

Analysis And Implementation Of Wireless Network Security Using The Penetration testing Method At Prof. Dr. Hazairin University, Sh

Nurain Octavia ¹⁾; Ade Fitrah Putra Akhir ²⁾; Ade Titin Sumarni ³⁾

^{1,2,3)} Universitas Prof. Dr. Hazairin, SH, Bengkulu

Email: ¹⁾ nurainioctavia8@gmail.com

How to Cite :

Octavia, N., Akhir, A, F, P., Sumarni, A, T. (2023). Analysis And Implementation Of Wireless Network Security Using The Penetration testing Method At Prof. Dr. Hazairin University, Sh. Jurnal Media Computer Science, 5(3)

ARTICLE HISTORY

Received [10 Juni 2026]

Revised [15 Juli 2026]

Accepted [22 Juli 2026]

KEYWORDS

Network Security, Wireless,
Penetration Testing, Wi-Fi, UNHAZ.

This is an open access article under the
[CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license



ABSTRAK

Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan keamanan jaringan nirkabel di Universitas Prof. Dr. Hazairin, SH (UNHAZ) dengan menggunakan metode penetration testing. Jaringan nirkabel di lingkungan kampus merupakan infrastruktur krusial, namun rentan terhadap serangan siber karena karakteristik transmisinya yang terbuka. Metodologi penelitian yang digunakan meliputi tahapan information gathering, scanning, vulnerability identification, dan Exploitation analisis hasil penangkapan paket data (packet capture). Hasil penelitian menunjukkan bahwa tingkat keamanan jaringan nirkabel di UNHAZ masih perlu ditingkatkan. Ditemukan beberapa access point yang masih menggunakan sistem Open Network (OPN) tanpa mekanisme autentikasi dan enkripsi, yang memungkinkan pihak tidak berwenang mengakses jaringan dengan mudah. Analisis menggunakan Wireshark mengungkapkan bahwa pada jaringan terbuka, lalu lintas data seperti ARP Request, UDP, MDNS, dan alamat IP perangkat dapat diamati secara langsung. Sebaliknya, jaringan yang menggunakan protokol WPA2-PSK dengan enkripsi AES-CCMP terbukti lebih aman dan mampu melindungi kerahasiaan komunikasi pengguna dari teknik passive sniffing. Penelitian ini menyimpulkan bahwa metode penetration testing efektif dalam mengevaluasi kondisi keamanan jaringan secara nyata. Sebagai upaya peningkatan keamanan, disarankan untuk menerapkan protokol WPA2 atau WPA3, menggunakan autentikasi yang lebih kuat, menerapkan firewall dan VLAN, serta melakukan pembaruan firmware dan pemantauan keamanan secara rutin..

ABSTRACT

This study aims to analyze and implement wireless network security at Prof. Dr. Hazairin University, SH (UNHAZ) using the penetration testing method. Wireless networks in the campus environment are crucial infrastructure, but are vulnerable to cyber attacks due to their open transmission characteristics. The research methodology used includes the stages of information gathering, scanning, vulnerability identification, and Exploitation analysis of data packet capture results. The results of the study indicate that the level of wireless network security at UNHAZ still needs to be improved. Several access points were found that still use the Open Network (OPN) system without authentication and encryption mechanisms, which allows unauthorized parties to easily access the network. Analysis using Wireshark revealed that on an open network, data traffic such as ARP Request, UDP, MDNS, and device IP addresses can be

directly observed. In contrast, networks using the WPA2-PSK protocol with AES-CCMP encryption are proven to be more secure and able to protect the confidentiality of user communications from passive sniffing techniques. This study concludes that the penetration testing method is effective in evaluating network security conditions in real time. To improve security, it is recommended to implement WPA2 or WPA3 protocols, use stronger authentication, implement firewalls and VLANs, and perform regular firmware updates and security monitoring..

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong perguruan tinggi untuk semakin bergantung pada jaringan nirkabel (Wi-Fi) sebagai infrastruktur utama dalam mendukung proses akademik, administrasi, dan berbagai layanan digital. Universitas Prof. Dr. Hazairin, SH merupakan salah satu perguruan tinggi yang memanfaatkan jaringan Wi-Fi secara luas untuk menunjang kegiatan perkuliahan, penelitian, sistem akademik berbasis daring, serta layanan administrasi. Oleh karena itu, jaringan nirkabel menjadi komponen strategis yang menentukan kelancaran operasional dan kualitas layanan akademik di lingkungan kampus.

Di sisi lain, jaringan nirkabel merupakan salah satu infrastruktur teknologi informasi yang paling rentan terhadap serangan siber karena karakteristik transmisinya yang bersifat terbuka dan dapat diakses dari area yang luas. Berdasarkan laporan Global Cybersecurity Index yang diterbitkan oleh International Telecommunication Union, ancaman siber yang mengeksploitasi jaringan nirkabel terus menunjukkan tren peningkatan secara global (Union, 2023). Selain itu, laporan keamanan dari Cisco mengungkapkan bahwa sebagian besar insiden pelanggaran data di sektor pendidikan berkaitan dengan lemahnya konfigurasi jaringan Wi-Fi, penggunaan mekanisme enkripsi yang tidak optimal, serta kurangnya pengelolaan dan pemantauan keamanan yang berkelanjutan (CISCO, 2024).

Meskipun standar keamanan jaringan nirkabel seperti WPA2 dan WPA3 telah tersedia dan digunakan secara luas, penerapannya di lingkungan operasional sering kali belum berjalan optimal. Beberapa faktor yang menyebabkan munculnya kerentanan meliputi kesalahan konfigurasi perangkat jaringan, penggunaan kata sandi yang lemah, minimnya pembaruan sistem keamanan, serta belum diterapkannya prosedur operasional standar dan pengawasan yang konsisten. Evaluasi keamanan yang hanya bersifat pasif, seperti audit konfigurasi dan kebijakan, belum mampu memberikan gambaran yang komprehensif mengenai ketahanan jaringan terhadap skenario serangan nyata.

Pendekatan penetration testing memberikan metode evaluasi keamanan yang lebih komprehensif dan empiris melalui simulasi serangan terkontrol untuk mengidentifikasi dan menganalisis kerentanan jaringan secara langsung. Sejumlah penelitian terdahulu menunjukkan efektivitas metode ini dalam mengungkap kelemahan keamanan jaringan nirkabel. Penelitian (santoso, ainurohman, 2022) membuktikan bahwa penetration testing mampu mengidentifikasi kelemahan WPA key melalui teknik Wordlist attack. Kemudian pada penelitian (Gede et al., 2024) menemukan bahwa jaringan nirkabel rentan terhadap serangan WPA key cracking dan MAC address bypassing. Sementara itu, (Satria Galang Saputra et al., 2023) menyimpulkan bahwa meskipun tingkat keamanan jaringan tergolong cukup baik, perbaikan pada konfigurasi dan topologi jaringan tetap diperlukan untuk meningkatkan ketahanan sistem secara menyeluruh.

Ada research gap dalam penelitian sebelumnya karena sebagian besar hanya dilakukan pada lingkungan sekolah atau pada organisasi non-PT dan lebih banyak melakukan kajian konseptual maupun melakukan analisis terhadap keamanan jaringan secara umum bukan langsung melakukan implementasi pen testing pada jaringan wifi pada kampus. Hal tersebut dikarenakan lingkungan perguruan tinggi memiliki kompleksitas jaringan yang lebih kompleks dibanding

lingkungan sekolah karena adanya jumlah user yang banyak, mobilitas user yang flot serta adanya implementasi dari konsep BYOD.

BYOD adalah kebijakan yang memberikan izin pada mahasiswa, dosen, maupun karyawan untuk membawa dan mengakses jaringan kampus menggunakan perangkat mereka sendiri seperti laptop, smartphone, tablet. Adanya BYOD memberikan keleluasaan bagi penggunaanya dalam melakukan kegiatan yang lebih fleksibel dan efisien dalam melaksanakan kegiatan akademik mereka, tetapi juga meningkatkan potensi ancaman keamanan jaringan karena adanya banyaknya perangkat dengan tingkat keamanan yang beragam yang terhubung ke jaringan wi-fi kampus (Ratchford et al., 2022). Selain itu, hingga saat ini belum ditemukan penelitian yang secara khusus memetakan kondisi keamanan jaringan nirkabel di Universitas Prof. Dr. Hazairin, SH menggunakan pendekatan penetration testing berbasis kondisi operasional nyata.

Urgensi pada penelitian ini semakin meningkat seiring dengan tingginya intensitas penggunaan jaringan nirkabel di lingkungan kampus dan meningkatnya ketergantungan terhadap layanan digital. Tanpa adanya evaluasi keamanan yang bersifat proaktif dan berbasis pengujian nyata, institusi berisiko mengalami gangguan layanan akademik, kebocoran data, serta penyalahgunaan akses terhadap sistem informasi kampus. Dampak dari serangan terhadap jaringan Wi-Fi tidak hanya bersifat teknis, tetapi juga dapat memengaruhi integritas data akademik, reputasi institusi, serta tingkat kepercayaan sivitas akademika terhadap layanan digital kampus. Penelitian ini memiliki kebaharuan yang terletak pada penerapan metode penetration testing secara empiris dan terstruktur pada jaringan Wi-Fi perguruan tinggi dengan karakteristik multi-pengguna dan mobilitas tinggi, serta menghasilkan rekomendasi peningkatan keamanan yang kontekstual dan aplikatif sesuai dengan kondisi operasional Universitas Prof. Dr. Hazairin, SH. Penelitian ini tidak hanya berfokus pada identifikasi kerentanan teknis, tetapi juga mengevaluasi kesiapan sistem keamanan jaringan kampus secara menyeluruh sebagai dasar penguatan keamanan yang berkelanjutan.

LANDASAN TEORI

Komputer merupakan suatu perangkat elektronik yang digunakan untuk mempermudah dalam menyelesaikan berbagai pekerjaan manusia (Kadir, 2017). Komputer merupakan alat yang dipakai untuk mengolah dan memproses data menurut perintah yang dirumuskan (Krisbiantoro, 2018). Berdasarkan pengertian tersebut, maka dapat diambil kesimpulan bahwa komputer merupakan perangkat elektronik yang digunakan untuk mengolah dan memproses data menurut instruksi yang diberikan. Komputer juga dapat diartikan sebagai mesin yang dapat diprogram untuk secara otomatis menjalankan rangkaian operasi aritmatika atau logika (perhitungan). Kemampuan lainnya yaitu sebagai alat pengetik, mengirim surat elektronik (email), bermain game, menjelajahi dunia maya, serta membuat slide presentasi (Bowo et al., n.d.).

Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi adalah mencakup semua jenis perangkat komputer (komputer desktop, komputer jinjing, smartphone, PC, tablet dan perangkat penghubung (router, switch, modem, hub) (Wasti et al, 2025). Jaringan komputer digunakan di perguruan tinggi untuk mendukung berbagai aktivitas akademik, termasuk akses ke pembelajaran online, sistem informasi akademik, layanan administrasi, perpustakaan digital, komunikasi internal kampus, dan penelitian berbasis internet. Dengan adanya jaringan komputer, proses pengolahan dan distribusi data menjadi lebih cepat, efektif, dan terintegrasi.

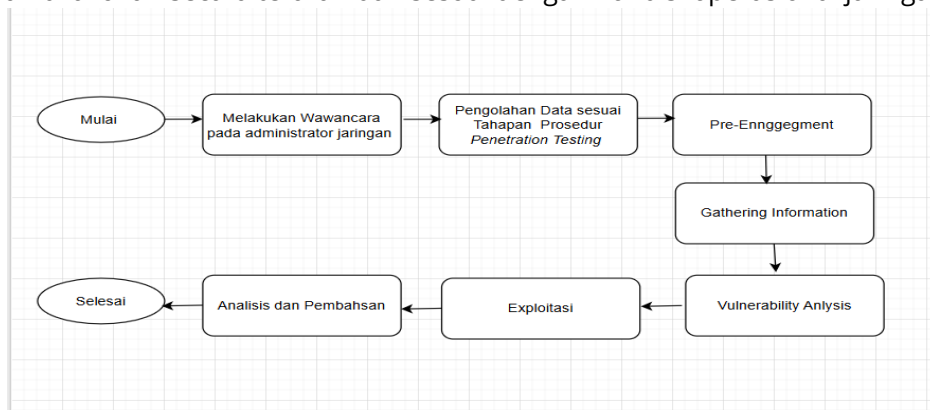
Jaringan nirkabel memanfaatkan gelombang radio yang dipancarkan secara broadcast dan bergerak bebas diudara. Tingkat keamanan jaringan nirkabel yang kurang baik jika dibandingkan dengan jaringan kabel perlu mendapatkan perhatian serius. Hal ini dikarenakan jaringan nirkabel bisa diakses secara diam-diam dan tidak memerlukan akses fisik ke gedung. Oleh karena itu, perancangan dan implementasi suatu topologi jaringan komputer yang menggunakan nirkabel memerlukan adanya suatu pent-test untuk menguji tingkat keamanan suatu jaringan nirkabel.

Tujuannya adalah menentukan dan mengetahui macam-macam serangan yang mungkin dilakukan pada sistem serta akibat yang bisa terjadi karena adanya kelemahan keamanan pada sistem komputer atau jaringan yang dimiliki (Hanafi, 2023). Gelombang elektromagnetik adalah cara jaringan nirkabel mengirimkan data. Perangkat akses point berfungsi sebagai pusat pemancar sinyal Wi-Fi kepada perangkat pengguna, yang memungkinkan komunikasi data di jaringan nirkabel. Standar IEEE 802.11, yang dikembangkan oleh Institute of Electrical and Electronics Engineers (IEEE), umumnya digunakan dalam teknologi nirkabel. Standar ini mengatur keamanan jaringan nirkabel, frekuensi radio, kecepatan transfer data, dan mekanisme komunikasi data.

Keamanan jaringan nirkabel adalah upaya perlindungan terhadap jaringan Wi-Fi dari berbagai ancaman seperti penyadapan, peretasan, dan akses ilegal. Pengamanan jaringan nirkabel dilakukan melalui mekanisme autentikasi, enkripsi, dan kontrol akses jaringan untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat menggunakan jaringan tersebut. Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak (Mulyanto et al., 2022). Dalam jaringan nirkabel, aspek keamanan menjadi lebih penting karena media transmisinya menggunakan gelombang radio yang dipancarkan secara broadcast melalui udara sehingga sinyal jaringan dapat ditangkap oleh siapa saja yang berada dalam jangkauan jaringan

METODE PENELITIAN

Analisis sistem dilakukan untuk memahami kondisi keamanan jaringan nirkabel yang sedang berjalan. Tahapan ini mencakup identifikasi konfigurasi access point, metode autentikasi yang digunakan, jenis enkripsi jaringan, serta potensi ancaman yang mungkin terjadi. Hasil analisis sistem digunakan sebagai dasar dalam menentukan ruang lingkup (scope) dan skenario penetration testing agar pengujian dilakukan secara terarah dan sesuai dengan kondisi operasional jaringan kampus.



Gambar 1. Diagram Alur Penelitian

HASIL DAN PEMBAHASAN

Hasil

Implementasi Metode *Penetration Testing*

Pada penelitian ini metode penetration testing diterapkan untuk mengidentifikasi kondisi keamanan jaringan wireless di lingkungan Universitas Prof. Dr. Hazairin, SH Bengkulu. Pengujian dilakukan menggunakan sistem operasi Kali Linux dengan tools Aircrack-ng sebagai media analisis keamanan jaringan wireless. Metode penetration testing pada penelitian ini dilakukan menggunakan pendekatan passive penetration testing, yaitu pengujian keamanan yang dilakukan

tanpa merusak sistem maupun mengganggu aktivitas jaringan utama kampus. Pengujian difokuskan pada proses identifikasi access point, pengumpulan informasi jaringan, dan analisis potensi kerentanan keamanan jaringan wireless.

Reconnaissance

Tahap reconnaissance merupakan tahap awal penetration testing yang bertujuan untuk mengidentifikasi jaringan wireless yang aktif di lingkungan kampus. Pada tahap ini peneliti melakukan pengamatan terhadap access point yang berada dalam jangkauan wireless adapter. Tahapan awal pengujian ini dilakukan dengan mengaktifkan monitor mode pada wireless adapter. Monitor mode merupakan mode khusus pada jaringan wireless yang memungkinkan perangkat menangkap seluruh paket data yang dipancarkan melalui udara tanpa harus terhubung langsung ke access point tertentu. Pada tahap selanjutnya, sebelum melakukan scanning menggunakan Aircrack-ng, mode ini biasanya diubah menjadi Monitor Mode menggunakan perintah: `sudo airmon-ng start wlan0`

```
(kali@kali)-[~]
$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
1661 NetworkManager
1694 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 iwlwifi Intel Corporation Wireless 8260 (rev 3a)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

Gambar 1. Tampilan Aktivitas Monitor Mode

Berdasarkan hasil pengujian, sistem berhasil mengubah interface wlan0 menjadi wlan0mon. Hal tersebut menunjukkan bahwa wireless adapter telah berhasil masuk ke monitor mode dan siap digunakan untuk melakukan proses scanning jaringan wireless.

Information Gathering dan Scanning

Tahap *information gathering* dilakukan untuk mengumpulkan informasi detail mengenai access point wireless yang terdeteksi. Setelah monitor mode berhasil diaktifkan, tahap berikutnya adalah melakukan scanning jaringan wireless menggunakan *tools airodump-ng*. Proses scanning dilakukan dengan perintah:

```
Session Actions Edit View Help
kali@kali: ~
$ airodump-ng wlan0mon

CH 12 [ Elapsed: 24 s ] [ 2026-06-05 10:58 ]

BSSID PWR Beacons #Data, M/s CH MB ENC CIPHER AUTH ESSID
DA:A3:15:82:FF:09 -83 2 0 0 11 85 WPA2 CCMP PSK vivo i220
EC:B9:70:9B:5E:49 -1 0 0 0 11 -1 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -89 3 0 0 0 360 WPA2 CCMP PSK <length: 0>
18:E8:29:EA:75:FA -86 6 0 0 1 195 WPA2 CCMP PSK <length: 0>
0A:DA:D2:83:C8:52 -90 2 0 0 1 130 WPA2 CCMP MGT seamlesswifi_id
0A:DA:D2:83:C8:52 -90 2 0 0 1 130 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -89 3 0 0 0 360 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -89 3 0 0 0 360 WPA2 CCMP PSK <length: 0>
0A:ED:DA:DE:C6:7A -88 3 27 0 0 180 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -88 13 0 0 0 360 WPA2 CCMP PSK <length: 0>
12:1B:3A:CB:13:09 -88 8 0 0 11 180 WPA2 CCMP PSK <length: 0>
82:1F:5C:B7:FA -91 5 0 0 11 180 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -88 3 0 0 0 360 WPA2 CCMP PSK <length: 0>
D6:88:8D:36:F8:05 -41 16 0 0 11 180 WPA2 CCMP PSK <length: 0>
20:1A:8B:77:A8:39 -86 5 0 0 0 360 WPA2 CCMP PSK <length: 0>
14:CA:56:5B:8E:C9 -86 17 3 0 5 130 WPA2 CCMP PSK <length: 0>
20:1A:8B:77:A8:39 -86 5 0 0 0 360 WPA2 CCMP PSK <length: 0>
DA:01:95:97:31:F7 -68 22 0 0 1 195 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -85 9 0 0 0 360 WPA2 CCMP PSK <length: 0>
8B:E8:56:E6:C9:68 -87 3 0 0 1 130 WPA2 CCMP PSK <length: 0>
EE:B9:70:9B:5E:49 -91 5 0 0 1 360 WPA2 CCMP PSK <length: 0>
EC:B9:70:9B:5E:49 -87 1 12 0 1 360 WPA2 CCMP PSK <length: 0>
06:85:6B:9C:6E:A2 -59 17 430 0 1 130 WPA2 CCMP PSK <length: 0>

BSSID STATION PWR Rate Lost Frames Notes Probes
EC:B9:70:9B:5E:49 72:75:AB:5E:E8:9F -89 0 - 1 59 17
EC:B9:70:9B:5E:49 C8:EE:FB:FE:5B:FF -85 0 - 1 0 3
0A:ED:DA:DE:C6:7A AB:E2:93:A2:BD:E8 -84 0e- 1e 0 29
82:1F:5C:B7:FA FA:5B:AE:ED:DF:AB -82 0 -24 0 2
```

Gambar 2. Hasil Scanning

Perintah tersebut digunakan untuk menangkap dan menampilkan seluruh *access point* yang berada dalam jangkauan adapter wireless, yang mana peneliti melakukan *scanning* di ruangan kelas Informatika.

Berdasarkan dari hasil *scanning* jaringan wireless di lingkungan Universitas Prof. Dr. Hazairin, SH Bengkulu yang dilaksanakan di ruangan kelas Informatika, menggunakan tools airodump-ng, ditemukan beberapa *access point* yang masih menggunakan sistem keamanan *Open Network* (OPN). *Open Network* merupakan jaringan wireless yang tidak menggunakan sistem autentikasi maupun enkripsi data sehingga pengguna dapat langsung terhubung ke jaringan tanpa harus memasukkan *username* ataupun *password*. Pada tahap *scanning* ini peneliti memperoleh beberapa informasi penting, antara lain:

Tabel 1. Tabel Informasi

SSID	BSSID	channel jaringan	Enkripsi	Autentifikasi	Kekuatan Sinyal
UNIHAZ	EC:B9:70:9B:5C:55	6	OPN	-	-89
TI_UNIHAZ	EC:B9:70:9B:5C:64	11	OPN	-	-52
UNIHAZ_TEKNIK	EC:B9:70:9B:5C:A5	6	OPN	-	-80
FAKULTAS_TEKNIK	06:05:88:9C:6E:A2	1	OPN	-	-59

Informasi tersebut digunakan untuk mengetahui konfigurasi keamanan jaringan wireless yang diterapkan pada masing-masing *access point*.

Vulnerability Identification

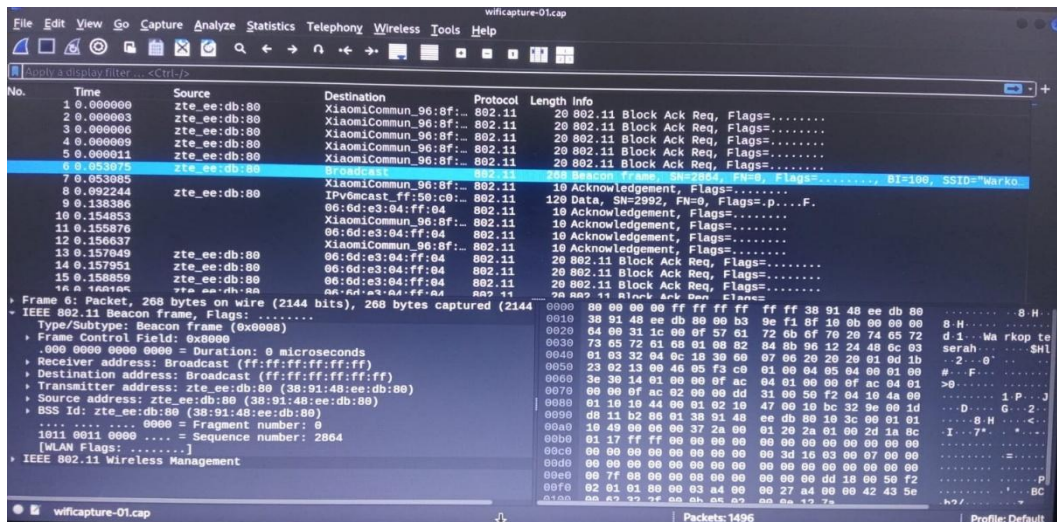
Tahap Vulnerability Identification merupakan proses analisis terhadap informasi yang diperoleh pada tahap reconnaissance dan scanning. Tujuan dari tahap ini adalah untuk mengidentifikasi potensi kerentanan keamanan yang terdapat pada jaringan wireless Universitas Prof. Dr. Hazairin, SH Bengkulu berdasarkan konfigurasi jaringan, mekanisme autentikasi, jenis enkripsi, serta kondisi operasional *access point* yang terdeteksi. Tahap ini sesuai dengan tahapan Vulnerability Analysis pada metode PTES yang berfungsi untuk menemukan dan menganalisis celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

Berdasarkan hasil *scanning* Airodump-ng menunjukkan bahwa beberapa titik akses masih menggunakan sistem keamanan Open Network (OPN), yaitu jaringan yang tidak menggunakan mekanisme autentikasi atau enkripsi data. SSID yang ditemukan menggunakan Open Network termasuk TI_UNIHAZ, UNIHAZ_TEKNIK, dan FAKULTAS_TEKNIK. Pada kondisi seperti ini, pengguna dapat terhubung ke jaringan tanpa melakukan proses verifikasi identitas atau kata sandi.

Exploitation

Tahap ini dilakukan untuk membuktikan bahwa informasi celah keamanan yang diperoleh pada tahap reconnaissance, scanning, dan vulnerability identification dapat digunakan untuk melakukan analisis lebih lanjut terhadap lalu lintas jaringan wireless. Pengujian dilakukan secara pasif dan terkontrol tanpa mengganggu operasional jaringan kampus serta tanpa melakukan serangan yang dapat menyebabkan gangguan layanan. Untuk membuktikan kerentanan tersebut, dilakukan tahap exploitation secara terbatas dan terkontrol menggunakan metode passive sniffing melalui aplikasi Wireshark. Passive sniffing merupakan teknik pengumpulan informasi jaringan dengan cara menangkap dan memantau paket data yang melintas pada jaringan tanpa melakukan interaksi langsung atau mengirimkan paket ke target. Teknik ini tidak mengganggu aktivitas jaringan sehingga aman digunakan dalam proses analisis keamanan jaringan nirkabel di lingkungan kampus.

Hasil *capture* berhasil disimpan ke dalam file berformat .cap, .csv, .netxml, dan .log.csv untuk dianalisis menggunakan Wireshark.



Gambar 3. Hasil Capture WPA2-PSK pada Wireshark

Hasil analisis file capture WPA2 menggunakan Wireshark pada access point "Warkop terserah" yang sebelumnya direkam menggunakan Airodump-ng. Dari hasil capture terlihat beberapa frame kontrol dan manajemen IEEE 802.11 yang berhasil ditangkap. Setelah file wificapture-01.cap dibuka menggunakan Wireshark, diperoleh sebanyak 1496 paket wireless yang berhasil direkam selama proses monitoring yang didominasi oleh *Beacon Frame*, *Block Acknowledgement Request*, *Acknowledgement*, dan *Data Frame*. Pada paket *Beacon Frame* dengan informasi: SSID "Warkop terserah". *Beacon Frame* merupakan frame manajemen yang dipancarkan secara berkala oleh access point untuk mengumumkan keberadaan jaringan wireless.

Block Acknowledgement Request (Block Ack Req)

Pada bagian atas hasil capture terlihat beberapa paket: 802.11 Block Ack Req, frame ini digunakan untuk meminta konfirmasi penerimaan sejumlah paket data sekaligus. Fungsinya: meningkatkan efisiensi komunikasi, mengurangi jumlah ACK individual, mempercepat transfer data. Keberadaan *Block Ack Request* menunjukkan bahwa jaringan sedang melakukan komunikasi data secara aktif.

Acknowledgement (ACK) digunakan untuk memberikan konfirmasi bahwa paket sebelumnya telah diterima dengan baik oleh perangkat tujuan. Fungsi ACK: memastikan paket berhasil diterima, mengurangi kehilangan data, menjaga stabilitas komunikasi wireless. Keberadaan ACK menunjukkan bahwa komunikasi antara access point dan klien berlangsung normal.

Data Frame pada hasil capture juga terlihat paket: Data. *Data Frame* merupakan frame yang digunakan untuk membawa informasi atau payload dari pengguna. Namun pada jaringan WPA2, isi *Data Frame* tidak dapat dibaca secara langsung karena: menggunakan WPA2, menggunakan enkripsi AES-CCMP, data pengguna telah diamankan.

Berbeda dengan jaringan *Open Network* (OPN), informasi komunikasi pengguna tidak dapat diamati secara langsung karena seluruh data telah dilindungi oleh mekanisme enkripsi WPA2. Temuan ini menunjukkan bahwa WPA2 memberikan tingkat perlindungan yang lebih baik terhadap risiko penyadapan lalu lintas jaringan dibandingkan jaringan yang tidak menggunakan enkripsi.

Pembahasan

Berdasarkan dua hasil capture Wireshark yang telah dilakukan, terlihat perbedaan yang cukup jelas antara jaringan OPN (*Open Network*) pada SSID TI_UNHAZ dan jaringan WPA2-PSK pada SSID Warkop terserah.

Tabel 2. Tabel Perbandingan Hasil OPN dan WPA2-PSK

Aspek Analisis	Jaringan OPN (TI_UNIHAZ)	Jaringan WPA2-PSK (Warkop terserah)
Jenis Keamanan	Open Network (OPN)	WPA2-PSK
Enkripsi Data	Tidak ada	AES-CCMP
Jumlah Paket Capture	11.229 paket	1.496 paket
Beacon Frame	Terlihat	Terlihat
ARP Request	Terlihat	Tidak terlihat
UDP	Terlihat	Tidak terlihat
MDNS	Terlihat	Tidak terlihat
ICMPv6	Terlihat	Tidak terlihat
Alamat IP Perangkat	Terlihat	Tidak terlihat
Block ACK	Ada	Ada
Acknowledgement	Ada	Ada
Data Frame	Dapat diamati	Terenkripsi
Informasi Klien	Lebih mudah diamati	Lebih terbatas
Risiko Passive Sniffing	Tinggi	Rendah

Berdasarkan hasil analisis *packet capture* menggunakan Wireshark, terdapat perbedaan yang signifikan antara jaringan *Open Network* (OPN) dan jaringan WPA2-PSK. Pada jaringan TI_UNIHAZ yang menggunakan OPN, peneliti berhasil mengidentifikasi berbagai jenis lalu lintas jaringan seperti ARP Request, UDP, MDNS, ICMPv6, Broadcast Traffic, serta informasi alamat IP perangkat yang sedang aktif berkomunikasi. Kondisi ini menunjukkan bahwa lalu lintas jaringan dapat diamati secara lebih terbuka karena tidak adanya mekanisme enkripsi pada lapisan wireless. Sebaliknya, pada jaringan WPA2-PSK "Warkop terserah", paket yang dominan terdeteksi adalah *Beacon Frame*, *Block Acknowledgement Request*, *Acknowledgement*, dan *Data Frame* yang telah terenkripsi. Informasi komunikasi pengguna seperti alamat IP, ARP, maupun layanan jaringan tidak dapat diamati secara langsung. Hasil tersebut menunjukkan bahwa implementasi WPA2 dengan algoritma enkripsi AES-CCMP mampu meningkatkan kerahasiaan data dan mengurangi risiko penyadapan melalui teknik *passive sniffing* dibandingkan jaringan yang menggunakan *Open Network* (OPN).

Berdasarkan hasil *penetration testing* dan analisis keamanan jaringan wireless yang telah dilakukan, terdapat beberapa rekomendasi yang dapat diterapkan untuk meningkatkan keamanan jaringan wireless di lingkungan Universitas Prof. Dr. Hazairin, SH Bengkulu.

Mengganti *Open Network* (OPN) dengan WPA2 atau WPA3

Hasil scanning menunjukkan masih terdapat beberapa access point yang menggunakan sistem keamanan *Open Network* (OPN), yaitu jaringan yang tidak menerapkan autentikasi maupun enkripsi data. Kondisi ini memungkinkan siapa saja untuk terhubung ke jaringan dan meningkatkan risiko penyadapan lalu lintas data. Oleh karena itu, seluruh access point yang masih menggunakan OPN disarankan untuk segera dikonfigurasi menggunakan WPA2-PSK atau WPA3 agar komunikasi data pengguna terlindungi melalui mekanisme enkripsi.

Menerapkan Kebijakan Password yang Kuat

Penggunaan kata sandi yang lemah dapat mempermudah pelaku melakukan serangan *brute force* maupun *dictionary attack*. Oleh karena itu, administrator jaringan disarankan menerapkan kebijakan password yang kuat dengan kombinasi huruf besar, huruf kecil, angka, dan simbol khusus dengan panjang minimal 8–12 karakter. Selain itu, pergantian password secara berkala perlu dilakukan untuk mengurangi risiko kebocoran kredensial.

Implementasi Sistem Autentikasi Terpusat

Untuk meningkatkan kontrol akses pengguna, jaringan kampus dapat menerapkan sistem autentikasi terpusat menggunakan captive portal, RADIUS Server, atau WPA2/WPA3 Enterprise. Dengan sistem ini, setiap pengguna diwajibkan melakukan login menggunakan akun resmi kampus sehingga aktivitas pengguna dapat dipantau dan dikelola dengan lebih baik.

Penerapan VLAN dan Segmentasi Jaringan

Segmentasi jaringan menggunakan Virtual Local Area Network (VLAN) dapat digunakan untuk memisahkan lalu lintas jaringan berdasarkan kelompok pengguna, seperti mahasiswa, dosen, staf administrasi, dan tamu. Dengan adanya segmentasi jaringan, risiko penyebaran serangan maupun akses tidak sah ke sumber daya penting dapat diminimalkan.

Mengaktifkan Firewall dan Access Control List (ACL)

Firewall pada router maupun Mikrotik perlu dikonfigurasi untuk memfilter lalu lintas jaringan yang mencurigakan. Selain itu, Access Control List (ACL) dapat digunakan untuk membatasi akses ke layanan tertentu sehingga hanya pengguna yang memiliki hak akses yang dapat menggunakan sumber daya jaringan kampus.

Penerapan Intrusion Detection System (IDS)

Untuk meningkatkan kemampuan deteksi ancaman secara real-time, administrator jaringan disarankan mengimplementasikan Intrusion Detection System (IDS) seperti Snort atau Suricata. Sistem ini mampu mendeteksi aktivitas mencurigakan seperti port scanning, brute force attack, maupun percobaan akses ilegal terhadap jaringan.

Pembaruan Firmware dan Monitoring Berkala

Seluruh perangkat jaringan seperti access point, router, dan Mikrotik perlu diperbarui (update firmware) secara berkala untuk menutup celah keamanan yang ditemukan oleh vendor. Selain itu, monitoring jaringan secara rutin perlu dilakukan untuk mendeteksi perubahan konfigurasi maupun aktivitas yang tidak normal.

Audit dan Penetration Testing Secara Berkala

Pengujian keamanan jaringan tidak hanya dilakukan sekali, tetapi perlu dilakukan secara berkala sebagai bagian dari proses evaluasi keamanan. Penetration testing yang dilakukan secara rutin dapat membantu administrator mengidentifikasi kerentanan baru serta memastikan bahwa mekanisme keamanan yang diterapkan tetap efektif dalam menghadapi perkembangan ancaman siber.

Dengan menerapkan rekomendasi tersebut, diharapkan tingkat keamanan jaringan nirkabel Universitas Prof. Dr. Hazairin, SH dapat meningkat sehingga risiko penyadapan data, akses tidak sah, dan gangguan layanan jaringan dapat diminimalkan, serta kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian mengenai Analisis dan Implementasi Keamanan Jaringan Nirkabel Menggunakan Metode Penetration Testing di Universitas Prof. Dr. Hazairin, SH, maka dapat diambil beberapa kesimpulan sebagai berikut:

Berdasarkan hasil pengujian keamanan jaringan wireless menggunakan metode penetration testing, diketahui bahwa tingkat keamanan jaringan nirkabel di lingkungan Universitas Prof. Dr. Hazairin, SH masih perlu ditingkatkan. Hasil scanning menunjukkan beberapa access point masih

menggunakan sistem keamanan Open Network (OPN) tanpa mekanisme autentikasi dan enkripsi sehingga berpotensi dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses jaringan.

Penerapan metode penetration testing yang dilakukan melalui tahapan information gathering, scanning, vulnerability identification, dan exploitation analisis packet capture berhasil mengidentifikasi berbagai informasi penting mengenai konfigurasi jaringan wireless, jenis keamanan yang digunakan, channel jaringan, kekuatan sinyal, serta potensi kerentanan yang terdapat pada access point yang diuji.

Hasil analisis menggunakan Wireshark menunjukkan bahwa jaringan yang menggunakan sistem keamanan Open Network (OPN) memiliki risiko keamanan yang lebih tinggi karena lalu lintas jaringan seperti ARP Request, UDP, MDNS, ICMPv6, dan informasi alamat IP perangkat dapat diamati secara langsung, akibatnya, informasi aktivitas pengguna dapat diketahui oleh pihak yang tidak berwenang. Sebaliknya, jaringan yang menggunakan WPA2-PSK dengan enkripsi AES-CCMP mampu melindungi kerahasiaan komunikasi pengguna sehingga informasi sensitif tidak dapat diamati secara langsung melalui teknik passive sniffing. Passive sniffing merupakan serangan dengan cara menangkap lalu lintas jaringan tanpa mengubah data yang dikirim.

Metode penetration testing terbukti efektif untuk mengevaluasi kondisi keamanan jaringan nirkabel secara nyata karena mampu memberikan gambaran mengenai kerentanan yang ada, tingkat risiko yang mungkin terjadi, serta efektivitas mekanisme keamanan yang telah diterapkan pada jaringan wireless kampus.

Berdasarkan hasil pengujian analisis, peningkatan keamanan jaringan dapat dilakukan melalui penerapan protokol keamanan yang lebih kuat seperti WPA2 atau WPA3, penggunaan autentikasi pengguna yang lebih baik, penerapan firewall dan VLAN, pembaruan firmware perangkat jaringan secara berkala, serta pelaksanaan monitoring dan penetration testing secara rutin untuk menjaga keamanan jaringan secara berkelanjutan.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk meningkatkan keamanan jaringan nirkabel di Universitas Prof. Dr. Hazairin, SH, yaitu sebagai berikut:

Kepada pihak pengelola jaringan disarankan untuk mengganti seluruh access point yang masih menggunakan sistem keamanan Open Network (OPN) dengan sistem keamanan WPA2-PSK atau WPA3 agar komunikasi data pengguna terlindungi oleh mekanisme enkripsi yang lebih baik. Administrator jaringan perlu menerapkan kebijakan penggunaan kata sandi yang kuat dan melakukan pergantian password secara berkala guna mengurangi risiko akses tidak sah terhadap jaringan wireless.

Untuk meningkatkan pengendalian akses pengguna, disarankan menerapkan sistem autentikasi terpusat seperti captive portal atau WPA2/WPA3 Enterprise yang terintegrasi dengan akun pengguna kampus. Pengelola jaringan perlu menerapkan segmentasi jaringan menggunakan VLAN untuk memisahkan akses antara mahasiswa, dosen, staf administrasi, dan tamu sehingga risiko penyebaran serangan dapat diminimalkan. Diperlukan implementasi sistem keamanan tambahan seperti firewall, Access Control List (ACL), dan Intrusion Detection System (IDS) untuk meningkatkan kemampuan deteksi serta pencegahan terhadap aktivitas yang mencurigakan pada jaringan

DAFTAR PUSTAKA

Ariyadi, T., & Pohan, M. R. (2023). Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators. *Jurnal Penelitian Pendidikan IPA*, 9(12), 10768–10775. <https://doi.org/10.29303/jppipa.v9i12.5551>

- BINUS. (2024). Standard IEEE untuk Wi-Fi. <https://binus.ac.id/malang/computer-science/2024/12/04/standard-ieee-untuk-wi-fi/>
- Bowo, I. T., Kurniawan, F. I., Mukhlis, I. R., Yutanto, H., Marpaung, S. H., & Mandowen, S. A. (n.d.). BUKU AJAR.
- CISCO. (2024). Cybersecurity Readiness Index 2024. Cisco Systems, Inc. <https://www.cisco.com>
- Diana, E. (2024). Decision Support System for Selecting Peer-to-Peer Lending Applications using ARAS and Rank Sum Approaches. 8, 674–684. <https://doi.org/10.30865/mib.v8i1.7179>
- Diana, E., Akhir, A. F. P., & Darmi, Y. (2021). Penerapan Sistem Autentifikasi dan Pengamanan pada Jaringan Hotspot Berbasis Captive Portal. 1, 24–28.
- EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi Volume 5 Nomor 3, Juni 2025. (2025). 5, 664–672.
- Faizi, M. A., & Christanto, F. W. (2024). Manajemen Perangkat Jaringan Access Point Menggunakan UniFi Controller di Jaringan Kampus Access Point Network Device Management Using UniFi Controller on Campus Networks. 9(2), 67–76. <https://doi.org/10.32528/justindo.v9i2.1471>
- Gede, I., Agus, P., Jaya, P., Sukerti, N. K., Made, I., Santosa, A., & Komputer, S. (2024). Analisis Keamanan Jaringan Nirkabel Melalui Metode Penetration Testing Pada SD Kartika VII-3 Denpasar. Seminar Hasil Penelitian Informatika Dan Komputer (SPINTER) | Institut Teknologi Dan Bisnis STIKOM Bali, 1(3), 581–586. <https://spinter.stikom-bali.ac.id/index.php/spinter/article/view/431>
- Hanafi, M. A. (2023). Analisa keamanan jaringan Wireless UNIMMA menggunakan metode Penetration Testing. 11.
- Intel. (2021). Berbagai Macam Protokol Wi-Fi dan Tingkat Data. <https://www.intel.co.id/content/www/id/id/support/articles/000045852/wireless/legacy-intel-wireless-products.html>
- Irawan, D., Hastini, S., Ardius, E., Isroqmi, A., & ... (2025). Optimalisasi Infrastruktur Jaringan Wi-Fi 7 Untuk Peningkatan Kualitas Pelayanan Akses Mahasiswa Pada Universitas PGRI Palembang. Jurnal Nasional ..., 8(4), 1990–1998. https://www.researchgate.net/profile/Abdul-Azis-14/publication/396524829_Optimalisasi_Infrastruktur_Jaringan_Wi-Fi_7_untuk_Peningkatan_Kualitas_Pelayanan_Akses_Mahasiswa_pada_Universitas_PGRI_Palembang/links/68f1049d220a341aa1559f54/Optimalisasi-Infrastru
- Mulyanto, Y., Herfandi, & Candra Kirana, R. (2022). 1528-Article Text-4037-1-10-20220219. JINTEKS (Jurnal Informatika Teknologi Dan Sains), 4(1), 26–35.
- Palopo, K. (2024). Nirkabel (Wifi) Menggunakan Routerboard Mikrotik Dan Firewall Pada Smk Kristen Palopo. JITET (Jurnal Informatika Dan Teknik Elektro Terapan), 12(3), 2229–2298.
- Ratchford, M., El-Gayar, O., & Noteboom, C. (2022). BYOD Security Issues: A Systematic Literature Review. Information Security Journal: A Global Perspective. <https://doi.org/10.1080/19393555.2021.1923873>
- santoso, ainurohman, K. (2022). Penerapan Metode Penetration Testing. 4(2), 162–167.
- Satria Galang Saputra, Parga Zen, B., & Abdurahman. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). Jurnal Sistem Informasi Galuh, 1(2), 43–51. <https://doi.org/10.25157/jsig.v1i2.3152>
- Teknokrat, C. (2025). Wi-Fi 6 dan 802.11ax: Teknologi Jaringan yang Wajib Anda Ketahui. <https://csirt.teknokrat.ac.id/wi-fi-6-dan-802-11ax-teknologi-jaringan-yang-wajib-anda-ketahui/>

Union, I. T. (2023). Global Cybersecurity Index 2023: Strengthening Cybersecurity Resilience. International Telecommunication Union.

University, I. T. T. (2024). Hub: Pengertian, Fungsi, Cara Kerja, Kelebihan, dan Kekurangan. IT Telkom University. <https://it.telkomuniversity.ac.id/hub-adalah/>