ANALISIS KERENTANAN JARINGAN WIFI WPA & WPA2 TERHADAP SERANGAN MENGGUNAKAN AIRGEDDON

SKRIPSI

disusun oleh

RAGEL OCTAVIANDRA

19.11.2972

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

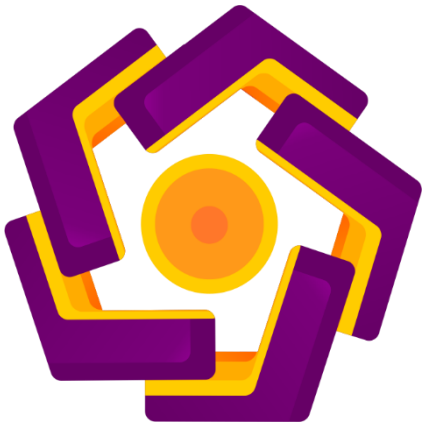
YOGYAKARTA

2023

ANALISIS KERENTANAN JARINGAN WIFI WPA & WPA2 TERHADAP SERANGAN MENGGUNAKAN AIRGEDDON

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai gelar Sarjana pada Program Studi Informatika



disusun oleh

RAGEL OCTAVIANDRA

19.11.2972

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KERENTANAN JARINGAN WIFI WPA&WPA2 TERHADAP SERANGAN MENGGUNAKAN AIRGEDDON

yang disusun dan diajukan oleh

Ragel Octaviandra

19.11.2972

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 2 Agustus 2023

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KERENTANAN JARINGAN WIFI WPA&WPA2 TERHADAP SERANGAN MENGGUNAKAN AIRGEDDON

yang disusun dan diajukan oleh

Ragel Octaviandra

19.11.2972

Telah dipertahankan di depan Dewan Penguji
pada tanggal 2 Agustus 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Lukman, M.Kom **NIK. 190302151**	
Yuli Astuti, M.Kom **NIK. 190302146**	
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 2 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ragel Octaviandra
NIM : 19.11.2972

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS KERENTANAN JARINGAN WIFI WPA&WPA2 TERHADAP SERANGAN MENGGUNAKAN AIRGEDDON

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 2 Agustus 2023

Yang Menyatakan,

Ragel Octaviandra

HALAMAN PERSEMBAHAN

"Dengan penuh rasa syukur, peneliti menghadirkan halaman persembahan ini sebagai ungkapan terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, dan inspirasi dalam perjalanan penulisan skripsi ini. Semoga hasil dari perjuangan ini dapat memberikan manfaat dan kontribusi bagi perkembangan ilmu pengetahuan dan masyarakat."

KATA PENGANTAR

Dalam kesempatan ini, penulis dengan rendah hati ingin mengucapkan terima kasih yang tak terhingga kepada semua pihak terutama kepada dosen pembibing Wahid Miftahul Ashari, S.Kom., M.T yang telah turut serta serta memberikan bantuan, dukungan, dan dorongan dalam penulisan skripsi ini. Tanpa kerjasama, bimbingan, dan motivasi dari berbagai pihak, penulisan skripsi ini tidak akan terwujud.

Ucapan terima kasih juga disampaikan kepada keluarga, teman-teman, dan semua yang telah memberikan semangat dan doa. Dengan kerendahan hati, penulis menyadari bahwa keterbatasan ilmu dan pengalaman yang dimiliki masih jauh dari sempurna, oleh karena itu kritik, saran, dan masukan yang membangun sangat diharapkan guna memperbaiki kualitas penulisan ini. Semoga hasil dari penelitian ini dapat memberikan manfaat dan kontribusi nyata bagi perkembangan ilmu pengetahuan dan masyarakat."

Yogyakarta, 04 Agustus 2023

Penulis

DAFTAR ISI

HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL x
DAFTAR GAMBAR xi
INTISARI xiii
ABSTRAK xiv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Sistematika Penulisan 3
BAB I I LANDASAN TEORI 5
2.1 Kajian Pustaka 5
2.2 Dasar Teori 7
2.2.1 Keamanan Jaringan 7
2.2.2 Ancaman (Threat) 8
2.2.3 Malware 8
2.2.4 Vulnerability (Kerentanan) 8
2.2.5 Serangan Jaringan 9
2.2.6 Wirelles Attack 9
2.2.7 Pixie Dust 9
2.2.8 Fake Acces Point (Evil Twin) 10

2.2.9 Bruteforce 12
2.2.10 Dictionary 13
2.2.11 Penanggulangan Serangan 14
2.3 Hipotesis 17
BAB III METODE PENELITIAN 17
3.1 Metode Penelitian 17
3.2 Flowchart 17
3.3 Pra Eksperimen 18
3.4 Eksperimen 19
3.5 Skenario Serangan 19
3.6 Skenario Perbaikan 21
3.7 Pasca Ekperimen 23
3.8 Analisis Hasil 23
3.9 Alat dan Bahan 25
BAB IV HASIL DAN PEMBAHASAN 26
4.1 Hasil Dan Pembahasan 26
4.2 Percobaan Awal 26
4.2.1 Data Percobaan 26
4.3 Dokumentasi Percobaan 28
4.4 Teknik Serangan 31
4.5 Perbaikan 32
4.6 Percoban Ulang 33
4.7 Hasil Efektifitas Percobaan ulang 54
4.8 Analisis Hasil 54
4.8.1 Tabel Perbandingan Serangan 54
4.8.2 Tabel Pengujian 55
4.8.3 Grafik Pengujian 56

BAB V PENUTUP 54
5.1 Kesimpulan.....54
5.2 Saran.....55
DAFTAR PUSTAKA 56

DAFTAR TABEL

Tabel 3. 1 Rencana Solusi.....22
Tabel 3. 2 Alat Dan Bahan.....25
Tabel 4. 1 Data Percobaan 26
Tabel 4. 2 Perbaikan 32
Tabel 4. 3 Perbandingan Serangan.....54
Tabel 4. 4 Tabel Hasil Pengujian.....55

DAFTAR GAMBAR

Gambar 3. 1 Tampilan Flowchart Penelitian 17
Gambar 3. 2 Tampilan Flowchart Eksperimen 18
Gambar 4. 1 Gambar tampilan awal airgeddon 27
Gambar 4. 2 Gambar tampilan awal airgeddon 27
Gambar 4. 3 Tools Pixie Dust 28
Gambar 4. 4 Tools Pixie Dust 28
Gambar 4. 5 Tools Pixie Dust 29
Gambar 4. 6 Tools Evil twin 29
Gambar 4. 7 Kombinasi Password Pada Tools Bruteforce 30
Gambar 4. 8 Proses Pengacakan Password 30
Gambar 4. 9 Password finded 31
Gambar 4. 10 Sudo Su Airgeddon 33
Gambar 4. 11 Tampilan Pemilihan Port Hub 34
Gambar 4. 12 Tampilan Tools Pixie-Dust Awal 34
Gambar 4. 13 Tampilan Masuk Pixie-dust 35
Gambar 4. 14 Opsi Monitor Mode 35
Gambar 4. 15 Pixie-dust Tools Running 36
Gambar 4. 16 Eror TimeOut Pixie-dust 36
Gambar 4. 17 Opsi Masuk Ke Evil Twin 37
Gambar 4. 18 Twin AP attack with captive 37
Gambar 4. 19 Pemilihan SSID Target 38
Gambar 4. 20 Deauth aireplay attack 38
Gambar 4. 21 Opsi Pengacakan MAC Address 39
Gambar 4. 22 Capture Handshake 39
Gambar 4. 23 Pemilihan Interval Value 40
Gambar 4. 24 Opsi Bahasa 40
Gambar 4. 25 Proses Evil Twin Berjalan 41
Gambar 4. 26 Password Terdeteksi 41
Gambar 4. 27 SSID Target Asli 42
Gambar 4. 28 Fake SSID Target 42
Gambar 4. 29 Tampilan Login Ke SSID Palsu 43

Gambar 4. 30 Opsi Masuk Ke Bruteforce 43
Gambar 4. 31 Scanning SSID Target 44
Gambar 4. 32 Capture Handshake 44
Gambar 4. 33 Set Value 45
Gambar 4. 34 Pembuatan File Baru 45
Gambar 4. 35 Penempatan File 46
Gambar 4. 36 File Handshake 46
Gambar 4. 37 Opsi Tools Bruteforce 47
Gambar 4. 38 Kombinasi Password 47
Gambar 4. 39 Kombinasi Password Huruf Kecil 48
Gambar 4. 40 Password Ditemukan 48
Gambar 4. 41 Sekumpulan Password 49
Gambar 4. 42 File txt dari Kumpulan Password 49
Gambar 4. 43 Explore for targets SSID 50
Gambar 4. 44 Opsi Capture Handshake 50
Gambar 4. 45 Opsi Deauth / disassoc amok mdk4 51
Gambar 4. 46 Pembuatan Folder 51
Gambar 4. 47 Opsi Dictionary Attack 52
Gambar 4. 48 Opsi Offline WPA/WPA2 decrypt 52
Gambar 4. 49 Pilihan Dictionary Attack 53
Gambar 4. 50 Pemilihan Capture File 53
Gambar 4. 51 Password Ditemukan 54
Gambar 4. 52 Grafik Pengujian 56

INTISARI

Jaringan wireless adalah sebuah teknologi yang digunakan untuk menerima maupun mengirim di jaringan lokal tanpa menggunakan kabel atau melalui gelombang radio. Kelemahan jaringan wireless adalah orang sekitar bisa melakukan hacking menggunakan tools yang tersedia di internet untuk mendapatkan password atau mengambil data secara illegal salah satunya keamanan wifi yang mengunakan keamanan wpa & wpa2.

Hal tersebut yang menjadi kerentanan pada keamanan wifi tersebut. Penelitian ini menggunakan metode serangan pixie-dust untuk melihat sistem kemanan pada jaringan wifi yang menggunakan kemanan wpa & wpa2. Tujuannya untuk melihat kerentanan jaringan wifi dari serangan pixie-dust dengan tools yang ada di kali linux. WPA (Wi-Fi Protected Access) adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel.

Metode pengamanan dengan WPA ini diciptakan untuk melengkapi dari sistem yang sebelumnya, yaitu WEP. Sedangkan WPA2 adalah versi kedua dari standar WPA. Hasil dari penelitian ini menunjukan bahwa kemanan jaringan wifi menggunakan wpa & wpa2 dapat dengan mudah di akses menggunakan serangan pixie-dust. oleh karena itu, pentingnya untuk meningkatkan kemanan wifi dan mencari solusi untuk mencegah kerentanan dari serangan pixie-dust tersebut.

Kata Kunci : Keamanan Wifi, Airgeddon, Pixie-dust, Evil Twin, Bruteforce, Dictionary, KaliLinux

ABSTRAK

Wireless networking is a technology that is used to receive and transmit on a local network without using cables or via radio waves. The weakness of wireless networks is that people around can do hacking using tools available on the internet to get passwords or take data illegally, one of which is wifi security using wpa & wpa2 security.

This is a vulnerability in the security of the wifi. This study uses the pixie-dust attack method to see the security system on a wifi network that uses wpa & wpa2 security. The goal is to see the vulnerability of the wifi network from pixie-dust attacks with the tools in Kali Linux. WPA (Wi-Fi Protected Access) is a system that can also be applied to secure wireless networks.

This security method with WPA was created to complement the previous system, namely WEP. While WPA2 is the second version of the WPA standard. The results of this study indicate that wifi network security using wpa & wpa2 can be easily accessed using pixie-dust attacks. Therefore, it is important to improve wifi security and find solutions to prevent the vulnerability from pixie-dust attacks.

Keyword : *Wifi Security, Airgeddon, Pixie-dust, Evil Twin, Bruteforce, Dictionary, KaliLinux*