

**EVALUASI KEAMANAN JARINGAN NIRKABEL
SSID UNDIKSHA EVENT MENGGUNAKAN METODE
PENETRATION TESTING BERBASIS PENETRATION
TESTING EXECUTION STANDARD(PTES)**



**PROGRAM STUDI ILMU KOMPUTER
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA**

2026



SKRIPSI

DIAJUKAN UNTUK MELENGKAPI TUGAS DAN MEMENUHI SYARAT-SYARAT UNTUK MENCAPAI GELAR SARJANA KOMPUTER

	
Pembimbing I	I Ketut Purnamawan, S.Kom., M.Kom. NIP.197905112006041004
Pembimbing II	Ir. I Ketut Resika Arthana, S.T., M.Kom. NIP.198412012012121002

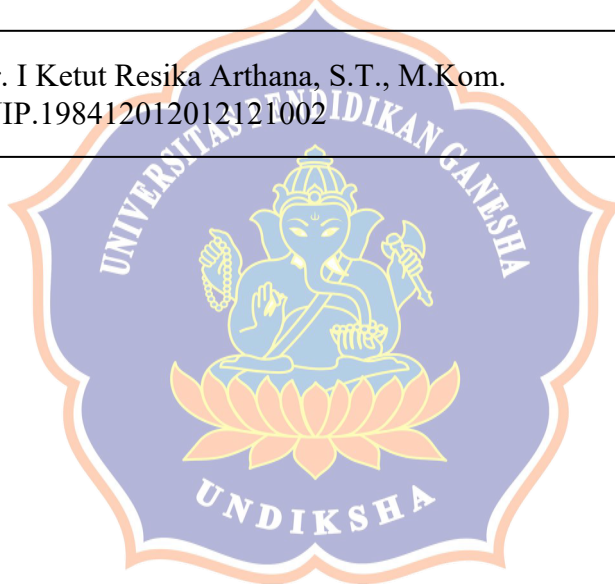


- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

Skripsi oleh Junaidi ini
telah dipertahankan di depan dewan penguji
Pada tanggal 02 Juli 2026

Dewan Penguji

Ketua	Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. NIP.197803242005011001
Anggota	Ir. Ketut Agus Seputra, S.ST.,M.T. NIP.199008152019031018
Anggota	I Ketut Purnamawan, S.Kom., M.Kom. NIP.197905112006041004
Anggota	Ir. I Ketut Resika Arthana, S.T., M.Kom. NIP.198412012012121002



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.



Balai Besar
Sertifikasi
Elektronik

Diterima oleh Panitia Ujian Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
guna memenuhi syarat-syarat untuk mencapai gelar Sarjana Komputer

Menyetujui

Ketua Ujian	Ir. Made Windu Antara Kesiman, S.T., M.Sc., Ph.D. NIP.198211112008121001
Sekretaris Ujian	I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs. NIP.198910262019031004



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

PERNYATAAN

Dengan ini saya menyatakan bahwa karya tulis yang berjudul “Evaluasi Keamanan Jaringan Nirkabel SSID Undiksha Event Menggunakan Metode *Penetration Testing* Berbasis *Penetration Testing Execution Standard*(PTES)” beserta seluruh isinya adalah benar-benar karya saya sendiri dan saya tidak melakukan penjiplakan maupun pengutipan dengan cara-cara yang tidak sesuai dengan etika yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko atau sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran atas etika keilmuan dalam karya saya ini atau terdapat klaim terhadap keaslian karya saya ini.

Singaraja, 13 Juli 2026
Yang membuat pernyataan,



Junaidi
NIM 1915101041

PRAKATA

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat, karunia, dan anugerah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “**Evaluasi Keamanan Jaringan Nirkabel SSID Undisksha Event Menggunakan Metode *Penetration Testing* Berbasis *Penetration Testing Execution Standard (PTES)*”**. Skripsi ini disusun guna memenuhi salah satu persyaratan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Ilmu Komputer, Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha.

Dalam proses penyusunan skripsi ini, penulis memperoleh banyak bantuan, bimbingan, arahan, motivasi, serta dukungan, baik secara moral maupun material dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Prof. Dr. Kadek Rihendra Dantes, S.T., M.T., selaku Dekan Fakultas Teknik dan Kejuruan Universitas Pendidikan Ganesha yang telah memberikan fasilitas dan dukungan sehingga penulis dapat menyelesaikan skripsi ini.
2. Made Windu Antara Kesiman, S.T., M.Sc., Ph.D., selaku Wakil Dekan I Fakultas Teknik dan Kejuruan Universitas Pendidikan Ganesha.
3. I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs., selaku Koordinator Program Studi S1 Ilmu Komputer yang telah memberikan motivasi dan dukungan dalam penyelesaian skripsi ini.
4. I Ketut Purnamawan, S.Kom., M.Kom., selaku Pembimbing I yang telah memberikan bimbingan, arahan, saran, serta motivasi kepada penulis selama proses penyusunan skripsi ini.
5. Ir. I Ketut Resika Arthana, S.T., M.Kom., selaku Pembimbing II yang telah memberikan bimbingan, arahan, saran, serta motivasi kepada penulis selama proses penyusunan skripsi ini.
6. Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D., selaku Penguji I yang telah memberikan masukan, saran, serta arahan yang membangun demi penyempurnaan skripsi ini.

7. Ir. Ketut Agus Seputra, S.ST.,M.T., selaku Penguji II yang telah memberikan masukan, saran, serta arahan yang membangun demi penyempurnaan skripsi ini.
8. Kepala UPA Teknologi Informasi dan Komunikasi (UPA TIK) Universitas Pendidikan Ganesha beserta seluruh staf yang telah memberikan izin, bantuan, dan dukungan selama pelaksanaan penelitian.
9. Kedua orang tua, keluarga, serta seluruh pihak yang tidak dapat disebutkan satu per satu yang telah memberikan doa, dukungan, semangat, dan motivasi selama proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki berbagai keterbatasan dan jauh dari kata sempurna mengingat keterbatasan kemampuan dan pengalaman yang dimiliki penulis. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun sebagai bahan perbaikan dan penyempurnaan di masa mendatang.

Akhir kata, penulis berharap semoga skripsi ini dapat memberikan manfaat dan kontribusi positif, khususnya dalam bidang keamanan jaringan nirkabel serta dapat menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan pengujian keamanan menggunakan metode *Penetration Testing*.

Singaraja, 13 Juli 2026

Penulis

DAFTAR ISI

	HALAMAN
PRAKATA.....	i
ABSTRAK	iii
DAFTAR ISI	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
DAFTAR LAMPIRAN	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	4
1.3 Batasan Penelitian	5
1.4 Rumusan Masalah	5
1.5 Tujuan Penelitian.....	6
1.6 Manfaat Penelitian	6
BAB II KAJIAN PUSTAKA.....	6
2.1. Konsep Jaringan Komputer.....	6
2.2. Wlan (<i>Wireless Local Area Network</i>)	7
2.3. Keamanan Jaringan Nirkabel	8
2.3.1. Protokol Keamanan Jaringan Nirkabel	9
2.3.2. Ancaman Keamanan Jaringan Nirkabel	11
2.4. Penetration Testing	14
2.5. Virtual box	16
2.6. Kali linux.....	16
2.7. Penelitian yang Relevan	17
BAB III METODOLOGI PENELITIAN.....	16
3.1 Jenis Penelitian.....	16
3.2 Metode Penelitian.....	16

3.2.1 Pre-engagement	17
3.2.2 Intelligence Gathering.....	21
3.2.3 Threat Modelling	25
3.2.4 Vulnerability Analysis.....	26
3.2.5 Exploitation.....	28
3.2.6 Post Exploitation.....	31
3.2.7 Reporting	37
3.3 Teknik Pengumpulan Data	39
3.4 Teknik Analisis Data	40
3.5 Alat dan Bahan Penelitian.....	42
3.6 Waktu dan Tempat Penelitian.....	43
BAB IV IMPLEMENTASI DAN EVALUASI.....	44
4.1 Hasil Pengujian Penetration Testing SSID Undiksha Event	44
4.1.1 Pre-Engagement.....	44
4.1.2 Intelligence Gathering.....	51
4.1.3 Threat Modelling	58
4.1.4 Vulnerability Analysis.....	58
4.1.5 Exploitation.....	59
4.2 Hasil Evaluasi Keamanan Jaringan Nirkabel SSID Undiksha Event.....	86
4.2.1 Post-exploitation	86
4.2.2 Reporting	102
BAB V PENUTUP.....	110
5.1. Simpulan	110
5.2. Rekomendasi	111
5.3. Keterbatasan Penelitian dan Saran untuk Penelitian Selanjutnya	112
DAFTAR PUSTAKA	114
LAMPIRAN.....	116

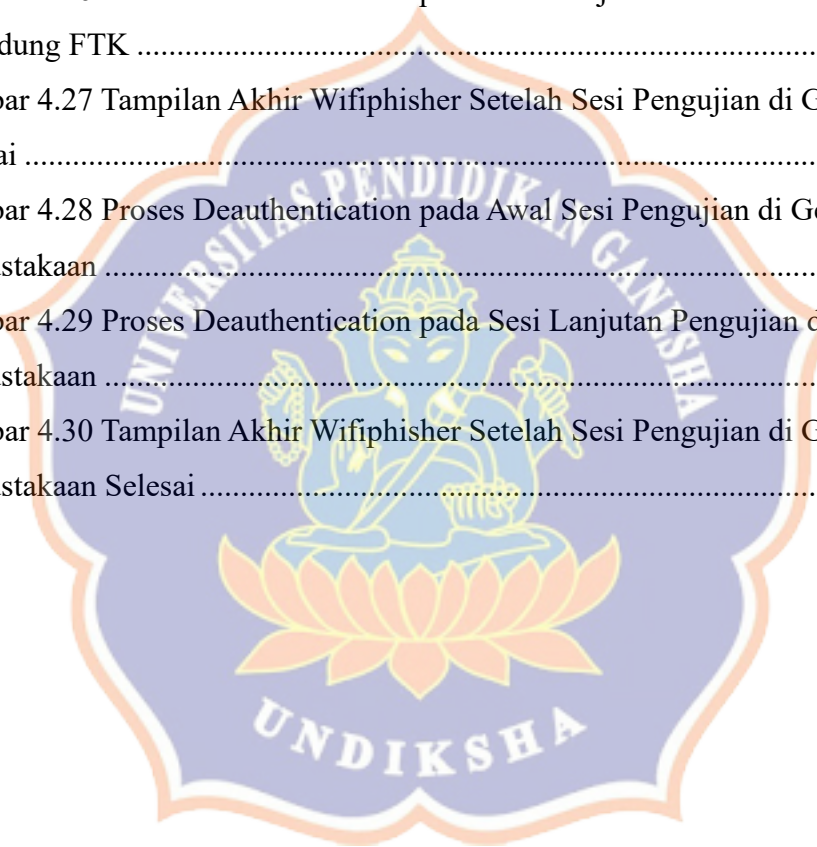
DAFTAR TABEL

Tabel	Halaman
Tabel 3.1 Parameter Informasi Hasil Pemindaian Umum Access Point	23
Tabel 3.2 Parameter Informasi Access Point dari Hasil Pemindaian Terfokus	24
Tabel 3.3 Parameter Informasi Station (Klien) dari Hasil Pemindaian Terfokus..	24
Tabel 3.4 Model Ancaman	26
Tabel 3.5 Kriteria Keberhasilan Setiap Tahapan Pengujian	32
Tabel 3.6 Kriteria Keberhasilan Teknik Pengujian secara Keseluruhan	33
Tabel 3.7 Skala Likelihood	35
Tabel 3.8 Skala Impact.....	35
Tabel 3.9 Kategori Tingkat Risiko	36
Tabel 4.1 Hasil Wawancara dengan Pengelola SSID Undiksha Event	45
Tabel 4.2 Ringkasan Dokumen Perizinan Pengujian	48
Tabel 4.3 Daftar Perangkat yang Digunakan dalam Pengujian.....	49
Tabel 4. 4 Hasil Pemindaian Umum Access Point Menggunakan Airodump-ng .	54
Tabel 4.5 Informasi Access Point Hasil Pemindaian Terfokus Airodump-ng.....	56
Tabel 4.6 Informasi Station (Klien) Hasil Pemindaian Terfokus Airodump	57
Tabel 4. 7 Ringkasan Hasil Pengujian Cracking the Encryption	70
Tabel 4.8 Data Jumlah Keseluruhan Pengguna Aktif SSID Undiksha Event di Seluruh Gedung Sebelum Pengujian.....	72
Tabel 4.9 Ringkasan Hasil Pengujian Evil Twin Attack	86
Tabel 4.10 Dokumentasi Hasil Pengujian Penetration Testing SSID Undiksha Event	88
Tabel 4.11 Evaluasi Hasil Pengujian Penetration Testing SSID Undiksha Event.	91
Tabel 4.12 Dasar Penilaian Risiko Kerentanan Jaringan SSID Undiksha Event..	93
Tabel 4.13 Hasil Perhitungan Tingkat Risiko Kerentanan Jaringan SSID Undiksha Event	95
Tabel 4.14 Evaluasi Efektivitas Keamanan Jaringan SSID Undiksha Event.....	100
Tabel 4.15 Ringkasan Hasil Pengujian Keamanan SSID Undiksha Event	103
Tabel 4.16 Kerentanan yang Berhasil Diidentifikasi pada SSID Undiksha Event	104
Tabel 4.17 Prioritas Penanganan Kerentanan SSID Undiksha Event	105

DAFTAR GAMBAR

Gambar	Halaman
Gambar 2. 1 Tahapan PTES	15
Gambar 3.1 Tahapan Penelitian	17
Gambar 4. 1 Kondisi Wireless Adapter Sebelum Monitor Mode Diaktifkan	51
Gambar 4. 2 Proses Aktivasi Monitor Mode dengan Airmon-ng	52
Gambar 4. 3 Konfirmasi Wireless Adapter Berhasil Beralih ke Monitor Mode...	53
Gambar 4. 4 Hasil Pemindaian Umum Seluruh Access Point Menggunakan Airodump-ng	54
Gambar 4. 5 : Hasil Pemindaian Terfokus pada BSSID Target SSID Undiksha Event	56
Gambar 4.6 Kondisi Wireless Adapter Sebelum Monitor Mode Diaktifkan	60
Gambar 4. 7 Proses Aktivasi Monitor Mode dengan Airmon-ng	61
Gambar 4. 8 Konfirmasi Wireless Adapter Berhasil Beralih ke Monitor Mode (wlan0mon)	61
Gambar 4.9 Pemindaian Seluruh Access Point Menggunakan Airodump	62
Gambar 4.10 Pemindaian Terfokus pada BSSID Target SSID Undiksha Event...	63
Gambar 4.11 Konfirmasi Pembuatan File Capture UNDIKSHA_EVENT-01.cap	64
Gambar 4.12 Proses Pengiriman Paket Deauthentication Menggunakan Aireplay- ng.....	65
Gambar 4.13 Notifikasi Keberhasilan Penangkapan Four-Way Handshake.....	66
Gambar 4.14 Perintah Aircrack-ng untuk Memulai Proses Dictionary Attack....	67
Gambar 4.15 Proses Dictionary Attack pada Menit Awal Pengujian.....	67
Gambar 4.16 Proses Dictionary Attack Setelah Berjalan Selama 58 Menit	68
Gambar 4.17 Hasil Akhir Proses Dictionary Attack Setelah Lebih dari 1 Jam Pengujian.....	69
Gambar 4.18 Perintah Membuat Tiruan SSID Undiksha Event Menggunakan Wifiphisher.....	73
Gambar 4.19 Hasil Pemindaian Jaringan Wi-Fi Sebelum Evil Twin Attack Aktif	74
Gambar 4.20 Hasil Pemindaian Jaringan Wi-Fi Setelah Evil Twin Attack Aktif SSID Undiksha Event Muncul Dua Kali	75

Gambar 4.21 halaman captive portal firmware palsu	77
Gambar 4.22 Proses pengujian awal di Gedung Rektorat	79
Gambar 4.23 Proses Deauthentication dan Connected Victims Sesi Lanjutan di Gedung Rektorat	79
Gambar 4.24 Tampilan Akhir Wifiphisher Setelah Sesi Pengujian di Gedung Rektorat Selesai.....	80
Gambar 4.25 Proses Deauthentication pada Awal Sesi Pengujian di Gedung FTK	81
Gambar 4.26 Proses Deauthentication pada Sesi Lanjutan dan Connected Victims di Gedung FTK	81
Gambar 4.27 Tampilan Akhir Wifiphisher Setelah Sesi Pengujian di Gedung FTK Selesai	82
Gambar 4.28 Proses Deauthentication pada Awal Sesi Pengujian di Gedung Perpustakaan	82
Gambar 4.29 Proses Deauthentication pada Sesi Lanjutan Pengujian di Gedung Perpustakaan	83
Gambar 4.30 Tampilan Akhir Wifiphisher Setelah Sesi Pengujian di Gedung Perpustakaan Selesai	83



DAFTAR LAMPIRAN

Lampiran	Halaman
Lampiran 01. Surat Permohonan Pengambilan Data	116
Lampiran 02. Dokumentasi Pemberian Surat Permohonan Pengambilan Data...	117
Lampiran 03. Dokumentasi Hasil Wawancara	118
Lampiran 04. Surat Permohonan Pengujian.....	119
Lampiran 05. Dokumentasi Pengujian Jaringan.....	120

