

**ANALISIS KEAMANAN JARINGAN INTERNET LOKAL  
DENGAN MENGGUNAKAN FITUR ARP MIKROTIK  
UNTUK MENGATASI SERANGAN DEAUTHER**

**SKRIPSI**



disusun oleh

**Na'Immla Hml Sudani**

**20.21.1454**

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

**2022**

**ANALISIS KEAMANAN JARINGAN INTERNET LOKAL  
DENGAN MENGGUNAKAN FITUR ARP MIKROTIK  
UNTUK MENGATASI SERANGAN DEAUTHER**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Na'immia Ilmi Sudani**

**20.21.1454**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2022**

# PERSETUJUAN

## SKRIPSI

### ANALISIS KEAMANAN JARINGAN INTERNET LOKAL DENGAN MENGUNAKAN FITUR ARP MIKROTIK UNTUK MENGATASI SERANGAN DEAUTHER

yang dipersiapkan dan disusun oleh

**Na'immia Ilmi Sudani**

**20.21.1454**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 21 Juli 2022

**Dosen Pembimbing,**

**SubektiNingsih, S.Kom., M.Kom.**

**NIK.**

## PENGESAHAN

### SKRIPSI

#### ANALISIS KEAMANAN JARINGAN INTERNET LOKAL DENGAN MENGUNAKAN FITUR ARP MIKROTIK UNTUK MENGATASI SERANGAN DEAUTHER

yang dipersiapkan dan disusun oleh

**Na'imma Ilmi Sudani**

**20.21.1454**

telah dipertahankan di depan Dewan Penguji

pada tanggal 21 Juli 2022

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

SubektiNingsih, S.Kom,M.Kom

NIK.

Nama dan Gelar Penguji 2

NIK. 190302xxx

Nama dan Gelar Penguji 3

NIK. 190302xxx

Skrripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer

Tanggal 21 Juli 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 : Na'imia Ilmi Sudani

NIM : 20.21.1454

Menyatakan bahwa Tugas Akhir dengan judul berikut:

### **Analisis Keamanan Jaringan Internet Lokal Dengan Menggunakan Fitur ARP Mikrotik Untuk Mengatasi Serangan Denial of Service**

Dosen Pembimbing : Subektiingath, S.Kom,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. 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, 21 Juli 2022

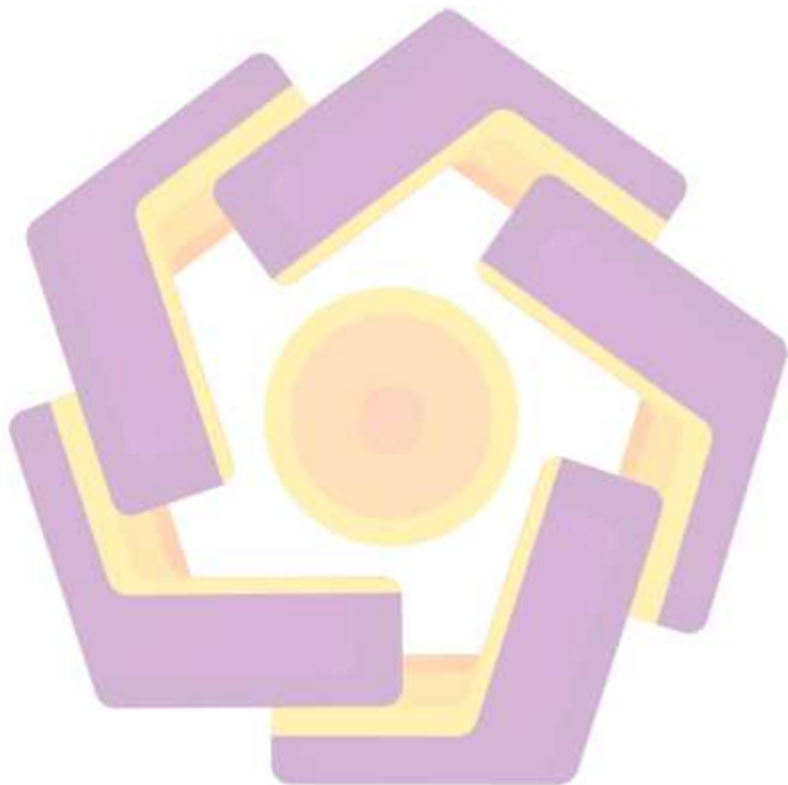
Yang Menyatakan,



Na'imia Ilmi Sudani

## **MOTTO**

**"JANGAN JADIKAN KESALAHAN SEBAGAI SEBUAH ALASAN KARENA  
SEHARUSNYA ITU MENJADI MOTIVASI UNTUK TERUS MELANGKAH  
KE DEPAN."**



## PERSEMBAHAN

Dengan segala puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia kami haturkan rasa syukur dan terimakasih kami kepada :

1. Allah SWT, karena hanya atas izin dan karunia-Nyalah maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa.
2. Orang tua kami, yang tidak pernah lelah memberikan kami dukungan dan doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat supaya kami bisa menyelesaikan skripsi ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa kami balaskan. Terimakasih banyak kami ucapkan untuk keduanya.
3. Bapak Dosen Pembimbing Subektiningsih, S.Kom,M.Kom yang selama ini telah tulus ikhlas meluangkan waktunya untuk menuntun dan mengarahkan kami, memberikan bimbingan dan pelajaran yang tiada ternilai harganya, agar kami menjadi lebih baik. Terimakasih banyak atas segala jasa yang telah diberikan kepada kami. Semoga ilmu yang telah di ajarkan kepada kami, menjadi lading amal dan semoga menjadi ilmu yang barokah untuk kami
4. Rekan-rekan kelas 20 S1 Transfer Informatika , yang telah memberikan kami dukungan, semangat serta menemani yang penuh dengan segala kondisi dalam hidup. Terimakasih atas kenang kenangan yang telah kita viii ukir bersama-sama. Semoga kita menjadi orang-orang yang bermanfaat dan dikenang menjadi pribadi yang baik.

Akhir kata saya persembahkan skripsi ini untuk kalian semua, orang-orang yang telah memberikan pengalaman yang sangat berarti dalam hidup kami. Semoga skripsi ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang.

## KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-Nya kepada penulis sehingga dapat menyelesaikan skripsi dengan judul Analisis Keamanan Jaringan Internet Lokal Dengan Menggunakan Fitur ARP Mikrotik Untuk Mengatasi Serangan Deauther sesuai yang diharapkan. Dalam penyusunan skripsi ini, tentu saja masih banyak kekurangan dan hambatan yang terkadang ditemui baik secara teknik maupun non-teknis sehingga dalam melengkapi penyusunan skripsi ini tidak lepas dari bimbingan, bantuan, dan dorongan dari berbagai pihak. Skripsini disusun sebagai salah satu syarat kelulusan Program Sarjana Jurusan Informatika Universitas Amikom Yogyakarta dan untuk memperoleh gelar Sarjana Komputer. Pada kesempatan ini penulis memberikan ucapan terimakasih kepada :

1. Allah SWT, yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Bapak Prof. Dr.M. Suyanto,MM selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al Fatta, S.Kom.,M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Ibu Windha Mega Pradya D, M.Kom selaku Ketua Program Studi S1 Informatika.
5. Ibu Subektiningsih, S.Kom.,M.Kom selaku dosen pembimbing yang telah memberikan arahan dan bimbingan kepada penulis.
6. Kedua orangtua beserta keluarga yang selalu memotivasi, doa dan juga dukungan.
7. Teman-teman dan pihak lain yang selalu memberikan dukungan selama pengerjaan skripsi ini. Penulis tentunya menyadari bahwa dalam penyusunan skripsi ini masih banyak kekurangan dan kelemahan. Oleh karena itu saran dan masukan dari pembaca sangat kami harapkan sebagai acuan untuk lebih baik di waktu yang akan datang. Semoga skripsi ini dapat bermanfaat bagi semua belah pihak yang membacanya.

Yogyakarta, 21 Juli 2022

Penulis

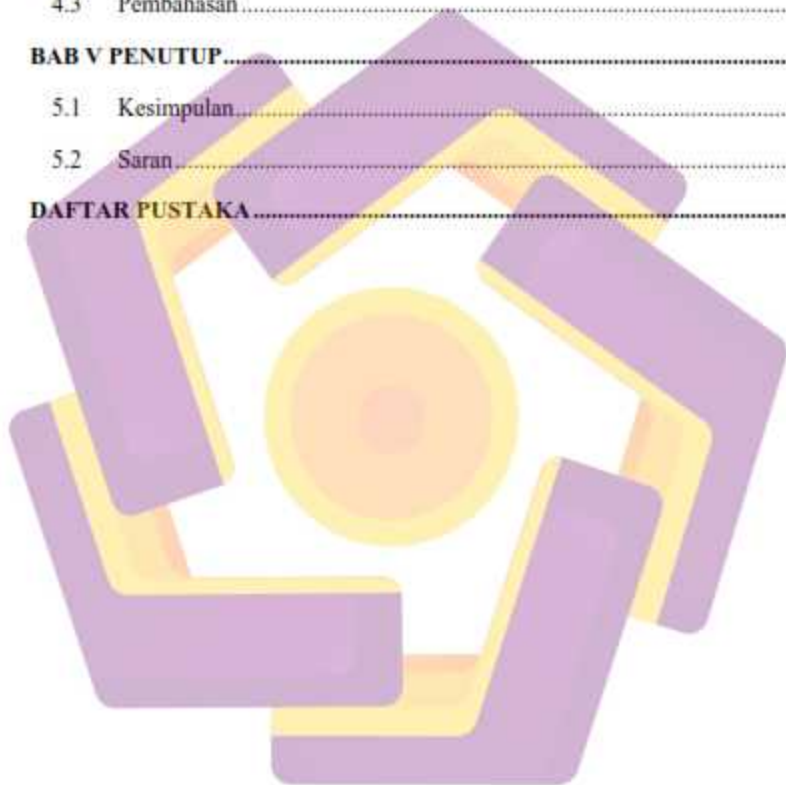


## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN JUDUL .....	ii
HALAMAN PERSETUJUAN .....	iii
HALAMAN PENGESAHAN .....	iv
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR .....	v
MOTTO .....	vi
PERSEMBAHAN .....	vii
KATA PENGANTAR .....	viii
DAFTAR ISI .....	ix
DAFTAR TABEL .....	xii
DAFTAR GAMBAR .....	xiii
INTISARI .....	xv
<i>ABSTRACT</i> .....	xvi
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.6 Metode Penelitian .....	3
1.7 Sistematika Penelitian .....	4
<b>BAB II LANDASAN TEORI .....</b>	<b>5</b>
2.1 Kajian Pustaka .....	5
2.2 Dasar Teori .....	13

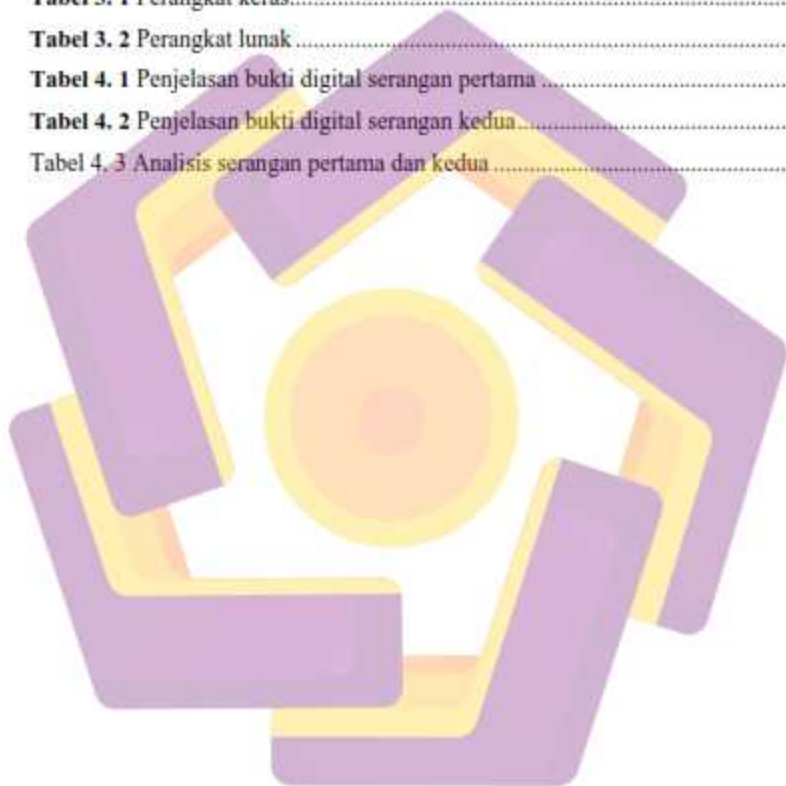
2.2.1	Jaringan Internet .....	13
2.2.2	WiFi (Wireless Fidelity) .....	14
2.2.3	Keamanan Jaringan .....	14
2.2.4	Standar WLAN IEEE .....	14
2.2.5	Alokasi Kanal .....	20
2.2.6	Kebijakan Negara tentang Alokasi Kanal .....	20
2.2.7	OSI (Open System Interconnection) Models .....	21
2.2.8	TCP/IP (Transmission Control Protocol) .....	24
2.2.9	Mikrotik .....	26
2.2.10	Modul Mikrokontroler ESP8266 .....	28
2.2.11	Deauther .....	28
2.2.12	HTTP (Hypertext Transfer Protocol) .....	30
2.2.13	Perangkat Jaringan .....	30
<b>BAB III METODOLOGI PENELITIAN .....</b>		<b>31</b>
3.1	Tahap Pelaksanaan Penelitian .....	31
3.1.1	Flowchart Penelitian Utama .....	31
3.1.2	Uraian Skenario .....	32
3.2	Metode Penelitian .....	33
3.2.1	Flowchart Pengujian .....	33
3.2.2	Live Forensic .....	39
3.3	Bahan dan Peralatan .....	40
3.3.1	Kebutuhan Fungsional .....	40
3.3.2	Kebutuhan Non-fungsional .....	41
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>44</b>
4.1	Implementasi .....	44

4.1.1	Flash NodeMCU ESP8266 Deauther.....	45
4.2	Pengujian Skenario.....	47
4.2.1	Pengujian Serangan Pertama.....	47
4.2.2	Pengujian Serangan Kedua.....	52
4.3	Pembahasan.....	61
<b>BAB V PENUTUP.....</b>		<b>65</b>
5.1	Kesimpulan.....	65
5.2	Saran.....	65
<b>DAFTAR PUSTAKA.....</b>		<b>66</b>



## DAFTAR TABEL

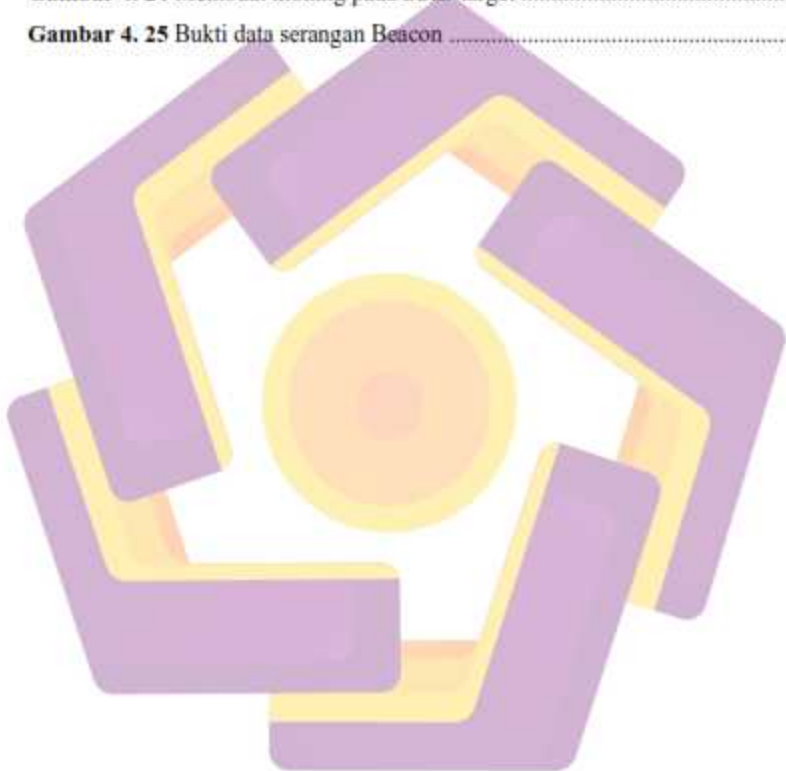
<b>Tabel 2. 1</b> Literatur Review dari masing - masing penelitian sebelumnya .....	7
<b>Tabel 2. 2</b> Standar WLAN IEEE [13] .....	15
<b>Tabel 3. 1</b> Perangkat keras.....	41
<b>Tabel 3. 2</b> Perangkat lunak .....	43
<b>Tabel 4. 1</b> Penjelasan bukti digital serangan pertama .....	61
<b>Tabel 4. 2</b> Penjelasan bukti digital serangan kedua.....	63
<b>Tabel 4. 3</b> Analisis serangan pertama dan kedua .....	64



## DAFTAR GAMBAR

<b>Gambar 2. 1</b> Cara Kerja OSI Layer [15] .....	21
<b>Gambar 2. 2</b> Lapisan dari setiap TCP/IP [17]. .....	25
<b>Gambar 2. 3</b> Microcontroler ESP8266 [21].....	28
<b>Gambar 3. 1</b> Flowchart Penelitian Utama .....	31
<b>Gambar 3. 2</b> Flowchart Serangan Pertama .....	34
<b>Gambar 3. 3</b> Flowchart Konfigurasi ARP .....	35
<b>Gambar 3. 4</b> Flowchart Serangan Kedua .....	36
<b>Gambar 3. 5</b> Desain prototipe perangkat .....	38
<b>Gambar 3. 6</b> Topologi Jaringan pada serangan ESP8266 .....	38
<b>Gambar 3. 7</b> Tahapan metode Live Forensic.....	40
<b>Gambar 4. 1</b> Halaman pada Github SpacehuhnTech.....	44
<b>Gambar 4. 2</b> File bin Deauther untuk Flash NodeMCU ESP8266.....	45
<b>Gambar 4. 3</b> Port COM pada Device Manager Windows .....	45
<b>Gambar 4. 4</b> Port COM terbaca oleh NodeMCU Flasher.....	46
<b>Gambar 4. 5</b> Menambahkan file bin pada NodeMCU Flasher .....	46
<b>Gambar 4. 6</b> Konfigurasi pada tab Advanced.....	47
<b>Gambar 4. 7</b> SSID dan Password default NodeMCU ESP8266 Deauther .....	48
<b>Gambar 4. 8</b> Alamat Web Interface ESP8266 Deauther .....	48
<b>Gambar 4. 9</b> Halaman peringatan penggunaan Deauther .....	49
<b>Gambar 4. 10</b> Scanning Access Points dan pemilihan target untuk Deauther ....	50
<b>Gambar 4. 11</b> Tipe serangan pada tab Attack.....	51
<b>Gambar 4. 12</b> Serangan Deauther diaktifkan pada serangan pertama .....	51
<b>Gambar 4. 13</b> Bukti data digital serangan pertama .....	52
<b>Gambar 4. 14</b> Fitur ARP pada menu IP Winbox Mikrotik.....	53
<b>Gambar 4. 15</b> Membuat IP Target menjadi Static .....	54
<b>Gambar 4. 16</b> Port Interface .....	54
<b>Gambar 4. 17</b> Interface target fitur ARP di ubah menjadi reply-only .....	55
<b>Gambar 4. 18</b> Interface target pada DHCP Server .....	55
<b>Gambar 4. 19</b> Ceklis pada fitur Add ARP For Leases .....	56

<b>Gambar 4. 20</b> Menyambungkan ESP8266 Deauther dengan komputer penyerang .....	56
<b>Gambar 4. 21</b> tab SCAN.....	57
<b>Gambar 4. 22</b> Menu serangan Deauther .....	58
<b>Gambar 4. 23</b> Bukti data serangan kedua.....	59
<b>Gambar 4. 24</b> Membuat kloning pada SSID target .....	60
<b>Gambar 4. 25</b> Bukti data serangan Beacon .....	60



## INTISARI

Sistem keamanan jaringan komputer adalah sistem untuk mencegah dan mendeteksi penggunaan jaringan komputer yang tidak sah. Tindakan pencegahan membantu mencegah pengguna yang tidak sah, yang disebut "penyerang," mendapatkan akses ke bagian-bagian dari sistem jaringan. Tujuan dari keamanan jaringan komputer adalah untuk memprediksi risiko terhadap jaringan komputer, baik secara langsung maupun tidak langsung berupa ancaman fisik dan logis yang mengganggu aktivitas yang sedang berlangsung pada jaringan komputer. Tujuan dari penelitian ini adalah untuk mencegah dampak dari serangan NodeMCU ESP8266 Deauther yang merupakan salah satu serangan terhadap jaringan komputer. Serangan ini dapat menonaktifkan semua klien secara bersamaan mengakses Internet melalui jaringan hotspot. Untuk mencegah akibat dari serangan ini, jaringan titik akses diamankan dengan mengaktifkan Address Resolution Protocol (ARP) pada server proxy, melindungi klien dan router dari serangan. Dari pengujian keamanan Jaringan Komputer Lokal dengan menggunakan fitur ARP pada Mikrotik Routerboard dengan metode serangan Deauther untuk mengambil data password user serta menduplikasi Mac Address. Dapat disimpulkan fitur ARP pada Mikrotik Routerboard berjalan dengan baik

***Kata Kunci: Keamanan Jaringan, ESP8266, Deauther, Mikrotik***

## **ABSTRACT**

*A computer network security system is a system to prevent and detect unauthorized use of computer networks. Precautions help prevent unauthorized users, called "attackers," from gaining access to parts of a network system. The purpose of computer network security is to predict risks to computer networks, either directly or indirectly in the form of physical and logical threats that interfere with ongoing activities on computer networks. The purpose of this study is to prevent the impact of the NodeMCU ESP8266 Deauther attack which is one of the attacks on computer networks. This attack can disable all clients simultaneously accessing the Internet through a network hotspot. To prevent the consequences of this attack, the access point network is secured by enabling the Address Resolution Protocol (ARP) on the proxy server, protecting clients and routers from attacks. From testing the security of the Local Computer Network by using the ARP feature on the Mikrotik Routerboard with the Deauther attack method to retrieve user password data and duplicating the Mac Address. It can be concluded that the ARP feature on the Mikrotik Routerboard is running well.*

**Keyword:** Network Security, ESP8266, Deauther, Mikrotik.

