JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Uji penetrasi jaringan wireless dan IoT dengan tools open- source pada lingkungan virtual

Hafiz Fadhillah[1*], Faris An Nura[2], Langlang Soeltanul Aulia Aurelsosa[3], Teuku Farhan Damiri[4], Muhammad Subhan[5], Muhammad Zada Zayyan[6]
[1,2,3,4,5,6]Teknik Informatika Universitas Malikussaleh, Indonesia
[1]hafiz.210170162@mhs.unimal.ac.id, [2]faris.240170227@mhs.unimal.ac.id, [3]langlang.240170136@mhs.unimal.ac.id, [4]teuku.240170146@mhs.unimal.ac.id, [5]muhammad.240170236@mhs.unimal.ac.id, [6]muhammad.240170203@mhs.unimal.ac.id

ABSTRACT

Wireless network security and Internet of Things (IoT) device vulnerabilities have become critical issues in the digital era, especially with the growing reliance on smart devices in household, industrial, and urban environments. Many IoT devices and Wi-Fi networks currently in use remain susceptible to various attacks such as sniffing, spoofing, and brute-force, which can be exploited by malicious actors to steal sensitive information or gain unauthorized control of devices remotely. This study aims to conduct penetration testing on wireless systems and IoT devices within a safe and controlled virtual environment to identify potential security loopholes. The methodology involves setting up a virtual testbed using VirtualBox and the Kali Linux operating system, employing open-source tools such as Aircrack-ng, Nmap, Bettercap, and Wireshark. Attack simulations were carried out on wireless network configurations and virtual IoT devices under common scenarios such as credential theft, traffic surveillance, and denial-of-service (DoS) attempts. The test results indicate that several IoT devices remain highly vulnerable to basic attacks such as sniffing and brute-force login attempts, while wireless networks using WPA2 encryption are also exploitable under certain conditions. These findings highlight the urgent need to improve network security through stronger encryption standards, network segmentation, and device hardening. This study is expected to serve as a reference for developing open-source-based cybersecurity defense systems to protect IoT ecosystems from increasingly sophisticated threats.

Keywords:
Penetration Testing, Wireless Security, IoT, Open-Source Tools, Virtual Environment.

PENDAHULUAN

Dalam beberapa tahun terakhir, perkembangan teknologi jaringan nirkabel dan perangkat Internet of Things (IoT) mengalami pertumbuhan yang sangat pesat. Perangkat seperti smart TV, kamera pengawas, kunci pintar, serta sensor industri semakin banyak terhubung melalui jaringan nirkabel untuk mendukung otomatisasi, pemantauan jarak jauh, dan peningkatan efisiensi operasional. Fenomena ini menjadi bagian penting dari era digital dan Revolusi Industri 4.0.

Namun, di balik kemajuan tersebut, muncul berbagai permasalahan terkait keamanan data dan kerentanan sistem. Berbagai laporan keamanan, termasuk dari Open Web Application Security Project (OWASP), menunjukkan bahwa banyak perangkat IoT dikembangkan tanpa mempertimbangkan aspek keamanan secara memadai. Hal ini menyebabkan meningkatnya insiden peretasan, seperti kebocoran data, pengambilalihan kendali perangkat secara tidak sah, serta pemanfaatan perangkat IoT sebagai botnet untuk melancarkan serangan Distributed Denial-of-Service (DDoS). Selain itu, jaringan nirkabel yang menjadi infrastruktur utama konektivitas IoT juga masih rentan terhadap berbagai ancaman, seperti penggunaan enkripsi yang lemah, serangan man-in-the-middle (MITM), dan serangan brute-force.

Penelitian-penelitian sebelumnya umumnya membahas serangan terhadap jaringan Wi-Fi atau perangkat IoT secara terpisah. Sementara itu, penelitian yang mengintegrasikan pengujian keamanan jaringan nirkabel dan perangkat IoT dalam satu pendekatan penetration testing masih relatif terbatas. Oleh karena itu, penelitian ini bertujuan untuk menguji kerentanan sistem jaringan nirkabel dan perangkat IoT dalam lingkungan virtual yang aman dengan memanfaatkan berbagai tools open-source. Tujuan utama dari penelitian ini adalah untuk mengevaluasi tingkat kerentanan sistem serta memberikan rekomendasi strategi mitigasi guna mengurangi potensi ancaman siber di masa mendatang.

KAJIAN LITERATUR

Keamanan jaringan nirkabel dan perangkat Internet of Things (IoT) telah menjadi fokus berbagai penelitian dalam bidang keamanan siber. Kasinathan et al. (2013) menyatakan bahwa perangkat IoT sangat rentan terhadap serangan jaringan akibat penggunaan protokol komunikasi yang lemah serta kurangnya mekanisme autentikasi yang

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

kuat. Sementara itu, Sharma et al. (2020) melakukan analisis keamanan jaringan Wi-Fi menggunakan tools Aircrack-ng dan menunjukkan bahwa enkripsi WPA2 masih dapat ditembus melalui serangan brute-force, terutama ketika kata sandi yang digunakan bersifat lemah.

Penelitian lain yang dilakukan oleh Rahman et al. (2019) mengevaluasi efektivitas tools Wireshark dan Nmap dalam mendeteksi lalu lintas mencurigakan pada jaringan IoT. Hasil penelitian tersebut menunjukkan bahwa tools open-source memiliki potensi yang besar dalam mendukung proses pemantauan jaringan dan pengujian keamanan. Di sisi lain, Silva dan Alessi (2021) menyoroti keterbatasan simulasi lingkungan IoT secara virtual, khususnya dalam merepresentasikan perilaku perangkat IoT yang sebenarnya secara akurat.

Meskipun demikian, sebagian besar penelitian yang ada masih berfokus pada satu aspek saja, seperti pengujian keamanan jaringan nirkabel secara terpisah atau analisis kerentanan perangkat IoT secara individual. Penelitian yang menguji kedua komponen tersebut secara bersamaan dalam satu skenario penetration testing terintegrasi dengan memanfaatkan berbagai tools open-source di lingkungan virtual masih relatif terbatas. Kesenjangan penelitian inilah yang menjadi dasar dilakukannya penelitian ini, yaitu untuk mengevaluasi efektivitas pengujian penetration testing terhadap sistem jaringan nirkabel dan perangkat IoT secara terintegrasi dalam lingkungan simulasi virtual.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental dengan menerapkan teknik penetration testing untuk menguji tingkat keamanan jaringan nirkabel dan perangkat Internet of Things (IoT) dalam sebuah lingkungan virtual. Tujuan dari penelitian ini adalah untuk mengidentifikasi potensi kerentanan sistem dengan memanfaatkan tools open-source secara aman dan terkontrol.

Lingkungan Virtual

Lingkungan pengujian dibangun menggunakan VirtualBox sebagai platform virtualisasi pada sistem operasi host. Beberapa mesin virtual yang digunakan dalam penelitian ini antara lain :

1. Kali Linux sebagai sistem operasi utama untuk melakukan penetration testing.
2. Metasploitable dan emulator perangkat IoT sebagai target simulasi serangan.
3. Router virtual yang dikonfigurasi menggunakan hostapd dan dnsmasq untuk mensimulasikan jaringan nirkabel.

Tools yang Digunakan

Penelitian ini memanfaatkan beberapa tools open-source, yaitu :

1. Aircrack-ng : digunakan untuk menguji kerentanan autentikasi jaringan Wi-Fi (WEP/WPA2).
2. Wireshark : digunakan untuk analisis lalu lintas jaringan (sniffing).
3. Nmap : digunakan untuk pemindaian port dan identifikasi (fingerprinting) perangkat IoT.
4. Bettercap : digunakan untuk mensimulasikan serangan man-in-the-middle (MITM).
5. Metasploit Framework : digunakan untuk mengeksploitasi kerentanan tertentu yang teridentifikasi.

Tahapan Penelitian

Tahapan penelitian yang dilakukan meliputi :

1. Persiapan laboratorium virtual dan konfigurasi jaringan.
2. Pemindaian serta identifikasi perangkat target.
3. Simulasi serangan, seperti sniffing, spoofing, dan brute-force.
4. Pencatatan serta dokumentasi hasil pengujian.
5. Evaluasi dan analisis tingkat keberhasilan serangan.

HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan beberapa temuan berdasarkan skenario penetration testing yang diterapkan pada jaringan nirkabel dan perangkat Internet of Things (IoT) dengan memanfaatkan tools open-source dalam lingkungan virtual. Pengujian diklasifikasikan ke dalam tiga kategori utama, yaitu pemindaian jaringan dan perangkat, serangan pada jaringan nirkabel, serta serangan pada perangkat IoT.

Hasil Pemindaian Jaringan dan Perangkat

Berdasarkan hasil pemindaian menggunakan Nmap, sistem berhasil mendeteksi perangkat IoT simulasi beserta port terbuka yang aktif, seperti HTTP (80), SSH (22), dan Telnet (23). Selain itu, proses operating system dan service fingerprinting mampu mengungkap informasi detail, termasuk jenis sistem operasi dan layanan yang berjalan pada perangkat target.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Tabel 1. Hasil Pemindaian Jaringan dan Perangkat IoT

Target IP	Port Terbuka	Sistem Operasi	Layanan Utama
192.168.1.10	22, 80, 23	Embedded Linux 3.x	Dropbear SSH, HTTP, Telnet
192.168.1.11	80, 443	Ubuntu IoT Core	Apache2, SSL

Hasil ini menunjukkan bahwa perangkat IoT dengan port terbuka yang tidak dibatasi berpotensi menjadi target serangan jika tidak diamankan dengan baik.

Hasil Serangan pada Jaringan Nirkabel

Pengujian terhadap jaringan nirkabel dilakukan menggunakan Aircrack-ng. Proses penangkapan WPA2 handshake berhasil dilakukan, kemudian dilanjutkan dengan serangan dictionary attack. Hasil pengujian menunjukkan bahwa kata sandi jaringan berhasil ditemukan dalam waktu sekitar 25 menit.

Tabel 2. Hasil Serangan Jaringan Wi-Fi

SSID Target	Jenis Enkripsi	Status Handshake	Durasi Brute-Force	Status Kata Sandi
IoT_Wifi	WPA2	Berhasil Ditangkap	± 25 menit	Berhasil

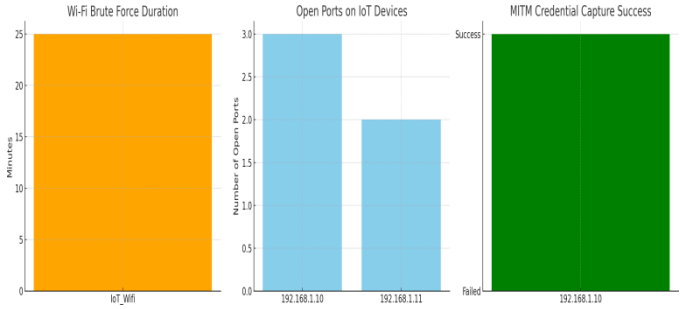
Temuan ini membuktikan bahwa penggunaan kata sandi yang lemah pada jaringan WPA2 masih sangat rentan terhadap serangan brute-force.

Hasil Serangan pada Perangkat IoT

Serangan terhadap perangkat IoT dilakukan menggunakan Bettercap dengan metode man-in-the-middle (MITM). Hasil pengujian menunjukkan bahwa lalu lintas HTTP dapat disadap (sniffing) dengan sukses. Selain itu, kredensial login dasar berhasil diperoleh menggunakan teknik brute-force sederhana.

Tabel 3. Hasil Serangan Perangkat IoT

Target IP	Protokol	Jenis Serangan	Status	Data yang Berhasil Dicegat
192.168.1.10	HTTP	MITM + Sniffing	Berhasil	Username: admin, Password: 1234



Gambar 1. Hasil Serangan Perangkat IoT

KESIMPULAN

Penelitian ini menunjukkan bahwa sistem jaringan nirkabel dan perangkat Internet of Things (IoT) masih rentan terhadap serangan dasar seperti brute-force, sniffing, dan man-in-the-middle. Melalui pengujian penetration testing dalam lingkungan virtual, ditemukan bahwa konfigurasi keamanan standar—seperti penggunaan protokol HTTP, port yang terbuka, serta kata sandi yang lemah—menjadi titik masuk utama bagi penyerang. Tools open-source terbukti efektif dalam mengidentifikasi dan mengeksploitasi kerentanan tersebut, sehingga menjadi solusi yang ekonomis untuk pengujian keamanan baik di lingkungan akademik maupun profesional.

Manfaat dari penelitian ini terletak pada penyediaan pendekatan yang praktis dan terjangkau untuk menilai tingkat keamanan sistem jaringan nirkabel dan IoT secara aman. Simulasi virtual memungkinkan pengujian dilakukan tanpa menimbulkan risiko terhadap jaringan di dunia nyata serta dapat direplikasi untuk keperluan pembelajaran atau pelatihan keamanan siber.

Namun, keterbatasan utama dari penelitian ini adalah ketergantungan pada perangkat IoT virtual, yang mungkin belum sepenuhnya mencerminkan perilaku dan kompleksitas perangkat fisik di lingkungan nyata. Oleh karena itu, penelitian selanjutnya disarankan untuk melibatkan lebih banyak perangkat IoT fisik dan menerapkan skenario serangan yang lebih kompleks. Selain itu, integrasi teknik machine learning juga dapat dieksplorasi untuk mendeteksi dan

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

mencegah serangan secara real-time.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Laboratorium Keamanan Siber Universitas Malikussaleh atas penyediaan lingkungan virtual dan sumber daya yang diperlukan untuk penelitian ini. Ucapan terima kasih khusus disampaikan kepada dosen pembimbing, T. Sukma Achriadi Sukiman, S.Kom., M.Kom., atas bimbingan dan dukungannya selama penelitian. Penelitian ini dilaksanakan secara mandiri tanpa dukungan dana atau hibah dari pihak luar.

REFERENSI

Setiawan, R., & Santoso, J. (2020). Analisis keamanan jaringan wireless menggunakan metode wardriving dan Wireshark. *Jurnal Teknologi dan Sistem Komputer*, 8(2), 125–131.

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing*, 21(2), 34–42.

Antunes, M., & Correia, M. (2011). Vulnerability detection of web applications in source code: A static analysis approach. *Journal of Internet Services and Applications*, 2(1), 5–16.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1), 20.

Liu, H., Ning, H., & Yang, Y. (2018). Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid. *IEEE Transactions on Vehicular Technology*, 67(3), 2837–2849.

Rahman, M. M., Rokonuzzaman, M., & Ahmed, M. (2019). IoT security: An end-to-end view and case study. *International Journal of Network Security & Its Applications*, 11(3), 1–15.

Silva, M., & Alessi, M. (2021). Simulation of attacks on IoT networks using open-source tools. *Journal of Cybersecurity Technology*, 5(1), 24–37.

Singh, S., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88–115.

Syafrudin, M., Fitriyani, N. L., Alfian, G., Rhee, J., & Hwang, J. (2019). Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing. *Sensors*, 19(18), 3867.

Hakim, L., & Yuliana, A. (2021). Uji penetrasi jaringan Wi-Fi menggunakan Aircrack-ng dan Kismet pada lingkungan virtual. *Jurnal Keamanan Siber Indonesia*, 4(1), 45–52.