UJI KERENTANAN DAN PENGAMANAN MENGGUNAKAN NIST SP 800-53 *RISK MANAGEMENT FRAMEWORKS* PADA *SMART HOME* BARDI (STUDI KASUS : BARDI *SMART LIGHT*)

TUGAS AKHIR

Diajukan oleh :

Muhammad Aufa Lukman
NIM. 190705094
Mahasiswa Program Studi Teknologi Informasi
Fakultas Sains dan Teknologi UIN Ar-Raniry

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI AR-RANIRY
BANDA ACEH
2024 M / 1444 H

LEMBAR PERSETUJUAN

UJI KERENTANAN DAN PENGAMANAN MENGGUNAKAN NIST SP 800-53 *RISK MANAGEMENT FRAMEWORKS* PADA *SMART HOME* BARDI (STUDI KASUS : BARDI *SMART LIGHT*)

TUGAS AKHIR

Diajukan Kepada Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Memperoleh Gelar Sarjana
pada Prodi Teknologi Informasi

Oleh:

Muhammad Aufa Lukman

NIM. 190705094

Mahasiswa Fakultas Sains dan Teknologi

Program Studi Teknologi Informasi

Disetujui untuk dimunaqasyahkan oleh :

Pembimbing I,	Pembimbing II,
Khairan AR, M.Kom	**Mulkan Fadhil, S.T., M.T.**
NIP. 198607042014031001	**NIP. 198811282020121006**

Mengetahui,
Ketua program studi teknologi informasi

Malahayati, M.T.
NIP. 198301272015032003

LEMBAR PENGESAHAN TUGAS AKHIR

UJI KERENTANAN DAN PENGAMANAN MENGGUNAKAN NIST SP 800-53 *RISK MANAGEMENT FRAMEWORKS* PADA *SMART HOME* BARDI (STUDI KASUS : BARDI *SMART LIGHT*)

TUGAS AKHIR

Diajukan kepada Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai salah satu Beban Studi Memperoleh Gelar Sarjana
Pada Prodi Teknologi Informasi

Pada Hari/Tanggal: Rabu/ 12- Juni 2024
Rabu/ 5 Dzulhijjah 1445 H

Panitia Ujian Munqasyah Skripsi

Ketua

Khairan AR, M.Kom
NIP. 198607042014031001

Sekretaris

Mulkan Fadhil, S.T., M.T
NIP. 198811282020121006

Penguji I

Baihaqi, M. T.
NIP. 198802212022031001

Penguji II

Aulia Syarif Aziz, S.Kom. ,M.Sc
NIP. 199305212022031001

Mengetahui:
Dekan Fakultas Sains dan Teknologi
UIN Ar-Raniry Banda Aceh,

Dr.Ir.Muhammad Dirhamsyah., MT.,IPU
NIDN.0002106203

LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama	:	Muhammad Aufa Lukman
NIM	:	190705094
Program Studi	:	Teknologi Informasi
Fakultas	:	Sains dan Teknologi
Judul	:	UJI KERENTANAN DAN PENGAMANAN MENGGUNAKAN NIST SP 800-53 RISK MANAGEMENT FRAMEWORKS PADA SMART HOME BARDI (STUDI KASUS : BARDI SMART LIGHT)

Dengan ini menyatakan bahwa dalam penulisan skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan;
2. Tidak melakukan plagiasi terhadap naskah karya orang lain;
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya;
4. Tidak memanipulasi dan memalsukan data;
5. Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh.

Demikian pernyataan ini saya buat dengan sesungguhnya dan tanpa paksaan dari pihak manapun.

Banda Aceh, 19 Juli 2024

Menyatakan,

Muhammad Aufa Lukman

ABSTRAK

Nama	:	Muhammad Aufa Lukman
NIM	:	190705094
Program Studi	:	Teknologi informasi
Judul	:	Uji Kerentanan Dan Pengamanan Menggunakan Nist Sp 800-53 *Risk Management Frameworks* Pada *Smart Home* Bardi (Studi Kasus : Bardi *Smart Light*).
Pembimbing I	:	Khairan AR, M.Kom
Pembimbing II	:	Mulkan Fadhil, S.T., M.T

Smart Home merupakan perangkat pintar yang menggunakan teknologi seperti *Internet Of Thing* (IOT) yang bertujuan untuk meningkatkan kenyamanan, efisiensi energi, keamanan, dan kualitas hidup penghuninya. namun terdapat beberapa permasalahan yang ada dalam *Smart Home* yang mana permasalah itu adalah kerentanan yang ada pada perangkat *smart home*, terutama pada Bardi *Smart Light* yang digunakan peneliti sebagai studi kasus pada penelitian ini. Peneliti menggunakan metoda NIST SP 800 – 53 untuk melakukan uji kerentanan dan pengamanan yang terdapat pada Bardi *Smart Light* menggunkan metode *Black Box Testing,* setelah dilakukan pengujian menggunakan *tools Nmap* dan *Wireshark* di temukannya kerentanan pada Bardi *Smart Light* yaitu terbacanya ip perangkat Bardi *Smart Light* yang dapat digunakan oleh *Attacker* untuk memanipulasi perangkat tersebut. Dengan begitu peneliti membrikan usulan keamanan berupa *device isolation metode* yang mana bertujuan untuk meningkatkan keamanan dengan cara mengisolasi akses antara perangkat-perangkat sehingga mengurangi resiko serangan siber yang dilakukan oleh *Attacker.*

Kata Kunci : *Internet of Thing* (IoT), *Smart Home*, NIST SP 800 - 53, *Black Box Testing, Smart Light*

ABSTRAK

Name	:	Muhammad Aufa Lukman
Nim	:	190705094
Study Program	:	Teknologi informasi
Title	:	Uji Kerentanan Dan Pengamanan Menggunakan Nist Sp 800-53 *Risk Management Frameworks* Pada *Smart Home* Bardi (Studi Kasus : Bardi *Smart Light*).
Advisors I	:	Khairan AR, M.Kom
Advisors II	:	Mulkan Fadhil, S.T., M.T

Smart Home is a smart device that uses technology such as the Internet Of Thing (IOT) which aims to improve the comfort, energy efficiency, security, and quality of life of its residents. However, there are several problems that exist in Smart Home, which are vulnerabilities that exist in smart home devices, especially in the Bardi Smart Light which researchers used as a case study in this study. Researchers used the NIST SP 800 - 53 method to test vulnerabilities and security contained in the Bardi Smart Light using the Black Box Testing method, after testing using the Nmap and Wireshark tools found vulnerabilities in the Bardi Smart Light, namely reading the ip of the Bardi Smart Light device which can be used by the Attacker to manipulate the device. That way researchers provide security proposals in the form of device isolation methods which aim to increase security by isolating access between devices so as to reduce the risk of cyber attacks carried out by attackers.

Keyword: *Internet of Thing* (IoT), *Smart Home*, NIST SP 800 - 53, *Black Box Testing, Smart Light*

KATA PENGANTAR

Alhamdulillah, Puji dan Syukur kita panjatkan kehadirat Allah Subhanahu Wata'ala. Dzat yang hanya kepada-Nya memohon pertolongan. Alhamdulillah atas segala pertolongan, rahmat, dan kasih sayang-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **Uji Kerentanan Dan Pengamanan Menggunakan Nist Sp 800-53 *Risk Management Frameworks* Pada *Smart Home* Bardi (Studi Kasus : Bardi *Smart Light*).** Shalawat dan salam senantiasa kita kirimkan kepada Rasulullah Shallallahu Alaihi Wasallam yang senantiasa menjadi sumber inspirasi dan teladan terbaik untuk umat manusia.

Tugas akhir ini dibuat untuk memenuhi tugas akhir perkuliahan dan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Strata 1 di Program Studi Teknologi Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry. Selain itu, skripsi ini juga dibuat sebagai salah satu wujud implementasi dari ilmu yang didapatkan selama masa perkuliahan di Program Studi Teknologi Informasi.

Penulis menyadari bahwa tugas akhir masih jauh dari kata sempurna. Oleh karena itu, penulis berharap dapat belajar lebih banyak lagi dalam mengimplementasikan ilmu yang didapatkan. Tugas akhir ini tentunya tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, sudah sepantasnya penulis dengan penuh hormat mengucapkan terima kasih dan mendoakan semoga Allah memberikan balasan terbaik kepada:

1. Ibunda Husna AR dan Ayahanda Lukman Ibrahim serta keluarga tercinta yang telah mendoakan, memberikan dukungan dan memotivasi dalam menyelesaikan tugas akhir ini.
2. Bapak Dr. Ir. Muhammad Dirhamsyah, M.T., IPU. Selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry Banda Aceh.
3. Bapak Bustami, M.Sc sebagai Penasehat Akademik dari semester 1 sampai semester 9 dan Bapak Mulkan Fadhil, S.T., M.T sebagai Penasehat Akademik pada semester 10 yang senantiasa memberikan arahan dan motivasi.

4. Bapak Khairan AR, M.Kom, selaku pembimbing 1 dan Bapak Mulkan Fadhil, S.T., M.T selaku pembimbing 2 yang telah meluangkan waktunya untuk membimbing saya dalam menyelesaikan tugas akhir.
5. Ibu Cut Ida Rahmadiana, S.Si selaku Staff Prodi Teknologi Informasi yang senantiasa membantu penulis dalam pemberkasan administrasi.
6. Ucapan terima kasih juga kepada kawan-kawan angkatan 2019 khususnya kepada grup bagi-bagi loker yang telah banyak membantu memberikan masukan dan motivasi.
7. Ucapan terima kasih juga kepada salah satu Adek Letting 2021 yang terkusus yang mana telah membantu penulis di saat keadaan krisis dalam hal apapun.
8. Terima kasih juga penulis haturkan untuk pihak yang telah membantu penulis dalam menyelesaikan tugas akhir ini yang tidak dapat penulis sebutkan satu persatu.

Akhir kata penulis menyadari bahwa tidak ada yang sempurna, penulis masih melakukan kesalahan dalam penyusunan tugas akhir. Oleh karena itu, penulis meminta maaf yang sedalam-dalamnya atas kesalahan yang dilakukan penulis. Penulis berharap semoga tugas akhir ini dapat bermanfaat bagi pembaca dan dapat dijadikan referensi demi pengembangan ke arah yang lebih baik. Kebenaran datangnya dari Allah dan kesalahan datangnya dari diri penulis. Semoga Allah SWT senantiasa melimpahkan Rahmat dan Ridho-Nya kepada kita semua.

Banda Aceh, 29 Mei 2024

Penulis,

Muhammad Aufa Lukman

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Thing (IoT) adalah suatu sistem yang memiliki tujuan untuk memperluas manfaat dari konektifitas internet yang terhubung secara terus menerus dan dapat mengirimkan data – data melalui jaringan agar dapat berinteraksi dengan perangkat – perangkat secara langsung (Efendi, 2018). Dalam beberapa tahun terakhir pengguna dari IoT untuk *smart home* mengalami kenaikan, perusahaan – perusahaan teknologi namun banyak juga yang tidak mempunyai *cloud service* sendiri dan menggunakan *Tuya Cloud* untuk PaaS (*Platform as a Service*) yang dapat melakukan otorisasi, interkoneksi, dan kendali melalui perangkat IoT sehingga menghemat biaya produksi dan *maintenance* dari perangkat IoT mereka (Tuya, 2021).

Platform Tuya telah mengembangkan perangkat IoT untuk lebih dari 7600 produsen dari berbagai merek, menciptakan ekosistem yang seragam dalam hal port komunikasi dan metode otentikasi. Akibatnya, aplikasi yang dibuat oleh satu merek perangkat IoT menggunakan Tuya Cloud PaaS dapat mengakses dan mengontrol perangkat dari merek lain, yang diciptakan oleh pembuat yang berbeda. Hal ini menciptakan celah keamanan dalam perangkat IoT yang perlu diuji kerentanannya melalui serangkaian aktivitas terstruktur untuk mendeteksi, menganalisis, dan mengevaluasi celah keamanan dalam sistem, aplikasi, atau infrastruktur TI (Kurnia Bakti dkk., 2023).

Keamanan pada perangkat IoT khususnya yang menggunakan Tuya Cloud sebagai PaaS (*Platform as a Service*) perlu di perhatikan dikarenakan dalam beberapa tahun terakhir serangan terhadap kerentanan terhadap perangkat IoT *Smart Home* yang sangat tinggi, memungkinkan perangkat *Smart Home* menjadi rentan terhadap serangan – serangan seperti *Man-In-The-Middle Attack*, *Replay Attack* dan *Packet Sniffing* (Hafi, 2023).

Penulis menerapkan pengamanan, yang mana pengamanan adalah upaya untuk melindungi dari ancaman atau bahaya, mencakup perlindungan, deteksi, respon, pencegahan, serta aspek keamanan fisik, informasi, komputer, dan

jaringan (Haris dkk., 2022), Tujuannya adalah untuk mempertahankan keamanan, keselamatan, serta integritas objek atau data yang diamankan.

Salah satu produk *Smart Home* dari Bardi adalah *Smart Light*, *smart ligtht* merupakan lampu pintar yang yang dapat dikendalikan secara *realtime* melalui aplikasi *mobile*. Dengan adanya sistem ini diharapkan dapat mempermudah pengguna untuk mengendalikan lampu ruangan yang ada di rumah, terutama ketika pengguna tidak berada di rumah, dengan kondisi lampu tetap terkoneksi ke internet. Penelitian ini menggunakan NIST SP 800-53 IoT Risk Management Framework dari NIST (National Institute of Standards and Technology) untuk menguji kerentanan dan pengamanan pada Bardi Smart Home. Pada tahun 2021, Amerika Serikat merilis panduan ini yang digunakan oleh pemerintah dan perusahaan untuk mengamankan perangkat IoT dan jaringan server. Oleh karena itu, penelitian ini berjudul: Uji Kerentanan dan Pengamanan Menggunakan NIST SP 800-53 Risk Management Framework pada Bardi Smart Home (Studi Kasus: Bardi Smart Light).

1.2 Rumusan Masalah

1. Bagaimana melakukan uji kerentanan dan pengamanan pada perangkat IoT *Smart Home* Bardi *Smart Light* menggunakan NIST SP 800-53 *Risk Management Frameworks* ?
2. Apa saja risiko celah keamanan pada *Smart Home,* khususnya pada perangkat lampu bardi, dan bagaimana NIST SP 800-53 *Risk Management Frameworks* dapat digunakan untuk mencari dan mengelola risiko tersebut ?

1.3 Tujuan Penelitian

1. Mengidentifikasi kerentanan keamanan dan pengamanan yang mungkin ada di perangkat IoT Bardi *Smart Light*.
2. Mengetahui kerentanan yang ada pada Bardi *Smart Home* menggunakan NIST SP 800 53 *Risk Management Frameworks.*

1.4 Batasan Masalah

1. Perangkat yang akan dipakai dalam penelitian ini adalah perangkat asli (*Real Device*) yaitu perangkat *Smart Home* bardi *Smart Light* yang akan dilakukan uji kerentanan dan keamanan.
2. Penelitian yang akan di lakukan mengacu pada NIST SP 800-53 *Risk Management Frameworks* Untuk menguji dan mengevaluasi tingkat keamanan Bardi *Smart Light*.
3. Penelitian di tujukan pada perangkat Bardi *Smart Light*

1.5 Manfaat Penelitian

1. Penelitian ini memberikan pengetahuan dan pemahaman tentang ilmu pengujian keamanan dalam mengidentifikasi kerentanan dalam *Smart Home.*
2. Penelitian ini mengidentifikasi potensi kerentanan atau celah keamanan yang terdapat dalam sistem *Smart Home*, maka perusahaan dan pengembang dapat memperbaiki dan memperkuat sistem agar lebih aman.
3. Penelitian ini bermanfaat untuk memastikan bahwa informasi dan privasi milik pengguna terlindungi dengan baik, dengan langkah – langkah untuk mengamankan data pribadi pengguna.

BAB II
LANDASAN TEORI

2.1 *Internet of Things* (IoT)

Internet of Things (IoT) adalah konsep yang memungkinkan entitas dilengkapi teknologi sensor, sistem, dan aplikasi untuk saling berkomunikasi, mengendalikan, dan bertukar data melalui internet (Junaidi, 2015). Integrasi IoT menjadi bagian esensial dalam pekerjaan saat ini yang menuntut konektivitas lintas bidang secara berkelanjutan. IoT berperan penting dalam revolusi industri 4.0 atau *cyber physical system* yang berfokus pada otomatisasi kolaboratif berbasis teknologi *cyber*.

IoT menjadi komponen inti revolusi industri 4.0 untuk meningkatkan manfaat konektivitas internet. Implementasi IoT dapat meningkatkan efisiensi, produktivitas, kualitas, serta memfasilitasi integrasi dan otomatisasi sistem Namun, adopsi IoT juga membawa tantangan keamanan data, privasi, dan standarisasi yang membutuhkan pendekatan komprehensif (Setiadi & Muhaemin, 2018).

Menurut penelitian (Dwi Santika dkk., 2022) IoT adalah sebuah revolusi teknologi yang menyatukan dunia fisik dengan dunia digital. Konsepnya adalah menghubungkan berbagai objek, peralatan, dan mesin ke dalam sebuah jaringan yang terintegrasi melalui internet. Setiap entitas dilengkapi dengan sensor dan penggerak (actuator) sehingga dapat saling berkomunikasi dan bertukar informasi secara real-time. Dengan IoT, manusia dapat memantau dan mengendalikan kinerja dari perangkat-perangkat tersebut melalui jaringan lokal maupun global.

2.2 *Smart Home*

Smart Home atau hunian cerdas merupakan sebuah konsep yang mengintegrasikan aplikasi, teknologi, dan layanan dalam lingkungan tempat tinggal dengan berbagai fungsi yang bertujuan untuk meningkatkan keamanan, efisiensi, serta kenyamanan bagi penghuninya. Sistem ini terdiri dari perangkat-perangkat yang memiliki kemampuan untuk memantau, mengendalikan, dan mengotomatisasi berbagai aspek dalam rumah yang dapat dioperasikan melalui

komputer. Hunian cerdas dirancang dengan bantuan komputer agar dapat memberikan kenyamanan, keamanan, dan penghematan energi secara otomatis sesuai dengan pengaturan yang telah diprogram oleh penghuni sebelumnya pada komputer yang terhubung dengan sistem di rumah atau gedung tersebut (Masykur & Prasetiyowati, 2018).

Beberapa teknologi *Smart Home System* :

1. *August Smart Pro* August Smart Pro merupakan teknologi yang digunakan untuk keamanan rumah yang bisa disinkronisasikan dengan ponsel pintar.
2. *IR Remote Control* Jika kamu ingin sesuatu yang praktis, teknologi satu ini bisa memudahkan seseorang ketika berada di rumah. Pasalnya, sistem ini memungkinkan untuk memiliki satu remote yang bisa digunakan pada semua perangkat elektronik yang ada di rumah.
3. *Mirror Smart Mirror* Teknologi smart home yang satu ini berbentuk seperti kaca cermin yang bisa digunakan untuk berbagai hal di rumah.
4. *Motion Sensor* bisa digunakan untuk mengontrol nyala dan mati lampu di rumah tanpa harus menggunakan saklar.
5. *Smart Refrigerator* atau kulkas pintar merupakan kullas berbasis teknologi Internet of Things (IoT) yang dapat menjadi salah satu alternatif mengatasi masalah tidak terpantaunya waktu batas pemanfaatan makanan yang tersimpan di kulkas,serta adanya pola belanja yang tidak berdasarkan kebutuhan dan kapasitas kulkas karena tidak terpantaunya isi kulkas yang sudah ada.
6. *Smart Home Speaker* System merupakan perangkat *smart home* berupa speaker cerdas yang dapat digunakan untuk mengontrol berbagai macam hal.
7. *Smart Entertaiment* merupakan perangkat *smart home* yang telah banyak digunakan di Indonesia.
8. *Smart Connectivity* Perangkat *smart home* yang satu ini memungkinkan seseorang untuk mengendalikan rumah dari jarak jauh hanya dengan satu perangkat, dengan menggunakan perangkat Smart Connectivity.
9. *Smart Security* memungkinkan adanya sistem pengamanan pada suatu rumah selama 24 jam penuh.

10. *Smart Door Lock* Perangkat Smart Door Lock akan memberikan pengamanan ganda pada suatu rumah dengan menggunakan teknologi kunci pintar berupa fingerprint, handphone, dan password.
11. *Smart Home Appliances* Adanya teknologi rumah pintar, peralatan di rumah menjadi lebih nyaman, aman, dan efisien.
12. *Smart Lighting* mampu mengintegrasikan hampir setiap aspek kehidupan di dalam rumah, termasuk pencahayaan.

Konsep hunian cerdas atau *Smart Home* bertujuan untuk mengintegrasikan berbagai perangkat sensor dan komunikasi digital secara terpadu. Dalam lingkungan hunian cerdas yang optimal, perangkat-perangkat tersebut mampu saling bertukar informasi dan berkomunikasi dengan lancar untuk menawarkan layanan seperti pengelolaan energi yang lebih efisien, peningkatan sistem keamanan terhadap upaya penyusupan, serta fitur-fitur inovatif untuk hiburan dan menciptakan suasana rumah yang lebih menyenangkan bagi penghuninya. (Gram-hanssen & Darby, 2016).

2.3 Bardi *Smart*

Bardi *Smart* adalah brand lokal di indonesia yang memproduksi produk elektronik pintar. Dengan menggunakan perangkat *Smartphone* yang sudah terinstal aplikasi BARDI, Pengguna dapat mengendalikan produk – produk pintar tersebut (Somantri & Marsono, 2021). ada beberapa Bardi *Smart* yaitu :

1. Bardi *Smart Light Bulb 9W RGBWW*
   Merupakan bohlam pintar yang bisa dinyalakan dan dimatikan, diubah warna, dan fitur kecerahan melalui aplikasi.
2. Bardi *Smart LED Bulb RGB*
   Merupakan Bohlam pintar yang dapat di atur warna dan kecerahannya melalui aplikasi yang ada.
3. Bardi *Smart IR Remote*
   Merupakan salah satu produk Bardi yang berupa *Universal IR Remote* yang bisa di kendalikan melalui aplikasi.
4. Bardi *Smart IP Camera Outdoor PTZ*
   Merupakan kamera pintar yang dapat menyalurkan video dan juga suara langsung melalui *Smartphone*.

5. Bardi *Smart IP Camera Outdoor Static*

   Merupakan kamera pintar yang bisa di pakai untuk pengawasan di luar ruangan yang bisa memberikan notifikasi dan mempunyai tiga mode malam yang dapat di pilih.

Dan juga memiliki banyak perangkat yang sangat berguna dalam berbagai kebutuhan seperti *Security Series, Pet Series, Living Series, lighting Series, Electrical Series,* dan *Curtain Series, dan semua perangkat tersebut bisa di akses melalui* aplikasinya sendiri yang terdapat di *Google Play Store* dan *App Store* dan bisa diitegrasikan dengan *Google Home, Alexa, Siri,* dan *Smartthing* yaitu BARDI *Smart Home.*

2.4. NIST SP 800 - 53

adalah panduan yang diterbitkan oleh National Institute of Standards and Technology (NIST) yang menyediakan kerangka kerja untuk mengelola risiko keamanan informasi. Dokumen ini menawarkan serangkaian kontrol keamanan dan privasi yang komprehensif untuk melindungi sistem informasi dan data yang diproses, disimpan, dan ditransmisikan oleh organisasi, terutama di sektor federal. Kontrol ini mencakup berbagai aspek, seperti manajemen akses, keamanan fisik, perlindungan data, dan pemulihan bencana, dan dirancang untuk membantu organisasi memastikan kepatuhan terhadap standar keamanan siber yang ketat (Afiansyah & Amiruddin, 2022).

2.5 *Risk Management*

Menurut Kamus Besar Bahasa Indonesia (KBBI) bisa di artikan sebagai penggunaan sumber daya secara efektif untuk mencapai sasaran, dan istilah manajemen risiko bersal dari kata *to manage* yang memiliki arti control, dan dalam bahasa indonesi di artikan sebagai pengendalian, menangani, mengelola (Akbar. C dkk., 2022). Dan terdapat beberapa tahap di dalam manajemen risiko sebagai berikut :

1. Identifikasi Risiko

   Langkah pertama di dalam manajemen risiko adalah mengidentifikasi risiko yang ada dan mungkin terjadi, risiko bisa berasal dari berbagai sumber yang tidak di ketahui, seperti lingkungan eksternal, operasional, keuangan, teknologi, atau faktor – faktor lainnya. Identifikasi risiko dilakukan dengan

cara memperluas cakupan kemungkinan dugaan risiko dengan melihat melalui berbagai aspek seperti aspek ekonomi, aspek sosial, aspek regulasi dan lainnya.

2. Penilaian Risiko

Setelah di identidikasi, langka berikutnya adalah menilai risiko. Penilaian risiko dapat dilakukan dengan melakukan *assesment* atau menilai setiap kemungkinan risiko yang dapat dilihat dari seberapa besar efek dari risiko tersebut, hal ini bertujuan agar risiko – risiko ini dapat diurutkan berdasarkan prioritas.

3. Pengelolaan/Respon Terhadap Risiko

   Langkah selanjutnya adalah memastikan bagaimana mengelola atau merespon risiko yang telash selesai dinilai/dianalisa. Hal ini untuk membuat srategi pengelolaan risiko yang efektif. Ada lima teknik dalam manajemen risiko, yaitu penghindaran, retensi, penyebaran, pencegahan dan pengurangan kerugian, dan tranfer melalui asuransi dan kontrak.

4. Implementasi

   Setelah tiga tahap di atas maka strategi pengelolaan risiko ditentukan, langkah berikutnya adalah mengimplementasikan strategi tersebut. Implementasi pun dilakukan dengan tindakan yang telah direncanakan untuk mengurangi risiko atau menghindar dari risiko yang telah diidentifikasi.

   Tahapan dalam manajemen risiko bisa bervariasi tergantung sumber yang digunakan, tahapan tersebut meliputi identifikasi risiko dan implementasi.

Management risiko merupakan proses tersistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko di dalam sebuah organisasi atau proyek, yang bertujuan untuk memanajement atau mengelola risiko dengan cara memonitor sumber risiko, melacak, dan menjalankan serangkaian percobaan agar dampak risiko bisa diminimalisasi (Dewi, 2019).

2.6 *Framework*

Merupakan sebuah struktur kerja atau kerangka yang digunakan dalam mengembangkan aplikasi atau program komputer. *Framework* menyediakan fungsi – fungsi yang dasar dan standar yang bisa digunakan pengembang untuk membangun sebuah aplikasi atau program secara konsisten dan efisien. *Framework* bisa berupa bebrapa instruksi atau fungsi dasar yang mengatur sebuah aturan tertentu dan berinteraksi sesama (Jaya & Sahlinal, 2017).

Terdapat beberapa tahapan dalam *Framework* sebagai berikut :

1. *Information Gathering*

   Hal pertama yang akan di lakukan dalam uji kerentanan adalah mencari informasi tentang sesuatu yang akan diuji. Informasi ini dapat diperoleh

melalui berbagai sumber, seperti pencarian publik, pencarian DNS, dan pencarian whois.

2. *Network Mapping*

   Langkah selanjutnya adalah pemetaan jaringan untuk mengetahui topologi jaringan dan sistem yang terhubung ke dalamnya.

3. *Vulnerability Identification*

   Langkah ketiga adalah mengidentifikasi kerentanan pada sistem yang telah dipetakan. Hal ini dilakukan dengan menggunakan alat pemindaian kerentanan untuk menemukan kerentanan yang mungkin ada pada sistem.

4. *Penetration*

   Langkah keempat adalah melakukan penetrasi ke dalam sistem untuk mengetahui seberapa dalam kerentanan tersebut dapat dimanfaatkan. Hal ini dilakukan dengan menggunakan teknik-teknik hacking untuk mengeksploitasi kerentanan yang telah teridentifikasi.

5. *Gaining Access*

   Langkah kelima adalah mendapatkan akses ke dalam sebuah sistem atau perangkat yang telah diuji. Hal ini dilakukan untuk mengetahui seberapa dalam kerentanan tersebut dapat dimanfaatkan dan untuk mengevaluasi tingkat keamanan sistem.

6. *Maintaining Access*

   Langkah keenam adalah mempertahankan akses ke dalam sistem yang telah diuji. ini dilakukan untuk mengetahui seberapa lama kerentanan tersebut dapat dimanfaatkan dan untuk mengevaluasi tingkat keamanan sistem.

7. *Covering Tracks*

   Langkah ketujuh adalah menutup jejak atau menghapus semua jejak yang ditinggalkan selama proses uji kerentanan. Hal ini dilakukan untuk menghindari deteksi oleh sistem keamanan.

Beberapa tahap *Framework* dalam melakukan uji kerentanan dalam sebuah sistem atau perangkat (Rojaburrohman, 2023).

2.7 Pengujian Kerentanan

Pada penelitian ini penulis menggunakan *Risk Management Framework* yang di kembangkan oleh *National Institute of Standard and Technology* (NIST)

SP 800-53, berikut merupakan tahapan dalam dokumen panduan NIST SP 800-53 yaitu : *Identify, Protect, Detect, Respond, Recover.* Penulis menggunakan NIST SP 800-53 dikarenakan *framework* ini memiliki kelengkapan dant erpercaya dalam mengamankan sistem informasi, termasuk perangkat IoT dalam jaringan rumah (Tan, 2020). Yang menunjukkan bahwa penggunaan *Framework* NIST dan CIS Controls dapat meningkatkan keamanan keamanan siber organisai dan mengurangi risiko yang mengancam aktivitas perangkat IoT, dan *Framework* ini dapat mengidentifikasi, melindungi, mendeteksi, merespon, dan memulihkan diri terhadap ancaman siber.

Berikut adalah tahapan – tahapan dalam metode NIST *Risk Management Framework* di penelitian ini :

1. *Identify*

   Penulis mengidentifikasi perangkat IoT yang akan digunakan untuk penelitian yaitu *Smart Home* bardi *Smart Light* dengan melakukan *scan adivice* IoT bardi menggunakan perangkat lunak Kali Linux untuk mengidentifikasi resiko pada perangkat *smart light* yang ada dalam jaringan rumah seperti kerentanan keamanan, oleh karna itu penulis melakukan penilaian resiko terhadap perangkat bardi *smart light.*

2. *Protect*

   Pada tahap *protect* Penulis menerapkan tindakan perlindungan untuk meningkatkan keamanan yang terdapat pada perangkat IoT *smart home* bardi *smart light* setelah mengidentifikasi kemungkinan kerentanan dengan sistem *divice isolation* atau pemisahan jaringan *smart home* dari jaringan utama.

3. *Detect*

   Pada tahap *detect* (deteksi) penulis melakukan rangkaian *Network Mapper* dan *Packet capturing* untuk melihat apakah ada port yang terbuka dan memantau lalu lintas jaringan yang ada pada perangkat IoT ketika digunakan.

4. *Respond and Recover*

   Pada tahapan *respond* ditujukan untuk menangani ancaman dan insiden keamanan yang terdeteksi pada tahap sebelumnya, selanjutnya *recover* penulis memberikan beberapa rekomendasi untuk meningkatkan keamanan pada perangkat IoT bardi *smart home.*

2.8 *Black Box Testing*

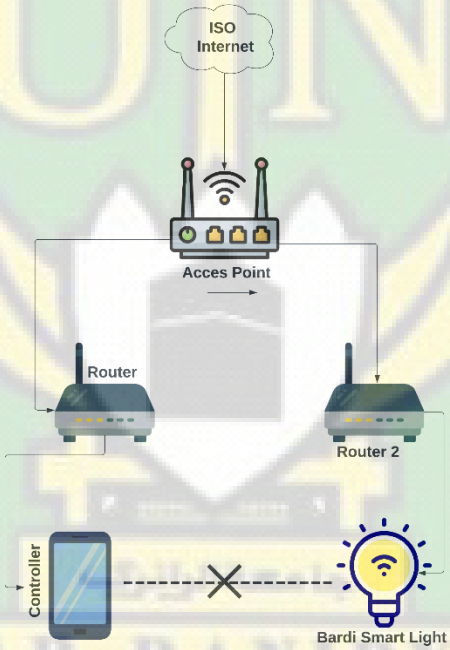
Black box testing adalah metode pengujian perangkat lunak yang dilakukan tanpa memahami struktur internal atau kode sumber aplikasi yang diuji. Pengujian ini berfokus pada aspek fungsionalitas aplikasi dari sudut pandang pengguna akhir. Tujuannya adalah untuk memvalidasi bahwa aplikasi beroperasi sesuai dengan spesifikasi persyaratan fungsional yang telah ditetapkan dan memberikan performa yang optimal bagi pengguna.

Dalam pengujian black box, penguji hanya perlu memahami spesifikasi perangkat lunak dan menguji aplikasi layaknya pengguna biasa. Penguji memasukkan berbagai jenis input dan mengamati output yang dihasilkan, tanpa mempedulikan bagaimana proses internal aplikasi bekerja. Aspek-aspek yang diuji meliputi fungsionalitas fitur, validasi input dan output, antarmuka pengguna, perilaku pada kasus batas (boundary values), isu keamanan, serta kompatibilitas dengan berbagai platform dan lingkungan.

Berbagai teknik dapat digunakan dalam black box testing, seperti pengujian partisi ekuivalen (equivalence partitioning), analisis nilai batas (boundary value analysis), tabel keputusan (decision table testing), dan pengujian berdasarkan use case. Data uji disiapkan berdasarkan spesifikasi persyaratan aplikasi. Melalui black box testing, penguji dapat mengidentifikasi cacat fungsional, kesalahan pada antarmuka pengguna, serta potensi celah keamanan pada aplikasi. Meskipun tidak memberikan informasi tentang perbaikan kode, pengujian ini sangat penting untuk memastikan aplikasi memenuhi persyaratan dan berfungsi dengan baik dari perspektif pengguna.

2.9 Pengamanan

Terdapat sebuah pendekatan yang ditawarkan sebagai metode pengamanan jaringan untuk sistem *Smart Home* berbasis *Internet of Things* (IoT). Pendekatan ini didasarkan pada mekanisme isolasi dan perlindungan berbasis perangkat keras yang dapat dikonfigurasi ulang dan beroperasi sebagai unit pemisah dinamis antara perangkat IoT dan jaringan (Dietz dkk., 2018), Prinsip kerja metode isolasi perangkat ini mengacu pada pemisahan perangkat IoT ke dalam segmen jaringan yang terpisah. Metode isolasi perangkat sangat direkomendasikan untuk digunakan sebagai langkah keamanan dalam melindungi perangkat cerdas (*Smart Device*) dari serangan pada sistem *Smart Home*. Untuk melakukan isolasi jaringan terhadap perangkat IoT, setidaknya dibutuhkan dua buah router agar dapat memisahkan jaringan pengguna dan jaringan *Smart Home* secara terpisah.



Gambar II. 1 *Device Isolation*

2.10 Penelitian Relevan

Penelitian relevan adalah beberapa kumpulan dari penelitian – penelitian sebelumnya yang telah di kumpulkan dan diterbitkan agar dapat mendukung penelitian, mendukung referensi penulis dalam melakukan penelitian, dan menghindari hasil yang sama dalam penelitian.

Penelitian pertama, yang dilakukan oleh Ahmad Bisyrul Hafi tahun 2023 dengan judul "Uji Kerentanan Dan Pengamanan Menggunakan NIST SP 800-53 *Risk Management Frameworks* Pada Jaringan *Off-The-Shelf Equipments Smart Home Internet Of Things* (IoT)" dari penelitian ini penulis mecoba untuk memberikan sebuah solusi yang mudah dan terjangkau dalam mengamankan perangkat IoT dalam jaringan rumah oleh pengguna yang tidak mengerti tentang keamanan jaringan, hasil dari penelitian ini menunjukkan terdapat kerentanan yang dapat diekploitasi menggunakan teknik *port scanning, Man-In-The-Middle Attack,* dan *brute-force attack* (Hafi, 2023).

Penelitian kedua, yang dilakukan oleh Fahrizal Satya Laksamana tahun 2019 dengan judul "Analisis Keamanan Jaringan Dalam *Smarthome Internet Of Things* (IoT) Menggunakan *Cisco Packet Tracer* Dengan Metode Square" dari penelitian ini penulis mencoba untuk menemukan dan mengurangi celah keamanan pada infrastruktur *Smarthome-Home Serve* dan *Smarthome-Remote Serve.* Hasil dari penelitian ini berupa menimbulkan prioritas persyaratan keamanan jaringan pada *Smarthome-home Serve* dan *Smarthome-Remote Serve* (Laksamana, 2019).

Penelitian ketiga, yang dilakukan oleh Muhammad Ikum tahun 2023 dengan judul "Implementasi Packet Tracer 8.0 Pada Simulator Pintu Rumah Pintar Berbasis Teknologi Radio *Frequency Identification*" dari penelitian ini penulis mencoba untuk meningkatkan pintu rumah pintar yang dirancang menggunakan *Packet Tracer* 8.0 agar dapat bertahan dari potensi serangan dunia maya dan akses tidak sah, hasil dari pengujian menunjukkan bahwa *Protocol Smart Home* yang diciptakan bisa berjalan dengan baik sesuai dengan tahapan yang telah di tentukan (Ikum, 2023).

Penelitian keempat, yang dilakukan oleh Dipamadya Kalingga tahun 2023 dengan judul "Perancangan Algoritma TwoFactor Authentication Untuk Keamanan Jaringan Internet of Things" dari penelitian ini penulis mencoba membangun suatu sistem keamanan jaringan IoT dua autentikasi yaitu berupa *password* dan OTP (*One time password*) yang perlu di input oleh client atau perangkat IoT untuk dapat mengirim data sensor suhu dan kelembapan ke dalam

server. Hasil pengujian sistem menunjukkan sistem yang memenuhi parameter keamanan jaringan (Kalingga, 2023).

Penelitian kelima, yang dilakukan oleh Muhammad Nur Ikhsyan tahun 2022 dengan judul "Perancangan Smart Aquarium Berbasis Internet Of Things (Iot)" dari penelitian ini penulis mencoba untuk merancang *Smart Aquarium* berbasis *Internet of Things* (IoT) yang bisa monitoring pH, suhu dan kekeruhan air akuarium serta sistem untuk pemberian makan secara otomatis berbasis IoT, hasil dari penelitian rancang bangun *Smart Aquarium* berbasi IoT berjalan dengan baik (Ikhsyan, 2022).

Berikut adalah rangkuman penelitian relevan yang terdapat pada tabel di bawah ini

No	Peneliti/Tahun	Judul Penelitian	Isi Penelitian	Hasil Penelitian
1	Ahmad Bisyrul Hafi (tahun 2023)	Uji Kerentanan Dan Pengamanan Menggunakan NIST SP 800-53 *Risk Management Frameworks* Pada Jaringan *Off-The-Shelf Equipments Smart Home Internet Of Things* (IoT)	Teknik & Perangkat Uji Kerentanan dan Pengamanan *Internet of Things Smart Home*	hasil dari penelitian ini menunjukkan kerentanan yang dapat diekploitasi menggunakan teknik *port scanning, Man-In-The-Middle Attack,* dan *brute-force attack*

2	Fahrizal Satya Laksamana tahun 2019	Analisis Keamanan Jaringan Dalam *Smarthome Internet Of Things* (IoT) Menggunakan *Cisco Packet Tracer* Dengan Metode Square	Teknik & Analisis Kerentanan dan Pengamanan *Internet of Things Smart Home*	Hasil dari penelitian ini berupa menimbulkan prioritas persyaratan keamanan jaringan pada *Smarthome-home Serve* dan *Smarthome-Remote Serve*
3	Muhammad Ikum tahun 2023	Implementasi Packet Tracer 8.0 Pada Simulator Pintu Rumah Pintar Berbasis Teknologi Radio *Frequency Identification*	Teknik & Perangkat Uji Kerentanan dan Pengamanan *Internet of Things Smart Home*	hasil dari pengujian menunjukkan bahwa *Protocol Smart Home* yang diciptakan bisa berjalan dengan baik sesuai dengan tahapan tertentu
4	Dipamadya Kalingga tahun 2023	Perancangan Algoritma TwoFactor Authentication Untuk Keamanan Jaringan Internet of Things	Teknik & Perancangan Keamanan Jaringan IoT	Hasil pengujian sistem menunjukkan sistem yang memenuhi parameter keamanan jaringan
5	Muhammad Nur Ikhsyan tahun 2022	Perancangan Smart Aquarium Berbasis *Internet Of Things* (Iot)	Teknik & Perancangan *Smart Home* Berbasis IoT	hasil dari penelitian rancang bangun *Smart Aquarium* berbasi IoT berjalan dengan baik

Tabel II. 1 Penelitian Relevan

2.11 Kerangka Teoritis

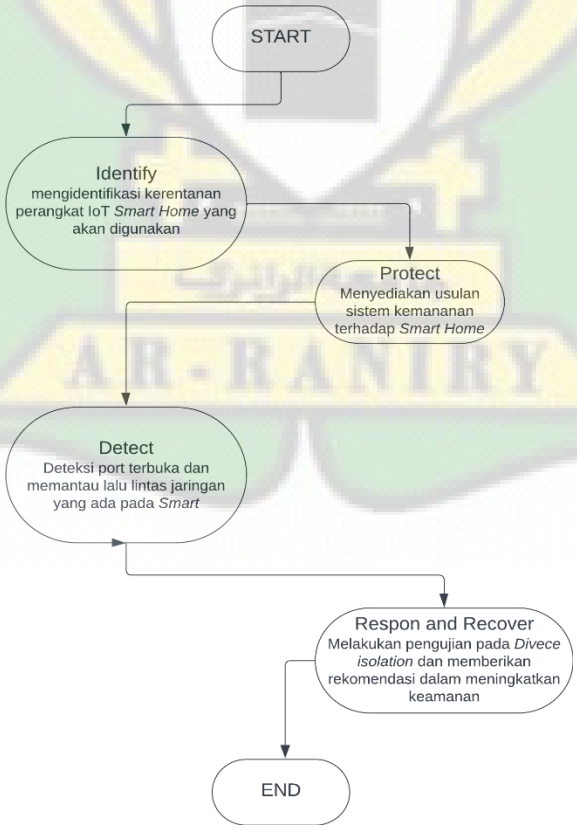
Penelitian ini terjadi dikarenakan banyaknya terjadi serangan dalam beberapa tahun terakhir terhadap kerentanan perangkat IoT *Smart Home* yang sangat tinggi, untuk mengantisipasi serangan terhadap perangkat IoT *Smart Home* khususnya Bardi *Smart Home* maka dilakukan perencanaan pengujian perangkat tersebut. Pengujian menggunakan metode Risk Management Framework dengan panduan NIST SP 800-53 pada perangkat *Smart Home*, setelah diidentifikasi resiko kerentanan penulis memberikan usulan kemanan berdasarkan risiko kerentanan, selanjutnya dilakukan deteksi pada perangkat *Smart Home* untuk melihat kerentanan, dan melakukan pemantauan port dan jaringan pada perangkat *Smart Home*, selanjutnya pengujian pada sistem usulan dan memberikan rekomendasi keamanan.

Gambar II. 2 Kerangka Teoritis

BAB III
METODELOGI PENELITIAN

3.1. Tahapan Penelitian

Metodologi yang digunakan dalam penelitian ini adalah Risk Management Framework (RMF) yang dikembangkan oleh National Institute of Standards and Technology (NIST) SP 800-53. Tujuan utamanya adalah untuk mengevaluasi kerentanan perangkat IoT Smart Home. Tahapan-tahapan yang terdapat dalam dokumen panduan NIST SP 800-53 meliputi Identify, Protect, Detect, Respond, dan Recover. Penulis memilih menggunakan NIST SP 800-53 karena framework ini diakui sebagai yang paling komprehensif dan dapat dipercaya dalam mengamankan perangkat IoT pada jaringan rumah, sebagaimana didukung oleh penelitian sebelumnya (Hafi, 2023). Berikut adalah tahapan-tahapan metode NIST Risk Management Framework yang diterapkan dalam penelitian ini. pada gambar III.1 merupakan tahapan penelitian yang di tuangkan pada gambar.



Gambar III. 1 Tahapan Penelitian

1. *Identify*

   Penulis mengidentifikasi perangkat IoT yang akan digunakan untuk penelitian yaitu *Smart Home* bardi *Smart Light* dengan melakukan *scan divice* IoT bardi menggunakan perangkat lunak Kali Linux untuk mengidentifikasi resiko pada perangkat *smart light* yang ada dalam jaringan rumah seperti kerentanan keamanan, oleh karna itu penulis melakukan penilaian resiko terhadap perangkat bardi *smart light.*

2. *Protect*

   Pada tahap *protect* Penulis menerapkan tindakan perlindungan untuk meningkatkan keamanan yang terdapat pada perangkat IoT *smart home* bardi *smart light* setelah mengidentifikasi kemungkinan kerentanan dengan sistem *divice isolation* atau pemisahan jaringan *smart home* dari jaringan utama.

3. *Detect*

   Pada tahap *detect* (deteksi) penulis melakukan rangkaian *Network Mapper* dan *Packet capturing* untuk melihat apakah ada port yang terbuka dan memantau lalu lintas jaringan yang ada pada perangkat IoT ketika digunakan.

4. *Respond and Recover*

   Pada tahapan *respond* ditujukan untuk menangani ancaman dan insiden keamanan yang terdeteksi pada tahap sebelumnya, selanjutnya *recover* penulis memberikan beberapa rekomendasi untuk meningkatkan keamanan pada perangkat IoT bardi *smart home.*

3.2. Objek penelitian

objek yang ingin di teliti, yaitu *Internet of Things* (IoT) *Smart Home* Bardi *Smart Light Bulb 9W.*

3.3. Teknik Pengumpulan Data

Penulis menggunakan teknik pengumpulan data pada penelitian ini adalah sebagai berikut

1. Studi Pustaka

Disini peneliti melakukan pengumpulan data menggunakan metode studi pustaka, yang mana informasi dan teori didapatkan dari buku, jurnal, skripsi, dan hasil penelitian terkait dengan penelitian ini, sebagai referensi dalam mengumpulkan informasi – informasi yang dibutuhkan.

2. Observasi

Di sini peneliti melakukan observasi pada perangkat *smart home Internet of Things* (IoT). Peneliti telah melakukan instalasi aplikasi *Bardi smart home* dan melakukan pemindaian menggunakan *software* Nmap (*Network Mapper*) dan *Wireshark* untuk mengetahui kerentanan dan lalu lintas jaringan pada perangkat *smart light*.

3.4. Alat dan Bahan Penelitian

Beberapa alat yang diperlukan dalam menjalankan penelitian ini yaitu perangkat keras dan perangkat lunak. Alat penelitian ini meliputi :

1. Perangkat Keras

   Berikut spesifikasi perangkat keras yang akan digunakan untuk pengumpulan data dalam penelitian pada tabel III.1 berikut:

Tabel III.1 Spesifikasi Perangkat Keras

Komponen	Spesifikasi
BARDI SMART LIGHT BUBL 9W	Daya 9 watt,fitur pintar,jenis koneksi wifi nirkabel
Dual Band Wireless AC750 ROUTER/ADSL2 + Modem Router	Triple WAN Fail-Over (ADSL / Ethernet WAN / 3G / 4G LTE)
CPU	*Intel(R) Core(TM) i5-11400H Processor @ 2.70GHz (12 CPUs),~ 2.69 GHz*

RAM	*DDR4 8,00 GB*
Storage	*512 GB SSD NVMe*
Graphic	*Intel(R) UHD Graphics Family / NVIDIA GeForce RTX 3050 Laptop GPU*

Tabel III. 1 Alat Penelitian

Dapat dilihat berdasarkan tabel di atas spesifikasi alat dan bahan yang dipakai dalam penelitian yang dilakukan terdiri dari :

A. BARDI SMART LIGHT

Spesifikasinya memiliki daya 9 wat,fitur pintar yang memiliki jenis koneksi wifi nirkabel.

B. Dual Band Wireless AC750 ROUTER/ADSL2 + Modem Router

Triple WAN Fail-Over (ADSL / Ethernet WAN / 3G / 4G LTE)

C. CPU *(Central Processor Unit)*

Spesifikasinya yaitu *Intel(R) Core(TM) i5-11400H Processor* dan kecepatan oprasi yaitu *@ 2.70GHz (12 CPUs),~ 2.69 GHz.*

D. RAM *(Random Access Memory)*

Yang memiliki *RAM* sebesar 8GB.

E. Storage

Penyimpanan yang dimiliki adalah 512 GB SSD (Solid State Drive) penyimpanan data pada komputer dan perangkat elektronik moderen

F. Graphic

Spesifikasinya yaitu *Intel(R) UHD Graphics Family / NVIDIA GeForce RTX 3050 Laptop GPU*

2. Perangkat Lunak

A. Perangkat Kali Linux

Penulis menggunakan perangkat lunak dalam penelitian ini yaitu Kali Linux. Kali Linux merupakan distribusi Linux yang telah dirancang untuk melakukan uji penetrasi dan keamanan informasi, dan kali linux sendiri merupakan perangkat lunak *open source*, Kali Linux merupakan sistem informasi

yang sangat populer digunakan oleh kalangan profesional keamanan komputer dan para ahli keamanan.

B. Tools

Tools yang digunakan oleh peneliti dalam melakukan penelitian ini yaitu *Nmap, Wireshark, Tuya library* dan Bardi *Smart home,* berikut penjelasan dari tools yang di gunakan.

a. *Nmap*

Nmap(Network Mapper) adalah alat pemindaian jaringan yang akan digunakan dalam menemukan host dan layanan jaringan komputer, memungkinkan pengguna untuk dapat memeriksa port yang terbuka, protokol yang digunkan, sistem oprasi yang berjalan dan informasi yang berguna dari komputer. Nmap dapat membantu untuk mendeteksi kemanan jaringan yang mungkin terdapat kerentanan.

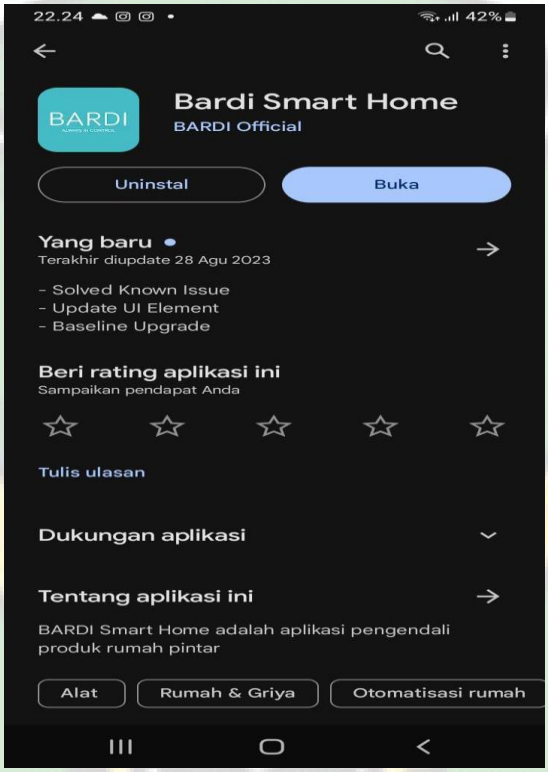
b. *Wireshark*

Yaitu perangkat lunak yang digunakan untuk menganalisis paket jaringan. Dengam menggunkan *wireshark* penulis dapat menangkap dan menganalisis data lalu lintas jaringan secara mendetail.

BAB IV
HASIL DAN PEMBAHASAN

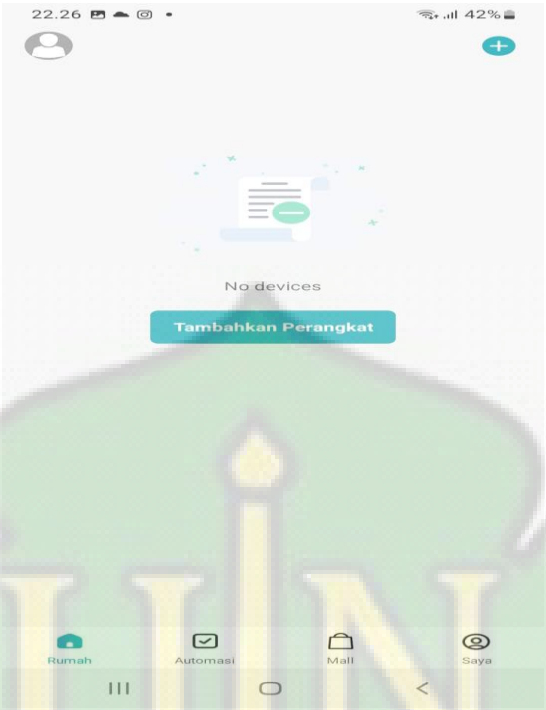
4.1 IoT *Device Installation* (Instalasi Perangkat IoT)

Pada tahap ini peneliti melakukan instalasi perangkat IoT mulai dari pengunduhan aplikasi Bardi hingga penggunaan perangkat *Smart Home* BARDI *Smart Bulb 9W RGB Wifi.*

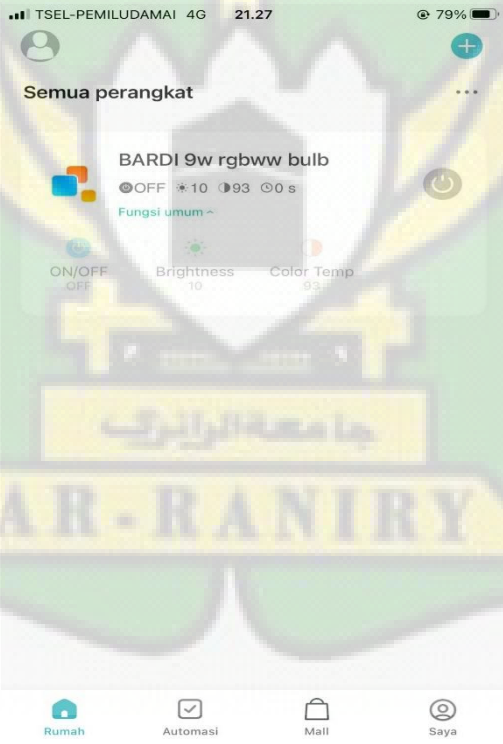


Gambar IV. 1 Unduh Aplikasi Bardi

penulis mengunduh aplikasi bardi *smart home* agar dapat terhubung dengan perangkat IoT *Smart Home* bardi *Smart Light* yang terlihat pada gambar di atas, dan gambar di bawah menunjukkan halaman awal di saat aplikasi bardi *Smart Home* di buka.

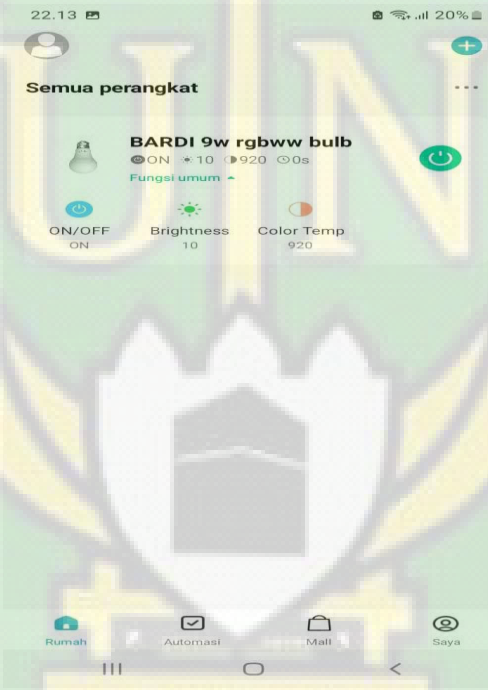


Gambar IV. 2 Halaman Aplikasi

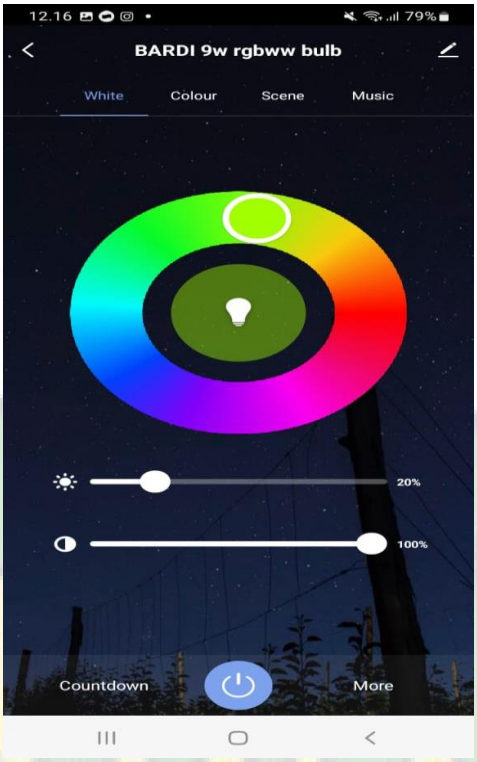


Gambar IV. 3 Terhubung Pada Perangkat *Smart Light*

Di atas terdapat gambar yang mana penulis telah menghubungkan aplikasi dengan perangkat smart home dengan cara tambahkan perangkat dan selanjutnya hubungkan perangkat smart home ke jaringan internet yang tersedia setelah perangkat tersebut terhubung ke internet maka pengguna bisa langsung mengendalikannya dan bisa di lihat pada gambar yang ada di bawah merupakan tampilan di mana pengguna bisa menghidupkan, mematikan, mengatur warna dan mengatur kecerahan lampu pada perangkat IoT bardi *smart home.*



Gambar IV. 4 Smart Light Saat Aktif



Gambar IV. 5 Halaman Kontrol

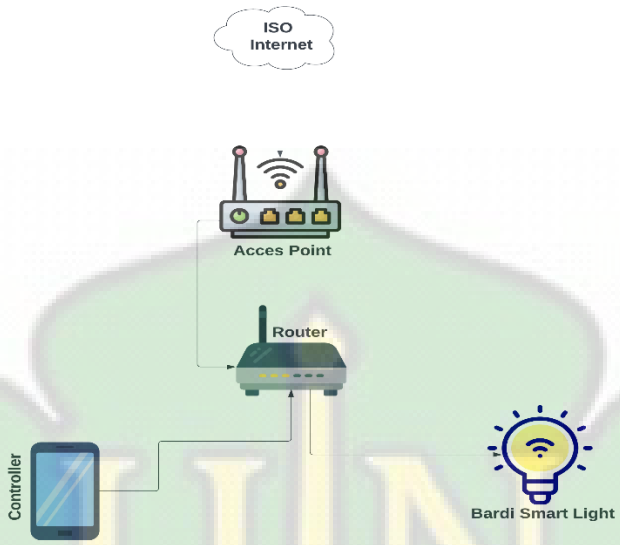
4.2 *Identify*

Pada tahap ini peneliti akan mengidentifikasi perangkat IoT bardi *Smart Home* untuk mengetahui resiko kerentanan yang terdapat pada perangkat.

A. Ruang Lingkup Penelitian

Peneliti melakukan pengujian kemanan pada IoT dilakukan dalam jangkauan peneliti. *Smarthome* IoT dapat dikendalikan dari jarak jauh dengan cara perangkat IoT tersebut terhubung ke jaringan internet atau server cloud yang sesuai.

B. Sistem Berjalan



Gambar IV. 6 Instalasi Umum Sistem *Smart Home*

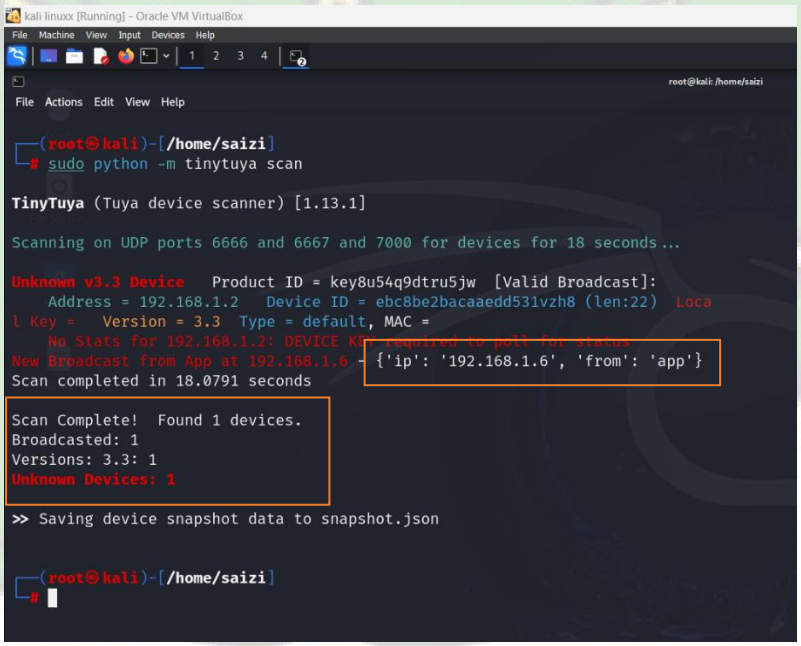
Pada Gambar IV.6 menunjukkan sistem berjalan. Sistem instalasi IoT pada umumnya tampa mempertimbangkan faktor keamanan jaringan hanya dengan menghubungkan langsung ke access point saja yang langsung terhubung ke ISP (*Internet Service Provider*), Perangkat IoT yang langsung terhubung dengan jaringan utama pada sebuah rumah. Jika perangkat IoT tersebut memiliki kerentanan, maka besar kemungkinan perangkat yang terhubung dengan jaringan yang serupa untuk dapat diserang atau dieksploitasi dari kerentanan tersebut.

C. *Scan Device IoT Bardi*

Pada tahap ini dilakukan scan menggunakan tool Nmap dalam perangkat lunak kali linux sebelum dilakukan pengujian pada perangkat bardi, peneliti melakukan scaning perangkat bardi yang berada di area sekitar dengan memasukkan perintah "**sudo p -m tinytuya scan".** Perintah sudo python -m tinytuya scan digunakan untuk melakukan pemindaian jaringan untuk menemukan perangkat IoT yang dapat dikontrol menggunakan protokol Tuya.

- Sudo ini adalah perintah dalam sistem Unix dan Unix-like yang memberikan izin superuser atau izin administratif kepada perintah yang berikutnya. Perintah ini digunakan karena akses root diperlukan untuk menjalankan perintah tersebut.
- python: Ini adalah interpret bahasa pemrograman Python yang digunakan untuk menjalankan skrip atau modul Python.
- -m tinytuya: Ini adalah argumen untuk menjalankan modul Python bernama "tinytuya". Modul ini digunakan untuk berinteraksi dengan perangkat IoT yang menggunakan protokol Tuya.
- scan: adalah sub-perintah atau fungsi spesifik dari modul tinytuya yang digunakan untuk melakukan pemindaian jaringan. Pemindaian ini bertujuan untuk menemukan perangkat-perangkat IoT yang terhubung ke jaringan dan dapat dikendalikan melalui protokol Tuya.

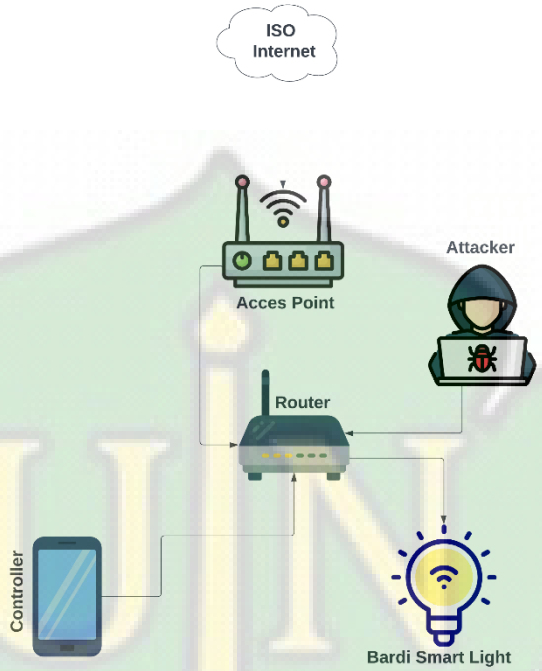
Hasil scan perangkat IoT tinytuya dapat dilihat pada Gambar dibawah ini



Gambar IV. 7 Scan Perangkat *Smart Home*

Dari Gambar IV.7 terdapat 1 perangkat IoT yang menggunakan Tuya Server sebagai cloud gateway serta ditemukan IP Address, Product ID, Device IDE, Local Key, Version, dan Type dari perangkat IoT. Informasi ini seharusnya tidak boleh diketahui dan harus terenkripsi, sedangkan pada perangkat IoT yang

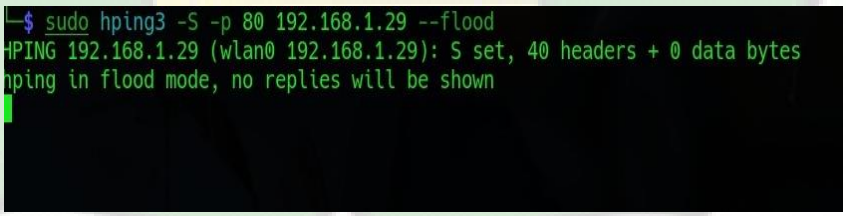
menggunakan Tuya sebagai PaaS (Platform as a Service) informasi dan komunikasi perangkat justru tidak terenkripsi sehingga memudahkan pihak yang



Gambar IV. 8 Alur Pengujian

tidak memiliki akses sah untuk mengendalikan perangkat IoT, Selanjutnya peneliti melakukan pengujian keamanan pada sistem berjalan bardi *smart home.*

Selanjutnya peneliti mencoba melakukan penyerangan DdoS menggunakan Hping3 dengan metode *syn flood* pada ip 192.168.1.29 terlihat pada gambar di bawah ini :



Gambar IV. 9 Penyerangan DDoS

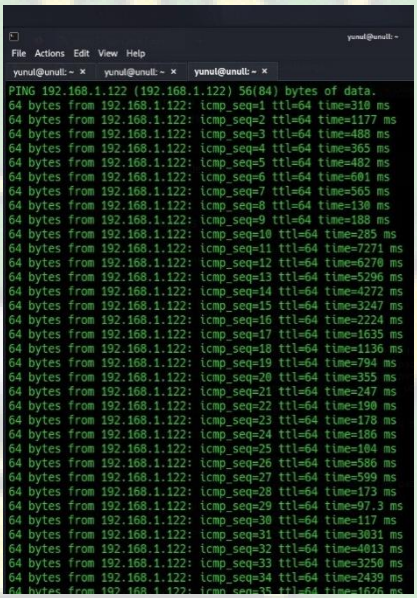
Peneliti pun mendapatkan 2 hasil setelah dilakukan DdoS terhadapat perangkat bardi *smart light bulb* yang dapat dilihat pada tabel di bawah ini

No	Hasil dari DdoS
1	*Respon Light Bulb* Bardi delay hingga 2 Detik untuk setiap perintah yang

	dilakukan baik mengubah tingkat kecerahan,warna dan hidup/mati lampu melalui APP *Smart Home* Bardi yang telah di Install di *smartphone*
2	Aplikasi *Smart Home* Bardi terkesan *error* ketika mengubah banyak pengaturan untuk lampu dalam satu waktu

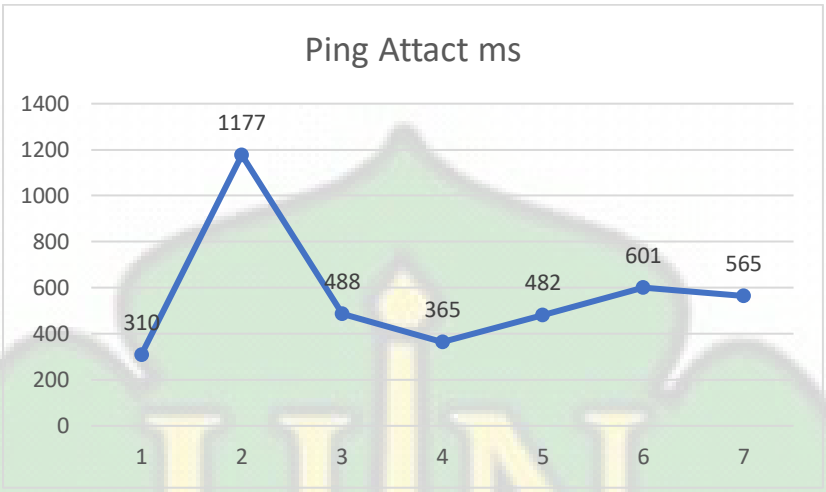
Tabel IV. 1 Hasil DDoS

di bawah ini terdapat dua gambar *network scanning* menggunakan wireshark yang menunjukkan perbedaan ping yang terdapat di saat pengguna menggunakan aplikasi bardi pada saat peneliti melakukan penyerangan DdoS pada perangkat *smart light* dan di saat perangkat tidak dalam penyerangan Ddos.



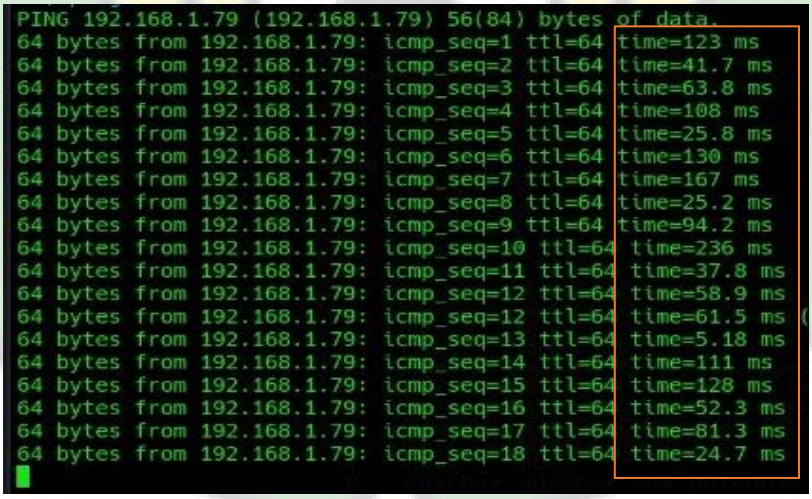
Gambar IV. 10 Dalam Penyerangan DDoS

Pada saat penyerangan DdoS terlihat ping yang di dapatkan dari ip bardi *smart light* begitu tinggi yang bisa di lihat pada grafik di bawah ini.



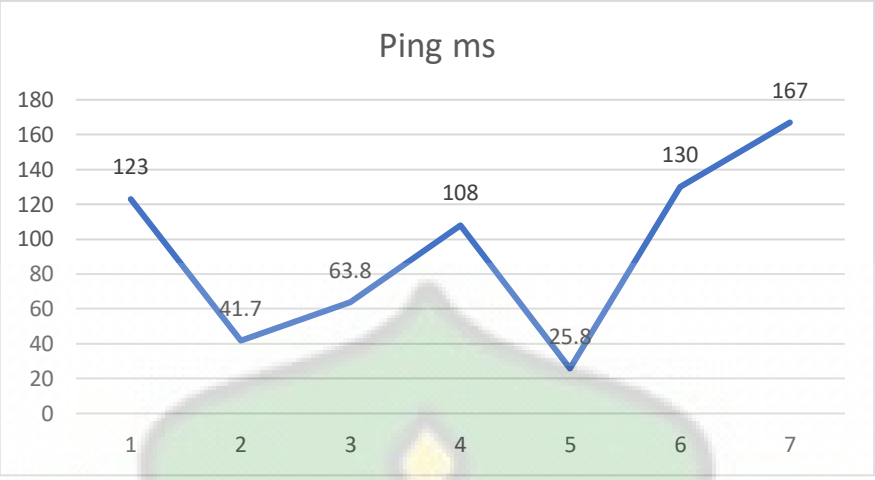
Gambar IV. 11 Grafik Dalam Penyerangan

Tingginya ping yang terjadi pada saat dilakukan penyerangan dapat dilihat pada grafik yang ada di atas.



Gambar IV. 12 Tidak Dalam Penyerangan

Pada gambar IV.11 terlihat ping yang rendah pada ip *smart home* yang didapatkan pada saat tidak dalam penyerangan DdoS.



Gambar IV. 13 Grafik Tidak Dalam Penyerangan

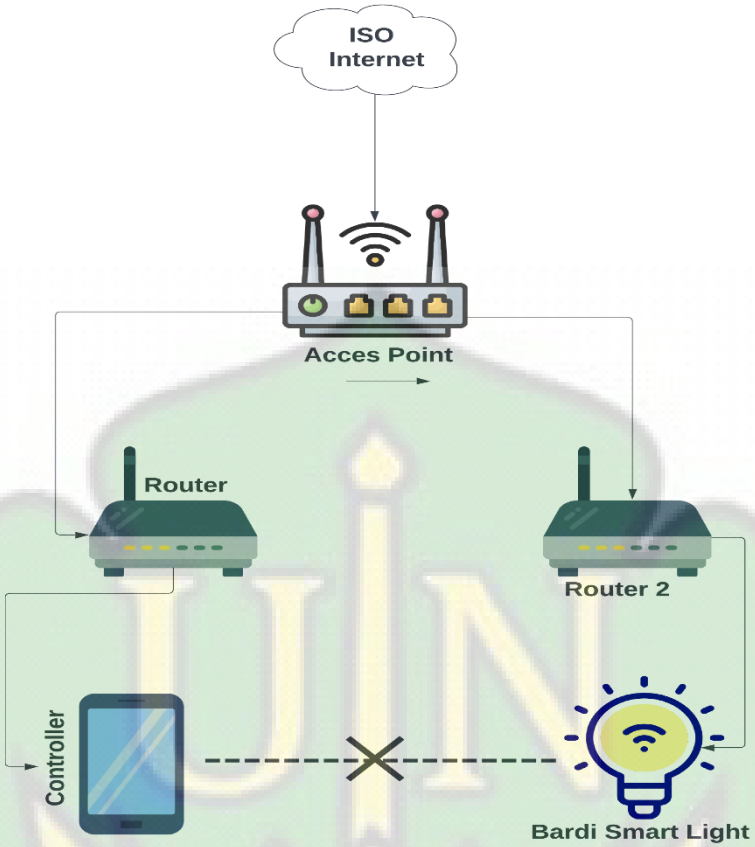
Pada gambar di atas terlihat grafik yang menunjukkan ping yang stabil di saat tidak dalam penyerangan.

4.3 *Protect*

Setelah melewati tahap *identify* yang mana penulis telah mengidentifikasi kerentanan yang ada pada sistem bawaan perangkat bardi *smart home* maka peneliti menerapkan sistem *Device Isolation* .

A. Sistem *Divice Isolation*

Device isolation adalah praktik memisahkan perangkat dalam jaringan untuk meningkatkan keamanan dengan membatasi akses antar-perangkat, mengurangi risiko serangan atau infeksi malware, dan memberikan kontrol yang lebih ketat terhadap lalu lintas data, berikut merupakat sistem usulan peneliti :



Gambar IV. 14 Instalasi Usulan Peneliti

Dapat dilihat pada Gambar IV.12 merupakan rancangan sistem jaringan yang di usulkan oleh peneliti untuk pengamanan jaringan setelah diketahui adanya kerentanan pada perangkat IoT yang terhubung dengan perangkat lain. Terdapat beberapa metode untuk mengendalikan perangkat pintar tersebut yaitu melalui jaringan yang sama antara *controller* dengan perangkat IoT, cara lainnya yaitu melalui aplikasi yang terhubung ke *cloud server* perangkat IoT untuk pengamanan jaringan utama.

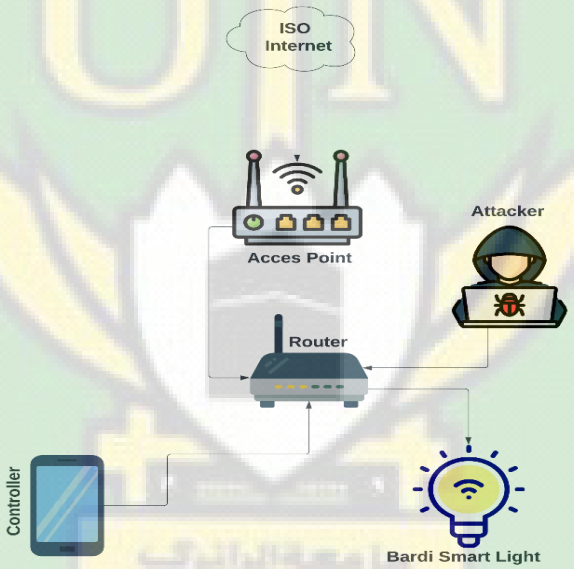
peneliti melakukan pemisahan jaringan terhadap perangkat IoT menggunakan fitur Multiple SSIDs (Service Set Identifiers) adalah fitur pada router atau access point yang memungkinkan pembuatan beberapa jaringan Wi-Fi dengan nama dan konfigurasi berbeda. Setiap SSID memiliki kebijakan keamanan dan pengaturan jaringan tersendiri, memungkinkan isolasi perangkat dan meningkatkan keamanan perangkat pribadi.

4.4 *Detect*

Pada tahapan ini peneliti melakukan rangkaian *Network Mapper* dan *Packet capturing* untuk melihat apakah ada port yang terbuka dan memantau lalu lintas jaringan yang ada pada perangkat IoT ketika digunakan.

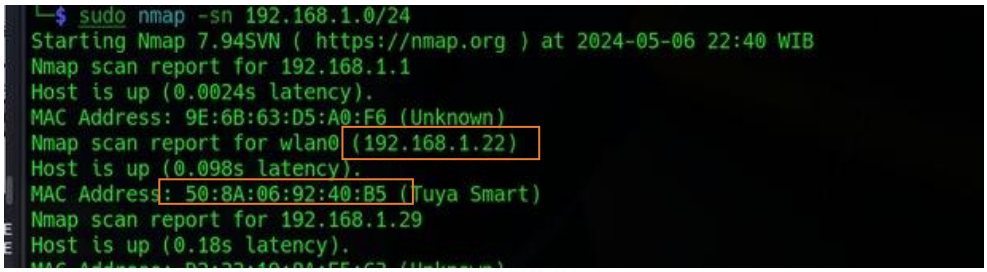
1. Pengujian Sistem *Smart Home*

Pada tahap ini akan dilakukan pemindaian vulnerability pada sistem IoT *Smart Home* untuk mengetahui apakah perangkat IoT bardi yang diuji terdapat kerentanan atau tidak dan seberapa tinggi tingkat kerentanan perangkat IoT tersebut. Tools yang digunakan pada pengujian ini adalah Nmap (yang berguna untuk mengetahui status port yang digunakan apakah Open, Filtered, atau close) dan Tools wireshark untuk menangkap dan menganalisis lalu lintas data jaringan.



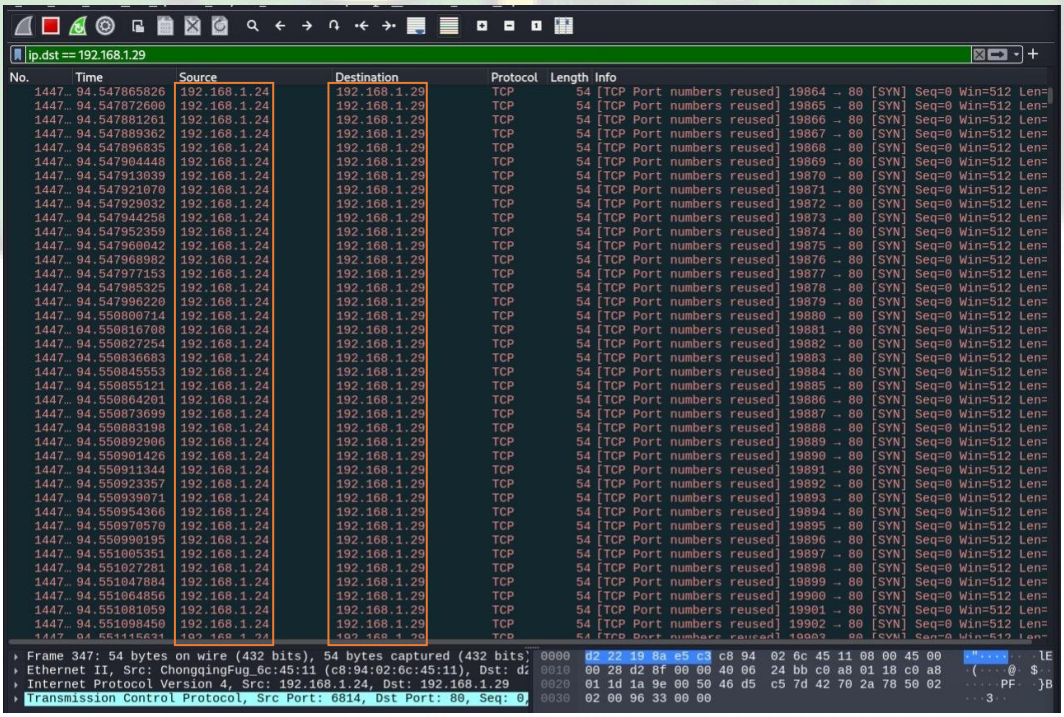
Gambar IV. 15 Pengujian Sistem Bawaan

Pada tahap pertama dijalankan Tools *Network Mapping* (Nmap) untuk mengetahui informasi port pada perangkat IoT bardi. Hasil pemindain dengan tool Nmap terdapat pada Gambar IV.14.



Gambar IV. 16 Nmap *Scanning*

Dari hasil nmap *scanning* diperoleh ip dari perangkat *smart home* bardi *smart light* (192.168.1.22) dan terdapat juga mac address :50:8A:06:92:40:B5 yang terdaftar pada (Tuya *Smart*), pada pengujian menggunakan nmap *scanning* tidak ditemukan adanya port yang terbuka.



Gambar IV. 17 *Network Scanning With Wireshark*

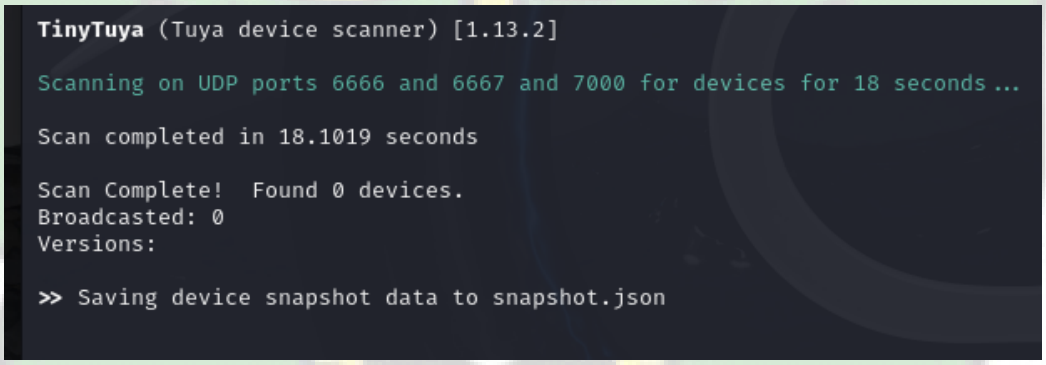
jaringan perangkat IoT bardi dapat di *capturing* dengan menggunakan tool wireshark, hal ini dapat dimanfaatkan attacker untuk memanipulasi perangkat IoT bardi, terlihat perangkat IoT bardi melakukan komunikasi dengan IP address.

4.5 *Respond and Recover*

Selanjutnya pada tahap *respond* peneliti akan melakukan pengujian seperti sebelumnya yang dilakukan pada sistem bawaan *smart home* pada perangkat IoT *smart home* yang telah diterapkan sistem *device isolation.*

A. Hasil Pengujian *Device Isolation*

Setelah melakukan pengujian dengan memanfaatkan data yang diperoleh menggunakan modul tinytuya dan memindai perangkat IoT yang menggunakan tuya sebagai platform IoT, peneliti melakukan pengujian terhadap arsitektur pengamanan device isolation. Berikut hasil dari pengujian sistem *smart home* setelah dilakukan *device isolation*.



Gambar IV. 17 Pemindaian Smart Home Setelah Di isolasi

Dari hasil Gambar IV.17 Perangkat IoT yang telah diisolasi tidak dapat dideteksi dengan menjalankan scan modul tinytuya, dengan begitu peneliti tidak dapat melanjutkan pengujian dikarenakan sistem *device isolation* berhasil mengamankan perangkat IoT *smart home.*

Penerapan *Device Isolation* pada sistem *smart home* sangat di anjurkan karna dapat mengamankan sistem dari kerentanan yang ada pada sistem bawaan perangkat IoT *Smart Home* bardi *smart light.*

Pada tahap *recover* penulis memberikan beberapa rekomendasi umum untuk meningkatkan keamanan perangkat IoT seperti Bardi Tinytuya (Alsalem & Almaiah, 2023):

1. Terapkan metode isolasi perangkat (*Device Isolation Method*) dengan memisahkan jaringan IoT dari jaringan utama untuk mencegah akses langsung perangkat IoT dari perangkat pribadi yang terhubung dalam jaringan yang sama.
2. Perbarui Perangkat Lunak Secara Teratur: Pastikan perangkat lunak pada perangkat IoT selalu diperbarui dengan versi terbaru. Perbaruan perangkat lunak sering kali memperbaiki kerentanan keamanan yang telah ditemukan.
3. Gunakan Koneksi Jaringan yang Aman: Pastikan perangkat terhubung ke jaringan yang aman, misalnya jaringan WiFi yang dilindungi dengan sandi yang kuat dan enkripsi WPA2 atau WPA3.
4. Penggunaan Sandi yang Kuat: Jika perangkat memerlukan autentikasi, pastikan untuk menggunakan sandi yang kuat dan unik. Hindari menggunakan sandi bawaan atau sandi yang mudah ditebak.
5. Aktifkan Otentikasi Dua Faktor (2FA): Jika memungkinkan, aktifkan otentikasi dua faktor untuk lapisan keamanan tambahan. Ini akan mempersulit bagi pihak yang tidak sah untuk mengakses perangkat.
6. Monitor dan Atur Akses: Pastikan untuk memantau siapa yang memiliki akses ke perangkat IoT dan batasi akses hanya kepada mereka yang memerlukan. Nonaktifkan akses default jika tidak diperlukan.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang di peroleh dari penelitian ini yang berjudul Uji Kerentanan dan Pengamanan Menggunakan NIST SP 800 – 53 *Risk Management Frameworks* pada *Smart Home* Bardi (Studi kasus : Bardi *Smart Light*) sebagai berikut :

1. Menggunakan tahapan – tahapan yang di berikan oleh NIST SP 800 – 53 yaitu *Identify, Protect, Detect, Respond* dan *Recover* dengan begitu akan ditemukan kerentanan yang ada pada Bardi *Smart Light* maka dengan begitu dapat direkomendasikan pengamanan yaitu Device Isolation.
2. Teridentifikasinya beberapa kerentanan yaitu terdeteksi ip dan informasi lalu lintas jaringan yang ada pada perangkat *Smart Home* IoT Bardi *Smart Light* dan metode NIST SP 800-53 *Risk Management Framework* dapat mengamankan Bardi *Smart light.*

5.2 Saran

Hasil dari penelitian yang berjudul Uji kerentanan dan pengamanan menggunakan nist sp 800 – 53 *Risk management frameworks* pada *smart home* bardi (Studi kasus : Bardi *Smart Light*) yaitu terdeteksinya kerentanan yang ada pada perangkat yang di uji dan pengamanan yang di terapkan berhasil, maka saran dari penulis untuk selanjutnya agar penelitian ini dapat di lanjutkan dengan lebih sempurna dan dikembangkan dengan menambah perangkat *smart home* yang digunakan, sehingga akan terciptanya kemanan bagi pengguna *Smart Home.*

DAFTAR PUSTAKA

Afiansyah, H. G., & Amiruddin, A. (2022). Perancangan Rencana Tata Kelola dan Manajemen Teknologi Informasi Menggunakan COBIT 2019 dan NIST SP 800-53 Rev 5 (Studi Kasus: Instansi Pemerintah ABC). *Info Kripto*, *16*(1), 33–39. https://doi.org/10.56706/ik.v16i1.38

Akbar. C, Eril, Abdullah, M. W., & Awaluddin, M. (2022). Manajemen Risiko Di Perbankan Syariah. *Milkiyah: Jurnal Hukum Ekonomi Syariah*, *1*(2), 51–56. https://doi.org/10.46870/milkiyah.v1i2.230

Alsalem, T. S., & Almaiah, M. A. (2023). *elektronik Analisis Risiko Keamanan Siber dalam IoT : Tinjauan Sistematis*.

Dewi, I. A. M. S. (2019). *Manajemen Risiko*.

Dietz, C., Castro, R. L., Steinberger, J., Wilczak, C., Antzek, M., Sperotto, A., & Pras, A. (2018). IoT-Botnet Detection and Isolation by Access Routers. *Proceedings of the 2018 9th International Conference on the Network of the Future, NOF 2018*, 88–95. https://doi.org/10.1109/NOF.2018.8598138

Dwi Santika, G., Nine Amalia, K., & Agustina Nugraha, T. (2022). Enhancement of Softskill with Introduction and Utilization of the Internet of Things (IOT) for Elementary School Students and Teacher. *INTEGRITAS : Jurnal Pengabdian*, *6*(1), 203–209.

Efendi, Y. (2018). Internet Of Things (Iot) Sistem Pengendalian Lampu Menggunakan Raspberry Pi Berbasis Mobile. *Jurnal Ilmiah Ilmu Komputer*, *4*(2), 21–27. https://doi.org/10.35329/jiik.v4i2.41

Gram-hanssen, K., & Darby, S. J. (2016). *SH17Home+is+where+the+smart+is.+submitted_150917*. 1–18.

Hafi, A. B. (2023). Uji Kerentanan Dan Pengamanan Menggunakan NIST SP 800-53 Risk Management Frameworks Pada Jaringan Off-The-Shelf Equipments Smart Home Internet of Things (IoT). In *วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย* (Vol. 4, Nomor 1).

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis

Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika : Jurnal Sistem Komputer*, *11*(1), 67–76. https://doi.org/10.34010/komputika.v11i1.5227

Ikhsyan, M. N. (2022). Perancangan Smart Aquarium Berbasis Internet of Things (Iot). *Jurnal Comasie*. http://ejournal.upbatam.ac.id/index.php/comasiejournal

Ikum, M. (2023). *Implementasi Packet Tracer 8.0 Pada Simulator Pintu Rumah Pintar Berbasis Teknologi Radio Frequency Identification*.

Jaya, T. S., & Sahlinal, D. (2017). Perancangan Kantor Digital Berbasis Framework dengan Metode Waterfall pada Politeknik Negeri Lampung. *Jurnal Informatika: Jurnal Pengembangan IT*, *2*(2), 14–17. https://doi.org/10.30591/jpit.v2i2.518

Junaidi, A. (2015). Internet Of Things, Sejarah, Teknologi Dan Penerapannya : Review. *Jurnal Ilmiah Teknologi Informasi*, *IV*(3), 62–66.

Kalingga, D. (2023). *Perancanganalgoritma Two Factor Authenticationuntuk Keamanan Jaringan Internet of Things*.

Kurnia Bakti, V., Sutanto, A., & Basit, A. (2023). Sistem Monitoring Ruang Data Center Kombinasi Multi Sensor dengan Application Programming Interface (API) Tuya. *Smart Comp: Jurnalnya Orang Pintar Komputer*, *12*(3), 806–818. https://doi.org/10.30591/smartcomp.v12i3.5306

Laksamana, F. S. (2019). *Analisis Kemanan Jaringan Dalam Smarthome Internet Of Things (IoT) Menggunakan Cisco Packet Tracer Dengan Metode Square*.

Masykur, F., & Prasetiyowati, F. (2018). Aplikasi Rumah Pintar (Smart Home) Pengendali Peralatan. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, *3*(1), 51–58.

Rojaburrohman, I. (2023). *Analisis Keamanan Sistem, Teknik dan Sains UMP*, *2023*. 7–36.

Setiadi, D., & Muhaemin, M. N. A. (2018). Penerapatn Internet of Things (IoT)

pada sistem Monitoring Irigasi. *Jurnal Infrontonik, 03*(2), 96–97.

Somantri, B., & Marsono. (2021). Pembuatan Dan Pengujian Alat Pemberi PakanIkan Dengan Sistem Kendali Jarak JauhMenggunakan Bardi Smart Plug. *Diseminasi Fti-3*, 1–10.

Tan, W. (2020). Risk Management Framework. *Principles of Project and Infrastructure Finance*, 150–168. https://doi.org/10.4324/9780203962503-15

Tuya. (2021). *Tuya Smart White Paper on Information Security & Compliance Catalog*. *1–8*.