SKRIPSI

**ANALISIS KEAMANAN OPERASI DAN PENGELOLAAN DATA *SMART* CCTV IOT TERHADAP SERANGAN *DENIAL OF SERVICE***

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

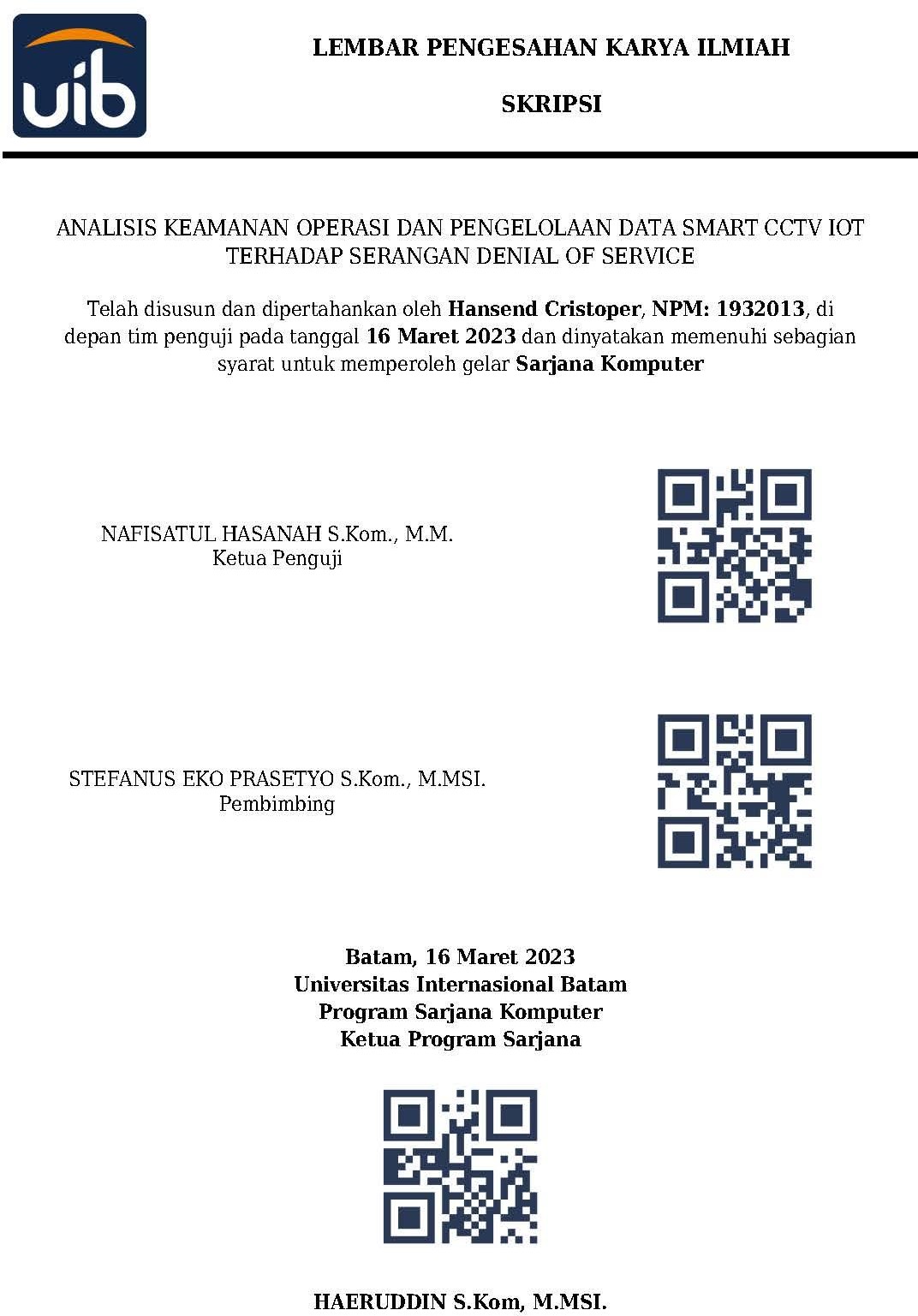
# HANSEND CRISTOPER

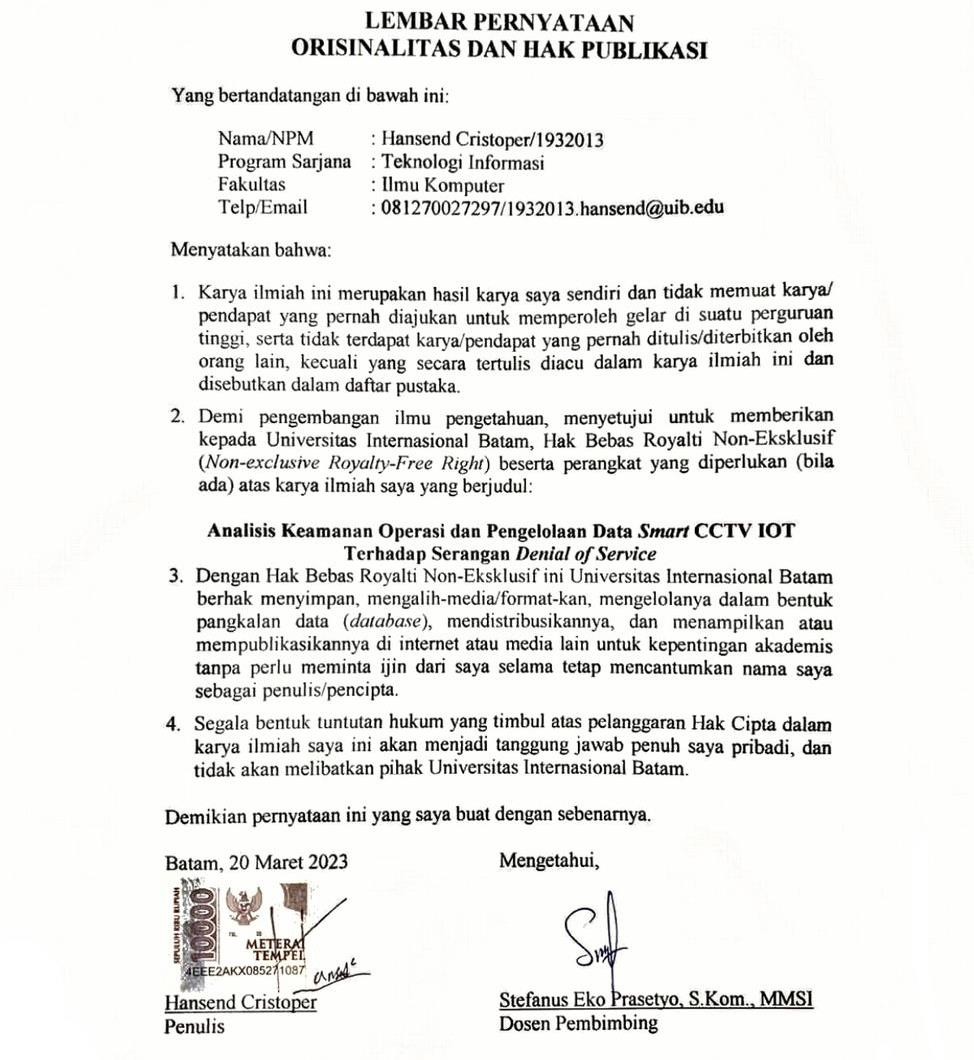
**NPM: 1932013**



# PROGRAM SARJANA TEKNOLOGI INFORMASI FAKULTAS ILMU KOMPUTER

**UNIVERSITAS INTERNASIONAL BATAM 2023**





**Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service***

**Hansend Cristoper NPM: 1932013**

# ABSTRAK

Salah satu kebutuhan dasar manusia adalah menjalankan kehidupannya dengan rasa aman. Dengan bantuan teknologi yang digunakan dalam membantu proses kehidupan, dan dapat memperbaiki kualitas ekonomi, manusia juga bisa memanfaatkan teknologi untuk mendapatkan rasa aman. Salah satu teknologi yang dapat meningkatkan rasa aman pada manusia adalah CCTV. CCTV merupakan suatu perangkat yang dapat beroperasi dan memproses pengelolaan data video rekaman di media penyimpanan DVR berdasarkan hasil pantauan kamera yang terpasang pada CCTV. Selarasnya perkembangan teknologi dan internet, manusia saat ini masuk ke dalam dunia *Internet of Things*, di mana perangkat dapat terhubung ke internet dan dikelola menggunakan perangkat *Smartphone*. Salah satu perangkat yang bertransformasi akibat adanya IoT ini adalah CCTV menjadi *Smart* CCTV, di mana seseorang sekarang bisa mengoperasikan, memantau lingkungan sekitar dan pengelolaan data CCTV dari *Smartphone*. Penelitian ini akan menguji keamanan operasi dan keamanan pengelolaan data *Smart* CCTV yang terpasang langsung pada jaringan dengan serangan *Denial of Service*. Metode yang dilakukan dalam serangan ini adalah *Penetration Testing*, tahapan dimulai dari *footprinting* untuk mencari tau *IP Address* dan sistem operasi perangkat yang terhubung pada jaringan, dilanjutkan tahap *scanning* dan *enumeration* untuk memperdalam analisa pada perangkat yang telah ditemukan sebelumnya dengan tujuan mendapatkan target yang sesuai dan *port* yang terbuka sebagai jalan masuk serangan. Pada tahapan exploitasi, *port* yang ditemukan akan diserang menggunakan *Denial of Service* untuk menguji ketahanan keamanan *Smart* CCTV. Dari hasil serangan *Denial of Service* pada *Smart* CCTV keamanan operasi dan keamanan pengelolaan data dapat dilumpuhkan secara langsung.

**Kata kunci:** *Keamanan Operasi, Keamanan Pengelolaan Data, DOS, Smart CCTV, IoT*.

***Analisis Keamanan Operasi dan Pengelolaan Data Smart CCTV IOT Terhadap Serangan Denial of Service***

**Hansend Cristoper NPM: 1932013**

# ABSTRACT

*One of the basic human needs is to live life safely. With the help of technology that is used to assist life processes, and can improve economic quality, humans can also use technology to gain a sense of security. One technology that can increase the sense of security in humans is CCTV. CCTV is a device that can operate and process the management of recorded video data on DVR storage media based on the monitoring results of cameras installed on CCTV. In harmony with the development of technology and the internet, humans are now entering the world of the Internet of Things, where devices can be connected to the internet and managed using Smartphone devices. One of the devices that are transformed due to the presence of IoT is CCTV to Smart CCTV, where one can now operate, monitor the surrounding environment and manage CCTV data from a Smartphone. This study will examine the operational security and data management security of Smart CCTV that is installed directly on the network with a Denial-of-Service attack. The method used in this attack is Penetration Testing, the stages start from footprinting to find out the IP Address and operating system of devices connected to the network, followed by the scanning and enumeration stages to deepen the analysis of devices that have been found previously with the aim of getting the appropriate target and port. open as an entry point. At the exploit stage, the ports found will be attacked using Denial of Service to test the robustness of Smart CCTV security. From the results of Denial-of-Service attacks on Smart CCTV, operational security and data management security can be disabled immediately.*

***Keywords*:** *Operational Security, Data Management Security, DOS, Smart CCTV, IoT.*

**Keamanan Operasi dan Pengelolaan Data Smart CCTV IOT Terhadap Serangan Denial of Service**” ini dapat diselesaikan untuk memenuhi syarat kelulusan atau penyelesaian pendidikan Sarjana pada jurusan Teknologi Informasi.

Keamanan pada teknologi sangat berperan penting pada era sekarang, khususnya pada pengguna CCTV. Oleh sebab itu Penulis memiliki ketertarikan untuk membahas keamanan operasi dan pengelolaan data pada CCTV terhadap adanya ancaman dari luar.

Penulis juga sangat menyadari bahwa tanpa adanya dukungan, bimbingan, arahan dan masukan dari berbagai pihak skripsi ini tidak dapat berjalan sepenuhnya dengan sempurna. Penulis juga berharap sepenuhnya akan kritikan dan saran bagi pembaca agar dapat membangun penulis untuk lebih baik lagi kedepannya, Terima kasih.

Batam, 20 Maret 2023

Penulis

# UCAPAN TERIMAKASIH

Dalam penyusunan laporan skripsi ini, penulis banyak mendapat saran, ide, dan motivasi dari berbagai pihak secara langsung maupun tidak langsung. Selain itu juga, suka dan duka juga banyak dialami dan dapat dilalui dari berbagai pihak pula. Untuk itu pada kesempatan ini penulis ingin menyampaikan terima kasih kepada semua pihak yang telah membantu penulis di dalam penyusunan laporan kerja praktek ini, antara lain:

1. Tuhan Yang Maha Esa, atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan kerja praktek ini dengan baik.
2. Orang tua penulis yang telah membesarkan, melindungi dan mengajarkan seluruh pengetahuan serta selalu memberi dukungan bagi penulis.
3. Bapak Dr. Iskandar Itan, S.E. MM. yang terhormat selaku Rektor Universitas Internasional Batam.
4. Bapak Dr. Hendi Sama, S.Kom, MM.e-Bussines, selaku Dekan Fakultas Ilmu Komputer Universitas Internasional Batam.
5. Bapak Haeruddin, S.Kom, MMSI, selaku Ketua Program Sarjana Sistem Informasi Universitas Internasional Batam.
6. Bapak Stefanus Eko Prasetyo, S.Kom., MMSI. yang telah memberikan saran dan nasehat sehingga penulis dapat menyelesaikan laporan skripsi ini dengan tepat waktu dan benar.
7. Para dosen dan staf perpustakaan Universitas Internasional Batam yang telah banyak memberikan bantuan kepada penulis dalam proses penyelesaian laporan skripsi ini.
8. Keluarga penulis yang sudah membantu dan menyemangati penulis dalam proses pembuatan laporan skripsi ini sehingga penulis dapat menyelesaikannya.
9. Keluarga besar Universitas Internasional Batam beserta teman teman penulis dan pihak lain yang membantu penulis, sehingga penulis dapat menyelesaikan laporan skripsi ini.

Semoga segala bimbingan, saran, kritik, pengarahan, dan budi baik yang telah diberikan kepada penulis mendapat balasan yang sebesar-besarnya dari Tuhan Yang Maha Esa dan semoga makalah ini semakin memperkaya ilmu pengetahuan bagi kalangan akademisi dan menambah wawasan baru bagi kalangan praktisi serta tentunya bermanfaat bagi kita semua.

Batam, 20 Maret 2023

Penulis

# DAFTAR ISI

LEMBAR PENGESAHAN KARYA ILMIAH SKRIPSI ii

LEMBAR PERNYATAAN ORISINALITAS DAN HAK PUBLIKASI iii

[ABSTRAK iv](#_bookmark0)

[ABSTRACT v](#_bookmark1)

[KATA PENGANTAR vi](#_bookmark2)

[UCAPAN TERIMAKASIH vii](#_bookmark3)

[DAFTAR ISI ix](#_bookmark4)

[DAFTAR TABEL xi](#_bookmark5)

[DAFTAR GAMBAR xii](#_bookmark6)

[BAB I PENDAHULUAN 1](#_bookmark7)

* 1. [Latar Belakang 1](#_bookmark8)
  2. [Rumusan Masalah 3](#_bookmark9)
  3. [Batasan Masalah 3](#_bookmark10)
  4. [Tujuan Penelitian 3](#_bookmark11)
  5. [Manfaat Penelitian 3](#_bookmark12)
  6. [Sistematika Penelitian 4](#_bookmark13)

[BAB II TINJAUAN PUSTAKA 5](#_bookmark14)

* 1. [Tinjauan Pustaka 5](#_bookmark15)
  2. [Landasan Teori 6](#_bookmark17)
     1. [Internet of Things 6](#_bookmark18)
     2. [Smarthome atau Rumah pintar 6](#_bookmark19)
     3. [Cybersecurity 7](#_bookmark20)
     4. [CCTV 8](#_bookmark21)
     5. [MITM atau Man In The Middle 8](#_bookmark22)
     6. [Networking 9](#_bookmark23)
     7. [Keamanan Jaringan 10](#_bookmark24)
     8. [Hacker 10](#_bookmark25)
     9. [Penetration Test 11](#_bookmark26)

[BAB III METODOLOGI PENELITIAN 12](#_bookmark27)

* 1. [Alur Penelitian 12](#_bookmark28)
  2. [Rancangan Instrumen Penelitian 13](#_bookmark30)
     1. [Kebutuhan Perangkat Keras 13](#_bookmark31)
     2. [Kebutuhan Perangkat Lunak 13](#_bookmark32)

[BAB IV IMPLEMENTASI DAN PEMBAHASAN 14](#_bookmark33)

* 1. [Implementasi 14](#_bookmark34)
     1. [Perancangan Jaringan Simulasi 14](#_bookmark35)
     2. [Footprinting 17](#_bookmark41)
     3. [Scanning dan enumeration 19](#_bookmark46)
     4. [Exploit 21](#_bookmark51)

[BAB V KESIMPULAN DAN SARAN 24](#_bookmark54)

* 1. [Kesimpulan 24](#_bookmark55)
  2. [Saran 24](#_bookmark56)

[DAFTAR PUSTAKA 25](#_bookmark57)

[Tabel 2. 1 Tinjauan Pustaka 5](#_bookmark16)

[Tabel 4. 1 Kebutuhan Konfigurasi *Access Point* 14](#_bookmark36)

[Tabel 4. 2 Hasil *Footprinting* Menggunakan Angry IP Scanner 18](#_bookmark43)

[Tabel 4. 3 Hasil Pencarian Sistem Operasi Menggunakan Nmap 19](#_bookmark45)

[Tabel 4. 4 Hasil *Scan Port* Protokol TCP dan UDP 21](#_bookmark50)

[Gambar 3. 1](#_bookmark29) *[Diagram Flow Chart](#_bookmark29)* [12](#_bookmark29)

[Gambar 4. 1 Add Device Pada Tuya Smart 15](#_bookmark37)

[Gambar 4. 2 Qrcode Tuya Smart 16](#_bookmark38)

[Gambar 4. 3 Proses Penambahan *Smart* CCTV Pada Tuya Smart 16](#_bookmark39)

[Gambar 4. 4 Kamera Berhasil Ditambahkan 17](#_bookmark40)

[Gambar 4. 5 *Footprinting* Menggunakan Angry IP Scanner 18](#_bookmark42)

[Gambar 4. 6 Hasil *Scan* Sistem Operasi Menggunakan NMAP 19](#_bookmark44)

[Gambar 4. 7 Hasil *Scan* Protokol TCP Pada 192.168.1.1 20](#_bookmark47)

[Gambar 4. 8 Hasil *Scan* Protokol TCP Pada 192.168.1.50 20](#_bookmark48)

[Gambar 4. 9 Hasil *Scan* Protokol UDP Pada 192.168.1.50 21](#_bookmark49)

[Gambar 4. 10 Pengaturan Serangan LOIC Pada *port* 6668 22](#_bookmark52)

[Gambar 4. 11 Rekaman *Smart* CCTV Pada Saat Serangan Dilakukan 23](#_bookmark53)

# PENDAHULUAN

## Latar Belakang

Sekarang, kehidupan manusia tidak terlepas dari perangkat teknologi. Dengan adanya teknologi, banyak kelompok masyarakat yang terbantu dan dimudahkan dalam memperbaiki kualitas ekonominya. Teknologi saat ini juga dapat mempermudah masyarakat untuk saling berkomunikasi tanpa batasan ruang dan waktu. Teknologi juga dapat dimanfaatkan untuk mencari informasi apakah itu yang baik ataupun yang tidak baik. Salah satu kebutuhan dasar manusia dalam menjalankan kehidupannya adalah kebutuhan akan rasa aman. Menurut Maslow rasa aman berada pada urutan kedua hirarki kebutuhan manusia di bawah kebutuhan dasar seperti sandang, pangan dan papan (Zain, 2022). Dengan bantuan teknologi juga dapat digunakan untuk meningkatkan keamanan manusia dan pemantauan keamanan, salah satu perangkat teknologi yang dapat digunakan sebagai alat peningkatan kemanan dan pemantauan kejahatan adalah *Closed Circuit Television* (CCTV) (Pindarwati et al., 2022).

CCTV merupakan suatu perangkat yang dapat mengirimkan dan merekam data berupa video berdasarkan pantauan kamera yang berada pada alat CCTV tersebut (Sujono & Prayitno, 2021). Selain itu Perangkat CCTV dapat digunakan sebagai alat pemantauan keamanan, dalam bidang forensik kejahatan, CCTV dapat digunakan dalam membantu penyelidikan bahkan bukti dari sebuah kasus kejahatan (Nastiti et al., 2020), (Girsang & Purba, 2017). Selarasnya perkembangan teknologi internet dan memasuki era *Internet of Things* (Iot) (Nahdi & Dhika, 2021). Saat ini CCTV dilengkapi dengan fitur *Smart* IoT dimana CCTV dapat dikendalikan dari jarak jauh melalui internet, pemanfaatan *Smart* CCTV ini mempermudah manusia untuk mencapai kebutuhan rasa amannya. *Smart* CCTV dapat dengan mudah dikonfigurasi dan terhubung pada jaringan (Al- Begain et al., 2022). *Smart* CCTV dapat di akses melalui *Smartphone* untuk mengubah sudut pandangan kamera, memutar kembali hasil rekaman yang ada

1

pada media penyimpanan dan adanya sensor gerak pada umumnya (Venturini et al., 2022). Hasil rekaman pada *Smart* CCTV di simpan pada media penyimpanan *Memory Card, Digital Video Recorders* (DVR) dan langganan *Cloud*. *Memory Card* adalah media penyimpanan utama yang dapat langsung dipasang pada *Smart* CCTV.

Berdasarkan data statistik kriminal 2022 yang dikeluarkan oleh Badan Pusat Statistik Indonesia yang bersumber pada data registrasi Kepolisian Republik Indonesia, Survei Sosial Ekonomi Nasional dan Pendataan potensi Desa menunjukkan bahwa pada tahun 2021 terjadi perbaikan pada beberapa indikator kriminalitas seperti penurunan jumlah kejahatan sebanyak 3.13% dan penurunan tingkat resiko kejahatan sebesar 4.26% (Direktorat Statistik Ketahanan Sosial, 2022). Salah satu faktor penurunan tingkat kejahatan dikarenakan adanya CCTV yang terpasang pada berbagai area (Parenreng et al., 2021). Sebagai alat bantu pemantauan keamanan dan barang bukti forensik. Keamanan pada *Smart* CCTV juga harus terjaga dengan baik. Berbagai ancaman keamanan pada *Smart* CCTV antara lain ancaman keamanan fisik yaitu pengerusakan fisik perangkat *Smart* CCTV maupun media penyimpanan, ancaman keamanan operasi dimana mensabotase *Smart* CCTV melalui *logic system* sehingga tidak dapat bekerja sebagaimana mestinya dan ancaman keamanan sistem transmisi penyimpanan data dimana data rekaman tidak dapat tersimpan dengan baik pada media penyimpanan (Nastiti et al., 2020).

Dengan murahnya dan mudahnya *Smart* CCTV dikonfigurasi dan terhubung di jaringan lokal maupun internet, serta berbagai ancaman yang mungkin terjadi para perangkat *Smart* CCTV. Maka penelitian ini dilakukan untuk menguji dan menganalisa keamanan operasi dan keamanan pengelolaan data pada *Smart* CCTV menggunakan serangan *Denial of Service*. *Denial of Service* merupakan serangan dimana penyerang mencoba mengirimkan paket permintaan secara masif dengan tujuan untuk menghabiskan sumber daya atau *bandwidth* dari korban (Džaferović et al., 2019).

## Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka terdapat rumusan masalah yaitu:

* + 1. Bagaimana dampak Keamanan Operasi *Smart* CCTV jika dilakukan serangan *Denial of Service*?
    2. Bagaimana dampak Keamanan Pengelolaan Data *Smart* CCTV jika dilakukan serangan *Denial of Service*?

## Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

* + 1. Serangan CCTV hanya dilakukan dengan menggunakan *Denial of Service.*
    2. *Smart* CCTV yang digunakan adalah BARDI *Smart Indoor* PTZ *IP Camera*

CCTV Wifi IoT *Home Automation + Micro SD*.

* + 1. Tidak ada *Firewall* yang digunakan dalam penelitian ini.

## Tujuan Penelitian

Tujuan pada penelitian ini dengan judul “Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service*” yaitu untuk meningkatkan keamanan pada *Smart* CCTV yang bekerja dengan baik dan aman dari serangan *Denial Of Services*.

## Manfaat Penelitian

Adapun manfaat pada penelitian Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service* ini adalah :

* + 1. Bagi *User*

Memberikan edukasi kepada pengguna yang dimana mengenai keamanan pada CCTV yang mereka gunakan.

* + 1. Bagi Akademis

Memberikan pengetahuan mengenai keamanan pada CCTV terhadap serangan *Denial Of Service*.

## Sistematika Penelitian

Penelitian ini disusun secara sistematis agar mudah untuk dipahami dan dapat dipertanggungjawabkan. Hasil penelitian ini setidaknya memiliki lima bab yang disusun.

## BAB I PENDAHULUAN

Pada bab pendahuluan terdapat latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan juga sistematika penelitian.

## BAB II LANDASAN TEORI

Bab ini memuat beberapa teori yang yang didalamnya terdapat hasil penelitian dari para ahli dan juga landasan teori yang relevan dengan topik penelitian.

## BAB III METODOLOGI PENELITIAN

Dalam bab ini berisi tentang alur penelitian, rancangan instrumen penelitian serta metode yang akan digunakan sebagai pedoman dalam melakukan penelitian. **BAB IV IMPLEMENTASI DAN PEMBAHASAN**

Bab ini menjelaskan mengenai hasil implementasi yang dilakukan berdasarkan tahapan *Penetration Testing* dan pembahasan dari penelitian.

## BAB V KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan hasil penelitian serangan dari *Denial of Service* dan saran untuk pencegahan terhadap serangan *Denial of Service*

# BAB II TINJAUAN PUSTAKA

## Tinjauan Pustaka

Pada penelitian ini yang berjudul **“Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service*”** terdapat kesimpulan atau ringkasan dari beberapa ahli yang telah dilakukan mengenai judul sebagai berikut:

**Tabel 2. 1** Tinjauan Pustaka

|  |  |  |
| --- | --- | --- |
| **Nama Penulis** | **Tahun** | **Kesimpulan** |
| Segentar Alam, Yesi Novaria Kunang | 2021 | Pada penelitian ini berhasil dilakukan yang dimana *IP Address* yang terdapat pada CCTV 192.168.1.1 dan dengan protokol TCP, *port* 7777, dengan menggunakan *Brute Froce*. *Type* V380  pada aplikasi hydra. |
| Dedi Setiawan, Joni Eka Candra, Cosmas Eko Suharyanto | 2019 | Pada penelitian ini pengujian terhadap *Smart* CCTV yang menggunakan Arduino berbasis Telegram berhasil dilakukan, dengan keadaan rumah yang kosong, sensor tersebut selalu aktif dan memotret ketika ada pergerakan disekitar dan  dikirimkan ke aplikasi Telegram tersebut. |
| Fahlepi Roma Doni | 2020 | Dalam penelitian ini, dijelaskan bahwa hanya *local area network* saja yang bisa dipantau atau dimonitoringkan. CCTV dapat mengontrol dengan jarak jauh  dengan menggunakan aplikasi PSS*.* |
| Putu Riska, Putu  Sugiartawan, Ichsan | 2018 | Pada penelitian ini, terdapat port *knocking*  yang dapat menentukan apakah *port* bisa |

5

|  |  |  |
| --- | --- | --- |
| Wiratama |  | di akses oleh *client* atau tidak, jika tidak maka *file sharing* tidak bisa diakses oleh  *client* tersebut. |
| Barany Fachri , Fadli Hamdi Harahap | 2020 | Pada penelitian ini, menerangkan bahwa IDS atau *Intrusion Detection System* sangat baik untuk keamanan komputer yang bekerja sebagai sistem pendeteksi  dari adanya serangan dari luar. |

## Landasan Teori

### Internet of Things

IoT ditemukan atau dikenalkan pada tahun 1999 oleh Kevin Ashton. IoT berfungsi sebagai berbagi data atau mengumpulkan data dan informasi. IoT adalah singkatan dari *Internet of Things*, yang dimana semua perangkat yang menggunakan jaringan internet yang terdapat pada sistem, maupun jaringan wireless. IoT merupakan sebuah sistem yang dapat berfungsi sebagai alat transportasi dalam hal berkomunikasi melalui jaringan dalam menukar data tanpa dikontrol oleh manusia. Ada beberapan penerapan pada IoT (*Internet of Things*), antara lain Bidang Pendidikan, Bidang Kesehatan, Bidang Transportasi, Bidang Ekonomi, dan Bidang Keamanan (Erwan Eko Prasetiyo, 2017)

* + 1. ***Smarthome* atau Rumah pintar**

*Smarthome* adalah sebuah rumah pintar yang dimana dilengkapi perangkat perangkat yang canggih sehingga keamanan rumah dapat dikendalikan dengan remot kontrol. Selain itu, remot kontrol juga dapat mengaktifkan atau menonaktifkan Televisi, AC, kulkas, komputer, Pagar, dan perangkat perangkat lainnya. Bahkan di era saat ini, dengan menggunakan teknologi komputer, internet, dan *software* atau aplikasi pemograman serta dukungan sistem android (Safira Salsabila & Dian Kasoni, 2021).

*Smarthome* merupakan sistem yang dihubungkan atau yang dapat bekerja dengan bantuan komputer, hal ini bertujuan untuk mendapatkan kenyamanan,

menghematkan biaya atau penghematan perangkat elektronik dan terjaganya keamanan dirumah. Dengan adanya gabungan antara perangkat rumah dan adanya teknologi yang berguna untuk meningkatkan keamanan dan kenyamanan yang dimana ini merupakan arti dari *Smarthome* (Safira Salsabila & Dian Kasoni, 2021).

Definisi *Smarthome* yang dijelaskan oleh Lutolf (1992:277-278) “*Smarthome* merupakan sebuah konsep integrasi dari beberapa *service* didalam rumah menggunakan sistem komunikasi yang sama dan tetap menjamin keamanan dan kenyamanan dengan fungsi kecerdasan yang tinggi”. Keteledoran bagi pemilik atau penghuni rumah dapat menyebabkan keburukan seperti adanya tindak kriminal, sebagai contoh meninggalkan rumah dengan lupa mengunci pintu rumah atau lampu tidak dihidupkan (Safira Salsabila & Dian Kasoni, 2021).

### Cybersecurity

Sesuai dengan namanya, *Cyber* yang berarti siber dan *Security* yaitu keamanan, jadi *Cybersecurity* merupakan perlindungan keamanan atau upaya yang dapat melindungi suatu sistem yang terhubung ke suatu jaringan, komputer, dan data pada suatu keamanan sistem informasi. Hal ini dapat diterapkan dalam pada beberapa konteks mulai dari dunia bisnis sampai dengan sistem komputasi, berikut merupakan beberapa kategori besar:

* + - 1. *Network Security* merupakan pengamanan terhadap jaringan komputer dari penyerang atau peretas.
      2. Aplikasi Keamanan atau *Security Application*, berfungsi sebagai penjaga perangkat lunak yang bebas dari suatu ancaman dari luar.
      3. Informasi pada sebuah keamanan, bertugas untuk melindungi data-data yang tergolong privasi.

Pada umumnya suatu kejahatan berasal dari manusia itu sendiri, sebab semakin jauh suatu pemikiran manusia, maka semakin hebat atau canggih pula kejahatan yang dilakukannya. Adapun kasus *cyber* atau kejahatan yang biasa tersebar di media sosial antara lain peretasan situs, mencuri data pribadi pengguna, dan memalsukan data (Wahib et al., 2022).

## CCTV

Mengenai sejarah CCTV, CCTV pertama kali digunakan oleh tentara Amerika Serikat pada tahun 1940-an untuk menguji misil V2 guna untuk merekam suatu keselamatan pada waktu itu. Kemudian pada tahun 1942, terdapat pengamatan peluncuran roket V-2 tepatnya di Jerman oleh Siemens AG. Pada tahun 1960-an sistem CCTV sangat simple atau sederhana dimana kameranya beresolusi sangat rendah dan grafiknya masih hitam dan putih.

CCTV merupakan alat yang dipakai di era sekarang sebagai alat pengawasan . CCTV atau kepanjangan dari *Closed Circuit Television* merupakan sebuah sistem pengawasan kamera. Selain dari pengawasan kamera pada CCTV, juga dapat merekam atau menyimpan segala memori pelaksanaan terhadap apa yang telah diawasi. CCTV berfungsi untuk mencegah dari niat buruk atau niat jahat pelaku terhadap pencurian, perampokan, pembunuhan maupun kejahatan lainnya. CCTV sangat baik dalam membantu mengawasi atau memonitoring pada titik lokasi yang berpatok pada kegiatan (Doni, 2020).

CCTV (*Closed Circuit Television*) adalah alat perekaman yang menggunakan satu atau lebih kamera video dan menghasilkan data video atau audio. CCTV adalah penggunaan video kamera yang mentransmisikan sinyal atau penyiaran tertuju kepada lingkup perangkat tertentu, yakni seperangkat monitor “spesifik terbatas” (Doni, 2020).

* + 1. **MITM atau *Man In The Middle***

*Man In The Middle* adalah serangan dimana penyerang menstransfer dan mengubah korespondensi antara dua pihak yang dipercayai sedang berkomunikasi satu sama lain secara diam-diam. Pada serangan MITM atau *Man In The Middle* ini adalah hal yang lazim ketika adanya pelaku menempatkan di tengah-tengah sebuah percakapan baik dari pengguna dan aplikasi untuk mengamati atau meniru salah satu pihak dan membuat terlihatnya pertukaran informasi yang biasa sedang berlangsung (Riadi et al., 2020).

*Man In The Middle* atau yang dikenal sebagai MITM, merupakan bagian dari *cybercrime*, yang dimananya tujuannya adalah untuk mengambil data-data atau informasi-informasi pada komputer. Dalam penyerangan terhadap MITM memungkinkan untuk tidak dapat dilacak, sekalipun sudah menggunakan kata sandi pada jaringan tersebut (Riadi et al., 2020).

### Networking

*Networking* atau Jaringan komputer merupakan perangkat komputer, printer dan peralatan lainnya dengan menghubungkan satu sama lain. Internet merupakan sebuah jaringan komputer yang besar atau raksasa yang dimana saling terhubung satu sama lain dengan kemampuan dapat berinteraksi (Wiyanto, Hamza, & Sholeh, 2014). Dan Menurut Andrew S. Tanenbaum dan David J. Wetherall ( 2011: 1 ). Ditulisnya dalam buku *Computer Networks – Fifth Edition*, yaitu Jaringan komputer adalah sejumlah besar komputer yang saling berhubungan dan melayani kebutuhan komputasi suatu organisasi dan hanya dua komputer yang dianggap terhubung ketika komputer tersebut bisa saling bertukar informasi (Ardianto & Akbar, 2017).

## Keamanan Jaringan

Keamanan jaringan merupakan suatu upaya yang harus diterapkan atau dilaksanakan dan diperhatikan. Suatu keamanan jaringan merupakan kewajiban kita dalam menjaga sebuah komputer agar tidak terjadi hal yang tidak diinginkan terhadap serangan dari luar. *Firewall* merupakan sebuah sistem dari keamanan jaringan atau keamanan komputer. Penerapan *Firewall* dapat berupa perangkat lunak atau perangkat keras yang dimana dapat disaringkan melalui paket data yang lalu lalang. Dalam buku John D. Howard dengan judul “*An Analysis of security incidents on the internet* “ atau “Analisis insiden keamanan di internet” menjelaskan bahwasannya sebuah tindakan pencegahan dari beberapa serangan komputer atau seseorang yang mengakses jaringan yang dimana hal itu tidak dipertanggung jawabkan merupakan arti dari Keamanan komputer. Jika sesuatu kelemahan pada setiap jaringan komputer tidak diperhatikan atau tidak dilindungi maka dapat terjadi sebuah kejadian yang tidak diinginkan seperti adanya kehilangan data atau kerusakan pada sistem komputer (Ikhwan,2014).

### Hacker

Istilah *Hacker* yaitu berfokus kepada seseorang yang memiliki keminatan yang besar terhadap pembelajaran sistem komputer. *Hacker* merupakan seorang yang ahli dalam bidang teknologi baik bertujuan untuk kebaikan maupun kejahatan. Bahkan *Hacker* pun mampu menerobos atau memasuki sistem keamanan pada komputer guna untuk memperoleh data atau hak akses tersebut. Dengan demikian, *Hacker* memiliki 3 bagian, dimana ada yang namanya *Black Hat Hacker, White Hat Hacker* dan *Grey Hat Hacker* (Kelrey & Muzaki, 2019).

*Black Hat Hacker* merupakan tindakan *Hacker* yang berbahaya atau bertujuan jahat dengan alasan kriminal ataupun rasa ingin balas dendam. Kemudian *White Hat Hacker* yaitu tipikal kalem, atau tidak bertujuan untuk merusak sistem, akan tetapi *Hacker* satu ini berusaha ingin mengetahui apa saja kelemahan pada komputer tersebut. Yang terakhir adalah *Grey Hat Hacker*, dimana diposisikan sebagai penengah diantara Black Hat Hacker dan *White Hat Hacker* (Kelrey & Muzaki, 2019).

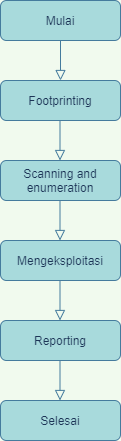
### Penetration Test

*Penetration Testing* merupakan sebuah tindakan yang dimana seseorang berupaya melakukan proses peniruan terhadap serangan yang ingin dilakukan kepada sebuah sistem komputer atau jaringan. *Penetration Testing* adalah sub-kategori daripada peretasan etis, itu terdiri dari metode dan prosedur yang ditujukan untuk menguji atau melindungi keamanan informasi pada organisasi. *Penetration Testing* telah terbukti berguna dalam menemukan kerentanan dalam suatu organisasi dan memverifikasi apakah penyerang dapat mengeksploitasinya untuk mendapatkan hak akses yang dimana itu tidak sah (Baloch, 2017).

# BAB III METODOLOGI PENELITIAN

## Alur Penelitian

Penelitian ini menggunakan metode *penetration testing*. Dimana nantinya akan dilakukan simulasi proses peniruan terhadap serangan yang ingin dilakukan penyerang kepada target. Target disini berupa *Smart* CCTV. Tahapan yang terdapat pada *penetration testing* dimulai dari tahapan *Footprinting* sampai dengan *Reporting*. Dibawah ini merupakan diagram alur penelitian yang disajikan pada Gambar 3.1 sebagai berikut:



**Gambar 3. 1** Diagram *Flow Chart*

Pada penelitian ini terdapat beberapa langkah melakukan *penetration testing*

yaitu sebagai berikut:

* + 1. *Footprinting*

12

13

Tahap pertama dimulai dengan mencari informasi sebanyak banyaknya tentang target.

* + 1. *Scanning* dan *enumeration*

Pada tahap ini dilanjutkan dengan mencari informasi mendalam dengan dilakukannya *scanning* pada target untuk mencari celah yang terbuka dan dilakukan pemetaan terhadap celah tersebut.

* + 1. *Exploit*

Pada tahap ini dilakukan serangan pada kerentanan yang ditemukan pada tahap *scanning* dan *enumeration*.

* + 1. *Reporting*

Pada tahap ini dibuat laporan hasil simulasi yang telah dilakukan.

## Rancangan Instrumen Penelitian

## Kebutuhan Perangkat Keras

Dalam pembuatan rancangan pada Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service*, terdapat kebutuhan Perangkat keras yaitu laptop VivoBook\_ASUSLaptop X412DA\_A412DA (AMD Ryzen 5 3500U *with* Radeon Vega Mobile Fdx (8 CPUs), -2.1GHz, 8192MB RAM), BARDI *Smart Indoor PTZ IP Camera* CCTV

Wifi IoT *Home Automation* + *Micro SD 128 GB* dan *Smartphone* Iphone 11 Promax.

## Kebutuhan Perangkat Lunak

Dalam pembuatan rancangan pada Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service*, terdapat kebutuhan Perangkat lunak sebagai berikut:

* + - 1. Angry IP Scanner
      2. Nmap – Zenmap GUI
      3. LOIC
      4. Tuya Smart Mobile Apps

# BAB IV IMPLEMENTASI DAN PEMBAHASAN

## Implementasi

Pada bagian ini akan dijelaskan hasil studi dan pembahasan yang komprehensif. Hasilnya bisa disajikan dalam bentuk gambar dan spesifikasi yang detail untuk memudahkan dalam pembacaan dan pemahaman. Bab ini berisi mengenai tahapan metode *penetration testing* yang akan diterapkan:

### Perancangan Jaringan Simulasi

Sebelum melakukan pengujian penetration testing, jaringan *Access Point* akan dikonfigurasi mengikuti topologi yang ada. Kebutuhan konfigurasi yang dilakukan adalah seperti pada tabel 4.1.

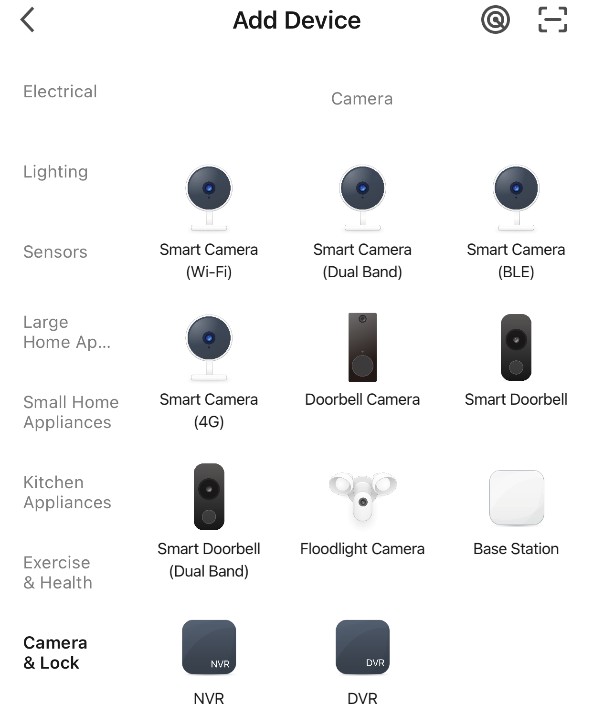
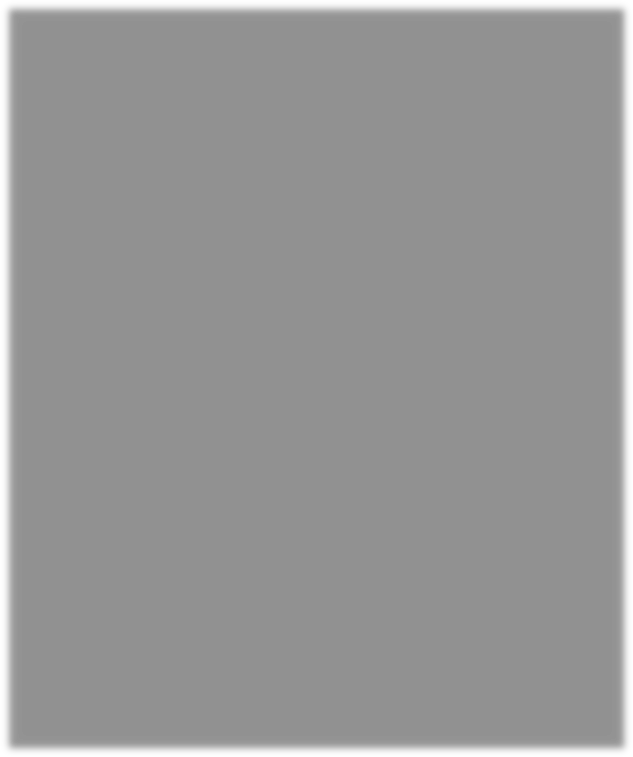
**Tabel 4. 1** Kebutuhan Konfigurasi Access Point

|  |  |  |
| --- | --- | --- |
| **NO** | **Konfigurasi** | **Field** |
| 1 | SSID | UIB |
| 2 | Password | UIB12345678# |
| 3 | Blok IP Address | 192.168.1.0/24 |
| 4 | Netmask | 255.255.255.0 |
| 5 | WiFi Frequency band | 2.4Ghz |

Perangkat laptop, *Smartphone* dan *Smart* CCTV dihubungkan ke jaringan wireless dengan SSID UIB, semua perangkat akan mendapatkan IP otomatis secara acak dengan rentang 192.168.1.2 sampai 192.168.1.255 dikarenakan ada konfigurasi *Dynamic Host Configuration Protocol* yang terpasang pada *Access Point.* Penggunaan wifi *frequency* band 2.4Ghz dikarenakan perangkat *Smart* CCTV hanya mendukung frekuensi 2.4Ghz. Menghubungkan *Smart* CCTV ke jaringan *wireless* menggunakan aplikasi Tuya Smart yang dioperasikan menggunakan *Smarthome*. Untuk menghubungkan *Smart* CCTV pilih menu add

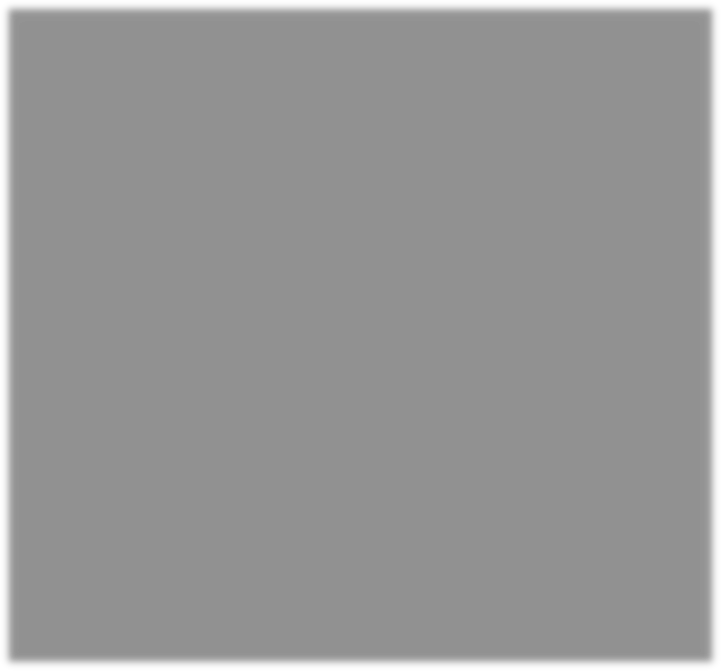
14

device pada Tuya Smart dan pilih camera kemudian Smart Camera (Wi-Fi) Seperti pada Gambar 4.1.

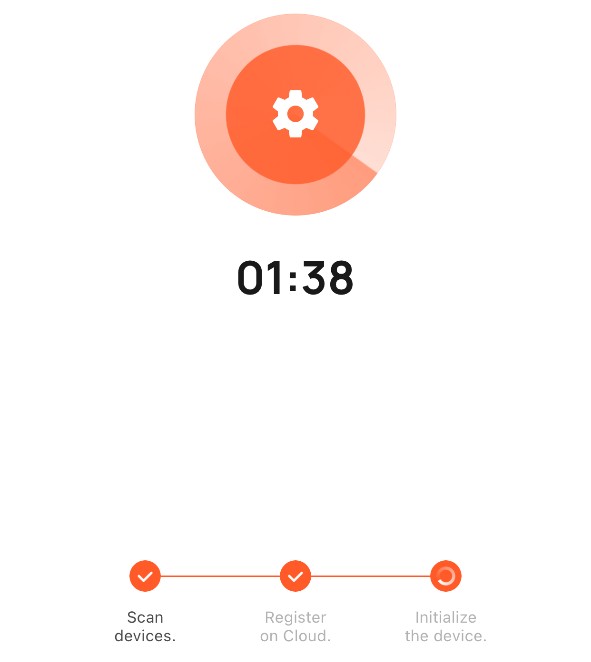
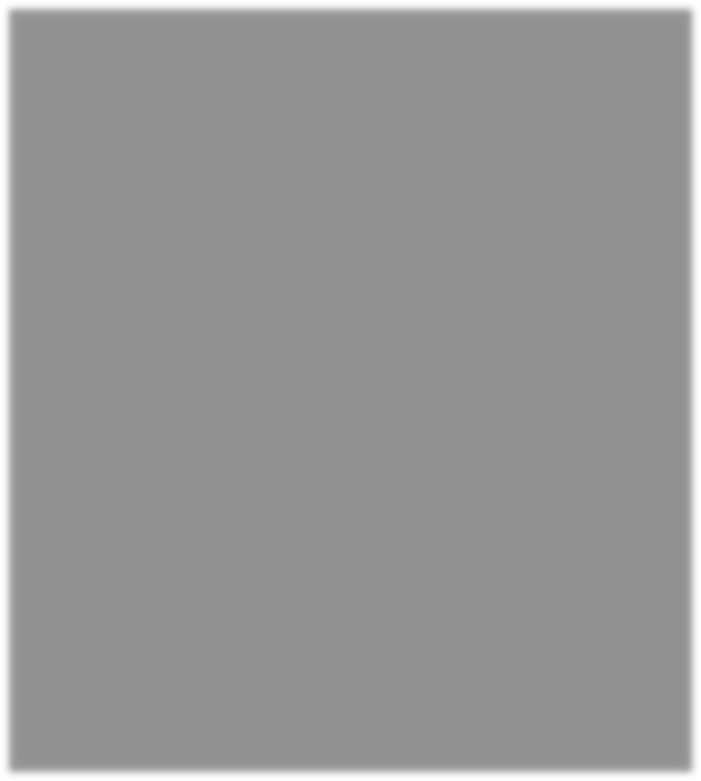


**Gambar 4. 1** *Add Device* Pada Tuya Smart

Selanjutnya pastikan perangkat *Smart* CCTV nyala dan terdapat lampu indikator berwarna merah yang berkedip dengan cepat. Tuya Smart akan menampilkan qrcode pada layar *Smartphone* yang perlu di *scan* pada *Smart* CCTV seperti pada Gambar 4.2



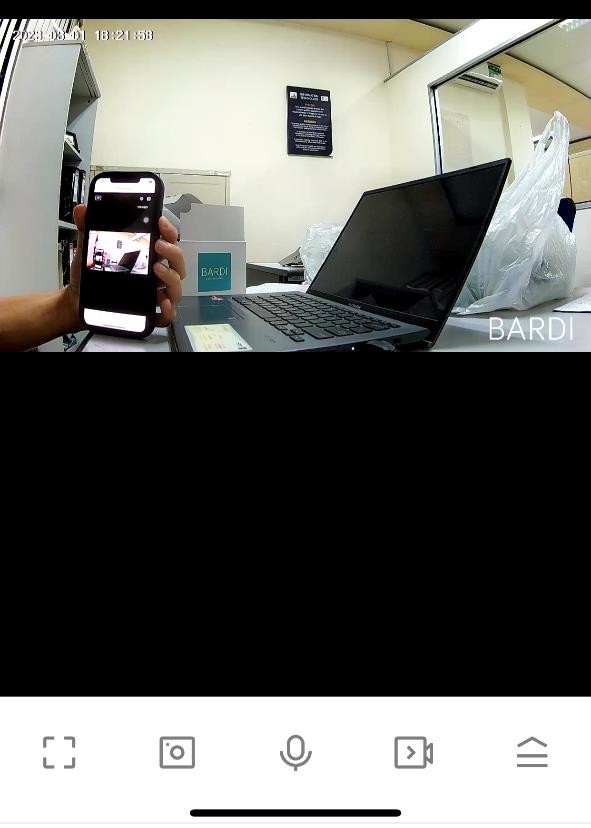
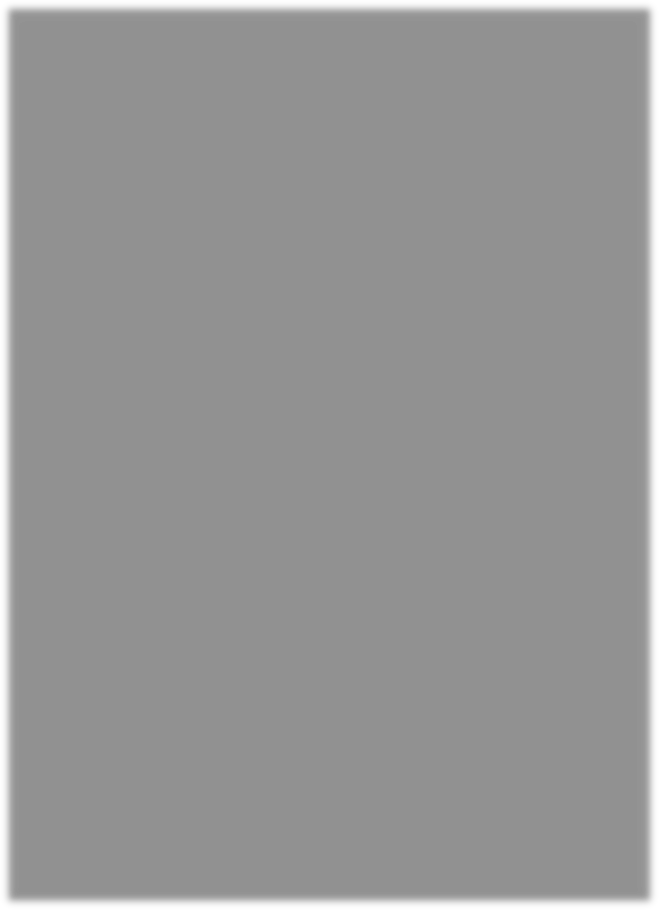
**Gambar 4. 2** Qrcode Tuya Smart



**Gambar 4. 3** Proses Penambahan *Smart* CCTV Pada Tuya Smart Arahkan gambar qrcode yang ada di layar ke *Smart* CCTV dan tunggu

sampai terdengar suara *prompt*, dan tunggu aplikasi Tuya Smart menyelesaikan

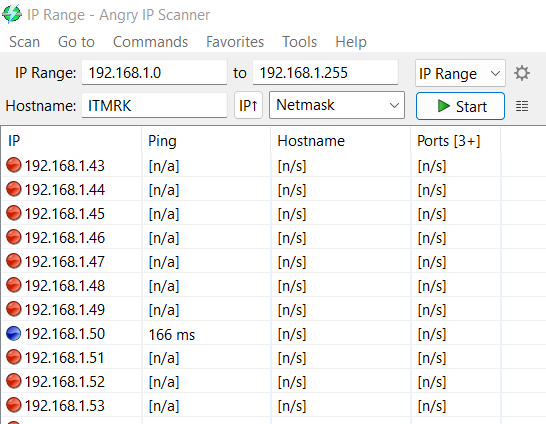
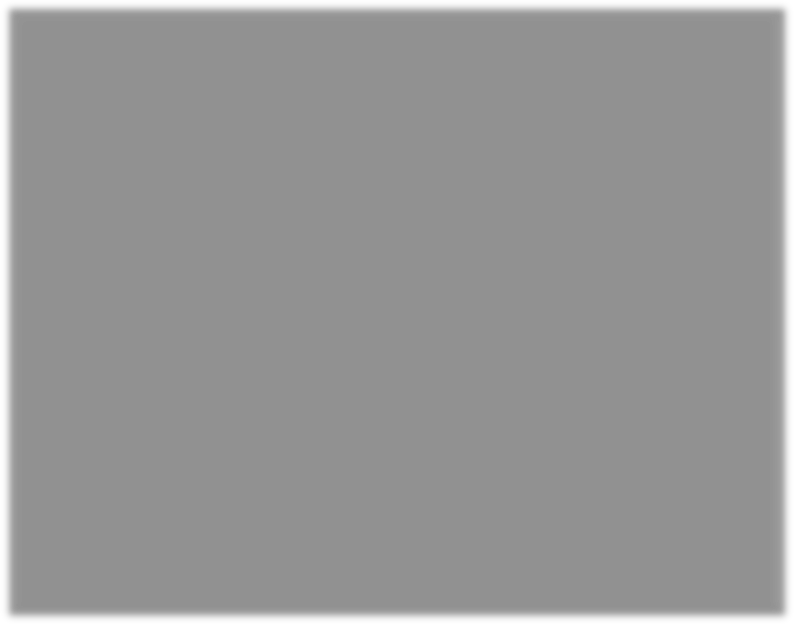
konfigurasi pada *Smart* CCTV seperti pada Gambar 4.3. Setelah selesai maka *Smart* CCTV berhasil ditambahkan dan dapat berfungsi untuk merekam lingkungan sekitar seperti pada Gambar 4.4.



**Gambar 4. 4** Kamera Berhasil Ditambahkan

### Footprinting

Pada tahapan *footprinting*, dilakukan pencarian informasi awal atau dasar dari target dan semua perangkat yang terhubung pada jaringan wifi CCTV. Salah satu informasi yang dicari adalah *IP address*. *IP address* yang ditemukan akan digunakan pada tahapan berikutnya. Aplikasi yang digunakan pada tahapan ini adalah Angry IP Scanner, seperti pada gambar 4.5.



**Gambar 4. 5** *Footprinting* Menggunakan Angry IP Scanner

Proses *footprinting* mendapatkan informasi perangkat yang terhubung ada 4

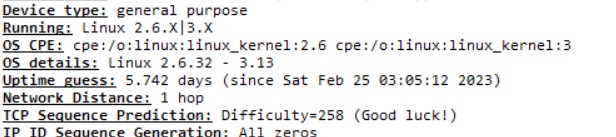
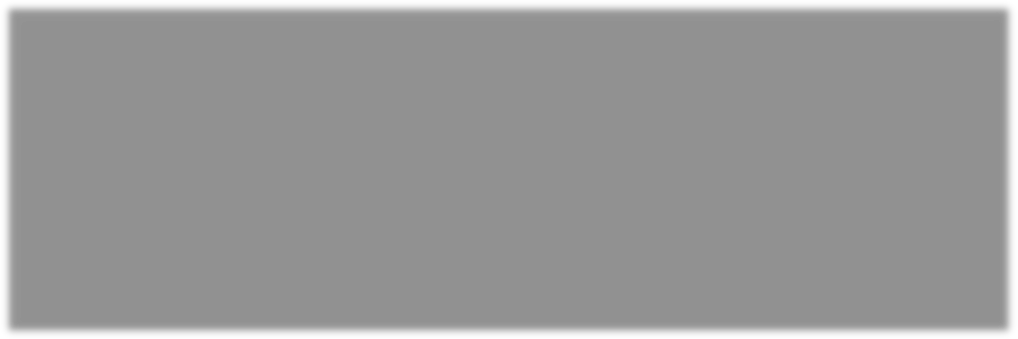
*device*, dengan alamat *IP Address* 192.168.1.1, 192.168.1.24, 192.168.1.25, dan

192.168.1.50 seperti pada tabel 4.2.

**Tabel 4. 2** Hasil *Footprinting* Menggunakan Angry IP Scanner

|  |  |
| --- | --- |
| **NO** | **IP Address** |
| 1 | 192.168.1.1 |
| 2 | 192.168.1.24 |
| 3 | 192.168.1.25 |
| 4 | 192.168.1.50 |

Setelah mendapatkan *IP Address* yang terhubung, selanjutnya mencari tahu tipe perangkat dari sistem operasi yang berjalan pada perangkat tersebut menggunakan Nmap – Zenmap. Tujuan mencari tau sistem operasi adalah mengklasifikasi dan memperkecil kelompok *IP Address* yang merupakan kemungkinan target. Peritah yang digunakan pada Nmap adalah nmap -O -v ip\_address. Hasil yang ditampilkan oleh Nmap dapat dilihat pada gambar 4.6.



**Gambar 4. 6** Hasil *Scan* Sistem Operasi Menggunakan NMAP

Dari hasil pencarian sistem operasi didapatkan 2 perangkat menggunakan Linux, 1 Perangkat menggunakan windows dan 1 perangkat yang tidak bisa ditemukan sistem operasinya seperti pada Tabel 4.3.

**Tabel 4. 3** Hasil Pencarian Sistem Operasi Menggunakan Nmap

|  |  |  |
| --- | --- | --- |
| **NO** | **IP Address** | **Sistem Operasi** |
| 1 | 192.168.1.1 | Linux 4.x |
| 2 | 192.168.1.24 | Tidak ditemukan |
| 3 | 192.168.1.25 | Windows 10 |
| 4 | 192.168.1.50 | Linux 2.6.x / 3.x |

Dari hasil *footprinting* seperti pada Tabel 4.3, dapat di klasifikasikan kemungkinan target *Smart* CCTV menggunakan linux kernel (Tuya Inc., 2023), penulis melanjutkan proses *scanning* dan *enumeration* pada *IP Address* 192.168.1.1 dan 192.168.1.50.

### Scanning dan enumeration

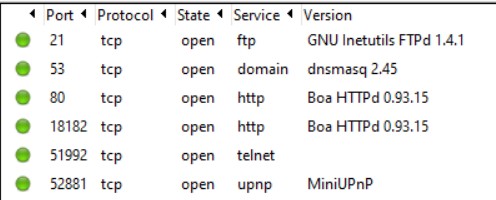
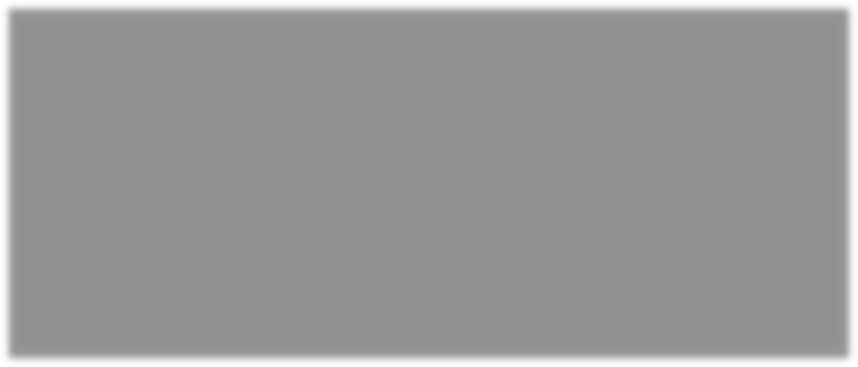
Pada tahapan ini penulis melakukan pencarian informasi mendalam menggunakan teknik *scanning* untuk menentukan target yang tepat dan mencari *port* yang terbuka pada kedua IP hasil *footprinting*. *Scanning* dan *enumeration* akan dilakukan pada dua protokol yaitu *Transmission Control Protocol* (TCP) dan *User Diagram Protocol* (UDP).

Proses *scanning* protokol TCP pada *IP Address* 192.168.1.1 menggunakan Nmap dengan perintah nmap -p 1-65535 -T4 -A -v 192.168.1.1 untuk mencari tau

*port* protokol TCP apa saja yang terbuka dari 1 sampai 65535 mendapatkan 6 *port*

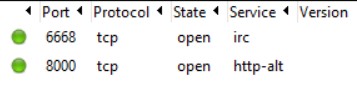
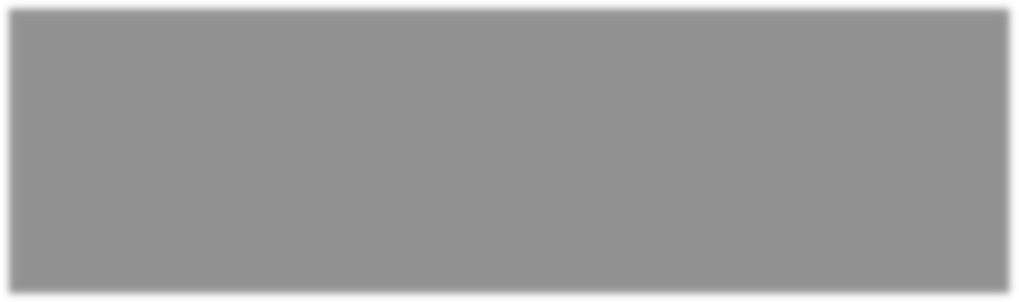
yang terbuka yaitu *port* 21, 53, 80, 18182, 51992, dan 52881 seperti pada Gambar

4.7.



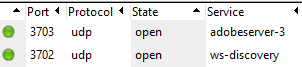
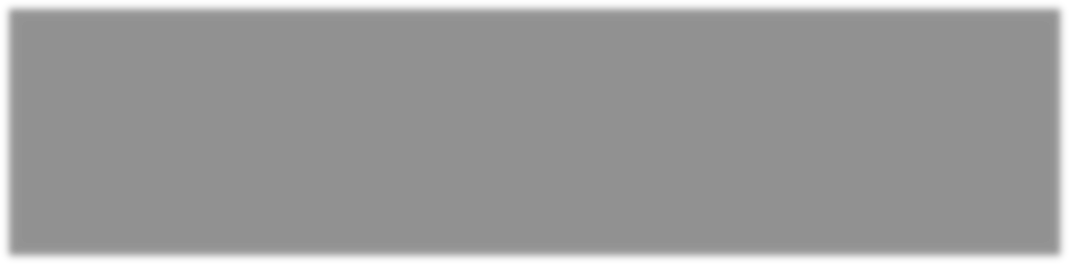
**Gambar 4. 7** Hasil *Scan* Protokol TCP Pada 192.168.1.1

Proses *scanning* protokol TCP pada *IP Address* 192.168.1.50 menggunakan Nmap dengan perintah nmap -p 1-65535 -T4 -A -v 192.168.1.50 untuk mencari tau *port* protokol TCP apa saja yang terbuka dari 1 sampai 65535 mendapatkan 2 *port* yang terbuka yaitu *port* 6668 dan 8000 seperti pada Gambar 4.8.



**Gambar 4. 8** Hasil *Scan* Protokol TCP Pada 192.168.1.50

Proses *scanning* protokol UDP pada *IP Address* 192.168.1.1 menggunakan Nmap dengan perintah nmap -sS -sU -T4 -A -v 192.168.1.1 untuk mencari tau *port* protokol UDP apa saja yang terbuka namun tidak mendapatkan *port* yang terbuka. Proses *scanning* protokol UDP pada *IP Address* 192.168.1.50 menggunakan Nmap dengan perintah nmap -sS -sU -T4 -A -v 192.168.1.50 untuk mencari tau *port* protokol UDP apa saja yang terbuka mendapatkan 2 *port* yang terbuka yaitu *port* 3702 dan 3703 seperti pada Gambar 4.9.



**Gambar 4. 9** Hasil *Scan* Protokol UDP Pada 192.168.1.50

Dari hasil *scanning* pada Tabel 4.4, ditemukan *port* protokol TCP 6668 dan 8000 yang terbuka pada *IP Address* 192.168.1.50. *Port* 6668 adalah *port* Tuya Custom Protocol yang biasa digunakan oleh *Smart* CCTV dan port 8000 adalah *port* ONVIF yang digunakan untuk menghubungkan *Smart* CCTV dengan perangkat DVR (Johannesson & Pettersson, 2022). Sementara *port* UDP 3702 adalah *port endpoint* untuk ONVIF untuk menjalankan WCF *Service* pada aplikasi controller *Smartphone* (Johannesson & Pettersson, 2022).

**Tabel 4. 4** Hasil *Scan Port* Protokol TCP dan UDP

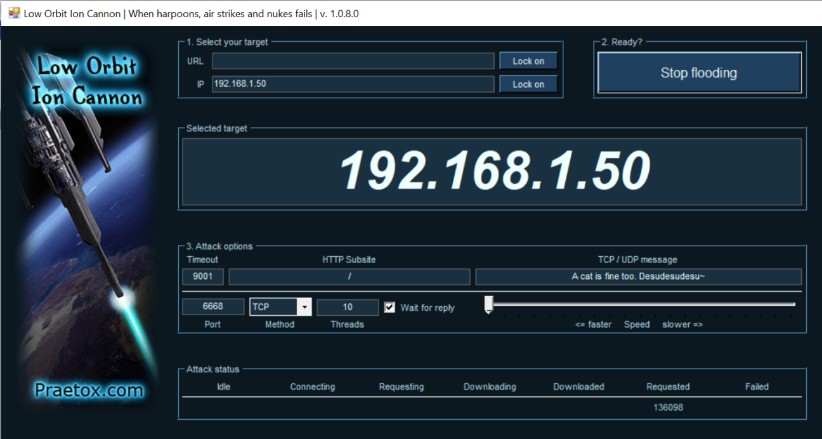
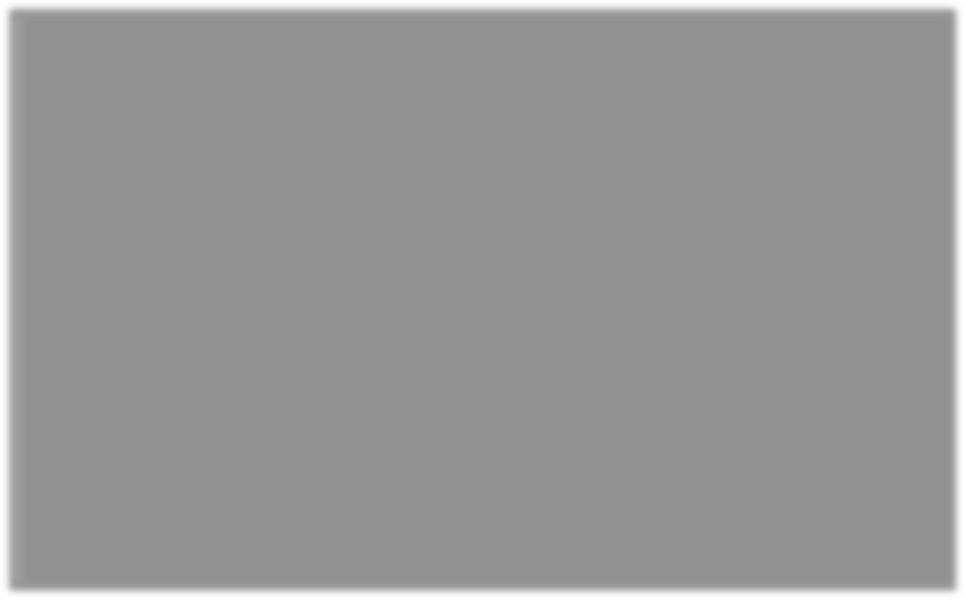
|  |  |  |  |
| --- | --- | --- | --- |
| **NO** | **IP Address** | ***Port* TCP** | ***Port* UDP** |
| 1 | 192.168.1.1 | 21, 53, 80, 18182,  51992, 52881 | Tidak ditemukan |
| 2 | 192.168.1.50 | 6668, 8000 | 3702, 3703 |

Dari hasil *scanning* dan *enumeration*, kita mendapatkan *port* terbuka yang berfungsi untuk mendukung kinerja perangkat CCTV pada *IP Address* 192.168.1.50. *IP Address* ini akan kita gunakan pada tahapan *exploit*.

### Exploit

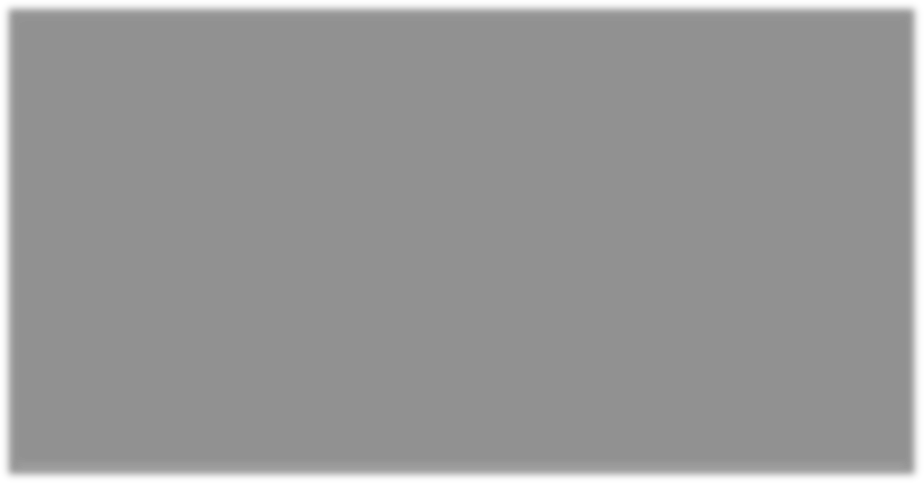
Pada tahapan *exploit* kita akan melakukan serangan *Denial of Service* dengan bertujuan untuk melumpuhkan ketersedian dari target. *Denial of Service* adalah serangan terhadap ketersediaan jaringan. Serangan *Denial of Service* mengirimkan paket permintaan dalam jumlah yang besar dengan tujuan menghabiskan sumber daya jaringan target (Maulana et al., 2022).

Serangan *Denial of Service* akan menggunakan aplikasi *Low Orbit Ion Cannon* (LOIC). LOIC merupakan salah satu senjata *Denial of Service* yang paling mudah di download dan digunakan, LOIC mampu melumpuhkan server dengan mengirimkan permintaan palsu sehingga menyebabkan gangguan pada layanan (Vry4n\_, 2019). Penulis menggunakan LOIC dengan menargetkan IP 192.168.1.50 dengan protokol TCP *port* 6668, protokol TCP *port* 8000 dan protokol UDP *port* 3702. Pengujian dilakukan pada *threads* 10, dan menyesuaikan jenis protokol berdasakan *port* yang akan diserang seperti pada Gambar 4.10.



**Gambar 4. 10** Pengaturan Serangan LOIC Pada *port* 6668

Dari serangan yang dilakukan pada *port* 6668, 8000, dan 3702 membuat perangkat *Smart* CCTV tidak dapat berfungsi dengan baik, *Smart* CCTV menjadi *offline* dan rekaman yang tersimpan pada *SD-Card Memory* CCTV juga terputus pada saat serangan dilakukan seperti pada Gambar 4.11. Warna biru pada gambar menunjukkan bahwa *Smart* CCTV berhasil menyimpan rekaman, sementara bar yang tidak berwarna atau hilang warnanya adalah disaat serangan dilakukan *Smart* CCTV tidak berhasil menyimpan rekaman.



**Gambar 4. 11** Rekaman *Smart* CCTV Pada Saat Serangan Dilakukan

# BAB V KESIMPULAN DAN SARAN

## Kesimpulan

Dari hasil pengujian footprinting mendapatkan beberapa perangkat dan tipe perangkat yang terhubung pada jaringan *wireless*. Ada 2 perangkat menggunakan sistem operasi linux dengan versi yang berbeda, linux 4.x dan linux 2.x. 1 Perangkat menggunakan sistem operasi Windows 10, dan 1 lagi perangkat terdeteksi tetapi tidak diketahui sistem operasinya. Dua perangkat yang menggunakan sistem operasi linux memiliki *IP Address* 192.168.1.1 dan 192.168.1.50. Hasil *scanning* dan *enumeration* pada kedua perangkat tersebut, pada perangkat yang memiliki *IP Address* 192.168.1.50 didapatkan beberapa *port* yang terbuka menggunakan Nmap - Zenmap, *port* yang terbuka ini menjadi celah keamanan potensial yang mengganggu operasional dan pengelolaan data pada perangkat *Smart* CCTV. *Port* yang didapatkan dari hasil *scanning* adalah *port* 6668 dengan protokol TCP yang merupakan *port* yang digunakan oleh *Smart* CCTV tuya dan pengembangannya. *Port* lain yang didapatkan adalah *port* 8000 dengan protokol TCP dan *port* 3702 protokol UDP yang digunakan sebagai fungsi ONVIF untuk mentransmisikan pengelolaan data ke DVR tambahan. Serangan *Denial of Service* menggunakan LOIC dengan *thread* 10 pada *port* yang terbuka di *Smart* CCTV berhasil melumpuhkan keamanan operasi dan keamanan pengelolaan data. Pada waktu serangan dilakukan, *Smart* CCTV menjadi *offline* sehingga bisa disimpulkan *Smart* CCTV tidak bisa beroperasi ketika mendapatkan serangan *Denial of Service*. Keamanan Pengelolaan Data juga berdampak ketika serangan *Denial of Service* dilakukan, dibuktikan dengan tidak tersimpannya rekaman pada *SDCard Memory* ketika *Smart* CCTV mendapatkan serangan.

## Saran

Pada tahap ini penulis akan memberikan beberapa saran yang mungkin bermanfaat bagi pengguna *Smart* CCTV dari serangan *Denial of Service* yaitu :

1. Kita dapat memisahkan jaringan CCTV dengan jaringan pengguna.
2. Menggunakan *Firewall* yang dapat memblokir serangan *Denial of Service*.

# DAFTAR PUSTAKA

Al-Begain, K., Khan, M., Alothman, B., Joumaa, C., & Alrashed, E. (2022). A DDoS Detection and Prevention System for IoT Devices and Its Application to Smart Home Environment. *Applied Sciences (Switzerland)*, *12*(22). https://doi.org/10.3390/app122211853

Ardianto, F., & Akbar, T. (2017). PERANCANGAN SISTEM MONITORING KEAMANAN JARINGAN JARAK JAUH MENGGUNAKAN MIKROTIK OPERATIONAL SYSTEM MELALUI VIRTUAL PRIVATE NETWORK.

*Jurnal Surya Energy*, *2*(1), 135–139.

Baloch, R. (2017). *Ethical Hacking and Penetration Testing Guide*.

Direktorat Statistik Ketahanan Sosial. (2022). *Statistik Kriminal 2022*. Badan Pusat Statistik Indonesia.

Doni, F. R. (2020). Akses Kamera Cctv Dari Jarak Jauh Untuk Monitoring Keamanan Dengan Penerapan Pss. *EVOLUSI : Jurnal Sains Dan Manajemen*, *8*(1), 1–9. https://doi.org/10.31294/evolusi.v8i1.7142

Džaferović, E., Sokol, A., Almisreb, A. A., & Mohd Norzeli, S. (2019). DoS and DDoS vulnerability of IoT: A review. *Sustainable Engineering and Innovation*, *1*(1), 43–48. https://doi.org/10.37868/sei.v1i1.36

Erwan Eko Prasetiyo. (2017). APLIKASI INTERNET OF THINGS ( IoT ) UNTUK PEMANTAUAN DAN PENGENDALIAN BEBAN LISTRIK DI RUANGAN. *Jurnal Teknika STTKD*, *4*(2), 28–39.

Girsang, J., & Purba, S. R. (2017). Efektivitas Pencegahan Kejahatan Melalui Kamera Pengaman Di Objek Vital Di Kota Batam. *Journal of Law and Policy Transformation*, *2*(2), 65–79.

Johannesson, S., & Pettersson, V. (2022). *Security analysis of a modern smart camera*.

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Maulana, A. B., Hertiana, S. N., & Fardan. (2022). Analisis Serangan Denial Of

25

Service (DOS) Pada Jaringan Privat Seluler 5G Stand Alone Berbasis Open Seluler. *E-Proceeding of Engineering*, *8*(6), 2792–2805.

Nahdi, F., & Dhika, H. (2021). Analisis Dampak Internet of Things (IoT) Pada Perkembangan Teknologi di Masa Yang Akan Datang. *INTEGER: Journal of Information Technology*, *6*(1), 33–40. https://doi.org/10.31284/j.integer.2021.v6i1.1423

Nastiti, F. E., Anggana, N. D., Gunawan, H., & Kristiana, U. (2020). Akusisi Barang Bukti Digital pada Smart CCTV Menggunakan Standarisasi ACPO dan SNI ISO/IEC 27037:2014. *Jurnal INFORMA Politeknik Indonusa Surakarta*, *6*(2), 23–37. https://doi.org/10.46808/informa.v6i2.179

Parenreng, M. M., Nas, M., Hamzidah, N. K., Shiddiq, M. F., & Fihriyanti. (2021). Penerapan Smart CCTV Untuk Meningkatkan Sistem Keamanan Lingkungan di Sekolah Islam Qurthuba Antang, Tamangapa. *Prosiding Seminar Nasional Penelitian & Pengabdian Kepada Masyarakat*, 447–450.

Pindarwati, A., Nurfebrian, A., Ray H, B., Hidayat, R., Salsabillah, A. M., Fikriyah, M., Dwiyanti, R., Anisa, S., Damayanti, E., L, S. I., & Nurfiqih. (2022). Implementasi Penggunaan CCTV Berbasis smartings (IoT) Sebagai Smart Security Untuk Menanggulangi Angka Kejahatan Studi Kasus SMK Insan CIta. *Jurnal Multidisiplin Indonesia*, *1*(2), 431–439.

Rahmawati, Y., Ikhwan, S., & Hadi, I. P. (2018). Perancangan Jaringan Multi Protocol Label Switching Virtual Private Network(MPLS VPN) Dengan Menggunakan SImulator Router MX JUNIPER 14.1R1.10. *INSTITUT TEKNOLOGI TELKOM PURWOKERTO*, 367–371.

Riadi, I., Umar, R., & Busthomi, I. (2020). Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain. *Journal of Information Engineering and Educational Technology*, *4*(1), 15– 19. https://doi.org/10.26740/jieet.v4n1.p15-19

Safira Salsabila, & Dian Kasoni. (2021). Prototype Smart Home Berbasis Internet of Things untuk Meningkatkan Efisiensi Penggunan Listrik. *Jurnal Teknik Informatika*, *7*(1), 01–08. https://doi.org/10.51998/jti.v7i1.345

Sujono, & Prayitno, A. (2021). Smart CCTV Berbasisi Internet of Things. *Exact*

*Papers in Compilation*, *3*(3).

Tuya Inc. (2023). *TuyaOS - Tuya Smart*.

Venturini, N., Muniz, P., Bícego, M. C., Martins, C. C., & Tommasi, L. R. (2022). Implementasi Internet of Things (IOT) Pada Sistem Kendali CCTV Berbasis NodeMCU. *Jurnal Cyber Tech*, *1*(12), 457–467. https://ojs.trigunadharma.ac.id/index.php/jct/article/view/1700

Vry4n\_. (2019). *LOIC – DoS attacking tool – Guide*. VK9 Security.

Wahib, P., Narotama, A. T., & Rijki, N. M. (2022). *SOSIALISASI CYBER SECURITY UNTUK MENINGKATKAN LITERASI DIGITAL*. *1*(2), 64–68.

Zain, S. G. (2022). *Pengembangan Sistem Pemantau Keamanan Rumah Menggunakan CCTV Berbasis Nodemcu*. *5*(3), 59–62.