

**ANALISIS VULNERABILITY KEAMANAN JARINGAN WIRELESS
PADA PROTOKOL WPA DAN WPA2 TERHADAP SERANGAN
AIRCRAK/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
AIRCRAK/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
AIRCRAK/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 AIRCRAK/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

Alhamdulillah, 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 kehadiran 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

PERSETUJUAN	II
PENGESAHAN	III
PERNYATAAN	IV
MOTTO	V
PERSEMBAHAN	VI
KATA PENGANTAR	VII
DAFTAR ISI	VIII
DAFTAR TABEL	XIII
DAFTAR GAMBAR	XIV
DAFTAR SINGKATAN	XVII
INTISARI	XX
ABSTRACT	XXI
BAB I	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian	4
1.5 Manfaat Penelitian.....	5
1.6 Metodologi Penelitian	5
1.7 Sistematika Penulisan.....	5
BAB II	7
2.1 Kajian Pustaka	7
2.2 Jaringan Nirkabel	8
2.2.1 Konsep Jaringan Nirkabel.....	8

2.2.2	Standar Jaringan Nirkabel.....	9
2.2.3	Kanal Frekuensi Jaringan Nirkabel.....	9
2.2.4	Model Jaringan Nirkabel.....	10
2.2.4.1	Ad-Hoc.....	10
2.2.4.2	Infrastruktur	10
2.2.5	Cakupan Skala Area Nirkabel.....	11
2.2.5.1	WPAN.....	11
2.2.5.2	WLAN	11
2.2.5.3	WMAN	11
2.2.5.4	WWAN	12
2.2.6	Antena	12
2.2.6.1	Antena Directional.....	12
2.2.6.2	Antena Omnidirectional	13
2.3	Model Referensi Jaringan.....	14
2.3.1	Model OSI.....	14
2.3.2	Model DARPA.....	14
2.4	Protokol TCP dan UDP	15
2.5	Topologi Jaringan.....	15
2.5.1	Topologi Bus.....	15
2.5.2	Topologi Ring	16
2.5.3	Topologi Star.....	17
2.5.4	Topologi Tree.....	17
2.5.5	Topologi Mesh.....	18
2.6	Firewall.....	18
2.6.1	Konsep Firewall	18
2.6.2	Jenis Firewall	19
2.6.2.1	Stateless Firewall	19
2.6.2.2	Statefull Firewall.....	19
2.7	Protokol Otentikasi.....	19
2.7.1	WPA.....	19
2.7.2	WPA2.....	20

2.8	Kerentanan Protokol WPA/WPA2	20
2.9	SSID	21
2.10	Mode Personal dan Enterprise.....	22
2.11	Kunci Enkripsi.....	22
2.12	Algoritma Enkripsi	23
2.13	4-Way Handshake	23
2.14	Pairwise Master Key Identifier.....	24
2.15	Serangan 4-Way Handshake	24
2.16	Serangan PMKID	26
2.16.1	Keuntungan Serangan PMKID	27
2.17	Penanggulangan Terhadap Serangan 4-Way Handshake.....	28
2.18	Penanggulangan Terhadap Serangan PMKID.....	28
2.19	Frame Jaringan Nirkabel	29
2.20	RouterBoard Mikrotik	30
2.21	Software Pendukung Penelitian.....	31
2.21.1	Kali Linux	31
2.21.2	Aircrack.....	31
2.21.3	Hashcat.....	31
2.21.4	Wireshark Network Protocol Analyzer.....	32
2.21.5	Winbox.....	32
2.22	Teknik Tapping Dan Wireless Sniffing.....	32
BAB III	33
3.1	Tinjauan Umum.....	33
3.2	Alur Penelitian.....	34
3.3	Rancangan Topologi Jaringan	35
3.4	Analisis Kebutuhan Perangkat Keras	38
3.5	Analisis Kebutuhan Perangkat Lunak	39
3.6	Rancangan Konfigurasi Pada Router Mikrotik RB931-2nD.....	40
3.6.1	Konfigurasi Interface	40
3.6.2	Konfigurasi Wireless Station	40

3.6.3	Konfigurasi Wireless Virtual Access Point.....	41
3.6.4	Konfigurasi Alamat IP	41
3.6.5	Konfigurasi DHCP Server.....	42
3.6.6	Konfigurasi NAT	42
3.6.7	Konfigurasi Security Profile	42
3.7	Rancangan Penggunaan Wireshark Pada Jaringan.....	43
3.7.1	Wireless Sniffing.....	44
3.8	Rancangan Pengujian	44
3.8.1	Parameter Pengujian.....	45
3.8.2	Cara Pengukuran Parameter Pengujian.....	45
3.8.3	Parameter Penilaian Tingkat Keamanan	46
BAB IV	47
4.1	Implementasi WPA Dan WPA2 Pada Mikrotik.....	47
4.1.1	Konfigurasi Alamat IP Administrator.....	47
4.1.2	Konfigurasi Interface Mikrotik	48
4.1.3	Konfigurasi Alamat IP Mikrotik	48
4.1.4	Konfigurasi Mikrotik Sebagai Wireless Station	49
4.1.4.1	Konfigurasi Security Profile	49
4.1.4.2	Konfigurasi Wireless	50
4.1.4.3	Konfigurasi DHCP Client.....	51
4.1.5	Konfigurasi Virtual Access Point.....	52
4.1.5.1	Konfigurasi Alamat IP Access Point	54
4.1.5.2	Konfigurasi DHCP Server	54
4.1.5.3	Konfigurasi NAT	55
4.1.6	Konfigurasi Mikrotik Wireless Sniffer	56
4.1.7	Konfigurasi Komputer Administrator.....	57
4.1.8	Konfigurasi USB Wireless Sniffer.....	58
4.2	Proses Uji Serangan 4-Way Handshake Pada Protokol WPA	59
4.2.1	Scanning.....	59
4.2.2	Menginjeksi Paket Deauthentication.....	61

4.3	Proses Uji Serangan PMKID.....	65
4.4	Serangan Dictionary Sebagai Pemecahan Kata Sandi	69
4.4.1	Serangan Dictionary Menggunakan Tool Aircrack	69
4.4.2	Serangan Dictionary Menggunakan Tool Hashcat	71
4.5	Penanggulangan Serangan 4-Way Handshake Dan PMKID.....	73
4.5.1	Mendeteksi Serangan Menggunakan Wireshark.....	73
4.5.2	Mendeteksi Serangan 4-Way Handshake.....	74
4.5.3	Pencegahan Serangan Deauthentication	76
4.5.4	Mendeteksi Serangan PMKID	79
4.5.5	Pencegahan Serangan PMKID.....	81
4.5.6	Penangkapan Penyerang dari Serangan Yang Diimplementasikan	83
4.6	Pengujian Dan Evaluasi.....	83
4.6.1	Uji Coba Skenario Satu.....	83
4.6.2	Uji Coba Skenario Dua	88
4.6.3	Uji Coba Skenario Tiga.....	89
4.6.4	Hasil Perbandingan Pengujian	91
4.7	Pembahasan	93
4.7.1	Evaluasi Hasil Pengujian.....	93
4.7.2	Tahap Scanning.....	94
4.7.3	Tahap Capture	94
4.7.4	Tahap Cracking	95
4.7.5	Tahap Monitoring dan Pencegahan.....	96
4.8	Hasil Vulnerability Yang Didapat.....	96
BAB V	98
5.1	Kesimpulan.....	98
5.2	Saran.....	99
DAFTAR PUSTAKA	101

DAFTAR TABEL

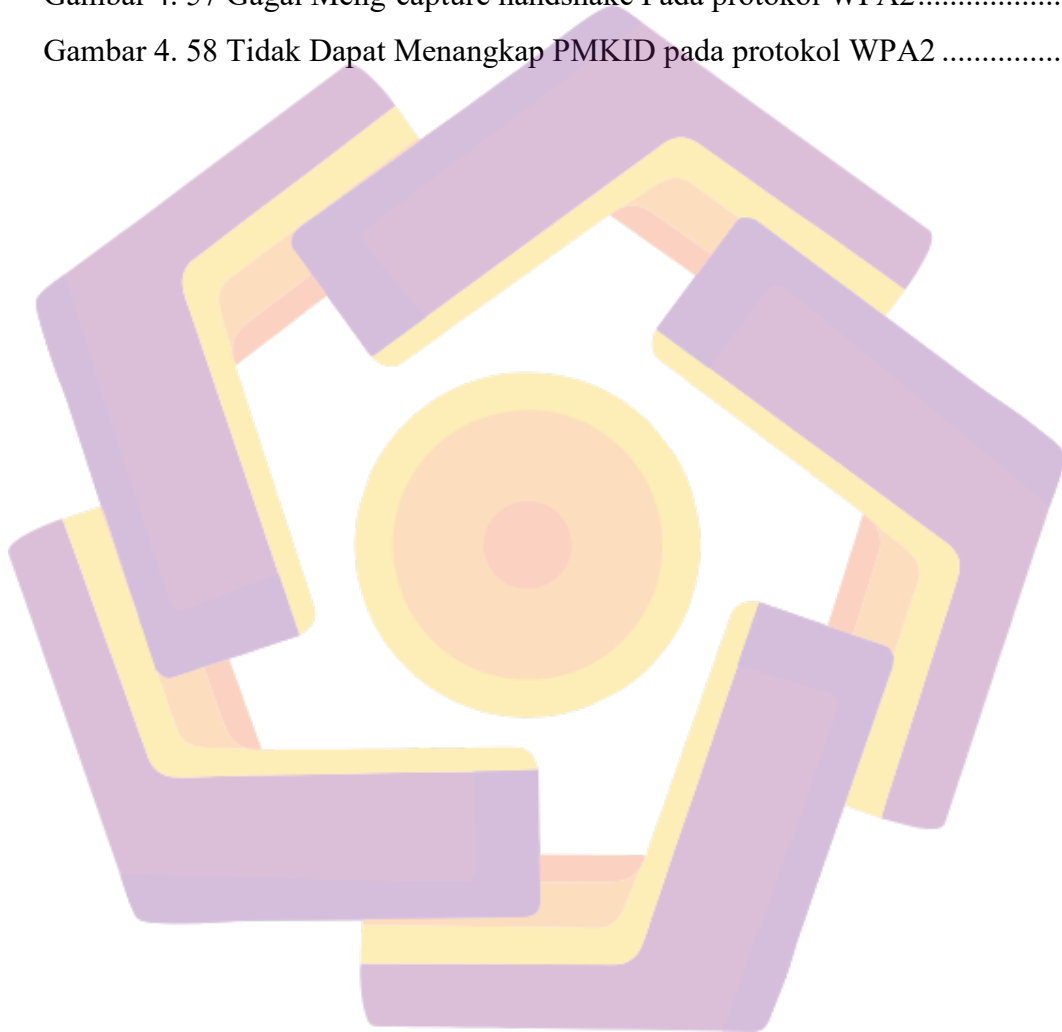
Tabel 2. 1 Standar IEEE 802.11 (a/b/g).....	9
Tabel 3. 1 Pengalamatan IP.....	37
Tabel 3. 2 Kebutuhan Perangkat Keras.....	38
Tabel 3. 3 Kebutuhan Perangkat Lunak.....	39
Tabel 3. 4 Konfigurasi Interface	40
Tabel 3. 5 Konfigurasi Alamat IP	41
Tabel 3. 6 Konfigurasi DHCP Server	42
Tabel 3. 7 Konfigurasi NAT	42
Tabel 3. 8 Konfigurasi Security Profile	43
Tabel 3. 9 Penilaian Tingkat Keamanan Kata Sandi	46
Tabel 4. 1 Filter Paket Deauthentication.....	74
Tabel 4. 2 Filter Frame Nirkabel Wireshark	74
Tabel 4. 3 Evaluasi Perbandingan Hasil Pengujian	92
Tabel 4. 4 Pembahasan Evaluasi Perbandingan Hasil Pengujian	93
Tabel 4. 5 Perbandingan Scanning Serangan.....	94
Tabel 4. 6 Perbandingan Capture Serangan	95
Tabel 4. 7 Perbandingan Password Cracking Pada Aircrack Dan Hashcat	95
Tabel 4. 8 Perbandingan Monitoring Dan Pencegahan Terhadap Serangan.....	96

DAFTAR GAMBAR

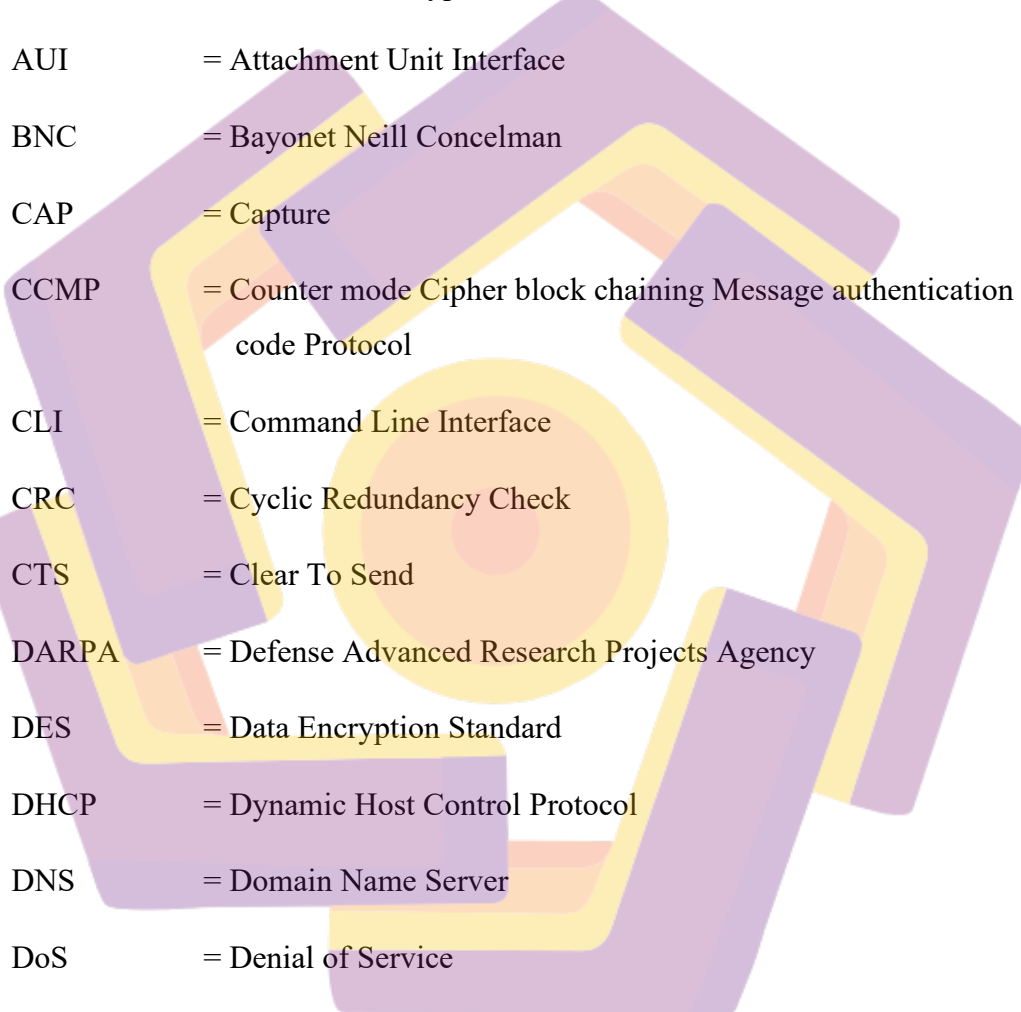
Gambar 2. 1 Topologi Bus	16
Gambar 2. 2 Topologi Ring	16
Gambar 2. 3 Topologi Star.....	17
Gambar 2. 4 Topologi Tree.....	17
Gambar 2. 5 Topologi Mesh	18
Gambar 2. 6 Kunci hirarki	23
Gambar 2. 7 Alur Pesan Yang Dipertukarkan	24
Gambar 3. 1 Alur Diagram Penelitian	34
Gambar 3. 2 Topologi Penelitian	35
Gambar 4. 1 Konfigurasi Alamat IP Pada Komputer Administrator	47
Gambar 4. 2 Konfigurasi Interface Pada Mikrotik.....	48
Gambar 4. 3 Konfigurasi Alamat IP Pada Mikrotik	48
Gambar 4. 4 Konfigurasi Security Profile Untuk Station	49
Gambar 4. 5 Scan Jaringan WIFI.....	50
Gambar 4. 6 Konfigurasi Wireless Station	51
Gambar 4. 7 Konfigurasi DHCP Client	52
Gambar 4. 8 Uji Coba ping ke PC Admin Dan Internet	52
Gambar 4. 9 Konfigurasi Security Profile Untuk Access Point.....	53
Gambar 4. 10 Konfigurasi Virtual Access Point.....	53
Gambar 4. 11 Konfigurasi Alamat IP WLAN2	54
Gambar 4. 12 Konfigurasi DHCP Server.....	55
Gambar 4. 13 Konfigurasi IP Pool.....	55
Gambar 4. 14 Konfigurasi Firewall NAT	56
Gambar 4. 15 Konfigurasi Wireless Sniffer.....	57
Gambar 4. 16 Konfigurasi Capture Filter Pada Wireshark	57
Gambar 4. 17 Hasil Tangkapan Lalu Lintas Paket Data.....	58
Gambar 4. 18 Konfigurasi Sniffer Menggunakan USB Wireless Adapter	59
Gambar 4. 19 Hasil Scanning Menggunakan Airodump	59
Gambar 4. 20 Output Penyimpanan Hasil Scanning.....	62

Gambar 4. 21 Sebelum Mendapat WPA Handshake	63
Gambar 4. 22 Frame Deauthentication Dikirim Secara Broadcast	64
Gambar 4. 23 Frame Deauthentucation Dikirim Pada Klien Tertentu.....	64
Gambar 4. 24 Klien Tidak Dapat Koneksi.....	64
Gambar 4. 25Penyerang Telah Mendapatkan Handshake	65
Gambar 4. 26 Informasi Hasil Tangkapan PMKID Pada Wireshark.....	66
Gambar 4. 27 Proses penangkapan PMKID	68
Gambar 4. 28 Daftar Tipe Hash Untuk Meretas Jaringan Nirkabel.....	68
Gambar 4. 29 Informasi PMKID Dan Konversi Ke Bentuk Hash.....	69
Gambar 4. 30 Hasil Pemecahan Kata Sandi Menggunakan Aircrack.....	71
Gambar 4. 31 Proses Pemecahan Kata Sandi Menggunakan Hashcat.....	72
Gambar 4. 32 Hasil Pemecahan Kata Sandi Menggunakan Hashcat.....	73
Gambar 4. 33 Penangkapan Frame Deauthentication Pada Wireshark.....	75
Gambar 4. 34 Konfigurasi Management Frame Protection	77
Gambar 4. 35 Paket Deauthentication Dikirim Pada Klien	78
Gambar 4. 36 Klien Masih Terhubung Dengan Jaringan	78
Gambar 4. 37 Penyerang Tidak Mendapatkan Handshake	79
Gambar 4. 38 Penangkapan PMKID Pada Wireshark	80
Gambar 4. 39 Informasi Yang Terdapat Pada 802.1X Authentication	81
Gambar 4. 40 Menonaktifkan PMKID Pada Access Point.....	82
Gambar 4. 41 Penangkapan PMKID Pada Access Point PenTest	83
Gambar 4. 42 Konfigurasi Pengujian WPA.....	84
Gambar 4. 43 Konfigurasi Pengujian WPA2.....	85
Gambar 4. 44 Proses Capture Berhasil Pada Protokol WPA.....	85
Gambar 4. 45 Proses Capture Handshake Berhasil Pada WPA2	86
Gambar 4. 46 Pemecahan kata sandi Aircrack.....	86
Gambar 4. 47 Pemecahan Kata Sandi Hashcat	86
Gambar 4. 48 Proses capture PMKID Gagal Pada Protokol WPA.....	87
Gambar 4. 49 Proses Capture PMKID Berhasi Pada Protokol WPA2	87
Gambar 4. 50 Pemecahan Kata Sandi Aircrak Pada Protokol WPA2	88
Gambar 4. 51 Pemecahan Kata Sandi Hashcat pada Protocol WPA2	88

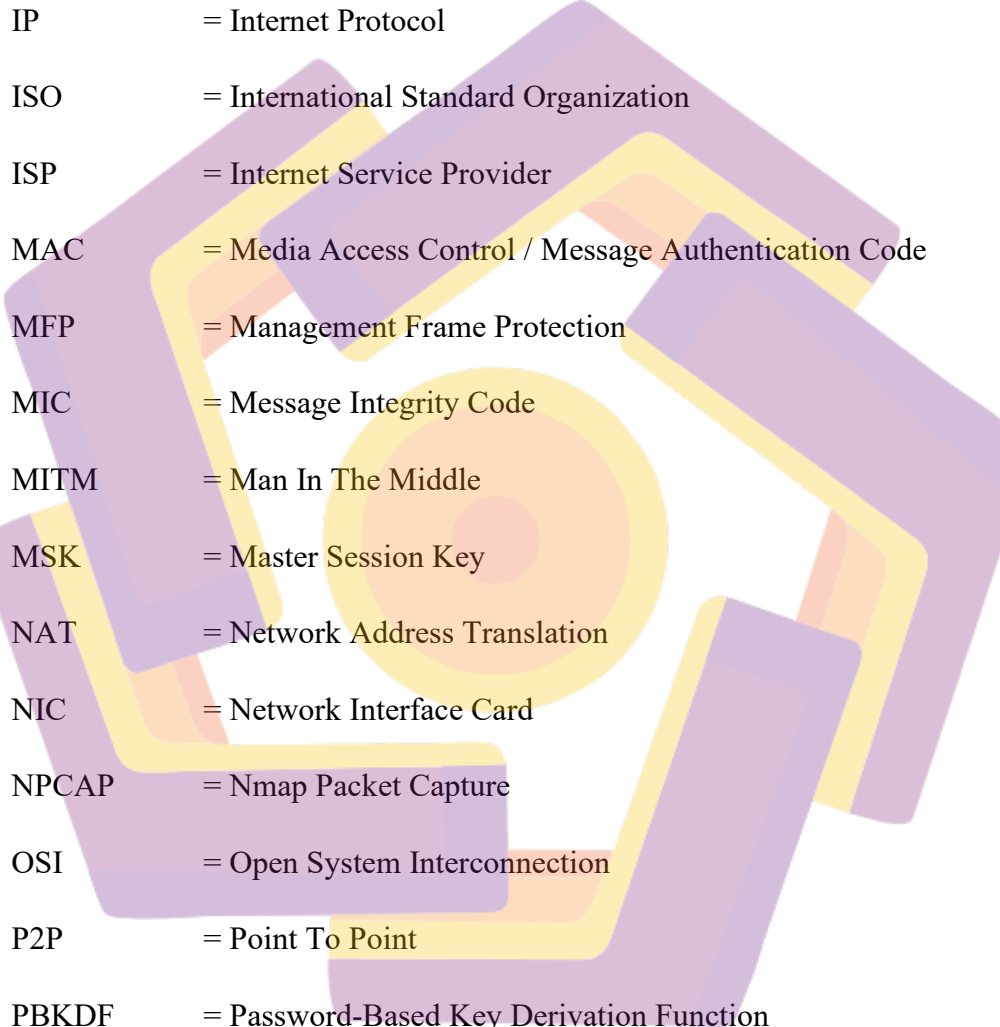
Gambar 4. 52 Kongifurasi Kata Sandi Terbaru	89
Gambar 4. 53 Hasil Pemecahan Kata Sandi Menggunakan Aircrack Gagal	90
Gambar 4. 54 Hasil Pemecahan Kata Sandi Menggunakan Hashcat Gagal	90
Gambar 4. 55 Konfigurasi Management Frame Protection Dan PMKID.....	91
Gambar 4. 56 Tidak dapat meng-capture handshake pada protokol WPA	91
Gambar 4. 57 Gagal Meng-capture handshake Pada protokol WPA2.....	92
Gambar 4. 58 Tidak Dapat Menangkap PMKID pada protokol WPA2	92



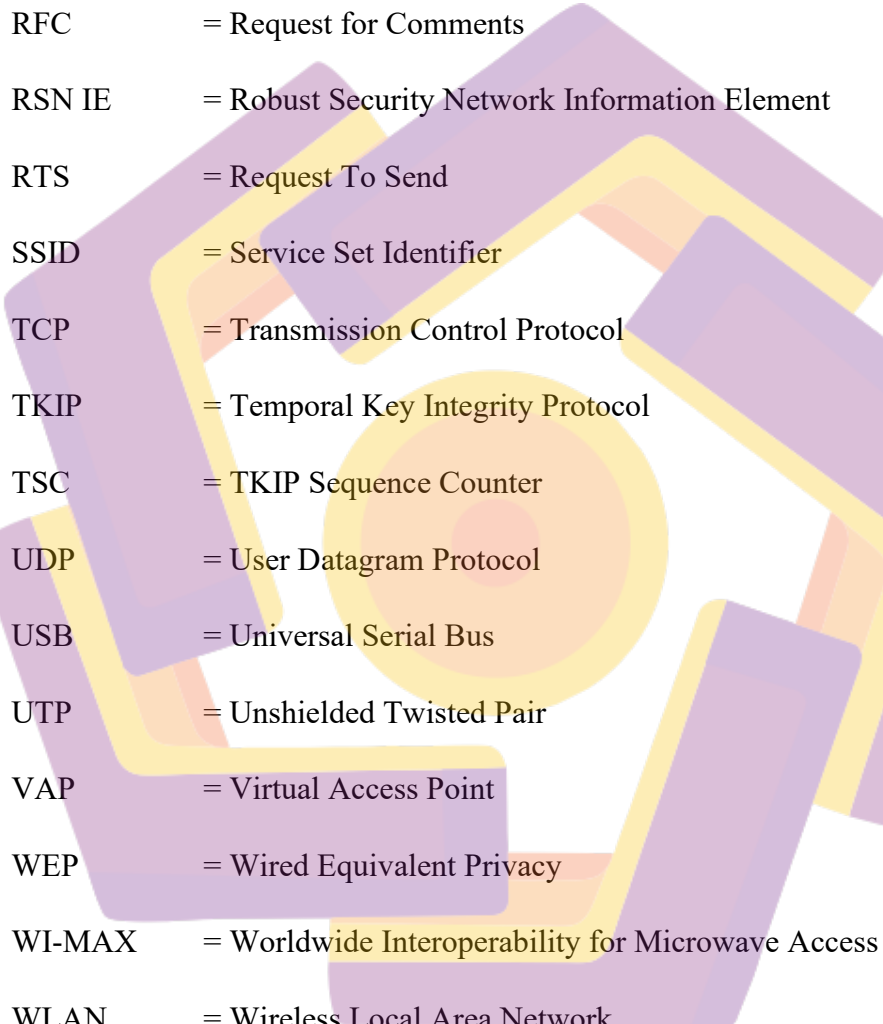
DAFTAR SINGKATAN



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*