ANALISIS DAN IMPLEMENTASI SERANGAN WIFI DEAUTHER ESP8266 TERHADAP JARINGAN WIFI ROUTER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

DIMAS PRIAMBODO

18.11.2032

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

ANALISIS DAN IMPLEMENTASI SERANGAN WIFI DEAUTHER ESP8266 TERHADAP JARINGAN WIFI ROUTER

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

DIMAS PRIAMBODO

18.11.2032

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI SERANGAN WIFI DEAUTHER ESP8266 TERHADAP JARINGAN WIFI ROUTER

yang disusun dan diajukan oleh

Dimas Priambodo

18.11.2032

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 17 Oktober 2022

Dosen Pembimbing,

Subektiningsih, M.Kom
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI SERANGAN WIFI DEAUTHER ESP8266 TERHADAP JARINGAN WIFI ROUTER

yang disusun dan diajukan oleh

Dimas Priambodo

18.11.2032

Telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Oktober 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Andriyan Dwi Putra, M.Kom **NIK. 190302270**	
Wahid Miftahul Ashari, S.Kom,. M.T **NIK. 190302452**	
Subektiningsih, M.Kom **NIK. 190302413**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Oktober 2022

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : DIMAS PRIAMBODO
NIM : 18.11.2032

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS DAN IMPLEMENTASI SERANGAN WIFI DEAUTHER ESP8266 TERHADAP JARINGAN WIFI ROUTER

Dosen Pembimbing : Subektiningsih, M.Kom

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, 17 Oktober 2022

Yang Menyatakan,

Dimas Priambodo

HALAMAN PERSEMBAHAN

Segala puji dan syukur atas berkat, Tuhan yang maha esa dengan kehendaknya dan bantuannya penulis mampu menyelesaikan skripsi dengan baik. Penulis juga mengucapkan terima kasih kepada pihak – pihak yang telah berkontribusi baik secara langsung maupun tidak langsung baik dalam penelitian maupun dalam penyusunan naskah. Skripsi ini saya persembahkan kepada :

1. Tuhan yang maha esa untuk segala atas kemudahannya yang telah diberikan.
2. Mama dan ayah atas limpahan kasih sayang yang telah diberikan selama ini dan cita-cita kedua orang tua yang berhasil menyekolahkan sampai tingkat perguruan tinggi ini.
3. Sahabat dan rekan seperjuangan selama saya melaksanakan perkuliahan yaitu, Reza Syahputra Hadiawan, Arya Yoga Widyatama, Yanuar Sadyatma, Wahid Rizka, Melano Habib, Nindra Reza, Samuel Aldi Lumantou, Ricky Chandra, Jalius You tree.
4. Semua pihak yang telah membantu baik secara langsung maupun tidak langsung.

KATA PENGANTAR

Segala puji dan syukur ke hadirat Tuhan Yang Maha Esa, karena dengan karunia dan rahmat-Nya, sehingga skripsi yang berjudul "Analisis dan Implementasi Serangan Wifi Deauther Esp8266 Terhadap Jaringan Wifi Router dapat terselesaikan dengan baik.

Skripsi ini diajukan untuk memenuhi syarat akademik dalam menyelesaikan program Strata 1 Sarjana Ilmu Komputer di Universitas Amikom Yogyakarta. Selain itu, tujuan dari penulisan skripsi ini adalah untuk memberikan pengetahuan kepada pembaca mengenai Serangan Deauther.

Proses penyelesaian skripsi ini tidak lepas dari bantuan, dukungan, kritik, dan saran dari berbagai pihak. Oleh karena itu penulis ingin menyampaikan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Ibu Subektiningsih, S.Kom, M.Kom. Selaku dosen pembimbing saya yang selalu dengan sabar dan tulus membimbing serta memberikan ilmu kepada penulis.
4. Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah banyak memberikan ilmunya selama kuliah.
5. Teman-teman dari kelas Informatika 4 yang telah menemani dan bersusah senang bersama selama perkuliahan.
6. Semua pihak yang telah membantu baik secara langsung maupun tidak langsung.

Yogyakarta, 18 Oktober 2022

Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR LAMPIRAN xi
DAFTAR LAMBANG DAN SINGKATAN xii
DAFTAR ISTILAH xiii
INTISARI xiv
ABSTRACT xv
BAB I Pendahuluan 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Batasan Masalah 5
1.5 Manfaat Penelitian 5
1.6 Metode Penelitian 5
BAB II Landasan Teori 9
2.1 Tinjauan Pustaka 9
2.2 Dasar Teori 23
2.2.3 Router 23
2.2.4 Jenis-jenis Frame koneksi wifi 24
2.2.5 Hacking 28
2.2.6 Wireless Security 31
2.2.7 Deauther Esp8266 32
2.2.8 Mikrokontroler NodeMCU Esp8266 34
BAB III Metodologi Penelitian 38
3.1 Tahap pelaksanaan proses penelitian 38
3.2 Studi Pustaka 39

3.3 Metode Observasi 39
3.4 Metode Penelitian 40
3.4.1 Waktu Pelaksanaan 40
3.4.2 Objek Penelitian 40
3.5 Alat dan Bahan Penelitian 40
3.5.1 Perangkat Keras 41
3.5.2 Perangkat Lunak 41
3.5.3 Wifi Router 42
3.6 Flowchart Pengujian 43
3.7 Metode dan Alur Penelitian 44
BAB IV HASIL DAN PEMBAHASAN 47
4.1 Scope 47
4.2 Reconnaissance 48
4.3 Vulnerability Detection 49
4.4 Information Analysis & Planning 50
4.4.1 Konfigurasi driver Ch430g 50
4.4.2 Instalasi program firmware deauther 51
4.5 Penetration Testing 54
4.6 Privilege Escalation 60
4.7 Reporting 63
BAB V PENUTUP 73
5.1 Kesimpulan 73
5.2 Saran 74
Daftar Pustaka 75
LAMPIRAN 77

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian 12
Tabel 2. 2 Spesifikasi NodeMCU Esp8266 36
Tabel 3 1 Perangkat keras 41
Tabel 3 2 Perangkat lunak 41
Tabel 4. 1 Perangkat yang digunakan 48
Tabel 4. 2 hasil evaluasi kelemahan dan ancaman deauther esp8266 72

DAFTAR GAMBAR

Gambar 2. 1 Penggambaran grafis dari serangan deauthentication.[10] 33
Gambar 2. 2 Mikrokontroler Nodemcu Esp2866[22] 35
Gambar 3. 1 flowchart penelitian 38
Gambar 3. 2 Metode VAPT[8] 43
Gambar 4. 1 Simulasi penyerangan dengan topologi PAN 47
Gambar 4. 2 Hasil scanning dengan Wi-fi Scanner 48
Gambar 4. 3 Sniffing traffic 802.11 menggunakan whireshark 49
Gambar 4. 4 proses instalasi driver 50
Gambar 4. 5 kode firmware program deauther 51
Gambar 4. 6 konfigurasi Board ESP8266 52
Gambar 4. 7 proses upload program deauther 53
Gambar 4. 8 proses menghubungkan pada Deauther Esp8266 54
Gambar 4. 9 tampilan web penyerang Deauther 55
Gambar 4. 10 Device hp 1 terputus 56
Gambar 4. 11 Device hp 2 terputus 57
Gambar 4. 12 Laptop 1 terputus 57
Gambar 4. 13 Komputer yang menggunakan LAN 58
Gambar 4. 14 Hide SSID pada router 59
Gambar 4. 15 Proses phising ssid evil twin 60
Gambar 4. 16 proses phising ssid berhasil 61
Gambar 4. 17 penyerangan mendapatkan kata sandi korban 62
Gambar 4. 18 device hp 1 terputus 63
Gambar 4. 19 device hp 2 terputus 64
Gambar 4. 20 Laptop 1 terputus 64
Gambar 4. 21 Penyerang mengirimkan phising ssid 65
Gambar 4. 22 Sandi router muncul pada web penyerangan deauther 66
Gambar 4. 23 Hide ssid router 67
Gambar 4. 24 Sniffing wifi traffic menggunakan whireshark 68
Gambar 4. 25 Menganalisis deauthentication pada wireshark 69
Gambar 4. 26 pola serangan deauther 70
Gambar 4. 27 Wireshark monitoring diassociate 70
Gambar 4. 28 Proses manipulasi probe response 71

DAFTAR LAMPIRAN

Lampiran kode Program deauther firmware 1 77
Lampiran alat Pengujian 1 Router wifi dan Node mcu Esp8266..... 84

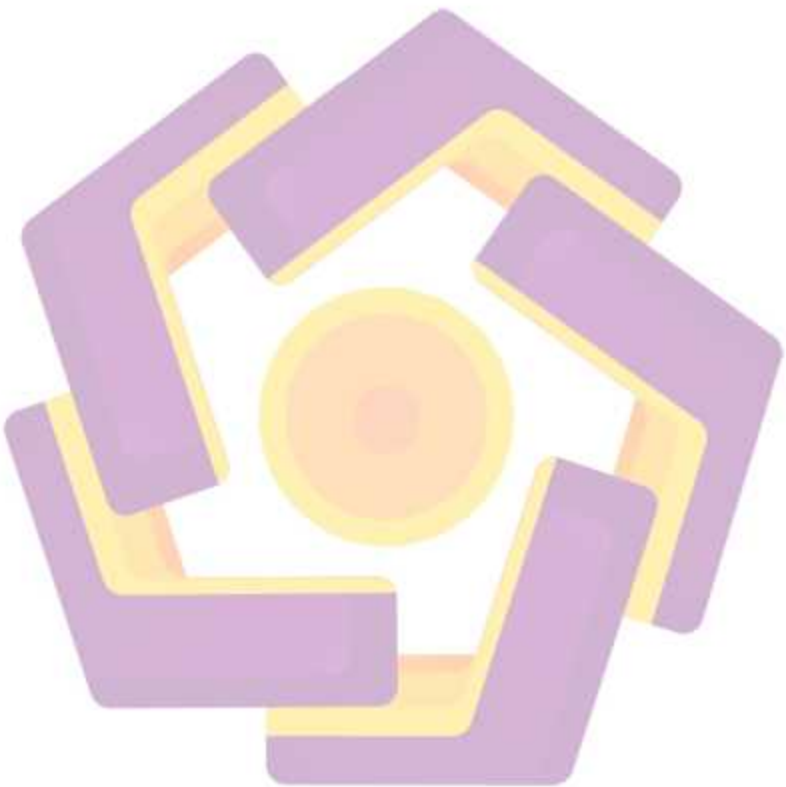
DAFTAR LAMBANG DAN SINGKATAN

WIFI	:	Wireless Fidelity
SSID	:	Service Set Identifier
WLAN	:	Wireless Local Area Network
PAN	:	Personal Area Network

DAFTAR ISTILAH

Phising : Serangan yang dilakukan untuk menipu atau memancing korban.

Hacking : Aktivitas penyusupan ke dalam sistem.



INTISARI

Jaringan nirkabel atau yang sering disebut dengan wifi, yang ditetapkan sebagai teknologi untuk menghubungkan perangkat digital seperti; ponsel pintar, tablet, laptop, dan perangkat IoT telah menimbulkan ancaman dalam keamanan data. Deauther merupakan serangan yang menghalangi semua perangkat untuk terhubung ke jaringan dengan cara memutuskan koneksi dari jaringan dan mencegahnya menyambung kembali. Deauther Esp8266 menggunakan hardware Microcontroller Esp8266 yang sudah dikonfigurasi untuk melakukan serangan Deauther dan melakukan phishing SSID yang bekerja di Data Link dan Network. dengan cara membuat paket-paket palsu. Memanfaatkan struktur data perangkat router, ketika saat paket dikirimkan dari deauther akan membuat terganggunya proses koneksi antara client dan router yang mengakibatkan terputusnya jaringan.

Metode yang digunakan dalam penelitian ini adalah VAPT (Vulnerability Assessment & Penetration Testing) sebagai penilaian serta pengujian terhadap kerentanan keamanan yang ada, meliputi, scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation dan reporting. Pengujian dilakukan terhadap router standar IEEE 802.11 b/g/n, frekuensi 2.4 ghz dengan melakukan serangan deauther esp8266. pada tahap pengujian simulasi serangan ini digunakan untuk mengetahui dampak yang terjadi saat serangan dilakukan, Metode Vapt dan penetration testing ini dapat digunakan secara efektif untuk penilaian kerentanan dan pengujian penetrasi dalam melakukan pengujian keamanan yang dirancang untuk mengidentifikasi dan mengatasi kerentanan keamanan siber, sebagai hasil dari analisis sebagai berikut.

Ancaman Serangan deauther esp8266 ini memanfaatkan celah pada manajemen frame WLAN standar 802.11 yang tidak di enkripsi dengan melakukan pengiriman paket-paket palsu kepada frame deautentikasi, membuat router dan client terputus secara paksa serta memblokade kedua akses jaringan. deauther esp8266 untuk saat ini hanya bisa dilakukan dan tersedia hanya pada frekuensi 2.4 Ghz. Dikarenakan cara kerja alat ini Penyerang akan membangkitkan satu frekuensi yang sama dengan frekuensi pada wireless LAN, jadi hanya menyandingkan frekuensi yang sama tidak membangkitkan frekuensi yang lebih tinggi pada target seperti jamming. dalam penelitian ini serangan menunjukan dimulai dari lapisan bawah, termasuk serangan yang berasal dari 802.11, yang berada di lapisan tautan tumpukan protokol OSI. Diharapkan penelitian ini dapat mengedukasi dan meningkatkan tentang keamanan nirkabel dan ancaman serangan deauther esp8266.

Kata kunci: WLAN, Router, Deauther, Vapt, OSI. Esp8266

ABSTRACT

Wireless network or often referred to as wifi, which is defined as a technology to connect digital devices such as; Smartphones, tablets, laptops and IoT devices have posed a threat to data security. Deauther is an attack that prevents all devices from connecting to the network by disconnecting them from the network and preventing them from reconnecting. Deauther Esp8266 uses an Esp8266 microcontroller hardware that has been configured to carry out Deauther attacks and perform SSID phishing that works on Data Link and Network. by creating fake packages. Utilizing the data structure of the router device, when the packet is sent from the deauther it will disrupt the connection process between the client and the router which results in network disconnection.

The method used in this study is VAPT (Vulnerability Assessment & Penetration Testing) as an assessment and testing of existing security vulnerabilities, including scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation and reporting. Tests were carried out on standard IEEE 802.11 b/g/n routers, frequency 2.4 ghz by performing deauther esp8266 attacks. at the testing stage, this attack simulation is used to determine the impact that occurs when the attack is carried out, this Vapt and penetration testing method can be used effectively for vulnerability assessment and penetration testing in conducting security tests designed to identify and overcome cybersecurity vulnerabilities, as a result of the analysis. as follows.

Threats This esp8266 deauther attack exploits a loophole in the management of unencrypted 802.11 WLAN frames by sending fake packets to the deauthentication frame, forcibly disconnecting routers and clients and blocking both network access. deauther esp8266 for now can only be done and is available only on the 2.4 Ghz frequency. Due to the way this tool works, the attacker will generate a frequency that is the same as the frequency on the wireless LAN, so only pairing the same frequency does not generate a higher frequency on the target such as jamming. in this study the attacks are shown to start from the lower layers, including attacks originating from 802.11, which are at the link layer of the OSI protocol stack. It is hoped that this research can educate and improve wireless security and the threat of deauther esp8266 attacks.

.

Keyword: *WLAN, Router, Deauther, Vapt, OSI. Esp8266*