Jurnal Rekayasa Sistem Informasi dan Teknologi
Volume 2, No 1 – Agustus 2024
e-ISSN : 3025-888X

ANALISIS SISTEM KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) MENGGUNAKAN AKSES TETHERING

Astutik Zaerani*[1], Lalu Delsi Samsumar[2], Muh Nasirudin Karim[3], Emi Suryadi[4]
[1,2,3,4]Universitas Teknologi Mataram
[1,2]Program Studi Rekayasa Sistem Komputer, FTIK UTM, Mataram
[3]Komputerisasi Akutansi, Fakultas Vokasi UTM, Mataram
[4]Teknik Komputer, FakultasVokasi UTM, Mataram
[1] **astutik.zaerani65@gmail.com**, [2] samsumarld@utmmataram.ac.id , [3] karimnasirudin@gmail.com , emisuryadi@gmail.com

Received: 18-08- 2024	Revised: 26-08-2024	Approved: 28-08-2024

ABSTRAK

Peranan teknologi didalam kehidupan tidak dapat dihindari terutama didalam dunia kerja, bisnis, serta pendidikan. Salah satu fasilitas teknologi saat ini memanfaatkan sebuah Smartphone menjadi sebuah Access Point (AP) agar dapat terhubung ke internet, dengan menggunakan tethering dalam sebuah jaringan wireless local area network (wlan) dan menjadikan udara sebagai media peyaluran informasi pada jaringan tersebut. Metode yang digunakan penetration testing sehingga sniffing dan scanning menggunakan tools Arp-scan dan Bettercap. Hasil yang diperoleh dari pengujian tersebut menunjukkan bahwa keamanan jaringan Wireless Local Area Network (WLAN) menggunakan akses tethering tidak cukup aman untuk digunakan. Perihal ini dibuktikan dari hasil pengujian tersebut berupa data yang didapatkan dari dampak serangan itu berupa Username, Password, dan situs yang diakses oleh target menunjukkan bahwa keamanan jaringan Wireless Local Area Network (WLAN) menggunakan akses tethering masih dikategorikan tidak aman dan perlu untuk di tingkatkan.

Kata Kunci: WLAN, Tethering, Pentest, Sniffing, Scanning

PENDAHULUAN

Teknologi informasi berubah dan berkembang sangat pesat dan secara umum sudah banyak digunakan pada zaman moderen saat ini, peranan teknologi didalam kehidupan tidak dapat dihindari terutama didalam dunia kerja, bisnis, serta pendidikan. Salah satu fasilitas teknologi saat ini memanfaatkan sebuah Smartphone menjadi sebuah Access Point (AP) agar dapat terhubung ke internet.

Teknologi tethering ini memanfaatkan gelombang radio untuk mentransmisikan data dengan frekuensi 2,4 GHz. Secara umum WLAN seperti terthering ini telah banyak digunakan dari pada koneksi menggunakan kabel (LAN), padahal dari segi keamanan komunikasi data pada jaringan tersebut rentan terhadap aktivitas illegal seperti sniffing dan scanning, jaringan yang sering digunakan masyarakat ini memiliki keamanan WPA2-PSK yang memiliki kelemahan yaitu password wifi (Haeruddin and Kurniadi 2021) dapat di retas serta tidak ada pengaturan MAC address filtering sehingga siapa saja bisa masuk karena tidak ada pembatasaan MAC address. Penelitian (Rusdi and Prasti 2019)ini sangat penting untuk dilakukan dikarenakan banyak dari kalangan Masyarakat terhubung ke jaringan yang bersifat publik yang tidak memiliki keamanan tinggi.

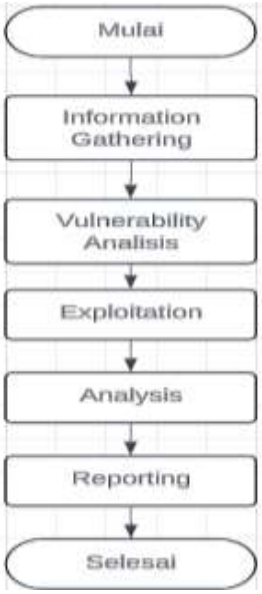
Dikarenakan lebih rentan diserang oleh penyusup, maka dibutuhkan sebuah metode untuk melakukan uji coba apakah jaringan (wireless) menggunakan akses tethering pada smatrphone (Hermanto and Anam 2020) yang telah terpasang sudah aman atau sesuai dengan standard operasional. Metode ini bisa disebut dengan metode penetration testing. Penelitian yang dilakukan oleh (Kurniawan and Sari 2018) dengan berjudul Analisis Sistem Keamanan Wireless Local Area Network (WLAN)

Pada Proses Tethering. Penelitian yang dilakukan oleh (As'ad, Hendradi, and Hanafi 2023) dengan berjudul Analisis Perfoma Jaringan Wifi Berbasis Smartpone Sebagai Tethering dan Smartphone Sebagai Modem dengan Metode Perbandingan.

Penelitian yang dilakukan oleh (Adiguna and Widagdo 2022)dengan berjudul Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Mercusys Mw302r). Penelitian yang dilakukan oleh (Hanipah and Dhika 2020)dengan judul Analisa Pencegahan Aktivitas Ilegal. Didalam Jaringan Menggunakan Wireshark. Penelitian yang dilakukan oleh (Hasanuddin et al. 2022) dengan berjudul Perancangan Sistem Manajemen User Hotspot Berbasis Web Menggunakan Application Programming Interface (API) Mikrotik.

METODE PENELITIAN

Penetration testing adalah sebuah metode yang dilakukan untuk mengevaluasi keamanan dari sebuah sistem dan jaringan komputer atau suatu kegiatan dimana seseorang melakukan simulasi serangan yang dapat dilakukan terhadap suatu jaringan (Mulyanto, Herfandi, and Candra Kirana 2022) tertentu menemukan kelemahan yang ada pada sistem jaringan tersebut.



Gambar 1 Alur Metode Penelitian

Dalam menjelaskan sebuah permaslahan tahapan-tahapan penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut.

Dalam penelitian ini peneliti (Jude Saskara, Oktap Indrawan, and Maha Putra 2019)menggunakan teknik pengumpulan data yang dilakukan dengan observasi secara langsung pada objek penelitian (Wahyudi, Luthfi, and Efendi 2019) setra mengamati langsung kondisi di Laboratorium mini.

Information Gethering (Pemrosesan Data)

Pada proses ini merupakan tahap awal melakukan Penetration Testing, yaitu (Prakoso and Khamas Heikmakhtiar 2024) menentukan ruang lingkup dan tujuan penguji. Dalam langkah pertama ini peneliti fokus pada ruang jaringan *Wireless Local Area Network (WLAN)* pada proses tethering di Laboratorium Mini, adapun tujuan penelitian (Jude Saskara et al. 2019) adalah untuk mengetahui tingkat keamanan jaringan tersebut.

Vulnerability Analysis (Scanning menggunakan Arp-scan)

Memindai target menggunakan *toolts Arp-scan* untuk mencari celah keamanan yang bisa digunakan untuk masuk ke dalam sistem dan berfungsi sebagai pencari *IP address* dari target(Gunawan, Rahmah, and Iskandar 2023). Merupakan proses mencari kerentanan sistem atau *Vurnelability Scanning*(Hermanto and Anam 2020).

Exploitation (Menggunakan Bettercap)

Pada tahap ini dimana peneliti melakukan serangan pada target menggunakan *tools Bettercap* dengan melakukan percobaan untuk menerobos masuk ke dalam sistem setelah *scanning* (Hae 2021) yang menemukan celah keamanan. Berbagai celah kamanan seperti *Arp Poisoning* dan *packet sniffing.*

Analysis

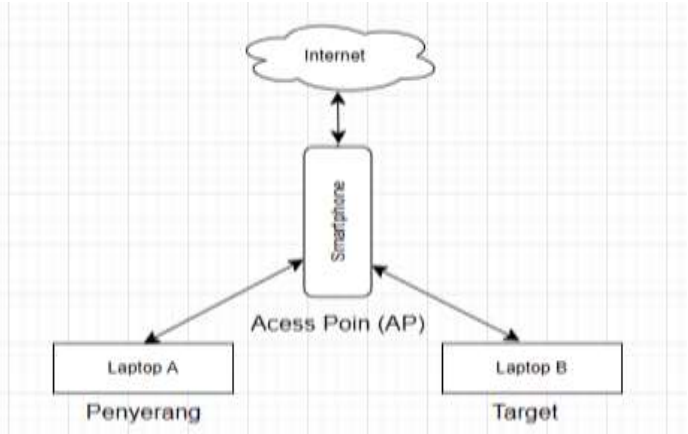
Analysis merupakan hasil data yang didapatkan untuk kemudian menjadi bahan data penting (Kurnia 2019).

HASIL DAN PEMBAHASAN

Information Gathering (Pemrosesan Data)

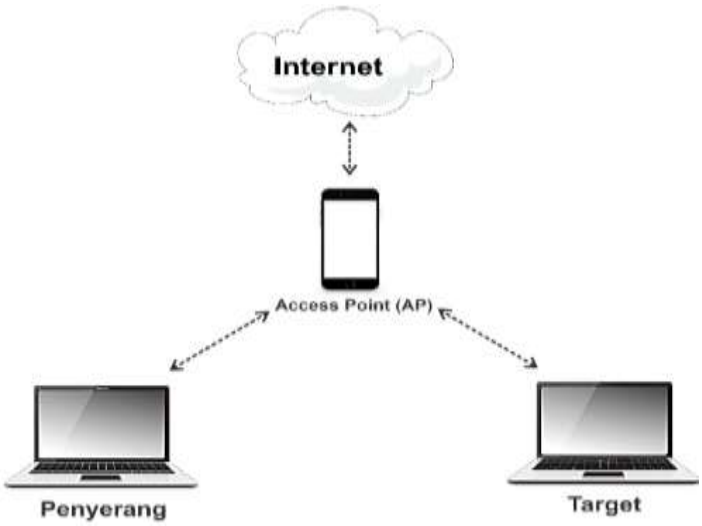
Pada proses ini merupakan tahap awal melakukan Penetration Testing, yaitu menentukan ruang lingkup dan tujuan penguji. Dalam langkah pertama ini peneliti (Samsumar and Gunawan 2017) fokus pada ruang jaringan *Wireless Local Area Network (WLAN)* pada proses tethering.

Pada penelitian ini dirancang desain jaringan yang digunakan dan disesuaikan dengan model infrastruktur jaringan pada *Wireless Local Area network (WLAN)*(Mursyidah et al. 2019).



Gambar 1 diagram blok sistem

Topologi uang digunakan pada penelitian menggunakan konsep *tethering/portable WI-FI* yang dapat menjadikan *smartphone android* sebagai *access poin* atau *gateway* untuk memanfaatkan koneksi internet dan digunakan oleh *laptop* maupun *smartphone*(Haeruddin and Kurniadi 2021).



Gambar 2 diagram perancangan perangkat keras

Vulnerability Analysis (Scanning menggunakan Arp-scan)

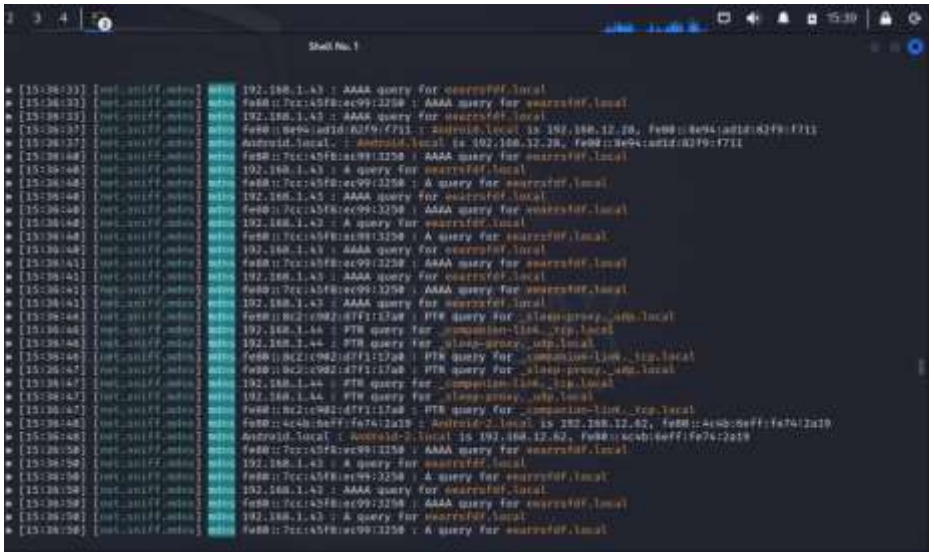
Dengan menggunakan *toolts Arp-scan* untuk mencari celah keamanan yang bisa digunakan untuk masuk ke dalam sistem dan berfungsi sebagai pencari *IP address* dari target. Merupakan proses mencari kerentanan sistem atau *Vurnelability Scanning*(Choiruman, Ginting, and Iryani 2022).

Gambar 3 Proses Scanning Target

Exploitation (Menggunakan Bettercap)

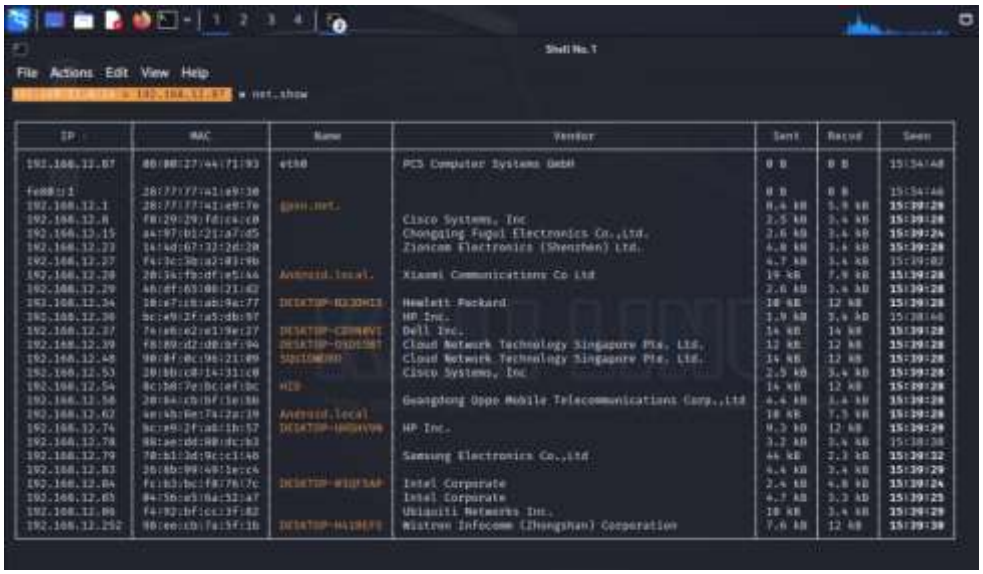
Dengan melakukan serangan pada target menggunakan *tools Bettercap* dengan melakukan percobaan untuk menerobos masuk ke dalam sistem setelah *scanning* yang menemukan celah keamanan.

Berbagai celah kamanan seperti *Arp Poisoning* dan *packet sniffing. Penetration Tester* kemudian mengeksploitasi (Ilham Firdaus, Januar Al Amien, and Soni 2020) celah keamanan ini dengan mencari data dari target, merupakan proses *monitoring* pengambilan data *username* dan *password*(Maulana et al. 2023).



Gambar 4 Monitoring Target

Celah keamanan yang dapat dieksploitasi, didapatkan ip *address, Mac Address,* dan *vendor* dari hardware interface yang terhubung ke sebuah jaringan.



Gambar 5 Peroses Monitoring Target

Bahan dan Alat yang digunakan untuk melakukan penelitian

Tabel 1 Kebutuhan Perangkat Keras

No	Nama Hardware	Spesifikasi	Fungsi
1.	ıptop Lenovo_MT_82C6_BU_idea_FM_V14 -ADA Lenovo E8CN34WW	PrProcessor: AMD 3020e with Radeon Graphics, 1200 Mhz, 2 Core (s), 2 Logical Prosesor (s), RAM 8.00 GB	Sebagai *Attacker*
2.	Laptop Lenovo_MT_80RK_BU_idea_FM_Len ɔvo ideapad 100-14IBD	Intel (R) Core (TM) i3-5005U CPU @ 2000 Mhz, 2 Core (s), 4 Logical Prosesor (s), RAM 2.00 GB	Sebagai *Client*
3.	Smartphone Android OPPO Reno5	Qualcomm Snapdragon 720G Octa-core, ram 8 GB, 4G (LTE)	Sebagai *Access Poin*

Tabel 2 Kebutuhan Perangkat Lunak

No	Nama Sofware	Spesifikasi	Fungsi
1.	Kali Linux	Sistem	Sebagai Attacker
2.	Windows 10	Sistem Oprasi	Sebagai Client
3.	Arp-scan	Versi 1.10.0	Tools Serangan
4.	Bettercap	Versi 1.6.2	Tools Serangan

KESIMPULAN

Dari hasil analisis yang sudah dicoba hingga bisa ditarik kesimpulannya yaitu pengujian keamanan jaringan *Wireless Local Area Network (WLAN)* menggunakan akses *tethering* dengan menggunakan metode Penetration Testing di Laboratorium Mini, melalui pengujian serangan Scanning dan Sniffing menggunakan tools Arp-scan dan Bettercap.

Dari hasil pengujian tersebut menunjukkan bahwa keamanan jaringan *Wireless Local Area Network (WLAN)* menggunakan akses *tethering* tidak cukup aman untuk digunakan. Perihal ini dibuktikan dari hasil pengujian tersebut berupa data yang didapatkan dari dampak serangan itu berupa Username, Password, dan situs yang diakses oleh target menunjukkan bahwa keamanan jaringan *Wireless Local Area Network (WLAN)* menggunakan akses *tethering* tidak aman dan perlu untuk di tingkatkan

DAFTAR PUSTAKA

Adiguna, Mochamad Adhari and Bambang Wisnu Widagdo. 2022. "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)." *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)* 5(2):1–8.

As'ad, Humaid Husain, Purwono Hendradi, and Mukhtar Hanafi. 2023. "Analisa Perfoma Jaringan Wifi Berbasis Smartphone Sebagai Tethering Dan Smartphone Sebagai Modem Dengan Metode Perbandingan." *Journal of Information System Research (JOSH)* 4(4):1102–8.

Choiruman, Muhammad Rizky, Jafaruddin Gusti Amri Ginting, and Nanda Iryani. 2022. "Analisis Pendeteksian Serangan ARP Poisoning Dengan Menggunakan Metode Live Forensic." *InfoTekJar :Jurnal Nasional InformatikadanTeknologiJaringan* 2:0–4.

Gunawan, Arie, Rosyidah Rahmah, and Agus Iskandar. 2023. "Rancang Bangun Jaringan Hotspot Menggunakan LINUX ClearOS Dengan Konsep Security Gateway." *JTIM : Jurnal Teknologi Informasi Dan Multimedia* 4(4):272–80.

Hae, Yacob. 2021. "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan

Metode Eksperimen." *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)* 8(4):2095–2105.

Haeruddin, H. and A. Kurniadi. 2021. "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)." *CoMBInES-Conference on Management …* 1(1):508–15.

Hanipah, Rahma and Harry Dhika. 2020. "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark." *DoubleClick: Journal of Computer and Information Technology* 4(1):11.

Hasanuddin, Chairunnisa, Winda Novianti, Syamsi Edi, Atiyah Suharti, Nur Chayati, I. Putu Agus Dharma Hita, Saparuddin, Edi Purwanto, Lila Pangestu Hadiningrum, Asti Febrina, Putu Eka Purnamaningsih, and Kadek Wiwin Dwi Wismayanti. 2022. *Perencanaan Pembelajaran (Kurikulum Merdeka Belajar)*. Vol. 3. Serang Banten: Sada Kurnia Pustaka.

Hermanto, Dedy and M. Syaiful Anam. 2020. "Implementasi Sistem Keamanan Hotspot Jaringan Menggunakan Metode OpenSSL (Secure Socket Layer)." *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi* 6(1):57.

Ilham Firdaus, Januar Al Amien, and Soni Soni. 2020. "String Matching Untuk Mendeteksi Serangan Sniffing (ARP Spoofing) Pada IDS Snort." *Jurnal CoSciTech (Computer Science and Information Technology)* 1(2):44–49.

Jude Saskara, Gede Arna, I. Putu Oktap Indrawan, and Putu Maha Putra. 2019. "Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru." *Jurnal Pendidikan Teknologi Dan Kejuruan* 16(2):236.

Kurnia, Dian. 2019. "Pemanfaatan Bettercap Sebagai Teknik Sniffing Pada Paket Trafik Jaringan WIFI." *SEMNASTEK Universitas Islam Sulawesi Utara* 83–85.

Kurniawan, M. R. and Linna Oktaviana Sari. 2018. "Analisis Sistem Keamanan Wireless Local Area Network (WLAN) Pada Proses Tethering." *Jom FTEKNIK* 5(2):1–7.

Maulana, R., M. Hatta, I. Syafrinal, Reza Kurniawan, Sutarti, Siswanto, Ariansyah Bachtiar, Arandha Aryton Astari, Barbara L. et al. Hoffman, Roby Nurbahri, Gunadi Widi Nurcahyo, Teguh Budyantara, Nofita Rismawati, Muhamad Femy Mulya, Sumardi Jayanto, Ahmad Tantoni, and Hasyim Asyari. 2023. "Analisis Keamanan Fasilitas Jaringan Wifi Terhadap Serangan Packet Sniffing Pada Protocol HTTP Dan HTTPS (7)." *JUST IT: Jurnal Sistem Informasi …* 10(1):37–44.

Mulyanto, Yudi, Herfandi Herfandi, and Randi Candra Kirana. 2022. "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi Kasus:RS H.LMANAMBAI ABDULKADIR)." *Jurnal Informatika Teknologi Dan Sains* 4(1):26–35.

Mursyidah, Husaini, Atthariq, Muhammad Arhami, Hari Toha Hidayat, Anita, and Ramadhona. 2019. "Analysis and Implementation of the Port Knocking Method Using Firewall-Based Mikrotik RouterOS." *IOP Conference Series: Materials Science and Engineering* 536(1).

Prakoso, Gilang and Aulia Khamas Heikmakhtiar. 2024. "Analisis Keamanan Jaringan: ARP Spoofing Dan DNS Spoofing Dengan Metode National Institute of Standards and Technology." *Journal on Education* 06(02):12895–902.

Rusdi, Muhammad Idham and Dianradika Prasti. 2019. "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux." *Seminar Nasional Teknologi Informasi Dan Komputer 2019* 260–69.

Samsumar, Lalu Delsi and Karya Gunawan. 2017. "Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus Di Kampus Stmik Mataram." *Jurnal Ilmiah Teknologi Infomasi Terapan* 4(1):73–82.

Wahyudi, Erfan, Emha Taufiq Luthfi, and Muhammad Masjun Efendi. 2019. "Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal ISSN : 2087-894 Jurnal Explore STMIK Mataram – Volume 9 No 1 Tahun 2019 ISSN : 2087-894." *Jurnal Explore STMIK Mataram* 9(1):1–7.