
2.2.1. Keamanan Siber (<i>cybersecurity</i>)	10
2.2.2. <i>Vulnerability Assessment</i>	11
2.2.3. <i>Common Vulnerabilities and Exposures (CVE)</i>	12
2.2.4. Kali Linux	14
2.2.5. <i>Network Mapper (Nmap)</i>	15
2.2.6. Python	17

2.2.7. <i>Structured Threat Information Expression (STIX)</i>	18
2.2.8. <i>Rule-Based System</i>	20
2.2.9. <i>Machine Learning</i>	23
2.3. Hipotesis	24
BAB III METODE PENELITIAN.....	25
3.1. Alat	25
3.1.1. Perangkat Keras	25
3.1.2. Perangkat Lunak.....	25
3.2. Sumber dan Jenis Data	30
3.2.1. Data Kerentanan CVE (MITRE).....	30
3.2.2. Data Hasil Pemindaian Nmap	31
3.2.3. Skenario Pengujian.....	32
3.3. Desain Sistem.....	34
3.3.1. Gambaran Umum Sistem	34
3.3.2. Arsitektur Sistem.....	34
3.3.3. Alur Proses Sistem	36
3.4. Tahapan Penelitian	41
3.4.1. Studi Literatur	41
3.4.2. Persiapan <i>Environment</i> Eksperimen	42
3.4.3. Skenario Pengujian CVE.....	43
3.4.4. Proses Pemindaian Menggunakan Nmap.....	46
3.4.5. Pengumpulan Data Hasil Pemindaian	49
3.4.6. <i>Parsing</i> dan Ekstraksi Data.....	50
3.4.7. <i>Preprocessing</i> Data	54
3.4.8. Efektivitas Teknik <i>Scanning</i> Nmap	59

3.4.9. Penyusunan Dataset Kerentanan CVE (MITRE/NVD)	61
3.4.10. Penerapan Metode <i>Rule-Based</i>	64
3.4.11. Evaluasi dan Analisis	68
BAB IV HASIL DAN PEMBAHASAN	73
4.1. Hasil Parsing dan Pembentukan Dataset	73
4.2. Analisis Efektivitas Teknik Scanning Nmap	76
4.3. Penyusunan Dataset Kerentanan CVE (MITRE/NVD)	78
4.4. Analisis Penerapan Metode <i>Rule-Based</i>	80
4.5. Pembahasan Hasil Penelitian	84
BAB V PENUTUP.....	87
5.1. Kesimpulan	87
5.2. Saran	88
DAFTAR PUSTAKA	89
LAMPIRAN.....	93