

DAFTAR GAMBAR

Gambar 1. 1 Grafik Survei Mengenai Pengguna Internet (APJII, 2019).....	2
Gambar 1. 2 Fase dan Tahapan <i>Assessment ISSAF WLAN Security Assessment Methodology</i>	4
Gambar 2. 1 Skema penyerangan <i>man in the middle attack</i> (Mallik, 2018).....	12
Gambar 2. 2 Skema Penyerangan IP <i>Spoofing</i> (Duddu dkk., 2020).....	13
Gambar 2. 3 Skema Penyerangan ARP <i>Spoofing</i> (Duddu dkk., 2020).....	14
Gambar 2. 4 Skema Penyerangan DNS <i>Spoofing</i> (Duddu dkk., 2020).....	15
Gambar 3. 1 Model Konseptual Penelitian.....	23
Gambar 3. 2 Sistematika Penelitian	24
Gambar 4. 1 Alur Perancangan Sistem Pengujian Penyerangan.....	34
Gambar 4. 2 Alur Pengujian Penyerangan.....	35
Gambar 4. 3 Skenario <i>Information gathering</i> Dengan Metode <i>Scanning</i>	37
Gambar 4. 4 Skenario Penyerangan <i>Deauthentication</i>	38
Gambar 4. 5 Skenario Penyerangan <i>Evil twin attack</i> dengan <i>Captive portal</i>	39
Gambar 4. 6 Tampilan <i>Captive portal</i> Pada Perangkat Korban.....	40
Gambar 4. 7 Skenario Penyerangan <i>Evil twin attack</i> dengan	41
Gambar 4. 8 Skenario <i>Unauthorized access</i>	43
Gambar 4. 9 Skenario Penyerangan <i>Telnet Attack</i>	44
Gambar 5. 1 Penyerangan <i>Deauthentication Attack</i> Pada Restoran X.....	51
Gambar 5. 2 Status <i>Reconnecting</i> Pada Laptop Korban Pada Restoran X.....	51
Gambar 5. 3 Penyerangan <i>Deauthentication Attack</i> Pada Restoran Y.....	52
Gambar 5. 4 Status <i>Reconnecting</i> Pada Laptop Korban Pada Restoran X.....	52
Gambar 5. 5 Penyerangan <i>Deauthentication Attack</i> Pada Restoran Z.....	53
Gambar 5. 6 Status <i>Reconnecting</i> Pada Laptop Korban Pada Restoran Z.....	53
Gambar 5. 7 <i>Captive portal</i> Pada Laptop Korban di Restoran X.....	55
Gambar 5. 8 Tampilan <i>Password</i> Yang Benar Pada <i>Captive portal</i>	56
Gambar 5. 9 Tampilan <i>Panel Control</i> Pada <i>Toolkit Airgeddon</i> di Restoran X...	56
Gambar 5. 10 Hasil Pada <i>File 404.txt</i>	56
Gambar 5. 11 Tampilan <i>Panel Control</i> Pada <i>Toolkit Airgeddon</i> di Restoran Y..	57
Gambar 5. 12 Hasil Pada <i>File passwordwifil.txt</i>	57
Gambar 5. 13 Halaman <i>Website</i> Facebook Sebelum Penyerangan.....	59

Gambar 5. 14 Halaman <i>Website</i> Facebook Selama Penyerangan Dilakukan.....	60
Gambar 5. 15 Hasil Pada <i>File</i> 404passweb.txt.....	60
Gambar 5. 16 Halaman <i>Website</i> LinkedIn Sebelum Dilakukan Penyerangan....	61
Gambar 5. 17 Halaman <i>Website</i> LinkedIn Selama Dilakukan Penyerangan.....	61
Gambar 5. 18 Hasil Pada <i>File</i> tangkappassword1.txt.....	62
Gambar 5. 19 Hasil Pada <i>File</i> passbaru.txt.....	62
Gambar 5. 20 Halaman <i>Login Website</i> Konfigurasi Restoran X.....	63
Gambar 5. 21 Halaman <i>Website</i> Konfigurasi Restoran X.....	63
Gambar 5. 22 Halaman <i>Login Website</i> Konfigurasi Restoran Y.....	64
Gambar 5. 23 Halaman <i>Website</i> Konfigurasi Restoran Y.....	64
Gambar 5. 24 Halaman <i>Login Website</i> Konfigurasi Restoran Z.....	65
Gambar 5. 25 Halaman <i>Website</i> Konfigurasi Restoran Z.....	65
Gambar 5. 26 Hasil Paket Telnet Pada Restoran X.....	66
Gambar 5. 27 Hasil <i>Sniffing</i> Dengan <i>Wireshark</i> Pada Restoran X.....	66
Gambar 5. 28 Hasil Paket Telnet Pada Restoran Y.....	67
Gambar 5. 29 Hasil <i>Sniffing</i> Dengan <i>Wireshark</i> Pada Restoran Y.....	67
Gambar 5. 30 Tampilan <i>Login</i> Telnet Gagal Pada Restoran Z.....	68