

DAFTAR GAMBAR

Gambar II.1 Ilustrasi <i>Control plane</i> dan <i>Data plane</i> (Haji et al., 2021).....	5
Gambar II.2 <i>Software Defined Network Layer</i> (Pradhan & Mathew, 2020).	6
Gambar III.1 Model Konseptual Penelitian	21
Gambar III.2 Sistematika Penelitian	23
Gambar IV.1 Perancangan Sistem	27
Gambar IV.2 Topologi yang akan digunakan	29
Gambar IV.3 Kode Python file Topologi.....	33
Gambar IV.4 Tampilan Topologi pada Ryu	34
Gambar IV.5 Pengujian Konektivitas	35
Gambar IV.6 Skema Pengujian.....	36
Gambar V.1 Tes Konektivitas <i>Host</i>	38
Gambar V.2 Xterm <i>Host</i>	39
Gambar V.3 Tabel ARP <i>Host</i> Penyerang.....	39
Gambar V.4 Grafik Latensi Sebelum Serangan.....	40
Gambar V.5 Tabel ARP pada Wireshark <i>Host</i> korban	41
Gambar V.6 <i>Command</i> Arping	41
Gambar V.7 <i>Interface</i> Penyerang.....	42
Gambar V.8 Alamat IP Korban.....	42
Gambar V.9 <i>Host</i> Hasil Scan dengan Ettercap	43
Gambar V.10 Tampilan fitur teknik serangan MITM pada Ettercap.....	43
Gambar V.11 Menjalankan <i>ARP Poisoning</i>	44
Gambar V.12 Tabel ARP korban setelah serangan.....	44
Gambar V.13 Grafik latensi setelah serangan.....	45
Gambar V.14 Hasil Tes Koneksi	46
Gambar V.15 Terminal Xterm <i>Host</i>	47
Gambar V.16 Tabel ARP <i>Host</i> Penyerang.....	47
Gambar V.17 Grafik latensi sebelum serangan.....	48
Gambar V.18 Tabel ARP korban pada semua <i>Host</i>	48
Gambar V.19 <i>Interface</i> Penyerang.....	49
Gambar V.20 alamat IP korban.....	49

Gambar V.21 Korban yang didapat dari hasil <i>scan</i>	50
Gambar V.22 Teknik Serangan pada Ettercap	50
Gambar V.23 Menjalankan <i>Port Stealing</i>	51
Gambar V.24 Tabel ARP setelah serangan.....	51
Gambar V.25 Bukti Komunikasi Setelah Serangan	52
Gambar V.26 Grafik Latensi Setelah Serangan	53
Gambar V.27 Grafik Perbandingan Latensi	55