

DAFTAR ISI

HALAMAN LEMBAR PERSETUJUAN	ii
HALAMAN LEMBAR PENGESAHAN	iii
HALAMAN LEMBAR PERNYATAAN	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan Penelitian	3
1.5. Manfaat	3
BAB II TINJAUAN PUSTAKA	4
2.1. Implementasi	4
2.2. Analisis	4
2.3. Keamanan	4
2.4. <i>Server</i>	5
2.5. <i>Honeypot</i>	5
2.5.1. <i>Honeypot Cowrie</i>	5
2.5.2. <i>Honeypot Kippo</i>	5
2.6. <i>Intrusion Detection System</i>	5
2.6.1. Jenis-Jenis <i>Intrusion Detection System</i>	6
2.6.2. Cara Kerja <i>Intrusion Detection System</i>	7
2.7. <i>SSH (Secure Shell)</i>	8
2.8. Raspberry Pi	8
2.9. <i>Nmap</i>	9
2.10. <i>Hydra</i>	9

2.11. <i>Medusa</i>	9
2.12. <i>Putty</i>	10
2.13. <i>Access Point</i>	10
2.14. <i>Laptop</i>	10
2.15. <i>Network Development Life Cycle</i>	11
2.15.1. <i>Analysis</i>	11
2.15.2. <i>Design</i>	12
2.15.3. <i>Simulation Prototyping</i>	12
2.15.4. <i>Implementation</i>	12
2.15.5. <i>Monitoring</i>	12
2.15.6. <i>Management</i>	13
2.16. <i>Tabel Penelitian Terkait</i>	14
BAB III METODE PENELITIAN	18
3.1. <i>Metode</i>	18
3.1.1. <i>Analysis</i>	18
3.1.2. <i>Design</i>	19
3.1.3. <i>Simulation Prototyping</i>	19
3.1.4. <i>Implementation</i>	20
3.1.5. <i>Monitoring</i>	20
3.1.6. <i>Management</i>	21
3.2. <i>Peralatan Penelitian</i>	21
3.2.1. <i>Perangkat Keras</i>	21
3.2.2. <i>Perangkat Lunak</i>	21
3.3. <i>Lokasi dan Waktu Penelitian</i>	22
3.4. <i>Prosedur Percobaan</i>	22
3.5. <i>Instalasi dan Konfigurasi</i>	21
3.6. <i>Pengujian</i>	22
BAB IV HASIL DAN PEMBAHASAN	27
4.1. <i>Persiapan Data</i>	27
4.2. <i>Tahap Instalasi dan Konfigurasi</i>	28
4.2.1. <i>Instalasi dan Konfigurasi Sistem Operasi Raspbian Buster</i>	28
4.2.2. <i>Instalasi dan Konfigurasi Honeypot Cowrie</i>	29

4.2.3. Instalasi dan Konfigurasi <i>IDS Snort</i>	31
4.2.4. Instalasi dan Konfigurasi <i>Kippo Graph</i>	32
4.3. Tahap Implementasi	33
4.3.1. Implementasi <i>Honeypot Cowrie</i>	33
4.3.2. Implementasi <i>IDS Snort</i>	34
4.4. Tahap Pengujian	34
4.4.1. Pengujian Dengan Teknik <i>Port Scanning</i>	35
4.4.2. Pengujian Dengan Teknik <i>Bruteforce Attack</i>	36
4.4.2. <i>Blocking IP Address</i> Peretas	39
4.5. Analisis Hasil Pengujian	40
BAB V PENUTUP	43
5.1. Kesimpulan	43
5.2. Saran	43
DAFTAR PUSTAKA	44
LAMPIRAN	

