ANALISIS VULNERABILITY KEAMANAN JARINGAN WIRELESS PADA PROTOKOL WPA DAN WPA2 TERHADAP SERANGAN AIRCRACK/HASHCAT MENGGUNAKAN METODE 4-WAY HANDSHAKE DAN PAIRWISE MASTER KEY IDENTIFIER

SKRIPSI

disusun oleh

Arief Kurniawan

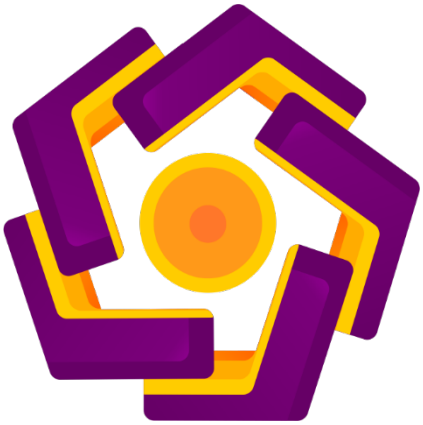
16.11.0243

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

ANALISIS VULNERABILITY KEAMANAN JARINGAN WIRELESS PADA PROTOKOL WPA DAN WPA2 TERHADAP SERANGAN AIRCRACK/HASHCAT MENGGUNAKAN METODE 4-WAY HANDSHAKE DAN PAIRWISE MASTER KEY IDENTIFIER

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana S1
pada Program Studi Informatika



disusun oleh

Arief Kurniawan

16.11.0243

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2020

PERSETUJUAN

SKRIPSI

ANALISIS VULNERABILITY KEAMANAN JARINGAN WIRELESS PADA PROTOKOL WPA DAN WPA2 TERHADAP SERANGAN AIRCRACK/HASHCAT MENGGUNAKAN METODE 4-WAY HANDSHAKE DAN PAIRWISE MASTER KEY IDENTIFIER

yang dipersiapkan dan disusun oleh

Arief Kurniawan

16.11.0243

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 Oktober 2019

Dosen Pembimbing,

Bayu Setiaji, M.Kom.
NIK. 190302216

PENGESAHAN

SKRIPSI

ANALISIS VULNERABILITY KEAMANAN JARINGAN WIRELESS PADA PROTOKOL WPA DAN WPA2 TERHADAP SERANGAN AIRCRACK/HASHCAT MENGGUNAKAN METODE 4-WAY HANDSHAKE DAN PAIRWISE MASTER KEY IDENTIFIER

yang dipersiapkan dan disusun oleh

Arief Kurniawan

16.11.0243

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Februari 2020

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ali Mustopa, M.Kom **NIK. 190302192**	
Bayu Setiaji, M.Kom **NIK. 190302216**	
Andika Agus S, M.Kom **NIK. 190302109**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Februari 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 1 Februari 2020

Arief Kurniawan

NIM. 16.11.0243

MOTTO

“Sebuah kebenaran tidak selalu dapat diterima oleh semua orang. Karena mereka hanya ingin mendengar apa yang ingin mereka dengar, melihat apa yang ingin mereka lihat.”

(Penulis)

PERSEMBAHAN

Alahamdulillah, puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, kita memuji-Nya, dan meminta pertolongan, pengampunan serta petunjuk kepada-Nya. Kita berlindung kepada Tuhan Yang Maha Esa dari kejahatan diri dan keburukan amal kita. Taburan cinta dan kasih sayang-Mu telah memberikanku kekuatan, membekaliku dengan ilmu serta memperkenalkanku dengan dunia. Atas karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan.

Kupersembahkan karya sederhana ini kepada orang yang sangat kukasihi dan kusayangi. Rasa terima kasih aku ucapkan untuk :

1. **Ibunda dan Ayahanda tercinta**. Sebagai tanda bakti, hormat dan rasa terima kasih yang tidak terhingga kupersembahkan karya kecil ini kepada Ibu (Yuli Astuti) dan Ayah (Sultan Damma) yang telah memberikan kasih sayang, dukungan, dan motivasi tanpa henti yang tidak mungkin dapat kubalas hanya dengan selembar kertas yang bertuliskan persembahan. Semoga ini menjadi langkah awal untuk membuat kalian bahagia karena kusadar, selama ini belum dapat berbuat lebih.
2. **Adik-Adik tercinta**. Sebagai rasa terima kasihku karena telah memberikanku dorongan untuk menjadi seorang kakak yang baik dan menjadi panutan serta tauladan.
3. **Teman-teman seperjuangan**. Terutama untuk anggota CEO Japox yang selalu memberikanku nasihat, pendapat, motivasi, serta candaan untuk menghilangkan beban pikiran. Dengan mengucapkan banyak terima kasih karena selama menyelesaikan studi telah memberikan banyak hal yang tak terlupakan kepadaku untuk dikenang.
4. **Dosen pembimbing tugas akhir**. Bapak Bayu Setiaji, M.kom selaku dosen pembimbing skripsi saya, terima kasih banyak Bapak sudah membantu selama ini, telah memberikan masukan, pendapat, ilmu, dan mengarahkan saya hingga skripsi ini selesai.

KATA PENGANTAR

Syukur Alhamdulillah kehadirat Tuhan Yang Maha Esa yang telah melimpahkan Rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Vulnerability Keamanan Jaringan Wireless Pada Protokol Wpa dan Wpa2 Terhadap serangan Aircrack/Hashcat Menggunakan Metode 4-Way Handshake Dan Pairwise Master Key Identifier".

Penulis menyadari sepenuhnya bahwa proses penyusunan skripsi ini telah melalui banyak sekali hambatan dan rintangan, namun berkat dorongan dan bantuan dari berbagai pihak, maka akhirnya penulisan ini dapat diselesaikan.

1. Bapak M. Suyanto, Prof., Dr., M.M. Selaku Rektor Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si, MT. Selaku Dekan Fakultas Ilmu Komputer, dan Ketua Program Studi S1 Sistem Informasi Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. Selaku dosen wali.
4. Seluruh Dosen, Karyawan, dan Seluruh Civitas Akademika Universitas Amikom Yogyakarta yang telah memberikan semangat dan banyak membantu dalam penulisan skripsi ini.

Penulis berharap semoga skripsi ini dapat memberikan manfaat bagi generasi mendatang khususnya dalam bidang teknologi dan informasi.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN

ACK = Acknowledgement

ADSL = Asymmetric digital subscriber line

AES = Advanced Encryption Standard

AUI = Attachment Unit Interface

BNC = Bayonet Neill Concelman

CAP = Capture

CCMP = Counter mode Cipher block chaining Message authentication code Protocol

CLI = Command Line Interface

CRC = Cyclic Redundancy Check

CTS = Clear To Send

DARPA = Defense Advanced Research Projects Agency

DES = Data Encryption Standard

DHCP = Dynamic Host Control Protocol

DNS = Domain Name Server

DoS = Denial of Service

DSL = Digital Subscriber Line

EAP = Extensible Authentication Protocol

EAPOL = Extensible Authentication Protocol over LAN

FCS = Frame Check Sequence

GMK = Group Master Key

GSM = Global System for Mobile

GTK = Group Temporal Key

HMAC = Hash-based Message Authentication Code

IEEE = Institute of Electrical and Electronics Engineers

IP = Internet Protocol

ISO = International Standard Organization

ISP = Internet Service Provider

MAC = Media Access Control / Message Authentication Code

MFP = Management Frame Protection

MIC = Message Integrity Code

MITM = Man In The Middle

MSK = Master Session Key

NAT = Network Address Translation

NIC = Network Interface Card

NPCAP = Nmap Packet Capture

OSI = Open System Interconnection

P2P = Point To Point

PBKDF = Password-Based Key Derivation Function

PCI = Peripheral Component Interconnect

PCMCIA = Personal Computer Memory Card International Association

PMK = Pairwise Master Key

PMKID = Pairwise Master Key Identifier

PSK = Pre-Shared Key

PTK = Pairwise Transit Key

RADIUS = Remote Authentication Dial-in User Service

RC4 = Rivest Cipher 4

RFC = Request for Comments

RSN IE = Robust Security Network Information Element

RTS = Request To Send

SSID = Service Set Identifier

TCP = Transmission Control Protocol

TKIP = Temporal Key Integrity Protocol

TSC = TKIP Sequence Counter

UDP = User Datagram Protocol

USB = Universal Serial Bus

UTP = Unshielded Twisted Pair

VAP = Virtual Access Point

WEP = Wired Equivalent Privacy

WI-MAX = Worldwide Interoperability for Microwave Access

WLAN = Wireless Local Area Network

WPA = Wifi Protected Access

INTISARI

Wireless network atau jaringan nirkabel telah menjadi bagian dari jaringan komputer yang paling banyak digunakan pada saat ini. Keamanan data pada jaringan nirkabel ini menjadi suatu ancaman yang sangat melekat. Karena sifat dari media nirkabel yang terbuka maka sangat memungkinkan bahwa penyusup atau peretas dapat memanfaatkan celah komunikasi tersebut. Berbeda dengan jaringan kabel yang sifatnya tertutup karena tidak menggunakan gelombang radio sebagai transmisi pengiriman antar data. Para peneliti telah mengusulkan beberapa protokol enkripsi untuk memberikan keamanan jaringan nirkabel seperti WEP, WPA, dan RADIUS.

Dalam tulisan ini, penulis akan melakukan analisis ekperimental dengan menggunakan metode *Penetration Test* untuk mempelajari kelemahan dari protokol enkripsi WPA. Jenis serangan yang dipakai dalam penetrasi adalah serangan *client* dan *clientless*. Penelitian ini akan membandingkan mekanisme dari setiap serangan terhadap protokol WPA dan WPA2 untuk pemahaman yang lebih baik tentang prinsip kerja dan bug keamanan dari protokol tersebut. Penulis akan menggunakan software *opensource* aircrack dan hashcat yang digunakan untuk serangan kata sandi dengan menggunakan metode *4-way handshake* dan *Pairwise Master Key Identifier* (PMKID).

Analisis dan temuan dari penelitian ini akan digunakan sebagai media pengetahuan agar kedepan para pakar keamanan jaringan dapat memperbaiki masalah yang ada, serta memberikan solusi alternatif kepada para pengguna akhir atau end-user protokol tersebut. Tidak lupa untuk pengguna akhir agar dapat merancang kembali keamanan jaringan untuk meminimalisir serangan yang kemungkinan besar akan terjadi.

Kata Kunci : WPA, Penetration Testing, Nirkabel, Enkripsi, Protokol, Aircrack, Hashcat, Analisis, Evaluasi, Pengguna Akhir, Kerentanan.

ABSTRACT

Wireless networks have become part of the most widely used computer networks at present. Data security on this wireless network becomes a very inherent threat. Because of the nature of open wireless media, it is very possible that intruders or hackers can exploit this communication gap. Unlike the cable network that is closed because it does not use radio waves as a transmission between data transmission. Researchers have proposed several encryption protocols to provide wireless network security such as WEP, WPA, and RADIUS.

In this paper, the author will conduct an experimental analysis using the Penetration Test method to study the weaknesses of the WPA encryption protocol. The types of attacks used in penetration are client and clientless attacks. This research will compare the mechanism of each attack on the WPA and WPA2 protocols for a better understanding of the working principles and security bugs of the protocol. The author will use opensource aircrack and hashcat software used for password attacks using the 4-way handshake method and Pairwise Master Key Identifier (PMKID).

Analysis and findings from this study will be used as a medium of knowledge so that in the future network security experts can fix existing problems, as well as provide alternative solutions to end users or end-user protocols. Do not forget for end users to be able to redesign network security to minimize attacks that are likely to occur.

Keyword : *WPA, Penetration Test, Wireless, Encryption, Protocol, Aircrack, Hashcat, Analysis, Evaluation, End-User, Vulnerability*