

Evaluasi Kerentanan Keamanan Pada Perangkat IoT: Studi Kasus Pada *Smart Home*

Ihsan Cahyo Utomo¹, Nurul Kholisatul 'Ulya², Karmila Muhammad Izudin Rojak³

icu88@ums.ac.id, nurul.kholisatul@itspku.ac.id, l200200251@student.ums.ac.id

^{1,3}Universitas Muhamadyah Surakarta

²ITS PKU Muhamadiyah Surakarta

Informasi Artikel

Diterima : 9 Mei 2024

Direview : 16 Mei 2024

Disetujui : 15 Jun 2024

Kata Kunci

Internet of things,
Smart home,
Keamanan

Abstrak

Kehadiran *Internet of things* (IoT) telah mengubah cara berinteraksi dengan perangkat elektronik dalam lingkungan sehari-hari. Salah satu implementasi dari IOT adalah *smart home*, di mana otomatisasi berbagai perangkat dalam rumah terhubung secara *online* untuk meningkatkan kenyamanan dan efisiensi. Namun, dalam penerapan *smart home* ada tantangan pada sisi keamanan. Karena aplikasi *smart home* terhubung dengan internet, hal tersebut menyebabkan kerentanan terhadap serangan keamanan seperti serangan hak akses, virus dan malware. Penelitian ini membahas perlunya evaluasi keamanan pada perangkat *smart home*, hal tersebut dikarenakan Karakteristik *smart home* yang heterogen, dinamis dan terhubung dengan jaringan internet, sehingga memiliki potensi kerentanan dari serangan siber. Tujuan dari penelitian ini adalah mengevaluasi kerentanan keamanan pada perangkat IoT dalam konteks *smart home*. Melalui studi kasus yang mencakup berbagai perangkat yang umumnya ditemukan dalam *smart home*, salah satunya adalah potensi kerentanan dan risiko keamanan yang terkait dengan penggunaan perangkat IoT. Metode penelitian yang digunakan mencakup pengujian penetrasi, analisis kerentanan, dan evaluasi kebijakan keamanan yang diterapkan. Hasil penelitian ini dapat memberikan gambaran tentang potensi risiko keamanan pada perangkat IoT dalam *smart home* dan membantu mengembangkan model perlindungan yang lebih kuat dalam menghadapi tantangan keamanan yang terus berkembang di penerapan IoT.

Keywords

Internet of things, Smart home, Security

Abstract

The presence of the Internet of things (IoT) has changed the way of interacting with electronic devices in everyday environments. One implementation of IoT is a smart home, where the automation of various devices in the home is connected online to increase comfort and efficiency. However, in implementing a smart home there are challenges on the security side. Because smart home applications are connected to the internet, they are vulnerable to security attacks such as access rights attacks, viruses and malware. This research discusses the need for security evaluation on smart home devices, this is because the characteristics of smart homes are heterogeneous, dynamic and connected to the internet network, so they have potential vulnerabilities from cyber attacks. The aim of this research is to evaluate security vulnerabilities in IoT devices in the context of a smart home. Through case studies covering various devices commonly found in smart homes, one of which is the potential vulnerabilities and security risks associated with the use of IoT devices. The research methods used include penetration testing, vulnerability analysis, and evaluation of implemented security policies. The results of this research can provide an overview of potential security risks to IoT devices in smart homes and help develop stronger protection models to face the growing security challenges in IoT applications.

A. Pendahuluan

Era Industri 4.0 telah membawa perubahan dalam cara berinteraksi dengan lingkungan sekitar. Salah satu pilar dari revolusi Industri 4.0 adalah *Internet of things* (IoT). IoT memungkinkan perangkat elektronik untuk terhubung, berkomunikasi, dan berbagi data melalui jaringan internet. Konsep ini telah merambah ke berbagai aspek kehidupan kita, termasuk dalam pembentukan "*smart home*" yang semakin populer. *Smart home* merupakan teknologi yang menggabungkan layanan dan teknologi melalui jaringan internet yang terdiri dari berbagai perangkat IoT [1]. Beberapa contoh penggunaan perangkat *Smart home* adalah lampu pintar, termostat cerdas, kamera keamanan, dan perangkat elektronik lainnya, untuk menciptakan lingkungan rumah yang lebih nyaman, efisien, dan terhubung ke jaringan internet[2].

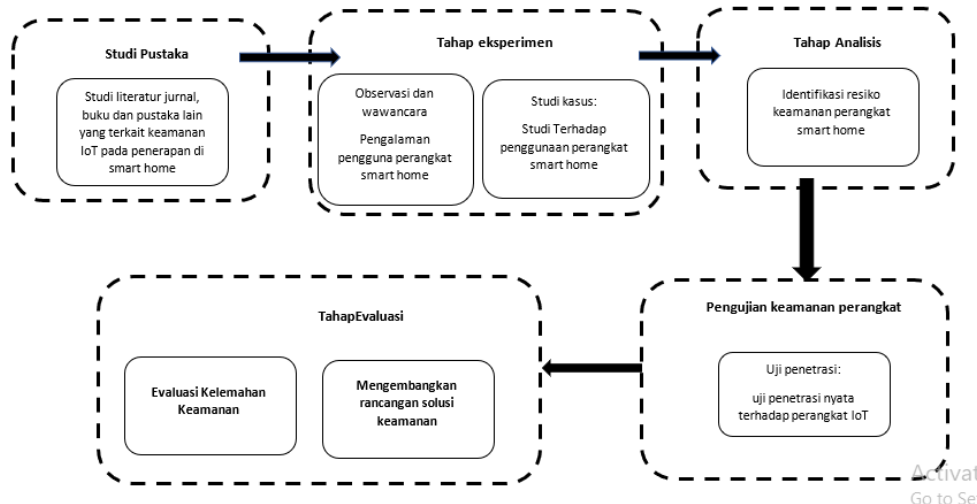
Teknologi *smart home* semakin populer dan memiliki manfaat yang luar biasa dalam menyediakan rumah yang nyaman dan aman. Namun, ada aspek yang tak boleh diabaikan, yaitu keamanan. Karakteristik *smart home* yang heterogen, dinamis dan terhubung dengan jaringan internet memiliki potensi kerentanan dari serangan siber [3]. Beberapa serangan fisik maupun siber yang dapat terjadi pada aplikasi *smart home* diantaranya adalah peretasan pada aplikasi dan serangan hak akses oleh pihak yang tidak bertanggung jawab [4]. Jika perangkat-perangkat ini tidak cukup dilindungi, maka dapat membuka pintu masuk bagi serangan siber yang dapat merusak dan melanggar privasi [5],[6]. Oleh karena itu, evaluasi kerentanan keamanan pada perangkat IoT dalam konteks *smart home* menjadi sangat penting.

Beberapa penelitian terkait *smart home* telah banyak dilakukan diantaranya adalah penelitian dengan judul "Security Framework of IoT-Based *Smart home*". Pada penelitian ini dirancang desain keamanan sebagai kerangka umum untuk meningkatkan keamanan pada *smart home*[7]. penelitian lain adalah penelitian yang mengidentifikasi faktor resiko keamanan dan evaluasi untuk merancang solusi keamanan perangkat *smart home*. [8]. Analisis yang dihasilkan dari penelitian ini adalah kerentanan keamanan berada pada lapisan persepsi, lapisan *transport*, dan lapisan aplikasi yaitu menganalisis serangan malware pada perangkat *smart home* dan merancang *smart router*. Pada penelitian ini dikembangkan penelitian terkait evaluasi kerentanan perangkat *smart home* dengan melakukan studi secara langsung pada perangkat *smart home*, kemudian dilakukan identifikasi faktor resiko keamanan dan dilakukan evaluasi untuk merancang solusi keamanan perangkat *smart home*.

Tujuan dari penelitian ini adalah untuk mengevaluasi kerentanan keamanan pada perangkat IoT dalam konteks *smart home*. Melalui studi kasus yang mencakup berbagai perangkat yang umumnya ditemukan dalam *smart home*, salah satunya adalah potensi kerentanan dan risiko keamanan yang terkait dengan penggunaan perangkat IoT. Selain itu penelitian ini juga bertujuan untuk memberikan kontribusi pengetahuan ilmu pengetahuan di bidang keamanan bagi majelis Diktilitbang Muhammadiyah pada khususnya dan seluruh masyarakat pada umumnya.

B. Metode Penelitian

Penelitian yang telah dilakukan memiliki beberapa tahap, dimulai dari tahap studi literatur terkait keamanan dan serangan pada perangkat *smart home*, tahap eksperimen yang terdiri dari studi kasus dan observasi dan wawancara, tahap analisis keamanan pada perangkat *smart home*, tahap implementasi pengujian keamanan *smart home* dan tahap evaluasi serta pengembangan rancangan solusi keamanan. Untuk memahami tahapan penelitian dapat dilihat pada gambar 1.



Gambar 1. Tahapan penelitian

Penjelasan lebih lanjut mengenai tahapan-tahap yang dapat dilihat pada gambar 2 adalah sebagai berikut

1. Studi Pustaka

Dalam penelitian ini mempelajari referensi berupa jurnal, buku maupun artikel lain yang terkait dengan penelitian. Adapun jurnal yang dijadikan referensi adalah jurnal yang membahas tentang *Internet of things*, *Smart home*, keamanan perangkat IoT dan perangkat IoT. Selain itu juga buku dan artikel tentang *Internet of things* dan *smart home* dijadikan referensi dalam penulisan penelitian ini.

2. Tahap eksperimen

Pada tahapan ini melakukan perencanaan eksperimen yang melibatkan pengujian perangkat IoT yang digunakan dalam rumah pintar. Ada 2 metode yang dilakukan dalam tahapan ini, yaitu:

a. Observasi dan wawancara

Metode ini dilakukan dengan melakukan survei kepada pemilik rumah yang menerapkan *smart home* atau pengguna perangkat IoT untuk mendapatkan wawasan tentang pengalaman mereka dengan perangkat tersebut. Selain itu, wawancara dengan pengguna *smart home* dapat memberikan perspektif tentang masalah keamanan yang mungkin ada.

b. Studi kasus

Pada tahapan ini dilakukan studi kasus terhadap penggunaan perangkat yang mendukung penerapan *smart home*. Studi kasus dilakukan dengan melakukan kajian lebih lanjut terhadap perangkat-perangkat *smart home*,

cara penggunaan dan penggunaan jaringan pada perangkat tersebut. Metode ini dapat melibatkan pemilihan beberapa rumah pintar sebagai studi kasus, kemudian akan melakukan analisis mendalam terhadap perangkat IoT yang digunakan dalam rumah pintar ini, mengidentifikasi kerentanan keamanan yang mungkin ada, dan mencoba menguji perangkat tersebut untuk melihat apakah perangkat tersebut memungkinkan untuk disusupi.

3. Tahap analisis

Pada tahap ini dilakukan identifikasi potensi ancaman yang dapat dihadapi oleh perangkat IoT dalam konteks rumah pintar. Ini melibatkan identifikasi berbagai serangan yang mungkin terjadi, seperti serangan *malware*, serangan *denial-of-service*, atau serangan fisik pada perangkat IoT [9],[10].

4. Uji Penetrasi keamanan perangkat *smart home*

Pada tahapan ini dilakukan uji penetrasi nyata terhadap perangkat IoT untuk mengidentifikasi kerentanan keamanan. Uji penetrasi merupakan bagian dari pengujian keamanan dan dilakukan untuk menentukan kerentanan perangkat IoT pada *smart home*. Uji penetrasi dapat membantu mengidentifikasi celah yang dapat dieksploitasi oleh penyerang [11], [12].

5. Evaluasi dan rancangan solusi keamanan

Tahapan ini merupakan tahapan dalam evaluasi keamanan perangkat *smart home*.

a. Evaluasi keamanan

Tahapan ini dilakukan untuk mengevaluasi ancaman keamanan yang dapat terjadi pada perangkat IoT pada *smart home*. Evaluasi dilakukan untuk melihat kelemahan keamanan, seperti kata sandi lemah, kerentanan perangkat lunak, atau konfigurasi yang tidak aman [13].

b. Mengembangkan rancangan solusi keamanan.

Setelah mengidentifikasi kerentanan keamanan, langkah berikutnya adalah mengembangkan solusi untuk mengatasi masalah ini. Solusi yang mungkin dilakukan mengganti kata sandi, memperbarui perangkat lunak, atau mengimplementasikan langkah-langkah tambahan untuk meningkatkan keamanan [14],[15].

C. Hasil dan Pembahasan

1. Identifikasi Perangkat IoT dan Infrastruktur *Smart home*

Identifikasi dilakukan dengan melakukan studi literatur, survei pasar, observasi dan wawancara ke sejumlah pengguna *smart home* untuk mengidentifikasi perangkat *smart home* yang umum digunakan dalam rumah pintar dan infrastruktur jaringan yang mendukungnya. Pada penelitian ini difokuskan pada beberapa perangkat *smart home* yang dijadikan obyek penelitian yaitu Kamera Pintar. Pada penelitian ini juga dilakukan identifikasi arsitektur yang terdapat pada perangkat *smart home* tersebut. Beberapa infrastruktur perangkat *smart home* yang diteliti adalah:

a. **Router Wi-Fi**

Router Wi-Fi adalah komponen kunci dalam infrastruktur *smart home* karena menghubungkan semua perangkat pintar dalam rumah ke jaringan internet. *Router* digunakan untuk berkomunikasi antar perangkat dan dengan pengguna melalui aplikasi ponsel pintar.

b. **Perangkat IoT:** Ini adalah perangkat pintar yang beroperasi dalam rumah pintar, dalam penelitian ini perangkat yang digunakan kamera keamanan pintar. Perangkat IoT ini terhubung ke jaringan Wi-Fi atau jaringan nirkabel lainnya dan dapat dikendalikan secara digital.

c. **Aplikasi Kontrol:**

Aplikasi kontrol merupakan perangkat lunak yang diinstal di ponsel pintar agar pengguna dapat mengontrol dan memantau perangkat IoT mereka dari jarak jauh. Melalui aplikasi ini, pengguna dapat menyalakan atau mematikan lampu CCTV, melihat *feed* kamera keamanan, dan melakukan berbagai tindakan lainnya.

d. **Protokol Komunikasi:** Protokol komunikasi yang digunakan pada perangkat yang diteliti adalah menggunakan Wi-Fi yang terhubung dengan *router Wi-Fi*.

2. Pemilihan Studi kasus

Pada penelitian ini dilakukan dengan studi kasus di rumah yang sudah menggunakan *smart home*. Adapun perangkat yang sering digunakan pada rumah yang menerapkan *smart home* adalah kamera keamanan cerdas yang bisa di pantau dan dikendalikan jarak jauh. Spesifikasi perangkat dapat dilihat pada penjelasan berikut,

- Merek : SPC -Smart Series BC1
- Resolusi : 3 MP
- Image Sensor : 1/3" Color CMOS
- Connection : Wi-Fi 2.4 HGZ
- Working Temperature 0 °C ~ 45 °C Working Humidity 10% - 95
- Audio Build-in Mic & Speaker
- Micro SD Card Up to 256 GB

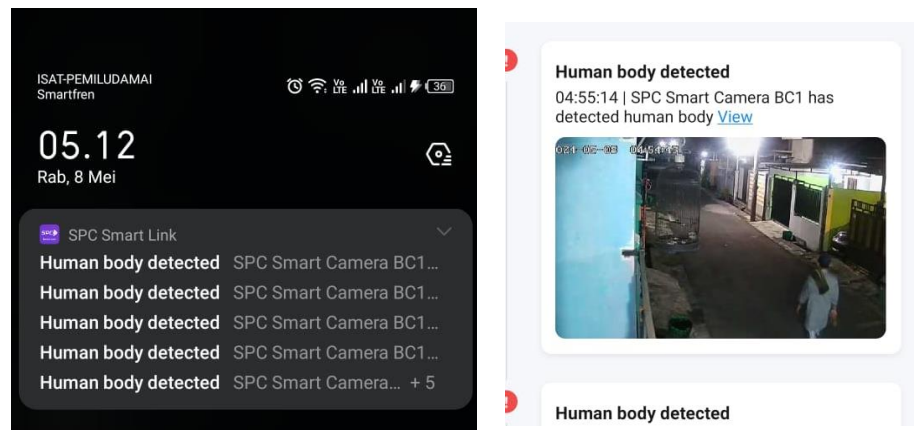
3. Analisis Kerentanan.

Pada tahapan ini dilakukan analisis kerentanan pada perangkat IoT yang diteliti yaitu Kamera Pintar. dari hasil penelitian diperoleh hasil sebagai berikut

a. Cara kerja perangkat

Kamera keamanan pintar bekerja dengan menggunakan teknologi sensor gambar dan koneksi internet untuk memantau dan merekam aktivitas di area yang dipantau. Ketika kamera keamanan mendeteksi gerakan atau aktivitas di area yang dipantau, sensor gerakan di dalam kamera akan memberi sinyal untuk mulai merekam atau mengirimkan pemberitahuan kepada pengguna melalui aplikasi ponsel pintar. Setelah mendeteksi gerakan, kamera akan mulai merekam video secara otomatis. Video ini dapat direkam langsung ke perangkat penyimpanan lokal seperti kartu SD di dalam kamera atau ke cloud *server* melalui koneksi internet. Kamera

keamanan pintar dapat dikonfigurasi untuk mengirimkan pemberitahuan langsung kepada pengguna ketika aktivitas yang mencurigakan terdeteksi. Pengguna akan menerima notifikasi melalui aplikasi ponsel pintar mereka yang memberi tahu mereka tentang kejadian yang sedang berlangsung. Notifikasi dapat dilihat pada gambar 2.



Gambar 2. Notifikasi dan tangkapan layar kamera keamanan

Melalui aplikasi ponsel pintar, pengguna dapat mengakses kamera keamanan dari jarak jauh. Mereka dapat melihat video langsung dari kamera, memutar ulang rekaman yang disimpan, atau mengatur pengaturan kamera seperti sensitivitas gerakan dan pemberitahuan. Video yang direkam oleh kamera keamanan pintar dapat disimpan secara lokal di perangkat penyimpanan internal atau kartu SD di dalam kamera. Beberapa kamera juga menawarkan penyimpanan video ke *cloud*, yang memungkinkan pengguna mengakses rekaman dari mana saja dengan koneksi internet. Kamera keamanan pintar dapat terintegrasi dengan sistem *smart home* yang lebih luas. Ini memungkinkan pengguna untuk mengatur aksi otomatis berdasarkan aktivitas yang dideteksi oleh kamera, seperti menyalakan lampu atau mengirim peringatan ke perangkat lain dalam rumah. Beberapa kamera keamanan pintar dilengkapi dengan fitur tambahan seperti penglihatan malam, kemampuan berbicara dua arah (untuk berkomunikasi dengan pengunjung atau anggota keluarga), dan deteksi suara.

b. Analisa kerentanan perangkat

Dalam penelitian ini dilakukan analisa mendalam terhadap perangkat. Analisa dilakukan dengan menganalisa spesifikasi perangkat, protokol komunikasi yang digunakan, fitur keamanan yang disediakan, dan kemampuan akses pada perangkat. Berikut hasil dari analisa kerentanan terhadap perangkat kamera keamanan pintar

1) Kerentanan akses ke perangkat

Dalam melakukan akses ke perangkat kamera keamanan pintar, dilakukan dengan instal aplikasi perangkat di play store dan mendaftar sebagai admin. Admin dapat mengatur pembatasan hak

akses pengguna. Akses terhadap perangkat dilakukan dengan mengirim link akses. Hal ini sangat rentan terhadap penyalahgunaan akses. Karena siapa saja yang memiliki link tersebut dapat mengakses perangkat. Sehingga hal tersebut dapat menjadi resiko keamanan pengguna.

2) Kata Sandi *default*

Salah satu kerentanan pada perangkat kamera keamanan pintar ini adalah penggunaan kata sandi *default* atau lemah. Hasil analisis mungkin menemukan bahwa perangkat kamera keamanan pintar menggunakan kata sandi *default* yang mudah ditebak atau tidak diubah dari pengaturan pabrik.

3) Kerentanan Jaringan

Berdasarkan hasil analisis pada penelitian ini ditemukan beberapa Kerentanan pada jaringan. Kerentanan tersebut merupakan kerentanan yang terdapat pada *router* Wi-Fi. Kerentanan pada *router* Wi-Fi meliputi kerentanan enkripsi Wi-Fi, Kerentanan manajemen akses, kerentanan firmware dimana beberapa versi perangkat lunak *router* rentan terhadap serangan dan kerentanan protokol jaringan .

4) Kerentanan Fisik

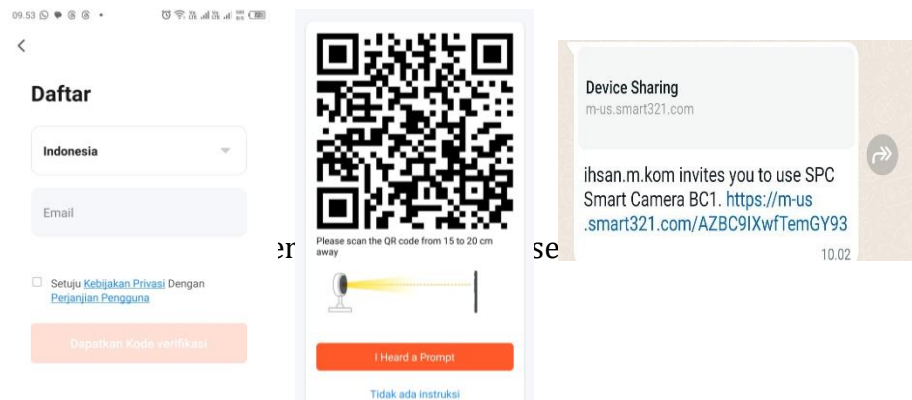
Berdasarkan hasil analisis kerentanan fisik terhadap perangkat kamera keamanan pintar adalah Kemungkinan Pencurian Perangkat kamera keamanan pintar yang dipasang terutama perangkat kamera keamanan yang dipasang di luar rumah. Selain itu kerentanan lain adalah penyerangan terhadap akses fisik ke perangkat kamera keamanan dapat memanipulasi atau merusak perangkat untuk mengganggu operasi pemantauan atau merekam. Salah satu upaya yang rawan dilakukan adalah penutupan atau penyaringan lensa, memotong kabel, atau merusak komponen internal. Selain itu kerentanan juga dapat terjadi pada data rekaman data, penyerang dengan akses fisik dapat mencuri atau memanipulasi data rekaman tersebut. Ini bisa menjadi masalah serius jika rekaman tersebut digunakan sebagai bukti dalam penyelidikan kejahatan. Kerentanan juga dapat terjadi pada rumah yang memiliki Beberapa perangkat *smart home* yang memiliki *port* atau sumber daya tambahan yang dapat dimanfaatkan oleh penyerang dengan akses fisik untuk mendapatkan akses ke jaringan yang lebih luas dan mengacaukan integrasi dengan perangkat lain yang digunakan di *smart home*. Penyerang juga dapat mengubah konfigurasi perangkat, seperti mengubah pengaturan resolusi atau sudut pandang kamera, untuk mengurangi efektivitas pemantauan atau merekam.

4. Uji Penetrasi

Uji penetrasi, atau sering disebut sebagai "penetrasi tes" atau "pentesting," adalah proses yang dilakukan untuk mengevaluasi keamanan suatu sistem, jaringan, atau aplikasi dengan cara mensimulasikan serangan yang mungkin dilakukan oleh penyerang berbahaya. Tujuan utama dari uji penetrasi adalah untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan yang mungkin ada dalam lingkungan yang diuji, sehingga pemilik sistem atau

organisasi dapat mengambil tindakan untuk memperbaiki kerentanan tersebut dan meningkatkan keamanan keseluruhan sistem.

- 1) Uji penetrasi Kerentanan Aplikasi:
 - a. Ditemukan mudahnya masuk aplikasi, dengan hanya memperoleh link akses. Akses kamera keamanan ini bekerja dengan menginstal aplikasi SPC dan setelah memiliki akun SPC hanya dengan klik link yang diberikan oleh admin atau *barcode* dari akun admin, maka langsung dapat mengakses aplikasi. Link akses aplikasi dapat dilihat pada gambar 3.

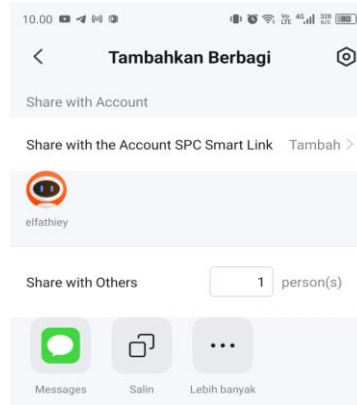


Gambar 3. Link akses aplikasi kamera keamanan pintar

Dengan kemudahan akses seperti itu, sangat rentan untuk penyalahgunaan akses oleh pihak yang tidak berwenang. Hasil uji penetrasi pada penelitian ini mencoba masuk sebagai akun berbagi dan berhasil masuk akses aplikasi.

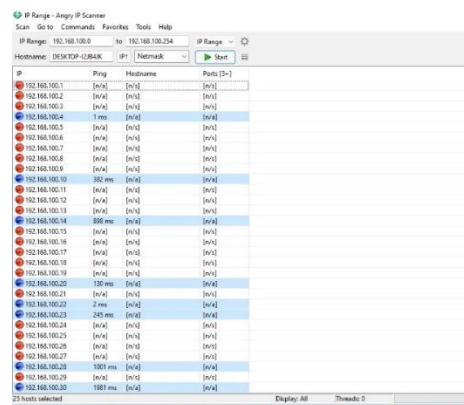
- b. Kelemahan akun

Selain pada kemudahan akses, uji penetrasi juga dilakukan dengan mencoba mengakses akun admin. Dan kebanyakan pengguna *smart home* masih menggunakan *password default* dari pabrik, yang dapat ditemukan pada panduan penggunaan perangkat. Sehingga ketika mencoba masuk akun admin dan dapat mengatur pengelolaan data dan manajemen user yang diperbolehkan akses.



Gambar 4. Mengakses halaman admin dengan menggunakan akun *default* pabrik

- 2) Uji penetrasi Kerentanan Jaringan
Kerentanan pada jaringan dilakukan dengan menganalisis keamanan *router*. Pada penelitian ini awal uji penetrasi dilakukan dengan melakukan identifikasi IP address perangkat. Untuk melihat identifikasi ip adress dapat dilihat pada gambar 5.



Gambar 5. Identifikasi IP Adress perangkat

Setelah IP adress teridentifikasi kemudian dilakukan uji penetrasi terhadap keamanan *router* Wi-Fi

a. Uji dengan DDoS (*Distributed Denial of Service*)

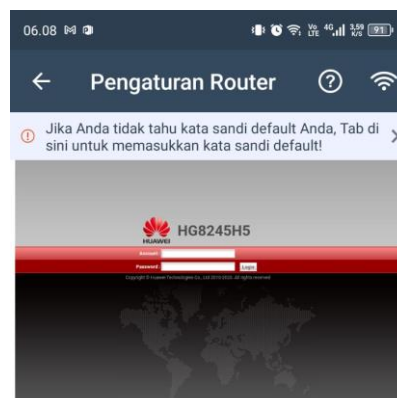
Ddos merupakan serangan yang ditujukan ntuk membuat layanan atau sumber daya tidak tersedia bagi pengguna yang sah dengan mengalirkan lalu lintas internet yang sangat tinggi ke target yang ditentukan. Pada uji penetrasi ini dilakukan *ping* terus menerus ke perangkat sehingga didapatkan hasil pengguna perangkat menjadi kesulitan untuk mengakses perangkat. Uji Ddos dapat dilihat pada gambar 6.

PING 192.168.100.1	
192.168.100.1 (192.168.100.1) 58(86) bytes of data.	
From 192.168.100.1	28.4 ms
66 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=28.4 ms	
From 192.168.100.1	2.59 ms
66 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=2.59 ms	
From 192.168.100.1	7.24 ms
66 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=7.24 ms	
From 192.168.100.1	7.25 ms
66 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=7.25 ms	
From 192.168.100.1	7.26 ms
66 bytes from 192.168.100.1: icmp_seq=5 ttl=64 time=7.26 ms	
--- 192.168.100.1 ping statistics ---	
Ping Statistics	
5 packets transmitted, 5 received, 0% packet loss, time 4018ms	

Gambar 6. Uji DDoS pada jaringan *router*

b. Uji dengan serangan brute force

Pada penelitian ini melakukan serangan brute force untuk menebak kata sandi *router* dengan mencoba semua kombinasi yang mungkin. Pada penelitian ini mencoba mengkombinasikan kombinasi angka-angka yang dianggap penting dan pada uji penetrasi ini berhasil masuk pada halaman admin perangkat. Percobaan serangan brute force dapat dilihat pada gambar 6. Dimana pengguna mencoba memasukkan email pemilik rumah dan menguji *password* dari tanggal lahir anggota keluarga.



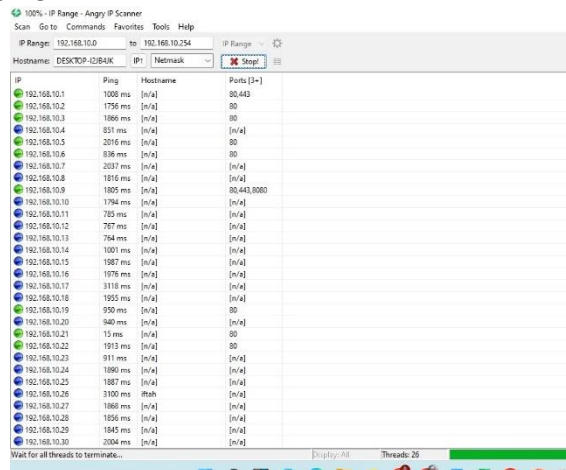
Gambar 7. Uji Penetrasi Dengan *Brute Force*

Setelah masuk ke halaman admin maka semua konfigurasi perangkat dapat dikacaukan dan dapat mengakses data pada perangkat.

c. Uji *Port* pada jaringan

Pada penelitian ini dilakukan skrining terhadap *port* yang terbuka. *Port* yang terbuka memungkinkan penyerang untuk masuk kedalam perangkat. Ada beberapa *port* yang masih terbuka diantaranya *port*

80, port 8080, port 443 dan port 3128. Uji port jaringan dapat dilihat pada gambar 8.

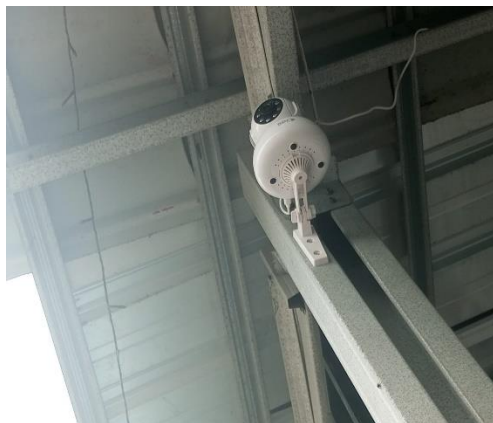


IP	Ping	Hostname	Ports (3+)
192.168.10.1	1000 ms	[n/a]	80,443
192.168.10.2	1795 ms	[n/a]	80
192.168.10.3	1866 ms	[n/a]	80
192.168.10.4	831 ms	[n/a]	[n/a]
192.168.10.5	2016 ms	[n/a]	80
192.168.10.6	838 ms	[n/a]	80
192.168.10.7	2037 ms	[n/a]	[n/a]
192.168.10.8	1816 ms	[n/a]	[n/a]
192.168.10.9	1805 ms	[n/a]	80,443,8080
192.168.10.10	1784 ms	[n/a]	[n/a]
192.168.10.11	785 ms	[n/a]	[n/a]
192.168.10.12	787 ms	[n/a]	[n/a]
192.168.10.13	784 ms	[n/a]	[n/a]
192.168.10.14	1001 ms	[n/a]	[n/a]
192.168.10.15	1987 ms	[n/a]	[n/a]
192.168.10.16	1076 ms	[n/a]	[n/a]
192.168.10.17	3118 ms	[n/a]	[n/a]
192.168.10.18	1855 ms	[n/a]	[n/a]
192.168.10.19	950 ms	[n/a]	80
192.168.10.20	940 ms	[n/a]	[n/a]
192.168.10.21	15 ms	[n/a]	80
192.168.10.22	1913 ms	[n/a]	80
192.168.10.23	911 ms	[n/a]	[n/a]
192.168.10.24	1890 ms	[n/a]	[n/a]
192.168.10.25	1887 ms	[n/a]	[n/a]
192.168.10.26	3100 ms	[n/a]	[n/a]
192.168.10.27	1868 ms	[n/a]	[n/a]
192.168.10.28	1856 ms	[n/a]	[n/a]
192.168.10.29	1845 ms	[n/a]	[n/a]
192.168.10.30	2054 ms	[n/a]	[n/a]

Gambar 8. Uji Port yang terbuka

3) Uji penetrasi perangkat fisik

Pada uji ini dilakukan skema pengujian terhadap pencurian dan pengrusakan perangkat. Uji penetrasi perangkat fisik dapat dilihat pada gambar 9.



Gambar 9. Uji penetrasi kerentanan fisik perangkat

5. Evaluasi hasil uji kerentanan

Ada beberapa hasil evaluasi kerentanan yang didapatkan dari hasil analisis dan uji penetrasi terhadap perangkat kamera keamanan pintar. Berikut hasil evaluasi dari penelitian ini:

1) Kerentanan Aplikasi:

- Ditemukan kerentanan terhadap akses karena mudahnya akses kedalam perangkat hanya dengan link akses atau *barcode* yang dibagikan oleh admin perangkat.
- Terdeteksi celah keamanan yang memungkinkan untuk masuk kedalam akun perangkat. Hal tersebut dikarenakan kebanyakan pengguna *smart home* menggunakan akun *default* perangkat dan jika merubah akun makan hanya menggunakan *password* yang

sederhana, seperti tanggal lahir, nomor rumah dan nama anggota keluarga

2) **Kerentanan Jaringan:**

- a. Teridentifikasi kerentanan pada konfigurasi jaringan yang memungkinkan serangan pengacauan lalu lintas dan pengacauan perangkat dengan mengirimkan permintaan berulang atau dikenal dengan serangan Ddos.
- b. Ditemukan kelemahan pada akses *router* dengan melakukan serangan brute force. Kelemahan *password* menjadi faktor utama dalam kerentanan jaringan *router* Wi-Fi
- c. Ditemukan beberapa *port* jaringan yang terbuka, sehingga hal tersebut rentan menjadi jalan masuk pengguna untuk mengakses perangkat jaringan.

3) **Kerentanan Fisik:**

- a. Penetrasi fisik berhasil mendemonstrasikan kerentanan terhadap manipulasi perangkat dan pencurian perangkat kamera keamanan.
- b. Ditemukan kerentanan terhadap akses fisik yang tidak sah ke komponen infrastruktur jaringan terkait, misalnya dengan melakukan scan *barcode* dan diarahkan pada perangkat

Dari hasil evaluasi tersebut, maka dapat disimpulkan Analisis kerentanan telah membuka berbagai potensi ancaman terhadap keamanan pada aplikasi *smart home* salah satu contohnya adalah pada sistem smart kamera keamanan (CCTV). Ada beberapa rekomendasi bagi pengguna perangkat *smart home* dalam melindungi keamanan perangkat, diantaranya :

- 1) **Kendali Akses:** Terapkan kontrol akses yang ketat terhadap perangkat *smart home*, termasuk siapa yang memiliki akses fisik ke perangkat, siapa yang memiliki hak akses ke aplikasi atau sistem pengontrol, dan siapa yang memiliki hak akses ke jaringan rumah.
- 2) **Pemantauan Keamanan:** Pemantauan keamanan secara teratur adalah kunci untuk melindungi perangkat *smart home* dari ancaman siber. Perhatikan perubahan perilaku atau aktivitas yang mencurigakan pada perangkat atau jaringan dan lakukan pergantian *password* secara berkala.
- 3) **Uji Pemutusan Sambungan (Disconnect):** Uji apakah perangkat *smart home* tetap berfungsi dengan benar ketika koneksi internet diputus. Hal tersebut untuk memastikan saat perangkat mati, fungsionalitas penyimpanan masih berjalan dengan baik.
- 4) **Pembaruan Peralatan Jaringan:** Pastikan peralatan jaringan Anda (seperti *router* dan *firewall*) memiliki perangkat lunak terbaru dan konfigurasi keamanan yang tepat untuk melindungi perangkat *smart home* Anda dari serangan dari luar.
- 5) **Pemindaian Jaringan:** Gunakan alat pemindaian jaringan untuk mengidentifikasi perangkat *smart home* yang terhubung ke jaringan. Pastikan untuk memeriksa apakah ada perangkat yang tidak dikenal atau tidak diotorisasi yang terhubung.

- 6) **Uji fisik perangkat:** dengan memastikan fisik perangkat *smart home* berfungsi dengan baik dan tidak ada kerusakan.

D. Simpulan

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa, perangkat *smart home* merupakan teknologi yang dapat mempermudah pengguna dalam menggunakan dan memantau perangkat karena terhubung dengan jaringan internet. Namun penggunaan *smart home* juga harus memperhatikan pentingnya keamanan. Beberapa kerentanan ditemukan pada penelitian ini diantaranya adalah kerentanan perangkat yang menyangkut keamanan akses dan keamanan akun pengguna, selain itu kerentanan juga terdapat pada jaringan *router* Wi-Fi yang menjadi protokol komunikasi perangkat serta kerentanan fisik yang memungkinkan terjadinya pencurian dan kerusakan fisik perangkat. Sehingga pengguna *smart home* harus mengantisipasi kerentanan tersebut dengan memperhatikan faktor keamanan untuk meminimalkan resiko serangan terhadap perangkat *smart home*.

E. Ucapan Terima Kasih

Ucapan terima kasih Kami ucapkan kepada seluruh pihak yang membantu terlaksananya penelitian ini, terutama kepada Majelis Pendidikan Tinggi Penelitian dan Pengembangan Pimpinan Pusat Muhammadiyah atas pendanaan penelitian melalui hibah penelitian RisetMu.

F. Referensi

- [1] U. Rijal Permana, Rumani, "Perancangan Sistem Keamanan dan Kontrol *Smart home* Berbasis *Internet of things*," vol. 43, no. 3, pp. 7–28, 2017.
- [2] E. dkk Erwin, *PENGANTAR DAN PENERAPAN INTERNET OF THINGS: Konsep dasar & Penerapan IoT di berbagai Sektor*. Sonpedia Publishing Indonesia, 2023. [Online]. Available: www.buku.sonpedia.com
- [3] K. Karimi, "Smart home-Smartphone Systems: Threats , Security Requirements and Open research Challenges," *2019 Int. Conf. Comput. Sci. Renew. Energies*, pp. 1–5, 2020.
- [4] A. Restu Mukti, C. Mukmin, E. Randa Kasih, D. Palembang Jalan Jenderal Ahmad Yani No, S. I. Ulu, and S. Selatan, "Perancangan *Smart home* Menggunakan Konsep *Internet of things* (IOT) Berbasis Microcontroller," *J. JUPITER*, vol. 14, no. 2, pp. 516–522, 2022.
- [5] T. Adiono, S. Harimurti, B. A. Manangkalangi, and W. Adijarto, "Design of *smart home* mobile application with high security and automatic features," *IGBSG 2018 - 2018 Int. Conf. Intell. Green Build. Smart Grid*, pp. 1–4, 2018, doi: 10.1109/IGBSG.2018.8393574.
- [6] M. Shariqsuhail, V. G, G. Rambabu, C. V. R. Dharmasavarni, and V. K. M, "Multi-Functional Secured *Smart home*," pp. 2629–2634, 2016.
- [7] S. Sotoudeh, S. Hashemi, and H. G. Garakani, "Security Framework of IoT-Based *Smart home*," *2020 10th Int. Symp. Telecommun. Smart Commun. a*

- Better Life, IST 2020*, pp. 251–256, 2020, doi: 10.1109/IST50524.2020.9345886.
- [8] R. Yu, X. Zhang, and M. Zhang, “Smart home Security Analysis System Based on the *Internet of things*,” *2021 IEEE 2nd Int. Conf. Big Data, Artif. Intell. Internet Things Eng. ICBAIE 2021*, no. Icbaie, pp. 596–599, 2021, doi: 10.1109/ICBAIE52039.2021.9389849.
- [9] M. Botticelli, L. Ciabattini, F. Ferracuti, A. Monteri, S. Pizzuti, and S. Romano, “A Smart home Services Demonstration : Monitoring , Control and Security Services Offered to the User,” *2018 IEEE 8th Int. Conf. Consum. Electron. - Berlin*, pp. 1–4.
- [10] A. Mude and L. B. F. Mando, “Implementasi Keamanan Rumah Cerdas Menggunakan *Internet of things* dan Biometric Sistem,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 1, pp. 179–188, 2021, doi: 10.30812/matrik.v21i1.1381.
- [11] M. Mushlih, R. Fitri, and I. Wardiah, “Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web,” *Semin. Nas. Ris. ...*, vol. 5662, no. November, pp. 41–47, 2019, [Online]. Available: <http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/409>
- [12] F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.
- [13] D. Suryono, “Analisis Keamanan Jaringan Hardware Trojan Pada IoT,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 4, pp. 3529–3537, 2022, doi: 10.35957/jatisi.v9i4.2845.
- [14] W. Najib, S. Sulistyono, and Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi *Internet of things*,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 9, no. 4, pp. 375–384, 2020, doi: 10.22146/jnteti.v9i4.539.
- [1] U. Rijal Permana, Rumani, “Perancangan Sistem Keamanan dan Kontrol Smart home Berbasis *Internet of things*,” vol. 43, no. 3, pp. 7–28, 2017.
- [2] E. dkk Erwin, *PENGANTAR DAN PENERAPAN INTERNET OF THINGS : Konsep dasar & Penerapan IoT di berbagai Sektor*. Sonpedia Publishing Indonesia, 2023. [Online]. Available: www.buku.sonpedia.com
- [3] K. Karimi, “Smart home-Smartphone Systems : Threats , Security Requirements and Open research Challenges,” *2019 Int. Conf. Comput. Sci. Renew. Energies*, pp. 1–5, 2020.
- [4] A. Restu Mukti, C. Mukmin, E. Randa Kasih, D. Palembang Jalan Jenderal Ahmad Yani No, S. I. Ulu, and S. Selatan, “Perancangan Smart home Menggunakan Konsep *Internet of things* (IOT) Berbasis Microcontroller,” *J. JUPITER*, vol. 14, no. 2, pp. 516–522, 2022.
- [5] T. Adiono, S. Harimurti, B. A. Manangkalangi, and W. Adijarto, “Design of smart home mobile application with high security and automatic features,” *IGBSG 2018 - 2018 Int. Conf. Intell. Green Build. Smart Grid*, pp. 1–4, 2018, doi: 10.1109/IGBSG.2018.8393574.
- [6] M. Shariqsuhail, V. G. G. Rambabu, C. V. R. Dharmasavarni, and V. K. M, “Multi-Functional Secured Smart home,” pp. 2629–2634, 2016.
- [7] S. Sotoudeh, S. Hashemi, and H. G. Garakani, “Security Framework of IoT-Based Smart home,” *2020 10th Int. Symp. Telecommun. Smart Commun. a*

- Better Life, IST 2020*, pp. 251–256, 2020, doi: 10.1109/IST50524.2020.9345886.
- [8] R. Yu, X. Zhang, and M. Zhang, “Smart home Security Analysis System Based on the *Internet of things*,” *2021 IEEE 2nd Int. Conf. Big Data, Artif. Intell. Internet Things Eng. ICBAIE 2021*, no. Icbaie, pp. 596–599, 2021, doi: 10.1109/ICBAIE52039.2021.9389849.
- [9] M. Botticelli, L. Ciabattini, F. Ferracuti, A. Monteri, S. Pizzuti, and S. Romano, “A Smart home Services Demonstration : Monitoring , Control and Security Services Offered to the User,” *2018 IEEE 8th Int. Conf. Consum. Electron. - Berlin*, pp. 1–4.
- [10] A. Mude and L. B. F. Mando, “Implementasi Keamanan Rumah Cerdas Menggunakan *Internet of things* dan Biometric Sistem,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 1, pp. 179–188, 2021, doi: 10.30812/matrik.v21i1.1381.
- [11] M. Mushlih, R. Fitri, and I. Wardiah, “Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web,” *Semin. Nas. Ris. ...*, vol. 5662, no. November, pp. 41–47, 2019, [Online]. Available: <http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/409>
- [12] F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.
- [13] D. Suryono, “Analisis Keamanan Jaringan Hardware Trojan Pada IoT,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 4, pp. 3529–3537, 2022, doi: 10.35957/jatisi.v9i4.2845.
- [14] W. Najib, S. Sulistyono, and Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi *Internet of things*,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 9, no. 4, pp. 375–384, 2020, doi: 10.22146/jnteti.v9i4.539.
- [15] R. Rahmaddi and R. N. Rohmah, “Sistem Keamanan dan Pengairan Ladang Pertanian Berbasis IOT,” *Emit. J. Tek. Elektro*, vol. 21, no. 2, pp. 126–134, 2021, doi: 10.23917/emit.v21i2.13720.