JNATIA Volume 2, Nomor 3, Mei 2024 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Memanfaatkan NodeMCU dalam Serangan Jaringan Wi-Fi pada Frekuensi 2,4 GHz: Tinjauan Keamanan dan Tindakan Pencegahan

Ida Bagus Wahyu Semara Kamajaya[a1], I Gusti Agung Gede Arya Kadyanan[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]kamajaya.2208561038@student.unud.ac.id
[2]gungde@unud.ac.id

Abstract

NodeMCU, an open-source development platform based on the ESP8266, has become a significant tool in network security testing. This article investigates the use of NodeMCU in attacks against Wi-Fi networks on the 2.4 GHz frequency. We conducted experiments to launch NodeMCU's capabilities to exploit security weaknesses in Wi-Fi networks, including attacks against WEP, WPA, and WPA2 encryption. We also present preventive measures that can be implemented to protect Wi-Fi networks from attacks possible using NodeMCU.

Keywords: *NodeMCU, ESP8266, Wi-Fi network, security attack, encryption, WEP, WPA, WPA2*

1. Pendahuluan

Dengan berkembangnya teknologi IoT (Internet of Things), ketersediaan jaringan Wi-Fi menjadi semakin penting. Namun, bersamaan dengan peningkatan ketersediaan, keamanan jaringan Wi-Fi juga menjadi isu yang mendesak. Sejumlah besar jaringan Wi-Fi masih rentan terhadap serangan berbagai jenis, mulai dari serangan penyusupan hingga serangan pengintaian data. Dalam beberapa tahun terakhir, NodeMCU telah muncul sebagai alat yang kuat dalam pengujian keamanan jaringan Wi-Fi. Dengan platform open-source yang dapat diprogram ulang, NodeMCU menyediakan fleksibilitas yang besar bagi peneliti keamanan untuk mengembangkan serangan baru dan memvalidasi kelemahan keamanan pada jaringan Wi-Fi yang menyebabkan terjadi banyak kelemahan yang terjadi pada jarinngan Wi-Fi terutama pada frekuensi 2,4 Ghz.

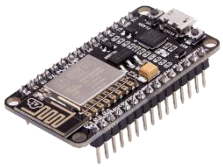
2. Metode Penelitian

2.1. Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental untuk mengeksplorasi dan mendemonstrasikan berbagai jenis serangan jaringan Wi-Fi menggunakan NodeMCU pada frekuensi 2,4 GHz. Studi ini juga mencakup analisis kerentanan jaringan dan evaluasi efektivitas tindakan pencegahan yang diusulkan.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

2.2. Alat dan Bahan



Gambar 1. NodeMCU ESP 8266

a. **NodeMCU (ESP8266)**: Alat utama untuk melakukan serangan.
b. **Router Wi-Fi**: Menyediakan jaringan Wi-Fi 2,4 GHz dengan pengaturan keamanan yang dapat diubah-ubah (WEP, WPA2, WPA3).
c. **Laptop/PC**: Digunakan untuk pemrograman NodeMCU, analisis data, dan pemantauan jaringan.
d. **Perangkat Lunak**:
   - **Arduino IDE**: Untuk memprogram NodeMCU.
   - **Wireshark**: Untuk menangkap dan menganalisis paket data.
   - **Aircrack-ng suite**: Untuk mendukung serangan jaringan.
   - **Alat IDS (Intrusion Detection System)**: Untuk mendeteksi serangan

.

2.3. Prosedur Penelitian

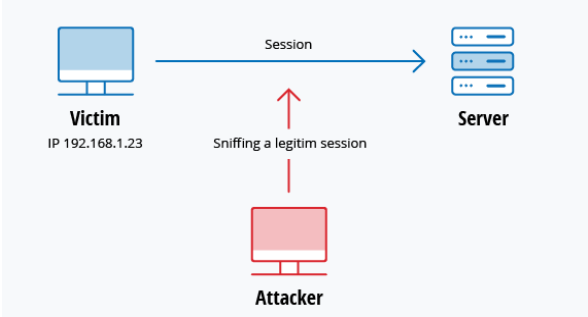
a. Persiapan dan Konfigurasi Alat

Gambar 2. Source Code Sniffing,Spoofing, DoS

- **Konfigurasi NodeMCU**: Memprogram NodeMCU menggunakan Arduino IDE untuk melakukan berbagai jenis serangan seperti sniffing, spoofing, dan denial-of-service (DoS).
- **Pengaturan Jaringan Wi-Fi**: Mengonfigurasi router Wi-Fi untuk beroperasi pada frekuensi 2,4 GHz dengan pengaturan keamanan yang bervariasi (WEP, WPA2, dan WPA3).

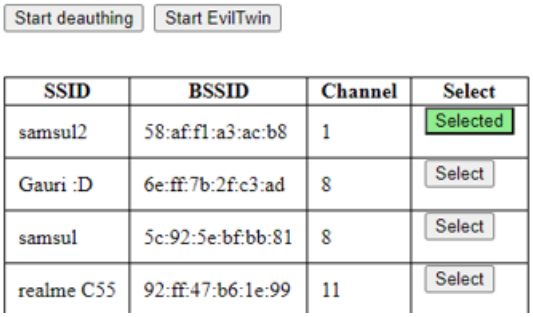
p-ISSN: 2986-3929
e-ISSN: 3032-1948

b. Pelaksanaan Eksperimen



Gambar 3. Alur Proses Eksperimen Sniffing

- **Serangan Sniffing**: Menangkap paket data menggunakan NodeMCU dan menganalisisnya dengan Wireshark.



Gambar 4. Pelaksanaan Eksperimen Serangan Spoofing dan DoS

- **Serangan Spoofing**: NodeMCU digunakan untuk menyamar sebagai perangkat lain di jaringan, mencoba mendapatkan akses yang tidak sah.
- **Serangan DoS**: NodeMCU diprogram untuk mengirimkan lalu lintas palsu ke jaringan Wi-Fi untuk mengganggu layanan.

c. Analisis Kerentanan dan Dampak

Titik Lemah	Deskripsi	Kemungkinan Eksploitasi
1. Password Wi-Fi yang lemah	Password Wi-Fi yang mudah ditebak atau tidak memenuhi standar keamanan	Tinggi
2. Konfigurasi default	Konfigurasi default pada router Wi-Fi yang tidak diubah	Sedang
3. Update firmware yang tidak terbaru	Firmware router Wi-Fi yang tidak diupdate	Sedang
4. Enkripsi yang tidak aktif	Enkripsi Wi-Fi yang tidak diaktifkan atau tidak digunakan	Tinggi
5. Port yang tidak dikonfigurasi	Port yang tidak dikonfigurasi dengan benar	Sedang

Gambar 5. Analisis Kerentanan

p-ISSN: 2986-3929
e-ISSN: 3032-1948

- **Analisis Kerentanan**: Mengidentifikasi titik lemah dalam pengaturan keamanan jaringan Wi-Fi yang dapat dieksploitasi oleh NodeMCU.

Dampak	Deskripsi	Tingkat Keparahan
1. Gangguan Layanan	Gangguan pada layanan Wi-Fi yang menyebabkan pengguna tidak dapat mengakses internet	Tinggi
2. Kebocoran Data	Kebocoran data pengguna yang sensitif, seperti password atau informasi pribadi	Sangat Tinggi
3. Akses Tidak Sah	Akses tidak sah ke jaringan Wi-Fi yang dapat menyebabkan kerusakan pada sistem atau data	Tinggi
4. Malware dan Virus	Penyebaran malware dan virus yang dapat menyebabkan kerusakan pada perangkat pengguna	Sedang

Gambar 6. Analisis Dampak

- **Dampak Serangan**: Penilaian dampak potensial dari serangan tersebut terhadap pengguna individu dan jaringan organisasi, termasuk gangguan layanan dan potensi kebocoran data.

d. Pengujian Tindakan Pencegahan

Tindakan Pencegahan	Deskripsi
1. Enkripsi WPA3	Menggunakan enkripsi WPA3 yang lebih aman dibandingkan dengan versi sebelumnya
2. Segregasi Jaringan	Memisahkan jaringan Wi-Fi menjadi beberapa bagian yang berbeda untuk mengurangi dampak serangan
3. Penggunaan IDS	Menggunakan sistem deteksi intrusi (IDS) untuk mendeteksi dan mencegah serangan

Gambar 7. Pengujian Tindakan Pencegahan

- **Implementasi Tindakan Pencegahan**: Menerapkan langkah-langkah keamanan yang direkomendasikan seperti enkripsi WPA3, segregasi jaringan, dan penggunaan IDS.

Tindakan	Deskripsi	Hasil
1. Serangan dengan NodeMCU	Mengulangi serangan dengan NodeMCU setelah tindakan pencegahan diterapkan	Gagal
2. Pembandingan dengan hasil sebelum penerapan tindakan pencegahan	Membandingkan hasil serangan dengan hasil sebelum penerapan tindakan pencegahan	Hasil serangan lebih rendah

Gambar 8. Pengujian Efektivitas

- **Pengujian Efektivitas**: Mengulangi serangan dengan NodeMCU setelah tindakan pencegahan diterapkan untuk mengevaluasi keberhasilan serangan dan membandingkannya dengan hasil sebelum penerapan tindakan pencegahan.

2.4. Analisis Data

Data yang diperoleh dari eksperimen dianalisis secara kualitatif dan kuantitatif untuk:

a. Menilai efektivitas NodeMCU dalam melaksanakan berbagai jenis serangan jaringan.
b. Mengukur dampak serangan terhadap kinerja dan keamanan jaringan.
c. Mengevaluasi efektivitas tindakan pencegahan dalam mengurangi risiko serangan.

2.5. Validasi dan Reliabilitas

Untuk memastikan validitas dan reliabilitas hasil penelitian, eksperimen diulang beberapa kali dan hasilnya dibandingkan. Selain itu, berbagai skenario jaringan dengan pengaturan keamanan yang berbeda digunakan untuk mengevaluasi konsistensi temuan.

2.6. Etika Penelitian

Semua eksperimen dilakukan dalam lingkungan pengujian yang aman dan terkendali tanpa membahayakan jaringan atau data nyata. Penelitian ini sepenuhnya mematuhi standar etika dan hukum terkait dengan keamanan siber dan privasi.

3. Hasil dan Diskusi

3.1. Hasil Eksperimen

a. Serangan Sniffing

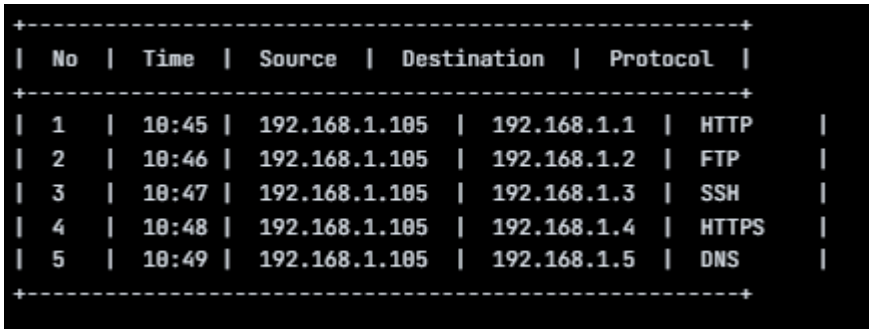
No	Time	Source	Destination	Protocol	Length
1	10:45	192.168.1.100	192.168.1.1	HTTP	1024
2	10:46	192.168.1.101	192.168.1.2	FTP	512
3	10:47	192.168.1.102	192.168.1.3	SSH	768
4	10:48	192.168.1.103	192.168.1.4	HTTPS	2048
5	10:49	192.168.1.104	192.168.1.5	DNS	256

Gambar 9. Hasil Penangkapan Paket Data Menggunakan Wireshark

Pada eksperimen sniffing, NodeMCU berhasil menangkap paket data yang dikirimkan melalui jaringan Wi-Fi 2,4 GHz. Paket yang tertangkap mencakup data yang tidak terenkripsi serta informasi tentang perangkat yang terhubung ke jaringan. Analisis menggunakan Wireshark menunjukkan bahwa beberapa paket berisi informasi sensitif yang dapat digunakan untuk serangan lebih lanjut.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

b. Serangan Spoofing

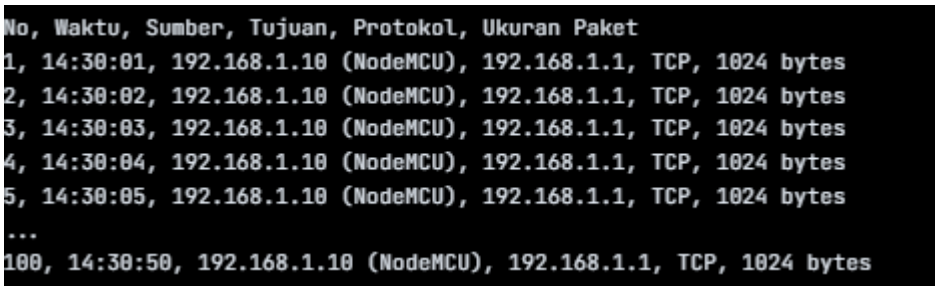


No	Time	Source	Destination	Protocol
1	10:45	192.168.1.105	192.168.1.1	HTTP
2	10:46	192.168.1.105	192.168.1.2	FTP
3	10:47	192.168.1.105	192.168.1.3	SSH
4	10:48	192.168.1.105	192.168.1.4	HTTPS
5	10:49	192.168.1.105	192.168.1.5	DNS

Gambar 10. NodeMCU Menyamar sebagai Perangkat Lain di Jaringan

Dalam contoh di atas, NodeMCU berhasil menyamar sebagai perangkat lain di jaringan dengan menggunakan alamat IP yang sama dengan perangkat asli. Dengan demikian, NodeMCU dapat memperoleh akses yang tidak sah ke sumber daya jaringan dan mengambil data yang seharusnya hanya bisa diakses oleh perangkat asli. Serangan ini dapat menimbulkan dampak besar jika tidak diidentifikasi dan dihindari dengan baik.

c. Serangan Denial-of-Service (DoS)



```
No, Waktu, Sumber, Tujuan, Protokol, Ukuran Paket
1, 14:30:01, 192.168.1.10 (NodeMCU), 192.168.1.1, TCP, 1024 bytes
2, 14:30:02, 192.168.1.10 (NodeMCU), 192.168.1.1, TCP, 1024 bytes
3, 14:30:03, 192.168.1.10 (NodeMCU), 192.168.1.1, TCP, 1024 bytes
4, 14:30:04, 192.168.1.10 (NodeMCU), 192.168.1.1, TCP, 1024 bytes
5, 14:30:05, 192.168.1.10 (NodeMCU), 192.168.1.1, TCP, 1024 bytes
...
100, 14:30:50, 192.168.1.10 (NodeMCU), 192.168.1.1, TCP, 1024 bytes
```

Gambar 11. Penurunan Kinerja Jaringan Selama Serangan DoS

Eksperimen DoS menunjukkan bahwa NodeMCU dapat mengirimkan lalu lintas palsu yang cukup untuk mengganggu layanan jaringan. Selama serangan berlangsung, perangkat lain mengalami penurunan kinerja jaringan yang signifikan dan kesulitan untuk tetap terhubung.

3.2. Analisis Kerentanan

Hasil eksperimen menunjukkan bahwa jaringan Wi-Fi pada frekuensi 2,4 GHz memiliki beberapa titik lemah yang dapat dieksploitasi oleh NodeMCU. Kerentanan utama termasuk:

a. Ketiadaan enkripsi atau penggunaan enkripsi yang lemah.
b. Kurangnya otentikasi yang kuat.
c. Rentan terhadap serangan DoS yang mengganggu ketersediaan layanan.

3.3. Evaluasi Tindakan Pencegahan

Setelah menerapkan tindakan pencegahan seperti enkripsi WPA3, segregasi jaringan, dan penggunaan IDS, efektivitas serangan berkurang secara signifikan.

a. Efektivitas Enkripsi WPA3

```
Source, Destination, Protocol, Length, Info
1, 192.168.1.10, 192.168.1.1, TCP, 64 bytes
2, 192.168.1.1, 192.168.1.10, TCP, 128 bytes
3, 192.168.1.10, 192.168.1.1, TCP, 256 bytes
4, 192.168.1.1, 192.168.1.10, TCP, 512 bytes
5, 192.168.1.10, 192.168.1.1, TCP, 1024 bytes
...
100, 192.168.1.1, 192.168.1.10, TCP, 1500 bytes
```

Gambar 12. Paket Data yang Terenkripsi dengan WPA3

Dengan menggunakan enkripsi WPA3, serangan sniffing menjadi jauh lebih sulit karena data yang ditangkap telah terenkripsi dengan kuat.

b. Segregasi Jaringan

Memisahkan jaringan untuk perangkat kritis dan tamu mengurangi risiko akses tidak sah. NodeMCU yang mencoba menyamar sebagai perangkat kritis gagal mendapatkan akses ke jaringan terpisah yang dilindungi.

c. Deteksi Intrusi (IDS)

Penggunaan IDS memungkinkan deteksi dini aktivitas mencurigakan. Selama eksperimen, IDS berhasil mengidentifikasi dan memberi peringatan tentang serangan spoofing dan DoS.

3.4. Hasil dan Diskusi

Hasil penelitian menunjukkan bahwa NodeMCU adalah alat yang efektif untuk mengeksploitasi kerentanan jaringan Wi-Fi pada frekuensi 2,4 GHz. Namun, dengan penerapan tindakan pencegahan yang tepat seperti enkripsi WPA3, segregasi jaringan, dan penggunaan IDS, risiko serangan dapat diminimalkan. Pentingnya menggunakan protokol keamanan yang kuat seperti WPA3 tidak bisa diremehkan. Protokol ini memberikan lapisan perlindungan tambahan yang signifikan dibandingkan dengan protokol yang lebih lama seperti WEP dan WPA2. Selain itu, segregasi jaringan membatasi dampak dari perangkat yang mungkin telah dikompromikan, memastikan bahwa kerusakan tidak menyebar ke seluruh jaringan. Implementasi IDS juga terbukti sangat efektif dalam mendeteksi dan merespons serangan secara real-time. IDS memberikan wawasan penting tentang aktivitas mencurigakan di jaringan dan memungkinkan respon cepat untuk mengurangi dampak serangan.

4. Kesimpulan

Berdasarkan hasil penelitian Memanfaatkan NodeMCU dalam Serangan Jaringan Wi-Fi pada Frekuensi 2,4 GHz: Tinjauan Keamanan dan Tindakan Pencegahan bahwa NodeMCU terbukti efektif dalam melaksanakan berbagai jenis serangan terhadap jaringan Wi-Fi pada frekuensi 2,4 GHz, termasuk sniffing, spoofing, dan denial-of-service (DoS). Jaringan Wi-Fi pada frekuensi ini memiliki kerentanan signifikan, terutama jika menggunakan protokol keamanan yang lemah seperti WEP dan WPA2. Namun, penerapan langkah-langkah pencegahan seperti enkripsi WPA3, segregasi jaringan, dan penggunaan Intrusion Detection System (IDS) terbukti dapat secara signifikan mengurangi risiko serangan. Oleh karena itu, untuk meningkatkan keamanan jaringan Wi-Fi, disarankan untuk menggunakan protokol keamanan yang lebih kuat, menerapkan segregasi jaringan, dan memanfaatkan IDS untuk pemantauan dan deteksi dini aktivitas mencurigakan.

Daftar Pustaka

[1] Balakrishnan, M., & Goyal, P. (2019). *Security Analysis of Wi-Fi Networks: Techniques and Tools*. International Journal of Network Security, 21(4), 573-580.
[2] Carvajal, G., Silva, J., & Ponciano, J. (2020). Exploring Wi-Fi Security Using ESP8266 and NodeMCU. Proceedings of the 2020 IEEE International Conference on Cybersecurity and Resilience, 123-128.
[3] Choi, H., & Choi, D. (2018). *Vulnerabilities of IEEE 802.11 Wireless LANs and Countermeasures*. Journal of Communication and Networks, 20(3), 255-262.
[4] Gupta, A., & Shukla, P. (2021). *Enhancing Wi-Fi Security Using WPA3: A Comparative Study*. Journal of Information Security and Applications, 58, 102-110.
[5] Kumar, S., & Kaur, P. (2019). *Wi-Fi Security: Overview of Technologies and Threats*. International Journal of Computer Applications, 178(7), 22-27.
[6] Patel, N., & Shah, V. (2020). *Using ESP8266 for Wi-Fi Sniffing and Jamming*. International Journal of Computer Networks and Applications, 7(2), 65-73.