E-ISSN: 2964-6219, P-ISSN: 2964-6200
Volume 4 Number 2 August 2026.
pp: 195-204. DOI: https://doi.org/10.58477/cj.v4i2.471.

Computer Journal

RESEARCH ARTICLE Open Access

Penerapan Metode OWASP *IoT Top 10* dalam Analisis Kerentanan Keamanan Perangkat *Internet of Things*: Studi Kasus *Smart Waste*

Arif Rahman Hakim [1*], **Rizki Surya Permana** [2], **Demi Adidrana** [3], **Hertanto Suryoprayogo** [4], **Deny Haryadi** [5]

[1*,3,4,] Center of Excellence for Intelligent Sensing-IoT, Research Institute of Sustainable Society, Telkom University, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, Indonesia.
[2] Program Studi Teknik Telekomunikasi Kampus Jakarta, Direktorat Kampus Jakarta, Universitas Telkom, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, Indonesia.
[5] The University Center of Excellence Human Centric Engineering (HUMIC), Telkom University, Indonesia.

*Correspondence email: arifhakimtukj@telkomuniversity.ac.id.

Received: 6 August 2026.
Revised: 7 August 2026.
Accepted: 24 August 2026.
Published: 30 August 2026.

Full list of author information is available at the end of the article.

Abstract

This study examines security vulnerabilities in a publicly accessible IoT-based smart waste system using Nmap, Wireshark, and OWASP ZAP to assess network services, packet traffic, and the web application layer. Results were mapped to the OWASP IoT Top 10 (2018). Because the assessment was external black-box testing without exploitation, the mapping is indicative rather than comprehensive. Nmap identified several active TCP ports, although only six open ports were explicitly documented. Wireshark captured 62,591 packets, indicating port-scanning activity and ongoing TCP communication. OWASP ZAP identified 14 web application weaknesses: six medium, five low, and three informational, with no high-risk findings. Four OWASP IoT Top 10 categories (I2, I3, I7, and I9) were supported by direct evidence, while I1 and I5 require further verification and I4, I6, I8, and I10 were outside the testing scope. Key risks involved insecure network services, default settings, and inadequate data protection during transmission and storage.

Keywords: Internet of Things; Network Security; OWASP IoT Top 10; Penetration Testing.

Abstrak

Penelitian ini mengkaji celah keamanan pada sistem smart waste berbasis IoT yang dapat diakses melalui domain publik menggunakan Nmap, Wireshark, dan OWASP ZAP untuk menguji layanan jaringan, lalu lintas paket, dan aplikasi web. Hasil pengujian dipetakan ke OWASP IoT Top 10 (2018). Karena menggunakan pengujian eksternal black-box tanpa eksploitasi, pemetaan bersifat indikatif dan tidak menyeluruh. Nmap mengidentifikasi sejumlah port TCP aktif, tetapi hanya enam port terbuka yang terdokumentasi secara eksplisit. Wireshark menangkap 62.591 paket yang menunjukkan aktivitas pemindaian port dan komunikasi TCP. OWASP ZAP menemukan 14 kelemahan aplikasi web, terdiri atas enam medium, lima low, dan tiga informational, tanpa temuan berisiko tinggi. Empat kategori OWASP IoT Top 10 (I2, I3, I7, dan I9) didukung bukti langsung, sedangkan I1 dan I5 memerlukan verifikasi lanjutan dan I4, I6, I8, serta I10 berada di luar cakupan pengujian. Risiko utama meliputi layanan jaringan tidak aman, konfigurasi bawaan tidak aman, serta perlindungan data yang belum memadai.

Kata Kunci: Internet of Things; Keamanan Jaringan; OWASP IoT Top 10; Penetration Testing.

1. Pendahuluan

Perkembangan teknologi Internet of Things (IoT) telah mengubah cara berbagai perangkat berinteraksi dan bertukar data melalui jaringan. Penerapan IoT semakin luas pada berbagai bidang, termasuk lingkungan rumah tangga, industri, layanan publik, dan pengelolaan fasilitas. Menurut Statista Research Department (2023), jumlah perangkat IoT yang terhubung secara global diperkirakan mencapai 29,4 miliar pada tahun 2030. Pertumbuhan jumlah perangkat tersebut diikuti oleh meningkatnya kompleksitas konektivitas dan potensi risiko keamanan siber. Kondisi ini menjadi perhatian karena sebagian perangkat IoT dikembangkan dengan prioritas pada fungsionalitas dan konektivitas, sementara aspek keamanan belum selalu menjadi bagian utama dalam perancangannya (Atzori *et al.*, 2010; Roman *et al.*, 2011). Ketergantungan terhadap jaringan, layanan web, kredensial, serta pertukaran data membuat perangkat IoT memiliki sejumlah titik yang berpotensi dimanfaatkan untuk memperoleh akses atau mengganggu layanan. Berbagai insiden keamanan menunjukkan bahwa kelemahan pada perangkat IoT dapat memberikan dampak yang luas. Salah satu contoh yang banyak dibahas adalah serangan Mirai Botnet pada tahun 2016 yang memanfaatkan jutaan perangkat IoT dengan kredensial default untuk membentuk jaringan botnet dan menyebabkan gangguan terhadap layanan DNS Dyn (Antonakakis *et al.*, 2017). Kerentanan keamanan juga ditemukan pada berbagai perangkat IoT rumah tangga dan komersial dalam penelitian lainnya (Sivaraman *et al.*, 2015; Siagian *et al.*, 2023). Temuan tersebut menunjukkan bahwa keamanan tidak hanya perlu diperhatikan pada perangkat secara individual, tetapi juga pada layanan jaringan, lalu lintas komunikasi, serta aplikasi yang menjadi bagian dari ekosistem IoT. Pengujian keamanan dengan cakupan yang terbatas pada satu komponen berpotensi tidak memberikan gambaran yang memadai mengenai kondisi keamanan sistem secara keseluruhan.

Open Web Application Security Project (OWASP) telah menerbitkan OWASP IoT Top 10 sebagai kerangka yang merangkum sepuluh kategori risiko keamanan utama pada perangkat dan sistem IoT (OWASP Foundation, 2018). Kerangka tersebut dapat digunakan sebagai acuan untuk mengidentifikasi dan mengklasifikasikan berbagai risiko yang ditemukan pada implementasi IoT. Dalam konteks pengujian keamanan, identifikasi kerentanan pada layanan jaringan, komunikasi data, dan aplikasi web dapat memberikan informasi yang saling melengkapi. Oleh karena itu, pemetaan temuan teknis terhadap kategori OWASP IoT Top 10 dapat membantu menghubungkan hasil pengujian dengan jenis risiko keamanan yang relevan. Sejumlah penelitian terdahulu telah melakukan evaluasi terhadap keamanan perangkat dan sistem IoT dengan pendekatan serta cakupan yang berbeda. Alrawi *et al.* (2019) melalui systematic review terhadap evaluasi keamanan IoT rumah tangga menemukan bahwa banyak penelitian berfokus pada komponen tertentu dalam ekosistem IoT, seperti perangkat, aplikasi seluler, atau cloud back-end, sehingga pengujian lintas komponen belum selalu dilakukan secara terintegrasi. Schiller *et al.* (2023) menerapkan pengujian penetrasi berbasis swarm pada jaringan smart home, sedangkan Kondru *et al.* (2025) melakukan asesmen kerentanan smart home melalui pengujian penetrasi konvensional. Murat *et al.* (2024) mengevaluasi keamanan firmware dan konektivitas perangkat smart home berbiaya rendah, sementara Utomo (2024) melakukan evaluasi kerentanan pada studi kasus smart home berbasis IoT di Indonesia. Penelitian-penelitian tersebut memberikan dasar penting bagi evaluasi keamanan IoT, tetapi memiliki objek, pendekatan, dan cakupan pengujian yang berbeda.

Berdasarkan penelitian terdahulu tersebut, masih terdapat ruang untuk menerapkan pengujian yang mencakup beberapa lapisan keamanan pada satu objek IoT yang dapat diakses secara publik. Penelitian ini menggunakan sistem smart waste berbasis IoT sebagai objek pengujian dan menerapkan pendekatan berlapis dengan tiga alat. Nmap digunakan untuk mengidentifikasi port dan layanan jaringan yang dapat diakses, Wireshark digunakan untuk mengamati pola lalu lintas paket, sedangkan OWASP ZAP digunakan untuk menguji sisi aplikasi web. Hasil dari ketiga pendekatan tersebut kemudian dipetakan terhadap OWASP IoT Top 10 (2018). Pendekatan ini memungkinkan temuan dari lapisan jaringan, lalu lintas komunikasi, dan aplikasi web dianalisis dalam satu kerangka klasifikasi. Namun, karena pengujian dilakukan secara eksternal dengan pendekatan black-box dan tanpa tahap eksploitasi, hasil pemetaan tidak dimaksudkan untuk menggambarkan seluruh kondisi keamanan sistem atau membuktikan kategori risiko yang memerlukan akses internal maupun eksploitasi langsung. Penelitian ini bertujuan untuk 1) mengidentifikasi kerentanan keamanan pada sistem smart waste berbasis IoT berdasarkan kerangka OWASP IoT Top 10; 2) menerapkan metodologi pengujian yang sistematis dan dapat direplikasi menggunakan Nmap, Wireshark, dan OWASP ZAP; dan 3) memberikan rekomendasi perbaikan yang praktis dan terukur berdasarkan temuan pengujian.

2. Landasan Teori

Penelitian mengenai keamanan IoT telah menggunakan berbagai pendekatan untuk mengidentifikasi kerentanan pada perangkat, jaringan, firmware, dan aplikasi. Sivaraman *et al*. (2015) mengusulkan mekanisme kontrol keamanan pada tingkat jaringan untuk perangkat smart home, sedangkan Siagian *et al*. (2023) menganalisis keamanan sistem IoT untuk pengendalian perangkat elektronik rumah tangga melalui pengujian kerentanan jaringan. Schiller *et al*. (2023) menerapkan pengujian penetrasi berbasis swarm pada jaringan smart home, sementara Kondru *et al*. (2025) melakukan asesmen kerentanan melalui pengujian penetrasi konvensional. Alrawi *et al*. (2019) melalui systematic review menunjukkan bahwa banyak penelitian keamanan IoT berfokus pada komponen tertentu tanpa mengintegrasikan pengujian lintas lapisan. Murat *et al*. (2024) mengevaluasi keamanan firmware dan konektivitas perangkat smart home berbiaya rendah, sedangkan Utomo (2024) melakukan evaluasi kerentanan pada studi kasus smart home berbasis IoT di Indonesia. Temuan-temuan tersebut menunjukkan beragam pendekatan dalam evaluasi keamanan IoT dengan cakupan yang berbeda pada setiap lapisan sistem. Penetration Testing Execution Standard (PTES) menyediakan kerangka proses umum untuk pengujian penetrasi, mulai dari pengintaian hingga pelaporan. Kerangka ini membantu mengorganisasi tahapan pengujian, tetapi tidak menyediakan taksonomi risiko yang secara khusus ditujukan untuk ekosistem IoT. Sebaliknya, OWASP IoT Top 10 (OWASP Foundation, 2018) menyediakan sepuluh kategori risiko yang mencerminkan karakteristik keamanan perangkat dan sistem IoT, termasuk *insecure default settings* dan *lack of physical hardening*. Dengan demikian, PTES dapat digunakan untuk mengatur proses pengujian, sedangkan OWASP IoT Top 10 digunakan untuk mengklasifikasikan temuan berdasarkan kategori risiko IoT. Penelitian ini menggunakan kedua kerangka tersebut sebagai dasar proses pengujian dan pemetaan hasil, sebagaimana dijelaskan pada bagian Metode. Sistem IoT yang terhubung dengan aplikasi web memiliki karakteristik keamanan yang berbeda dari aplikasi web konvensional karena melibatkan perangkat dengan keterbatasan sumber daya, layanan jaringan bawaan, serta mekanisme pembaruan keamanan yang dapat terbatas (Roman *et al*., 2011; Atzori *et al*., 2010). Lapisan web juga dapat menjadi salah satu titik akses terhadap sistem IoT sehingga konfigurasi keamanan yang tidak memadai, termasuk penerapan header keamanan dan kebijakan Content Security Policy, dapat menimbulkan risiko terhadap aplikasi dan data (Alrawi *et al*., 2019). Karakteristik tersebut menjadi dasar penerapan pengujian berlapis pada penelitian ini melalui pemeriksaan layanan jaringan, analisis lalu lintas, dan pengujian aplikasi web yang kemudian dipetakan ke dalam OWASP IoT Top 10.

3. Metode

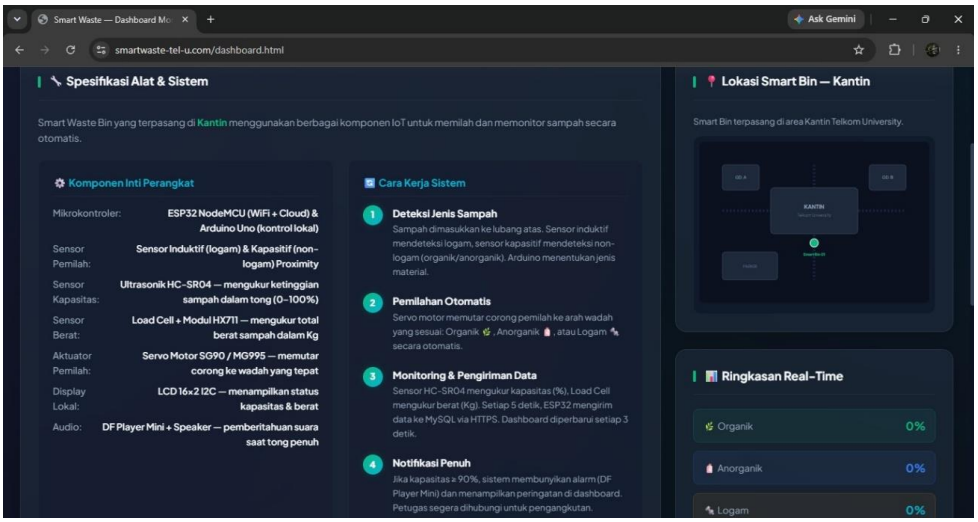
Penelitian ini menggunakan pendekatan eksperimental dengan metode pengujian penetrasi yang merujuk pada kerangka konseptual Penetration Testing Execution Standard (PTES) dan OWASP IoT Top 10. Pengujian dilakukan secara berlapis (*multi-layer security testing*) dari sisi eksternal dengan pendekatan *black-box*, tanpa akses terhadap kode sumber maupun konfigurasi internal sistem. Objek penelitian adalah sistem smart waste yang dapat diakses melalui domain publik dan selanjutnya disebut sebagai host target. Pengujian dilakukan secara non-intrusif dan tidak melibatkan eksekusi eksploitasi terhadap host target. Untuk menjaga etika keamanan dan integritas sistem produksi, identitas domain dan alamat IP host target tidak dicantumkan dalam naskah karena sebagian temuan keamanan, khususnya yang berkaitan dengan I2, I7, dan I9, belum dikonfirmasi telah diperbaiki oleh pihak pengelola. Rincian teknis temuan direkomendasikan untuk disampaikan kepada pengelola melalui mekanisme *responsible disclosure*. Tahapan pengujian yang benar-benar dilakukan meliputi 1) pemindaian jaringan menggunakan Nmap melalui antarmuka Zenmap dengan profil *Intense scan* dan perintah nmap -T4 -A -v <domain-target>; 2) penangkapan lalu lintas jaringan menggunakan Wireshark untuk menganalisis distribusi protokol, kombinasi flag TCP, dan kueri DNS; 3) pengujian keamanan aplikasi web menggunakan OWASP ZAP by Checkmarx versi 2.17.0 dalam mode pemindaian pasif terhadap host target melalui layanan HTTPS dan HTTP; dan 4) klasifikasi serta pemetaan temuan terhadap sepuluh kategori OWASP IoT Top 10 (2018).

Tabel 1. OWASP IoT Top 10 (2018)

No	Kategori	Deskripsi
I1	Weak, Guessable, or Hardcoded Passwords	Penggunaan kata sandi yang mudah ditebak, dapat di-brute force, atau hardcoded
I2	Insecure Network Services	Layanan jaringan yang tidak perlu atau tidak aman yang berjalan pada perangkat

I3	Insecure Ecosystem Interfaces	Antarmuka web, backend API, cloud, atau mobile yang tidak aman
I4	Lack of Secure Update Mechanism	Tidak adanya mekanisme pembaruan firmware yang aman
I5	Use of Insecure or Outdated Components	Penggunaan komponen perangkat lunak yang tidak aman atau sudah usang
I6	Insufficient Privacy Protection	Penyimpanan informasi sensitif pengguna secara tidak aman
I7	Insecure Data Transfer and Storage	Kurangnya enkripsi atau kontrol akses pada data sensitif
I8	Lack of Device Management	Tidak adanya dukungan manajemen keamanan perangkat di lingkungan produksi
I9	Insecure Default Settings	Perangkat dikirimkan dengan konfigurasi default yang tidak aman
I10	Lack of Physical Hardening	Tidak adanya perlindungan fisik yang memungkinkan akses tidak sah

Objek penelitian berupa sistem Smart Waste berbasis Internet of Things (IoT), yaitu sistem tempat sampah pintar yang dirancang untuk melakukan pemantauan (*monitoring*) dan pemilahan sampah secara otomatis pada area kantin. Sistem ini mendukung pengelolaan sampah melalui identifikasi jenis sampah, pemantauan kapasitas tempat sampah secara *real-time*, dan penyajian informasi melalui aplikasi berbasis web. Smart Waste mengklasifikasikan sampah ke dalam tiga kategori, yaitu organik, anorganik, dan logam. Proses identifikasi menggunakan kombinasi sensor induktif untuk mendeteksi material logam dan sensor *proximity* kapasitif untuk membedakan sampah non-logam. Setelah jenis sampah dikenali, aktuator berupa *servo motor* mengarahkan sampah ke wadah yang sesuai secara otomatis, sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. Tampilan objek pengujian web perangkat IoT.

Sistem Smart Waste menggunakan sensor induktif dan sensor *proximity* kapasitif untuk mengidentifikasi jenis sampah, kemudian servo motor mengarahkan sampah ke wadah yang sesuai secara otomatis, sebagaimana ditunjukkan pada Gambar 1. Pengujian menggunakan Nmap, Wireshark, dan OWASP ZAP. Nmap digunakan untuk pemindaian port dan layanan jaringan, Wireshark digunakan untuk menangkap dan menganalisis lalu lintas jaringan, sedangkan OWASP ZAP digunakan untuk menguji keamanan antarmuka aplikasi web dan API. Kerangka PTES secara umum mencakup tahapan *Reconnaissance*, *Vulnerability Scanning*, *Exploitation*, *Post-Exploitation*, dan *Reporting*. Dalam penelitian ini, pengujian dibatasi pada aktivitas pengumpulan informasi, pemindaian jaringan dan layanan, analisis lalu lintas jaringan, serta pengujian pasif pada aplikasi web. Tahap *Exploitation* dan *Post-Exploitation* tidak dilakukan karena penelitian menggunakan pendekatan *black-box* eksternal yang bersifat non-intrusif. Hasil pengujian selanjutnya didokumentasikan dan dipetakan ke dalam OWASP IoT Top 10 (2018).

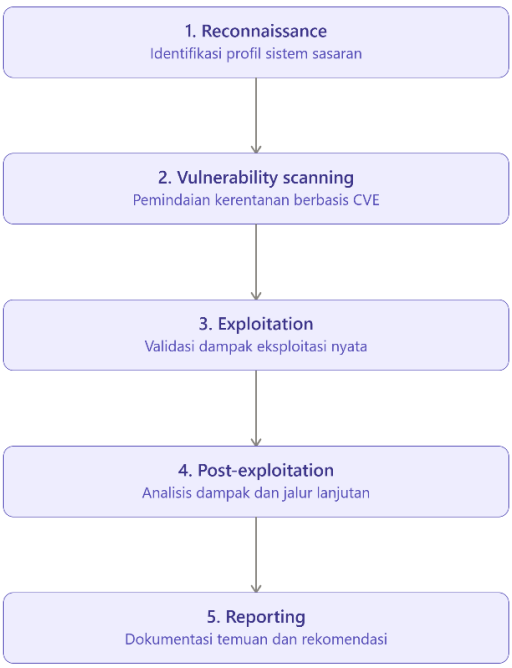
1) Reconnaissance.
   Tahap ini dilakukan untuk memperoleh informasi mengenai host target dan layanan yang dapat diakses dari sisi eksternal. Informasi dikumpulkan melalui pemindaian jaringan menggunakan Nmap, termasuk identifikasi port dan layanan yang merespons pada host target.
2) Vulnerability Scanning.
   Tahap ini dilakukan melalui pemeriksaan layanan jaringan dan aplikasi web menggunakan Nmap dan OWASP ZAP. Nmap digunakan untuk mengidentifikasi port serta layanan yang tersedia, sedangkan OWASP ZAP

digunakan dalam mode pemindaian pasif untuk mengidentifikasi kelemahan pada lapisan aplikasi web tanpa melakukan eksploitasi terhadap host target.

3) Exploitation.
Tahap eksploitasi tidak dilakukan. Penelitian hanya mengidentifikasi dan mendokumentasikan temuan berdasarkan hasil pengujian non-intrusif sehingga tidak dilakukan upaya untuk memperoleh akses tidak sah atau mengeksploitasi kerentanan pada host target.

4) Post-Exploitation.
Tahap pascaeksploitasi tidak dilakukan karena tidak terdapat aktivitas eksploitasi terhadap host target. Oleh karena itu, penelitian tidak melakukan analisis persistensi akses, pergerakan lateral, atau perluasan kompromi terhadap perangkat dan jaringan terkait.

5) Reporting.
Seluruh hasil pengujian didokumentasikan berdasarkan bukti yang diperoleh dari Nmap, Wireshark, dan OWASP ZAP. Temuan kemudian diklasifikasikan dan dipetakan terhadap kategori OWASP IoT Top 10 (2018) sesuai dengan bukti yang tersedia. Rekomendasi perbaikan disusun berdasarkan temuan yang dapat didukung oleh hasil pengujian.



Gambar 2. Tahapan pengujian.

Alur pengujian keamanan dilakukan melalui pengumpulan informasi, pemindaian jaringan dan layanan, analisis lalu lintas jaringan, pengujian pasif aplikasi web, serta pemetaan temuan ke OWASP IoT Top 10, sebagaimana ditunjukkan pada Gambar 2.

4. Hasil dan Pembahasan

4.1 Hasil

Pemindaian menggunakan Zenmap (Nmap) dengan profil Intense scan dan perintah nmap -T4 -A -v <domain-target> menunjukkan bahwa SYN Stealth Scan terhadap 1.000 port default selesai dalam waktu 42,30 detik. Service and version scan dijalankan melalui dua kali eksekusi Nmap pada rentang waktu yang berbeda. Log progres kedua eksekusi tersebut melaporkan jumlah layanan yang diperiksa sedikit berbeda, yaitu 927 dan 931 layanan, sehingga pada penelitian ini dilaporkan sebagai rentang 927–931 layanan dengan durasi total sekitar 1.946,42 detik (±32 menit). Selisih empat layanan tersebut berasal dari perbedaan status port antar-eksekusi dan penggabungan hasil kedua pemindaian, bukan dari satu kali pemindaian tunggal. Log yang tersedia tidak memuat rekap akhir jumlah total port terbuka. Hanya enam port yang secara eksplisit terdokumentasi pada tangkapan layar log pemindaian, sebagaimana ditunjukkan pada Tabel 2. Dengan demikian, Tabel 2 merupakan cuplikan port yang teridentifikasi dan bukan enumerasi lengkap seluruh port terbuka pada host target.

Tabel 2. Sebagian Port Terbuka yang Terdeteksi pada Log Pemindaian Nmap.

Port	Protokol	Status	Keterangan
1259/tcp	TCP	Open (SYN,ACK)	Terdeteksi terbuka pada tahap SYN Stealth Scan
2909/tcp	TCP	Open (SYN,ACK)	Terdeteksi terbuka pada tahap SYN Stealth Scan
5666/tcp	TCP	Open (SYN,ACK)	Umum digunakan oleh layanan monitoring (mis. NRPE)
2702/tcp	TCP	Open (SYN,ACK)	Terdeteksi terbuka, muncul dua kali pada log pemindaian
5200/tcp	TCP	Open (SYN,ACK)	Terdeteksi terbuka pada tahap SYN Stealth Scan
6789/tcp	TCP	Open (SYN,ACK)	Terdeteksi terbuka pada tahap SYN Stealth Scan

Karena jumlah total port terbuka tidak terdokumentasi secara lengkap, ukuran permukaan serangan tidak dapat ditentukan secara pasti dari hasil pemindaian yang tersedia. Durasi *service and version scan* sekitar 32 menit untuk 927–931 layanan yang diperiksa menunjukkan bahwa proses pemeriksaan berlangsung relatif lama, tetapi durasi tersebut tidak dapat digunakan sebagai ukuran langsung luasnya permukaan serangan. Oleh karena itu, interpretasi mengenai luasnya permukaan serangan perlu diverifikasi melalui pemindaian ulang yang mendokumentasikan seluruh port terbuka secara lengkap. Berkas tangkapan lalu lintas (*pcapng*) yang direkam selama sesi pengujian berisi 62.591 paket dengan total ukuran 9.783.668 byte. Distribusi protokol pada berkas tangkapan ditunjukkan pada Tabel 3.

Tabel 3. Distribusi Protokol pada Berkas Tangkapan Wireshark

Protokol	Jumlah Paket	Persentase	Keterangan
TCP	51.400	82,1%	Didominasi lalu lintas ke/dari host target 145.79.9.28
IPv6 (lain-lain)	10.624	17,0%	Lalu lintas latar belakang perangkat penguji, tidak terkait target
UDP	486	0,8%	Termasuk 470 kueri DNS
ARP	78	0,1%	Broadcast pada jaringan lokal
ICMP	3	0,0%	Paket kontrol/diagnostik
Total	62.591	100%	9.783.668 byte data tertangkap

Lalu lintas TCP merupakan protokol yang paling dominan dengan 51.400 paket atau 82,1% dari keseluruhan tangkapan. Lalu lintas IPv6 berjumlah 10.624 paket atau 17,0% dan diidentifikasi sebagai lalu lintas latar belakang perangkat penguji yang tidak berkaitan langsung dengan host target. Untuk melihat karakteristik lalu lintas TCP secara lebih rinci, distribusi kombinasi flag TCP ditunjukkan pada Tabel 4.

Tabel 4. Distribusi Kombinasi Flag TCP pada Lalu Lintas Tertangkap

Kombinasi Flag TCP	Jumlah Paket	Interpretasi
ACK	17.321	Paket penegasan pada sesi yang sudah terbentuk
SYN, ACK	8.792	Respons pembentukan koneksi dari host tujuan
SYN	7.970	Permintaan pembentukan koneksi (probe pemindaian port)
ACK, PSH	6.030	Pengiriman data pada sesi aktif
ACK, RST	5.881	Penolakan/penghentian paksa koneksi oleh salah satu pihak
ACK, FIN	5.387	Penutupan sesi secara normal (graceful close)
RST	19	Penolakan koneksi tanpa sesi aktif sebelumnya

Jumlah paket SYN murni sebanyak 7.970 paket menunjukkan adanya aktivitas pembentukan koneksi atau probe pemindaian port yang konsisten dengan proses SYN Stealth Scan pada Nmap. Sementara itu, 5.881 paket dengan kombinasi ACK, RST menunjukkan adanya koneksi yang dihentikan atau ditolak selama sesi pengujian. Analisis kueri DNS menunjukkan bahwa sebagian besar kueri yang tertangkap tidak berkaitan langsung dengan domain smartwaste-[diredaksi], melainkan berasal dari aktivitas latar belakang pada perangkat penguji. Dengan demikian, berkas tangkapan tidak sepenuhnya terisolasi terhadap host target dan memerlukan penyaringan lebih lanjut untuk memperoleh gambaran lalu lintas yang lebih spesifik. Pemeriksaan payload pada lalu lintas HTTP melalui port 80/8080 menemukan sedikit indikasi permintaan HTTP teks-jelas, sedangkan sebagian besar sesi menggunakan HTTPS. Pengujian menggunakan OWASP ZAP by Checkmarx versi 2.17.0 dalam mode pemindaian pasif terhadap layanan HTTPS dan HTTP pada host target mengidentifikasi 14 temuan keamanan tanpa temuan berisiko *High*. Distribusi temuan berdasarkan tingkat risiko dan tingkat keyakinan ditunjukkan pada Tabel 5.

Tabel 5. Distribusi Temuan OWASP ZAP Berdasarkan Risiko dan Keyakinan

Risiko	User Confirmed	High	Medium	Low	Total
High	0	0	0	0	0 (0,0%)
Medium	0	5	1	0	6 (42,9%)
Low	0	1	3	1	5 (35,7%)
Informational	0	0	2	1	3 (21,4%)
Total	0	6 (42,9%)	6 (42,9%)	2 (14,3%)	14 (100%)

Temuan risiko *Medium* terdiri atas enam temuan atau 42,9%, yang mencakup kelemahan konfigurasi Content Security Policy (CSP), penggunaan direktif unsafe-inline pada script-src dan style-src, penggunaan direktif wildcard, tidak adanya *fallback directive*, *Sub Resource Integrity Attribute Missing*, dan *Missing Anti-clickjacking Header*. Temuan risiko *Low* berjumlah lima atau 35,7%, yang mencakup *Strict-Transport-Security Header Not Set*, *X-Content-Type-Options Header Missing*, *Cross-Domain JavaScript Source File Inclusion*, *Big Redirect Detected*, dan *Timestamp Disclosure - Unix*. Tiga temuan *Informational* atau 21,4% terdiri atas *Information Disclosure - Suspicious Comments* pada berkas js/auth.js dan *Re-examine Cache-control Directives*. Temuan dari Nmap, Wireshark, dan OWASP ZAP dipetakan terhadap sepuluh kategori OWASP IoT Top 10 (2018) untuk mengidentifikasi kategori yang dapat dinilai berdasarkan bukti pengujian.

Tabel 6. Pemetaan Temuan Pengujian terhadap Kategori OWASP IoT Top 10

Kode	Kategori	Bukti/Temuan Terkait	Tingkat Risiko	Catatan
I1	Weak, Guessable, or Hardcoded Passwords	ZAP: komentar mencurigakan pada js/auth.js berpotensi memuat informasi kredensial/logika autentikasi sisi klien	Perlu verifikasi	Tidak diuji langsung (brute force/credential test tidak dilakukan)
I2	Insecure Network Services	Nmap: sejumlah besar port TCP merespons probe SYN pada rentang 1-1000, termasuk port non-standar dan layanan legacy	Tinggi	Permukaan serangan jaringan luas; perlu audit firewall/security group
I3	Insecure Ecosystem Interfaces	ZAP: CSP lemah, Missing Anti-clickjacking Header, Sub Resource Integrity Attribute Missing	Sedang	Antarmuka web belum menerapkan kontrol keamanan berlapis
I4	Lack of Secure Update Mechanism	Tidak ada bukti langsung dari ketiga alat	Tidak dapat dinilai	Di luar cakupan pengujian black-box
I5	Use of Insecure or Outdated Components	Nmap (deteksi versi/OS) mengindikasikan potensi komponen/OS lama; belum dikonfirmasi versi spesifik	Perlu verifikasi	Perlu fingerprinting versi lebih lanjut
I6	Insufficient Privacy Protection	Wireshark: lalu lintas ke domain pihak ketiga tercampur pada berkas tangkapan (bukan dari sistem target)	N/A	Bukan temuan pada sistem smart waste, melainkan lingkungan penangkapan
I7	Insecure Data Transfer and Storage	ZAP: Strict-Transport-Security Header Not Set, Cross-Domain JavaScript Source File Inclusion, Big Redirect Detected	Tinggi	Risiko downgrade HTTPS dan kebocoran informasi saat transfer data
I8	Lack of Device Management	Tidak ada bukti langsung dari ketiga alat	Tidak dapat dinilai	Pengujian tidak menyasar antarmuka manajemen perangkat IoT fisik
I9	Insecure Default Settings	Nmap: banyak port pada rentang default/well-known merespons aktif, mengindikasikan layanan bawaan belum dinonaktifkan	Tinggi	Konfigurasi default server tampak belum di-hardening

I10	Lack of Physical Hardening	Tidak ada pengujian fisik yang dilakukan	Tidak dapat dinilai	Di luar cakupan pengujian jarak jauh (remote testing)

Hasil pemetaan menunjukkan bahwa empat kategori, yaitu I2, I3, I7, dan I9, memiliki bukti langsung dari pengujian yang dilakukan. Kategori I1 dan I5 memerlukan verifikasi lebih lanjut karena bukti yang tersedia belum cukup untuk memastikan keberadaan kerentanan secara langsung. Sementara itu, I4, I6, I8, dan I10 tidak dapat dinilai secara memadai berdasarkan cakupan pengujian *black-box* jarak jauh.

4.2 Pembahasan

Hasil pengujian menunjukkan bahwa sistem Smart Waste memiliki temuan keamanan pada beberapa lapisan, terutama layanan jaringan dan antarmuka aplikasi web. Pada lapisan jaringan, Nmap mengidentifikasi enam port yang secara eksplisit terdokumentasi sebagai terbuka pada log yang tersedia. Namun, karena log tidak menyediakan rekap keseluruhan port terbuka, hasil tersebut tidak dapat digunakan untuk menyatakan jumlah pasti permukaan serangan. Temuan pada I2 dan I9 karena itu perlu dipahami sebagai indikasi konfigurasi layanan yang dapat memerlukan hardening, bukan sebagai ukuran definitif luasnya permukaan serangan. Pemindaian ulang dengan dokumentasi seluruh port terbuka diperlukan untuk memastikan kondisi tersebut. Pada lapisan lalu lintas jaringan, dominasi TCP sebesar 82,1% konsisten dengan aktivitas pemindaian Nmap dan komunikasi berbasis HTTP/HTTPS selama pengujian. Keberadaan 7.970 paket SYN serta 8.792 paket SYN, ACK juga konsisten dengan aktivitas pembentukan koneksi dan pemindaian port. Namun, karena tangkapan lalu lintas mencakup trafik latar belakang perangkat penguji, terutama IPv6 dan kueri DNS, hasil Wireshark tidak seluruhnya merepresentasikan komunikasi sistem Smart Waste. Kondisi ini membatasi interpretasi lalu lintas dan menunjukkan perlunya penyaringan berdasarkan alamat IP host target pada analisis lanjutan. Pada lapisan aplikasi web, OWASP ZAP menemukan 14 temuan yang terdiri atas enam temuan Medium, lima Low, dan tiga Informational, tanpa temuan High. Temuan tersebut terutama berkaitan dengan konfigurasi CSP, header keamanan, integritas sumber daya, dan konfigurasi transport. Temuan Strict-Transport-Security Header Not Set menunjukkan bahwa kebijakan HSTS belum diterapkan pada tingkat yang terdeteksi oleh ZAP. Sementara itu, temuan CSP dan Missing Anti-clickjacking Header menunjukkan adanya kontrol keamanan aplikasi web yang masih dapat diperbaiki. Temuan-temuan tersebut mendukung klasifikasi I3 dan sebagian aspek I7, tetapi tidak dengan sendirinya membuktikan adanya eksploitasi atau kebocoran data aktual karena penelitian tidak melakukan tahap eksploitasi.

Jika dibandingkan dengan penelitian terdahulu, pola temuan pada penelitian ini memiliki kesamaan dengan permasalahan keamanan IoT yang telah dilaporkan sebelumnya. Alrawi *et al*. (2019) menunjukkan bahwa banyak evaluasi keamanan IoT rumahan berfokus pada komponen tertentu dan menemukan pentingnya pemeriksaan lintas komponen dalam memahami postur keamanan ekosistem. Dalam penelitian ini, pengujian dilakukan pada lapisan jaringan, lalu lintas, dan aplikasi web sehingga temuan dapat dipetakan secara terpadu ke OWASP IoT Top 10. Temuan pada layanan jaringan dan konfigurasi yang perlu diperketat juga memiliki kesamaan pola dengan permasalahan keamanan yang dibahas dalam penelitian terdahulu, meskipun hasil tersebut tidak dapat digunakan untuk menyatakan bahwa sistem Smart Waste memiliki tingkat risiko yang sama dengan objek penelitian lain. Temuan terkait keamanan komunikasi juga memiliki kesamaan dengan hasil Murat *et al*. (2024), yang melaporkan permasalahan pada mekanisme keamanan komunikasi pada perangkat smart home berbiaya rendah. Dalam penelitian ini, indikasi tersebut terutama terlihat melalui temuan ZAP terkait HSTS dan beberapa konfigurasi keamanan aplikasi web. Kesamaan tersebut menunjukkan bahwa konfigurasi keamanan pada lapisan komunikasi dan aplikasi tetap menjadi aspek yang perlu diperhatikan dalam sistem IoT berbasis web. Namun, karena objek, lingkungan, dan metode pengujian berbeda, perbandingan tersebut sebaiknya dipahami sebagai kesamaan pola temuan, bukan sebagai perbandingan tingkat keamanan secara langsung. Secara keseluruhan, hasil penelitian menunjukkan bahwa pendekatan pengujian berlapis dapat memberikan gambaran yang lebih terstruktur mengenai aspek keamanan yang terlihat dari sisi eksternal. Nmap memberikan informasi mengenai layanan jaringan yang dapat diakses, Wireshark memberikan konteks mengenai pola lalu lintas selama pengujian, sedangkan OWASP ZAP mengidentifikasi kelemahan pada lapisan aplikasi web. Meskipun demikian, cakupan black-box dan ketiadaan eksploitasi membatasi kemampuan penelitian untuk memastikan beberapa kategori OWASP IoT Top 10, terutama yang berkaitan dengan mekanisme pembaruan, privasi internal, manajemen perangkat, perlindungan fisik, dan kredensial. Oleh karena itu, temuan penelitian perlu dipandang sebagai hasil asesmen eksternal yang bersifat indikatif, bukan sebagai representasi menyeluruh dari seluruh kondisi keamanan sistem Smart Waste.

5. Kesimpulan

Penelitian ini menunjukkan bahwa sistem smart waste berbasis IoT memiliki risiko keamanan terutama pada lapisan jaringan, konfigurasi layanan, dan keamanan transport data. Pengujian menggunakan Nmap, Wireshark, dan OWASP ZAP mengidentifikasi sejumlah layanan jaringan yang merespons aktif, pola lalu lintas yang konsisten dengan aktivitas pemindaian port, serta 14 kelemahan pada aplikasi web tanpa temuan berisiko High. Pemetaan terhadap OWASP IoT Top 10 menunjukkan bahwa kategori yang dapat dinilai dengan bukti langsung adalah I2, I3, I7, dan I9, dengan risiko utama pada Insecure Network Services (I2), Insecure Data Transfer and Storage (I7), dan Insecure Default Settings (I9). Penelitian ini memiliki keterbatasan karena menggunakan pengujian black-box jarak jauh dan non-intrusif sehingga eksploitasi dan pascaeksploitasi tidak dilakukan. Selain itu, jumlah total port terbuka tidak terdokumentasi secara lengkap, sedangkan kategori I1 dan I5 masih memerlukan verifikasi dan I4, I6, I8, serta I10 berada di luar cakupan pengujian. Oleh karena itu, hasil penelitian ini merupakan penilaian awal dan perlu dikonfirmasi melalui pengujian lanjutan dengan cakupan serta dokumentasi yang lebih lengkap. Perbaikan keamanan disarankan melalui audit dan penyederhanaan aturan firewall, penonaktifan layanan bawaan yang tidak diperlukan, penerapan Strict-Transport-Security dan X-Content-Type-Options, serta penguatan Content Security Policy dengan menghindari penggunaan unsafe-inline dan wildcard. Pengujian lanjutan juga diperlukan untuk mengevaluasi mekanisme pembaruan firmware, manajemen perangkat, dan kategori OWASP IoT Top 10 yang belum dapat dinilai. Untuk menjaga etika keamanan, identitas domain dan alamat IP target tetap dirahasiakan dan rincian kerentanan yang belum terverifikasi diperbaiki sebaiknya disampaikan melalui mekanisme responsible disclosure.

Referensi

Aljabbar, J. P., Rajaguguk, M. R. F., & Wijaya, N. (2025). Studi literatur keamanan data dalam sistem smart home berbasis IoT. *Device: Journal of Information System, Computer Science and Information Technology, 6*(1), 245–255.

Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). SoK: Security evaluation of home-based IoT deployments. *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 1362–1380.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai botnet. *Proceedings of the 26th USENIX Security Symposium*, 1093–1110.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

Burhani, L. F., & Priyawati, D. (2024). Analisis pengujian keamanan website pengelolaan internet Desa Kragan menggunakan metode Penetration Testing Execution Standard (PTES). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 9*(1), 307–319. https://doi.org/10.29100/jipi.v9i1.4455

Fahlevi, M. R., Sharipuddin, Kurniabudi, & Medika, D. C. (2026). Analisis keamanan aplikasi web menggunakan penetration testing berdasarkan standar OWASP pada DVWA. *Jurnal PROCESSOR, 21*(1).

Fiay, H. D., & Pakereng, M. A. I. (2026). Analisis keamanan jaringan WiFi dan CCTV menggunakan Zenmap sebagai network vulnerability scanner. *INTECOMS: Journal of Information Technology and Computer Science, 9*(2), 52–64. https://doi.org/10.31539/dr1nrv25

Firdaus, R. A. R. B., & Widyawan, T. I. (2025). Pengujian kerentanan website menggunakan metode penetration testing dengan OWASP (Studi kasus: Pemerintah Kabupaten Semarang). *CyberSecurity dan Forensik Digital, 8*(2), 106–115.

Kondru, K., Kancharla, P., Darlanka, M., & Sathuluri, B. C. (2025). Smart home, it's vulnerability assessment through penetration testing. *Journal of Informatics Electrical and Electronics Engineering (JIEEE), 6*(1), 1–7.

Murat, K., Topyła, D., Zdulski, K., Marzęcki, M., Bieniasz, J., Paczesny, D., & Szczypiorski, K. (2024). Security analysis of low-budget IoT smart home appliances embedded software and connectivity. *Electronics, 13*(12), 2371. https://doi.org/10.3390/electronics13122371

Nurelasari, E., & Al Farabi, D. G. (2024). Analisis keamanan sistem website menggunakan metode Open Web Application Security Project (OWASP) pada SIMANTEP.ID. *JATI (Jurnal Mahasiswa Teknik Informatika), 8*(3), 3049–3054.

OWASP Foundation. (2018). *OWASP IoT Top 10 2018*. https://owasp.org/www-project-internet-of-things/

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine, 7*(4), 6–14.

Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. *Computer, 44*(9), 51–58.

Schiller, T., Caulkins, B., Wu, A. S., & Mondesire, S. (2023). Security awareness in smart homes and Internet of Things networks through swarm-based cybersecurity penetration testing. *Information, 14*(10), 536. https://doi.org/10.3390/info14100536

Siagian, E. M. P., Siregar, J., & Siahaan, R. H. (2023). Analisis keamanan pada sistem Internet of Things untuk pengendalian perangkat elektronik rumah tangga. *Jurnal Teknologi Informasi dan Industri, 4*(1), 45–53.

Silmina, E. P., Firdonsyah, A., & Amanda, R. A. A. (2022). Analisis keamanan jaringan sistem informasi sekolah menggunakan penetration test dan ISSAF. *Transmisi: Jurnal Ilmiah Teknik Elektro, 24*(3), 83–91. https://doi.org/10.14710/transmisi.24.3.83-91

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. *Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 163–167.

Statista Research Department. (2023). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030*. Statista.

Supangat, S., Amna, A. R., & Rochman, M. Y. F. (2025). Penetration testing and vulnerability analysis of SINTA platform to strengthen privacy and data protection. *Journal of Information Technology and Cyber Security, 3*(2), 79–83. https://doi.org/10.30996/jitcs.12216

Utomo, I. C. (2024). Evaluasi kerentanan keamanan pada perangkat IoT: Studi kasus pada smart home. *The Indonesian Journal of Computer Science, 13*(3). https://doi.org/10.33022/ijcs.v13i3.3994

How Cites

Hakim, A. R., Permana, R. S., Adidrana, D., Suryoprayogo, H., & Haryadi, D. (2026). Penerapan Metode OWASP IoT Top 10 dalam Analisis Kerentanan Keamanan Perangkat Internet of Things: Studi Kasus Smart Waste. *Computer Journal*, *4*(2), 195-204. https://doi.org/10.58477/cj.v4i2.471.

Publisher's Note