



**ANALISA KEAMANAN JARINGAN NIRKABEL DI PEMERINTAHAN
PROVINSI SUMATERA SELATAN DENGAN MENGGUNAKAN
METODE WARDRIVING DAN PENETRATION TESTING**

Skripsi ini diajukan sebagai syarat memperoleh gelar sarjana komputer

**ERU SETIA UTAMA
151420039**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA
PALEMBANG
2019**

HALAMAN PENGESAHAN

**ANALISA KEAMANAN JARINGAN NIRKABEL DI
PEMERINTAHAN PROVINSI SUMATERA SELATAN DENGAN
METODE WARDRIVING DAN PENETRATION TESTING**

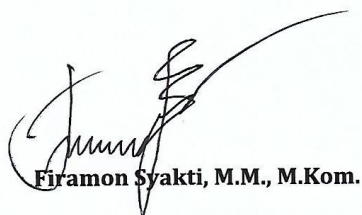
ERU SETIA UTAMA



151420039

**Telah diterima sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer pada Program Studi Teknik Informatika**

Palembang, 02 Agustus 2019
Fakultas Ilmu Komputer
Universitas Bina Darma
Dekan,

Pembimbing


Firamon Syakti, M.M., M.Kom.

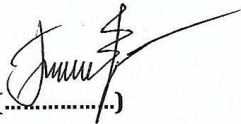

Fakultas Ilmu Komputer

Dedy Syamsuar, S.Kom., M.I.T., Ph.D

HALAMAN PERSETUJUAN

Skripsi Berjudul "ANALISA KEAMANAN JARINGAN NIRKABEL DI PEMERINTAHAN PROVINSI SUMATERA SELATAN DENGAN METODE WARDRIVING DAN PENETRATION TESTING" Oleh "Eru Setia Utama", telah dipertahankan di depan komisi penguji pada hari Jumat tanggal 02 Agustus 2019.


Komisi Penguji

1. Ketua : Firamon Syakti, M.M., M.Kom.



(.....)

2. Anggota : Ilman Zuhri Yadi, M.M., M.Kom.



(.....)

3. Anggota : Aan Restu Mukti, M.Kom., CCNA



(.....)

Mengetahui,
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma
Ketua,



Universitas Bina Darma
Fakultas Ilmu Komputer

A. Haidar Mirza, S.T., M.Kom.

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Eru Setia Utama

NIM : 151420039

Dengan ini menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar sarjana di Universitas Bina Darma atau perguruan tinggi lain.
2. Skripsi ini murni gagasan, rumusan dan penelitian saya sendiri dengan arahan tim pembimbing.
3. Didalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar rujukan.
4. Saya bersedia skripsi, yang saya hasilkan dicek keasliannya menggunakan *plagiarism checker* serta diunggah ke *internet*, sehingga dapat diakses publik secara daring.
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi sesuai dengan peraturan dari perundang-undangan yang terbukti.

Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, Agustus 2019

Yang membuat pernyataan,



Eru Setia Utama

151420039

MOTTO

MOTTO :

Selangkah aku maju sejangkalpun tak akan mundur.

Hiduplah layaknya hari ini engkau akan mati, maka engkau akan mengerti arti dari sebuah bersyukur.

Belajar yang baik itu adalah belajar dari kesalahan kita sendiri. apabila kita tidak punya masalah belajarlah dari kesalahan orang lain.

Sesungguhnya bersama kesulitan ada kemudahan, maka apabila engkau telah selesai (dari sesuatu urusan), tetaplah bekerja keras (untuk urusan yang lain). Dan hanya kepada Tuhanmu lah engkau berharap (QS. Al-Insyirah, 6-8)

PERSEMBAHAN :

Allah S.W.T. atas segala kenikmatan dan ridha-NYA serta memberikan kemudahan kepada saya dalam menyelesaikan skripsi ini.

Kedua Orang Tua (Mama & Papa), terima kasih untuk semua pengorbanan dan jerih payah kalian dalam mendidik dan membesarkan saya hingga saya berada dititik ini.

Kedua adik terkasih (Erzy Maryola & Erky Anugera) semoga kelak kalian bisa merasakan berada pada titik ini.

Serta teman-teman seperjuangan Angkatan 2015 khususnya kelas IFA15. Yang akan tetap menjaadi keluarga saat lulus dari universitas binadarma.

ABSTRAK

Pemerintahan provinsi Sumatera Selatan sudah menggunakan *Wireless* sebagai penyedia internet yang dapat digunakan oleh pegawai yang sudah memiliki izin login. Jaringan *Wireless* yang baik haruslah memiliki keamanan yang baik agar terhindar dari ancaman kejahatan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan metode-metode keamanan jaringan terhadap sistem keamanan yang ada dalam jaringan tersebut. Adapun metode yang digunakan untuk mengamankan keamanan jaringan *Wireless* adalah *Wardriving* dan *Penetration Testing*. *Wardriving* adalah suatu kegiatan dimana seorang maupun sekelompok orang yang dibekali alat dan keahlian untuk mengakses sebuah jaringan *Wireless* secara gratis ataupun tanpa melakukan login. Sedangkan *Penetration Testing* adalah tindakan pengujian sistem dengan cara mensimulasikan bentuk-bentuk serangan terhadap sistem. Pengujian dengan metode ini tentunya akan berisiko dan merugikan beberapa pihak dan bagi pelaku tentunya merupakan sebuah pelanggaran. Penelitian ini menggunakan kasus di pemerintahan provinsi Sumatera Selatan yang di jadikan objek untuk mengetahui keamanan jaringan *Wireless* dari ancaman kejahatan (*cyber*).

Kata Kunci : *Nirkabel, Wardriving, Penetration Testing.*

ABSTRACT

The South Sumatra provincial government already uses Wireless as an internet provider that can be used by employees who already have a login permission. A good Wireless network must have good security to avoid the threat of crime. To see the quality of network security, it is necessary to do network security methods for the existing security system in the network. The method used to secure Wireless network security is Wardriving and Penetration Testing. Wardriving is an activity where a person or group of people are equipped with tools and expertise to access a Wireless network for free or without logging in. Whereas Penetration Testing is the act of testing a system by simulating the forms of attacks on the system. Testing with this method will certainly be risky and detrimental to some parties and for the offender is certainly an offense. This research uses a case in the South Sumatra provincial government which is made an object to determine the security of Wireless networks from the threat of crime (cyber).

Keywords: Nirkabel, Wardriving, Penetration Testing.

KATA PENGANTAR



Puji syukur kehadiran Allah SWT karena berkat rahmat dan karunia- Nya jualah, penelitian ini dapat diselesaikan guna memenuhi salah satu syarat untuk memperoleh gelar sarjana sebagai proses akhir dalam menyelesaikan pendidikan dibangku kuliah.

Dalam skripsi ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasnya pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan skripsi ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun.

Pada kesempatan yang baik ini, tak lupa penulis menghaturkan terima kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dalam penulisan skripsi ini, terutama kepada :

1. Dr. Sunda Ariana, M.Pd., M.M., selaku Rektor Universitas Bina Darma Palembang.
2. Dedi Syamsuar, S.Kom., M.IT., Ph.D., selaku Dekan Fakultas Ilmu Komputer
3. A. Haidar Mirza, ST., M.Kom., selaku Ketua Program Studi Informatika.
4. Firamon Syakti, M.M., M.Kom., selaku Pembimbing yang telah memberikan bimbingan penulisan skripsi ini.
5. Ilman Zuhri yadi, M.M., M.Kom dan Aan Restu Mukti, M.Kom., CCNA, selaku Penguji saat Ujian Seminar Proposal dan Ujian Komprehensif.
6. Orang Tua saya, ibu Erlina dan bapak Umar Hasan yang selalu memberikan dorongan dan masukan serta bantuan baik moril maupun materil yang tak ternilai harganya.
7. Teman-teman seperjuangan kelas IFA Angkatan 2015.

Palembang, September 2019

Eru Setia Utama

DAFTAR ISI

HALAMAN COVER	i
HALAMAN JUDUL	ii
HALAMAN PENGESAHAN	iii
SURAT PERSETUJUAN	iv
SURAT PERNYATAAN	v
MOTTO DAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
ABSTRAK	viii
ABSTRACTxi
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian.....	4
1.4.1 Tujuan Penelitian.....	4
1.4.2 Manfaat Penelitian.....	4
1.5 Alat dan Bahan.....	5
1.6 Sistematika Penulisan.....	6
BAB II TINJAUAN PUSTAKA	
2.1 Tinjauan Umum.....	7
2.1.1 Profil Pemerintahan Provinsi Sumatera Selatan.....	7
2.1.2 Visi dan Misi Pemerintahan Sumatera Selatan.....	7
a. Visi.....	7
b. Misi.....	8
2.2 Landasan Teori.....	9
2.2.1 Jaringan Internet.....	9
2.2.2 Keamanan Jaringan.....	9
2.2.3 <i>Mac Filtering</i>	11
2.2.4 <i>WEP (Wired Equivalent Privacy)</i>	12

2.2.5		WPA-PSK Atau WPA2-	12
	PSK		
2.2.6		Wireless dan Wi-fi	13
2.2.7		Wardriving	14
2.2.8		WPS Cracking	14
2.2.9		Penetration Testing	14
	2.3 Penelitian Sebelumnya		17
	2.3.1 Penelitian Aditya Wahyu Setyawan, Gunawan Adi,		
		Muhammad Ary Murti	17
2.3.2		Penelitian Kreshna, Muh.	
		Yamin, LM Fid Aksara	18
	2.4 Kerangka Berpikir		19

BAB III METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian	20
3.1.1 Waktu Penelitian	20
3.1.2 Waktu Penelitian	20
3.2 Data Penelitian	20
3.3 Metode Penelitian	20
3.4 Metode Pengumpulan Data	21
3.5 Metode Pengujian	22

BAB IV HASIL DAN PEMBAHASAN

4.1 Hasil (Analisa)	26
4.1.1 Scanning dan Pemetaan	27
4.1.2 Wigle Wifi –Network List	28
4.1.3 Wigle Wifi - Dashboard	29
4.1.4 Hasil Pemetaan	30
4.2 Pre-engagement Interactions	32
4.3 Intelligence Gathering	32
4.4 Threat Modeling	33
4.5 Vulnerability Analysis	33
4.6 Exploitation	35
4.7 Post Exploitation	37
4.7.1 Pengujian Cracking Keys	40
4.8 Reporting (Pembahasan)	42

BAB V PENUTUP

1.1 Kesimpulan.....	43
1.2 Saran.....	44

JADWAL PENELITIAN

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar	Halaman
2.1 Kerangka Berpikir	19
4.1 Topologi Pemerintahan Provinsi Sumatera Selatan	27
4.2 Tampilan Awal Wicle Wifi	28
4.3 Tampilan Menu Network.....	28
4.4 Tampilan Menu Dashboard	29
4.5 Pemetaan Dipemerintahan Provinsi Sumatera Selatan	30
4.6 Tentang <i>Ip Address</i> Komputer Kali Linux Peneliti	32
4.7 Hasil Dari Monitoring Airmon-ng	33
4.8 Hasil Dari Monitoring Airmon-ng pada lantai 2	34
4.9 Hasil Dari Airodum-ng	34
4.10 Hasil dari airodump-ng pada <i>wiffi</i> P.Kendaraan Pada lantai 1.....	35
4.11 Hasil Dari airodump-ng pada <i>wiffi</i> BPPUP Pada lantai 2.....	35
4.12 Folder Hasil Penyimpanan Dari BSSID	36
4.13 Hasil dari Aireplay-ng	37
4.14 Hasil dari aireplay-ng dengan bssid 78:32:1B:58:31:4A yang berbeda.....	37
4.15 Hasil dari aireplay-ng dengan bssid 80:41:26:E8:87:48 yang berbeda.....	38
4.16 Hasil Handshake dari bssid target 80:41:26:E5:93:54.....	38
4.17 Hasil Handshake dari bssid target 78:32:1B:58:31:4A.....	39
4.18 Hasil Handshake dari bssid target 3C:15:FB:B3:15:80.....	39
4.19 Hasil <i>Cracking Keys / Password</i> Salah	40
4.20 Hasil <i>Cracking keys/password</i> dari bssid 80:41:26:E8:87:48 berhasil.....	40
4.21 Hasil <i>Cracking keys/password</i> dari bssid 3C:15:FB:B3:15:80 berhasil... 41	
4.22 Hasil <i>Cracking keys/password</i> dari bssid 48:8E:EF:E0:D1:74 berhasil... 42	

DAFTAR TABEL

Table	Halaman
4.1 Tabel Pemetaan <i>Wigle</i>	31