

**ANALISIS DAN PENGUJIAN KELEMAHAN
KEAMANAN JARINGAN NIRKABEL DENGAN
METODE *EVIL TWIN ATTACK* PADA KALI LINUX**

SKRIPSI



Oleh :

Antoni

140210007

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS PUTERA BATAM

2018

**ANALISIS DAN PENGUJIAN KELEMAHAN KEAMANAN JARINGAN
NIRKABEL DENGAN METODE *EVIL TWIN ATTACK* PADA KALI
LINUX**

SKRIPSI

**Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana**



Oleh

Antoni

140210007

**PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2018**

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : ANTONI
NPM/NIP : 140210007
Fakultas : Teknik dan Komputer
Program Studi : Teknik Informatika

Menyatakan bahwa “**Skripsi**” yang saya buat dengan judul:

**ANALISIS DAN PENGUJIAN KELEMAHAN KEAMANAN JARINGAN
NIRKABEL DENGAN METODE EVIL TWIN ATTACK PADA KALI
LINUX**

Adalah hasil karya sendiri dan bukan “duplikasi” dari karya orang lain. Sepengetahuan saya, didalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun

Batam, 3 Februari 2018

Materai 6000

ANTONI
140210007

**ANALISIS DAN PENGUJIAN KELEMAHAN KEAMANAN JARINGAN
NIRKABEL DENGAN METODE *EVIL TWIN ATTACK* PADA KALI
LINUX**

**Oleh
Antoni
140210007**

**SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana**

**Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini**

Batam, 02 Februari 2018

**Cosmas Eko Suharyanto, S.Kom., M.SI
Pembimbing**

ABSTRAK

Perkembangan teknologi jaringan yang sangat pesat, telah membuat penggunaan jaringan berpindah dari yang menggunakan kabel menjadi penggunaan jaringan nirkabel. Penggunaan perangkat jaringan nirkabel pada saat ini sudah begitu banyak digunakan, baik digunakan untuk komunikasi suara maupun data. Karena teknologi jaringan nirkabel memanfaatkan frekuensi tinggi untuk mengirimkan sebuah data, maka kerentanan terhadap keamanan juga lebih tinggi dibandingkan dengan teknologi jaringan kabel. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat jaringan yang digunakan oleh pengguna maupun oleh operator yang memberikan layanan hotspot. Disisi lain, banyak metode-metode yang digunakan oleh *hacker* untuk mencuri informasi pengguna melalui jaringan nirkabel ini. Salah metode yang sering digunakan adalah *Evil twin Attack* atau sering disebut juga *Rogue AP(access point)* yang berarti *access point* palsu. Pada setiap perangkat jaringan nirkabel, terdapat MAC (*Medium Access Control*) address yang dapat dipalsukan dan digunakan untuk menukar identitas tiruan Access Point sebagai *Access Point* yang asli. Pada metode ini, semua pengguna yang terhubung pada jaringan akan dikirim sebuah *deauthentication frame* yang membuatnya terputus dari jaringan dan secara segera mencoba untuk menghubungkannya kembali dengan *Access Point* tiruan yang telah disiapkan oleh *hacker*. Setelah pengguna terhubung kembali ke jaringan, secara tidak langsung pengguna telah terhubung ke *access point* yang telah disiapkan untuk melakukan penyerangan, bukan akses point aslinya.

Kata Kunci : *Evil Twin Attack, Rogue Access Point, Keamanan jaringan nirkabel, Hotspot, Alamat MAC*

ABSTRACT

The rapid development of network technology, has made the use of network switching from using the cable to the use of wireless networks. The use of wireless network devices is now widely used, both for voice and data communications. Because wireless network technology utilizes high frequencies to transmit data, security vulnerabilities are also higher than wired network technologies. Various security measures can be done through network devices used by users or by operators who provide hotspot services. On the other hand, there are many methods used by hackers to steal user information over this wireless network. One commonly used method is Evil twin Attack or often called Rogue AP (access point) which means fake access point. On any wireless networking device, there is a MAC (Medium Access Control) address that can be forged and used to redirect an Access Point artificial identity as the original Access Point. In this method, all users connected on the network will be sent a deauthentication frame that makes it disconnected from the network and immediately try to reconnect with the artificial Access Point that has been prepared by the hacker. After the user reconnects the network, indirectly the user has connected to the access point that has been prepared to do the attack, not the original access point.

Keyword : Evil Twin Attack, Rouge Acces Point, Wireless Security, Hotspots, MAC Address

KATA PENGANTAR

Segala puji syukur penulis ucapkan kepada Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika, Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Ibu Nur Elfi Husda, S.Kom, M.SI selaku Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika, Bapak Andi Maslan, S.T., M.SI.
3. Bapak Cosmas Eko Suharyanto, S.Kom., M.MSI selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Kedua orang tua yang selalu memberikan doa, semangat dan dorongan kepada penulis.
6. Teman-teman seangkatan yang selalu memberi motivasi dan sama-sama menyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Batam, Februari 2018

Penulis

DAFTAR ISI

HALAMAN SAMPUL DEPAN

HALAMAN JUDUL	ii
SURAT PERNYATAAN ORISINALITAS.....	iii
HALAMAN PENGESAHAN.....	iv
ABSTRAK.....	v
ABSTRACK.....	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
BAB I.....	1
PENDAHULUAN.....	1
1.1. Latar Belakang Penelitian.....	1
1.2. Identifikasi Masalah	5
1.3. Pembatasan Masalah.....	6
1.4. Perumusan Masalah.....	6
1.5. Tujuan Penelitian	7
1.6. Manfaat Penelitian.....	7
1.6.1. Manfaat Teoritis.....	7
1.6.2. Manfaat Praktis	7
BAB II.....	8
KAJIAN PUSTAKA	8
2.1. Teori Dasar	8
2.1.1. Jaringan Komputer	8
2.1.2. Standar Jaringan Komputer	11
2.1.3. Jenis Jaringan Komputer	13
2.1.4. Model OSI Layer	16
2.2 Teori Khusus.....	24
2.2.1. Keamanan Jaringan	24

2.2.2.	Penetrasi Testing dan PTES (Penetration Testing Execution Standard).....	27
2.2.3.	Evil Twin Attack	28
2.2.4.	Kali Linux.....	29
2.3.	Tools.....	34
2.3.1.	Kali Linux	34
2.3.1.1.	Airodump-ng	35
2.3.1.2.	Airbase-ng	36
2.3.1.3.	Fluxion.....	37
2.4.	Penelitian Terdahulu	41
2.5.	Kerangka Pemikiran.....	45
BAB III.....		46
METODE PENELITIAN.....		46
3.1.	Desain Penelitian	46
3.2.	Standar dan Indikator Pengujian Keamanan	48
3.2.1.	Pre-engagement Interations.....	48
3.2.2.	Intelligence Gathering.....	49
3.2.3.	Threat Modeling.....	49
3.2.4.	Vulnerability Analysis.....	50
3.2.5.	Exploitation	51
3.2.6.	Post Exploitation	51
3.2.7.	Reporting.....	52
3.3.	Metode dan Skenario Pengujian.....	52
3.3.1.	Metode Pengujian.....	53
3.3.2.	Skenario Pengujian.....	54
3.4.	Lokasi dan Jadwal Penelitian.....	55
3.4.1.	Lokasi Penelitian	55
3.4.2.	Jadwal Penelitian	55
BAB IV		57
HASIL PENELITIAN DAN PEMBAHASAN		57
4.1.	Hasil Penelitian.....	57
4.1.1.	Hasil Pengujian Metode Evil Twin Attack.....	57
4.2.	Pembahasan.....	65
4.2.1.	Pengujian Metode <i>Evil Twin Attack</i>	65

4.2.2. Rekomendasi dan Mitigasi	76
BAB V	78
SIMPULAN DAN SARAN	78
5.1. Simpulan	78
5.2. Saran	79
DAFTAR PUSTAKA	80
RIWAYAT HIDUP	82
SURAT KETERANGAN PENELITIAN	84
LAMPIRAN	83

DAFTAR TABEL

	Halaman
Tabel 3.3 Cafe Tempat Penelitian.....	53
Tabel 3.4 Lokasi dan Jadwal Penelitian.....	56
Tabel 4.2.1.1 Data Hasil Scan Malaya Cafe – Nagoya Hill.....	68
Tabel 4.2.1.2 Data Hasil Scan Byza Cafe – Mega Mall Batam.....	70
Tabel 4.2.1.3 Data Hasil Scan Coffe Town – Kepri Mall.....	71
Tabel 4.2.1.4 Data Hasil Pengujian Evil Twin Attack.....	76

DAFTAR GAMBAR

	Halaman
Gambar 2.1.4 Lapisan OSI.....	17
Gambar 2.3.1 Menu Bar Kali Linux.....	36
Gambar 2.3.1.1 Airodump-ng.....	37
Gambar 2.3.1.2 Airebase-ng.....	39
Gambar 2.3.1.3. Fluxion.....	40
Gambar 2.3.1.3.1 Instalasi Fluxion.....	41
Gambar 2.3.1.3.2 Instalasi Fluxion.....	41
Gambar 2.3.1.3.3 Instalasi Fluxion.....	45
Gambar 2.5 Kerangka Penelitian.....	46
Gambar 3.1. Desain Penelitian.....	48
Gambar 3.2 Logo PTES.....	54
Gambar 3.3.1 Ilustrasi Metode Evil Twin Attack.....	57
Gambar 4.1.1.1 Hasil Penelitian Malaya Café.....	58
Gambar 4.1.1.2 Hasil Penelitian Byza Café.....	59
Gambar 4.1.1.3 Hasil Penelitian Coffe Town.....	59
Gambar 4.1.1.4 Hasil Penelitian Coffe Town.....	61
Gambar 4.1.1.6 Spesifikasi Redmi Note 3 Pro.....	62
Gambar 4.1.1.7 Spesifikasi Redmi Note 3 Pro.....	63
Gambar 4.1.1.8 Spesifikasi Redmi Note 4x.....	64
Gambar 4.1.1.8 Spesifikasi Redmi Note 4x.....	64
Gambar 4.2.1.1 Virtual Adapter dan IP Local.....	67
Gambar 4.2.1.2 Network Interface.....	67
Gambar 4.2.1.3 Monitoring Interface.....	68

Gambar 4.2.1.4 Konfigurasi Bridge.....	74
Gambar 4.2.1.5 Tampilan Saat Penyerangan.....	75
Gambar 4.2.1.6 Hasil Pengujian.....	75