



**ANALISA SISTEM KEAMANAN JARINGAN NIRKABEL
MENGUNAKAN KERANGKA KERJA ISSAF PADA PT.
GERAK PUNCAK LANCAR**

LAPORAN TUGAS AKHIR



**UNIVERSITAS
MERCU BUANA**

ARI NUR SHAFFAN

41520110053

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2023



**ANALISA SISTEM KEAMANAN JARINGAN NIRKABEL
MENGUNAKAN KERANGKA KERJA ISSAF PADA PT.
GERAK PUNCAK LANCAR**

LAPORAN TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

**UNIVERSITAS
MERCU BUANA**

ARI NUR SHAFFAN

41520110053

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2023

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Ari Nur Shaffan
NIM : 41520110053
Program Studi : Teknik Informatika

Judul Proposal Penelitian : ANALISA SISTEM KEAMANAN JARINGAN
NIRKABEL MENGGUNAKAN KERANGKA
KERJA ISSAF PADA PT. GERAK PUNCAK
LANCAR

Menyatakan bahwa proposal penelitian ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam proposal penelitian saya terdapat unsur plagiat, maka saya akan siap mendapatkan sanksi akademisi yang berlaku di Universitas Mercu Buana.

Jakarta, 30 November 2023



Ari Nur Shaffan

HALAMAN PENGESAHAN

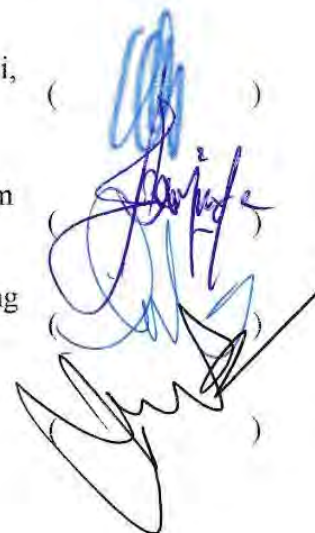
Laporan Skripsi ini diajukan oleh:

Nama : Ari Nur Shaffan
NIM : 41520110053
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Analisa Sistem Keamanan Jaringan Nirkabel
Menggunakan Kerangka Kerja ISSAF Pada PT.
Gerak Puncak Lancar

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Dr. Nungky Awang Chandra, S.Si,
M.TI
NIDN : 0306117303
Ketua Penguji : Muhammad Rifqi, S.Kom,M.Kom
NIDN : 0301067101
Penguji 1 : Prastika Indriyanti, S.Kom, M.Eng
NIDN : 0312089401
Penguji 2 : Rushendra, S.Kom, MT
NIDN : 0408067402



Jakarta, 20 Juli 2024

Mengetahui,

Dekan



Dr. Bambang Jokonowo, S.Si., MTI
NIDN : 0320037002

Ketua Program Studi



Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0225067701

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tugas akhir ini. Penulisan tugas akhir ini dilakukan dalam rangka kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan Magang/Skripsi/Tesis/Disertasi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Ir. Andi Adriansyah, M.Eng selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, M.T.I selaku Dekan Fakultas Ilmu Komputer/Direktur Program Pascasarjana.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom selaku Ketua Program Studi.
4. Bapak Sabar Rudianto, M.Kom Selaku Dosen Pembimbing Akademik.
5. Bapak Dr. Nungky Awang Chandra, S.Si, M.T.I selaku Dosen Pembimbing Skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tugas akhir ini.
6. Ibu Sari Yochebet Selaku Manager pada PT. Gerak Puncak Lancar yang telah memberikan izin magang di PT. Gerak Puncak Lancar.
7. Bapak Eko Priyadi S.Kom selaku mentor pada PT. Gerak Puncak Lancar yang mengarahkan dan meluangkan waktunya untuk membantu tugas akhir ini.
8. Orang Tua saya, Ibu dan Alm. Bapak saya serta Kakak saya yang selalu mendoakan dan menjadi motivasi saya dalam mengerjakan tugas akhir ini.
9. Syifa Nurul Aini yang selalu memberikan saya semangat dalam mengerjakan tugas akhir ini.
10. Teman-teman saya yaitu Ravi Rinaldi, Ricky Gunawan, teman kampus mas Yoga Dianto, Ahlil Jannah, dan lainnya, serta teman-teman kantor dan rumah yang selalu membawa canda dan tawa bagi penulis.

11. Semua pihak yang tidak bisa disebutkan satu per satu, yang telah tulus ikhlas memberikan doa, dukungan dan motivasi agar dapat menyelesaikan tugas akhir ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Penelitian ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 20 Juli 2024



Ari Nur Shaffan



**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR
UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : Ari Nur Shaffan
NIM : 41520110053
Program Studi : Teknik Informatika
Judul Laporan Skripsi : ANALISA SISTEM KEAMANAN
JARINGAN NIRKABEL MENGGUNAKAN
KERANGKA KERJA ISSAF PADA PT.
GERAK PUNCAK LANCAR

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 20 Juli 2024

Yang menyatakan,



Ari Nur Shaffan

ABSTRAK

Keamanan data sebuah perusahaan adalah suatu hal yang sangat penting, maka diperlukannya keamanan untuk menjaga data-data penting tersebut agar tidak disalahgunakan. Salah satu celah yang dapat diserang ialah jaringan nirkabel karena dapat terlihat oleh publik. Pada PT. Gerak Puncak Lancar sendiri mempunyai jaringan nirkabel untuk akses internet karyawannya. Penelitian ini bertujuan untuk menguji seberapa kuat sistem keamanan dari perusahaan tersebut dengan metode Penetration Test ISSAF. ISSAF merupakan sebuah framework standard pengujian Penetration Test untuk berbagai keamanan. Seperti keamanan WLAN, website, keamanan Router, keamanan Firewall dan lain-lainnya. ISSAF sendiri mempunyai 9 aktivitas atau langkah meliputi Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access dan Covering tracks. Untuk Wlan Security Assessment sendiri mempunyai 6 tahap yakni, Information Gathering, Scanning, Audit, Analysis & Research, Exploit & Attacks, Reporting & Presentation. Hasil analisa penelitian ini, keamanan jaringan nirkabel Access Point staff PT. Gerak Puncak Lancar. Mempunyai nilai Overall Risk Rating tinggi atau High. Evaluasi pun dilakukan pada keamanan jaringan PT. Gerak Puncak Lancar, dan hasil evaluasi tersebut menurunkan Overall Risk Rating menjadi Medium.

Kata Kunci : Uji Penetrasi, ISSAF, WLAN, Keamanan Jaringan, Aircrack-ng

ABSTRACT

The security of a company's data is highly important, requiring measures to protect the crucial information from potential misuse. One vulnerability lies in the wireless network, which can be visible to the public. PT. Gerak Puncak Lancar has its own wireless network for its employees' internet access. This research aims to assess the strength of the company's security system using the ISSAF Penetration Test method, a standard framework for testing various security aspects like WLAN, website, router, firewall, and more. ISSAF involves 9 activities, including Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromising Remote Users/Sites, Maintaining Access, and Covering Tracks. The WLAN Security Assessment has 6 stages: Information Gathering, Scanning, Audit, Analysis & Research, Exploit & Attacks, and Reporting & Presentation. The research analysis results indicate that the wireless network security of PT. Gerak Puncak Lancar's staff Access Point has a high Overall Risk Rating. An evaluation was conducted on the network security of PT. Gerak Puncak Lancar, and the evaluation results lowered the Overall Risk Rating to Medium.

Keywords : Pentest, ISSAF, WLAN, Network Security, Aircrack-ng

MERCU BUANA

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERNYATAAN KARYA SENDIRI	ii
HALAMAN PENGESAHAN.....	iii
KATA PENGANTAR.....	iv
HALAMAN PERNYATAAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS.....	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	6
1.3 Tujuan Penelitian.....	6
1.4 Manfaat Penelitian.....	6
1.5 Batasan Penelitian	7
BAB II TINJAUAN PUSTAKA.....	8
2.1 Penelitian Terdahulu.....	8
2.2 Teori Pendukung	15
2.2.1 Wireless Local Area Network.....	15
2.2.2 Penetration Testing.....	17
2.2.3 ISSAF.....	18
2.2.4 CIA TRIAD.....	21
2.2.5 A Threat Model.....	23
2.2.6 Types of Threats.....	23
2.2.7 Alat Penetration Test.....	25
2.2.8 Penggunaan Alat Pentest.....	27

BAB III METODE PENELITIAN	31
3.1 Jenis Penelitian	31
3.2 Tahapan Penelitian	31
3.2.1 Metodologi	32
3.2.2 Persiapan Alat	42
3.3 Timeline Penelitian.....	42
BAB IV HASIL DAN PEMBAHASAN	44
4.1 Dataset	44
4.2 Perbandingan Hasil Metode	65
4.3 Analisis	67
4.3.1 Sebelum Evaluasi.....	67
4.3.2 Sesudah Evaluasi.....	68
BAB V KESIMPULAN DAN SARAN	74
5.1 Kesimpulan.....	74
5.2 Saran.....	74
DAFTAR PUSTAKA	78
LAMPIRAN.....	81
Lampiran 1 Kartu Asistensi.....	81
Lampiran 2 Lampiran Halaman Pernyataan Luaran Tugas Akhir	82
Lampiran 3 Naskah Artikel Jurnal	83
Lampiran 4 Curriculum Vitae	84
Lampiran 5 Surat Pernyataan HAKI	85
Lampiran 6 Sertifikat BNSP.....	88
Lampiran 7 Surat Ijin Riset Perusahaan	89
Lampiran 8 Form Revisi Dosen Penguji	91
Lampiran 9 Hasil Cek Turnitin	93
Lampiran 10 Halaman Persetujuan	94

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	8
Tabel 2.2 Tabel Penggunaan dan Fungsi Alat-Alat Pentest.....	27
Tabel 3.1 Level Kerentanan	39
Tabel 3.2 Contoh Penilaian Tingkat Resiko Yang Diterima Perusahaan	41
Tabel 3.3 Timeline Proposal Penelitian	42
Tabel 3.4 Timeline Penelitian	43
Tabel 4.1 Hasil Information Gathering	44
Tabel 4.2 Hasil Scanning	47
Tabel 4.3 Hasil Wawancara pada tahap Audit & Review.....	47
Tabel 4.4 Hasil Security Analysis & Research	49
Tabel 4.5 Hasil Exploit & Attacks	63
Tabel 4.6 Hasil Pentest PT. Gerak Puncak Lancar	65
Tabel 4.7 Rekomendasi Evaluasi Untuk Keamanan Jaringan	66
Tabel 4.8 Hasil Pentest Setelah Evaluasi	72
Tabel 4.9 Perbandingan Hasil Pentest Sebelum dan Sesudah Evaluasi.....	73
Tabel 4.10 Penilaian Tingkat Resiko Yang Dapat Diterima Oleh Perusahaan.....	74
Tabel 4.11 Tabel Penilaian Resiko Perbandingan.....	75



DAFTAR GAMBAR

Gambar 1.1 Perbandingan Beberapa Fitur ISSAF dan NIST	4
Gambar 2.1 Garis Besar Kerangka Kerja ISSAF.....	21
Gambar 3.1 Tahapan Metodologi WLAN Security Assessment	32
Gambar 3.2 Contoh Hasil Risk Assessment	40
Gambar 3.3 Parameter Hasil Keseluruhan Pengujian	40
Gambar 3.4 Penilaian Tingkat Resiko	41
Gambar 4.1 Penggunaan Kismet Untuk Memantau AP Sekitar	45
Gambar 4.2 Informasi Yang Didapat Pada Access Point Target.....	45
Gambar 4.3 Pengguna dari AP Target.	46
Gambar 4.4 Pemantauan Paket Pada Perangkat.....	46
Gambar 4.5 Penggunaan AirCrack-ng Pada AP Target.....	50
Gambar 4.6 Melakukan Deauth Pada AP Target	51
Gambar 4.7 Hasil Aircrack-ng Attack	52
Gambar 4.8 Menggunakan Reaver Untuk WPS Attack.....	53
Gambar 4.9 Hasil Serangan Reaver	53
Gambar 4.10 Melakukan DDOS AP Target	54
Gambar 4.11 Hasil DDOS Aireplay-ng	55
Gambar 4.12 Melakukan Scanning Menggunakan NMAP.....	56
Gambar 4.13 Menggunakan Ettercap Untuk Melakukan MITM Attack	57
Gambar 4.14 Sniffing Menggunakan Wireshark	58
Gambar 4.15 DNS Spoofing Attack.....	59
Gambar 4.16 Hasil DNS Spoofing Attack	60
Gambar 4.17 Hasil DNS Spoofing Tanpa HSTS.....	61
Gambar 4.18 DDOS Attack Internal Menggunakan Ettercap.....	62
Gambar 4.19 Hasil DDOS Attack.....	63
Gambar 4.20 Test Serangan DDOS Aireplay untuk WPA3	68
Gambar 4.21 Hasil Serangan Pada AP Target WPA3	69
Gambar 4.22 Hasil Penerapan MAC Filtering	69
Gambar 4.23 Firewall Blokir HTTP	70
Gambar 4.24 Hasil Saat Blok HTTP Non-aktif	70
Gambar 4.25 Percobaan Serangan Menggunakan NMAP dan ARP Spoofing Untuk Menguji Snort IDS	71
Gambar 4.26 Penggunaan Snort IDS	71

DAFTAR LAMPIRAN

Lampiran 1 Kartu Asistensi	81
Lampiran 2 Lampiran Halaman Pernyataan Luaran Tugas Akhir	82
Lampiran 3 Naskah Artikel Jurnal	83
Lampiran 4 Curriculum Vitae	84
Lampiran 5 Surat Pernyataan HAKI.....	85
Lampiran 6 Sertifikat BNSP	88
Lampiran 7 Surat Ijin Riset Perusahaan.....	89
Lampiran 8 Form Revisi Dosen Penguji.....	91
Lampiran 9 Hasil Cek Turnitin	93
Lampiran 10 Halaman Persetujuan	94

