CHAPTER I
INTRODUCTION

1.1 Background Problem

With the advances of technology information in the era that we living right now, the need for fast and up to date information and communication is needed to support daily life activities. When this opportunity comes, an idea emerged to create a CCTV monitoring application just for mobile devices that can be accessed online by using and internet connection so it will be easier for the users to do remote monitoring.(Okkita & Hamidah, 2016)

On the main perspective, this IoT (Internet of Things) has shifted the definition of the internet as it can be computed anywhere, anytime, and any services. The Internet of Things is a network that connects various hardware objects that have identities and IP addresses in order for them to be able to communicate and exchange information about themselves and their perceived. Only the issue that is still the weakness in IoT implementation is the issue of security and privacy. The attacks on IoT security can be included attacks on RFID labels, communication networks and data privacy. To prevent and overcome the threat, the improvement security ,mechanism, and protocol are needed for priority secureness.(Meutia, 2015)

Because of the advanced technology system that we using right now CCTV able to be controlled just by a smartphone from far distance as long as there is connection with the internet. One of the newest ways that it can directly monitor the event or monitoring the situation of the targeted place is with the installation of CCTV. The following requirement can be done successfully just by putting an

setting for Wireless LAN and Network Address Translation that is configure correctly within the Digital Video Recorder and WIFI that been used against it. (Rohmadi, 2016)

IP camera is one of the component parts for CCTV. This is the type of digital camera video that commonly used for security monitoring that can send and receive data through computer and internet networks. although webcam can also do this the term of IP camera or Network camera is only used for security surveillance systems IP camera use TCP/IP networks to transmit data. Unlike Web camera which requires a PC / computer with software to be used, the IP Camera can be directly connected to switches / hubs in TCP / IP networks and can be accessed online via the internet through laptops, mobile phones, tablets and mobile devices. With how the widespread uses is the security for IP cameras appears to be a main problem and need to be investigate in detail. The IP camera that is connected to the internet, it also increasing the security risk awareness of this IP camera device. For this reason, a review of some threats and attacks that might occur on an IP camera network is really necessary.(Indriyanto & Rahardjo, 2018)

There's a case related to the research by (Jinsu, Namje, Geonwoo, & Seunghun, 2019) telling about how advanced technology is also increasing various type of risks for the technology. Back then in New York, USA they are operating domain system for an intelligent which is called Domain Awareness System (DAS), on the other perspective in South Korea, the Songdo international city is building a system place called the smart surveillance solution (SSS) as their surveillance security system. Explaining about various type of security that secure the government around one of the securities needed is of course an intelligent video

surveillance system. But as they said the more advance learning through the technology, these video surveillance system much likely to be more reliable behaviour recognition and high probability of risk assessment. In other word, the CCTV with advanced technology with of open source system going through the hacked granted may cause big problem for the company. The description can be shown in figure 1 below.

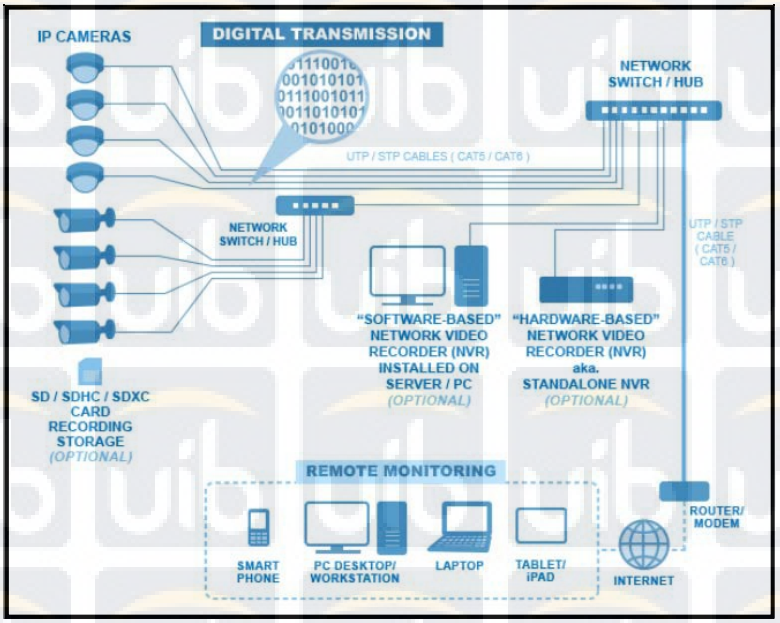

Figure 1.1 Network Video Surveillance System

In order to find out if there's a flaw security in the CCTV. The implementation method is using penetration testing which focus to analyse the network WLAN configuration between the router that are connected with CCTV. The way of this method works is to form an attack such as Eavesdropping, Attacking the Infrastructure, Cracking the Encryption, or Man in the middle to the network which has been simulated by the configuration. The result to this method is to find out if any of this attacks manage to breach the security which built inside the CCTV and the router so the research can simplify and came which type of

security can come out with the breach attack of the router security which connected to the CCTV.(Imam Bayu, Muhammad Yamin, 2017)

The way to Prevent the cybercrime attacks, the implementation using security that will be used from the hardware called Mikrotik Router which is using the feature called firewall that will be put in CCTV topology. The role for this router is to become the traffic regulator and filtering any several attacks that can interfere the CCTV network connectivity. The design is done to create a form of computer network design that is suitable to applied to the gateway system as well as a firewall that implements packet filtering where the filter method will regulate all packets that are headed, past or will be addressed by the packet. The packet will be arranged whether it will be received, forwarded or rejected. At this stage the firewall method will be analysed which is often used in general in one-layer filtering, one of which is using the Firewall Packet Filtering method, this type of firewall filters data packets based on the address and options that have been specified for the package. This method works in the IP level of the data package and makes decisions about the next action (forwarded or not forwarded) based on the condition of the package. this method is designed to control the packet flow based on the address of origin, destination, port and type of packet information contained in each packet.(Komang & Mardiyana, 2015)

Based to the explanation of the background problem telling about the flaw inside CCTV security network, the writer able to simply the explanation towards with the title "**Analysis and Design Wireless Network Security CCTV using Mikrotik Router with Penetration Testing Method"**

1.2 Formulation Problem

Based on the problem Background what written above, the writer can conclude for several problems from what the writer simplify , as the following:

1. How to make a better systematic security for CCTV that is completely secure?
2. How to analyze that the security system of CCTV is not completely safe yet?
3. How to give the exclusive access between the CCTV and the admin?

1.3 Limitation Problem

In order for the topic discussion to be more directed and focused to makes it easier for the researchers to understand what the main purpose for this implementation, the limitation of the discussion problem is the following:

1. Network Security hardware is using the configuration of Mikrotik Router, as an internet access point.
2. The CCTV component is using only Hikvision CCTV IP type camera to grant access to the network IP address.
3. The network attack range is only limited within HTTP and RTSP range protocol.

1.4 Project Purpose

The purpose with doing the final project with the topic “Analyse and Implementation Network Security CCTV using Mikrotik with Penetration Testing Method (Pentest)” with the purpose is among others:

1. To increase the value security for the user who using this CCTV

2. Developing new improved security for the design topology in CCTV provided.
3. Knowing how to prevent upcoming cybercrime attacks from other network breaching access.
4. As a requirement for graduating Strata (S-1) at Universitas Internasional Batam.
5. For the writer to be able to demonstrate knowledge about the design network security for CCTV.

1.5 Project benefit

There is also benefit for final project named analysis and designing wireless security network CCTV using Mikrotik Router with penetration testing method and that is:

1. For user
   a. To be able to learn how to hack or defend against cybercrime attacks in network.
   b. Giving an upgrade to the security facility.
2. For researcher
   a. To be able to gain about the method towards various of cybercrime attacks and network security in CCTV.
   b. To find even more specific threat in the network security
3. For academic
   a. To improve the topic knowledge about penetration security that are going be thought in the college.

b. Giving a knowledge method to all of the upcoming students who is interested in this particular research.

1.6 Systematics Discussion

The following is a systematic discussion in a briefly made research

CHAPTER I INTRODUCTION

For this chapter briefly describes a clear and solid summary of the background of the problem, the formulation of the problem, the boundaries of the problem, the objectives of the project, the benefits of the project, and the systematic discussion of the report.

CHAPTER II LITERATURE REVIEW

In this chapter there is a literature review which is the consideration of the researcher towards this study and the theoretical basis relating to the making of the security network of the whole large topology for CCTV, can be in the form method of penetration testing related to the cybercrime or breaching attacks.

CHAPTER III RESEARCH METHODOLOGY

This chapter contains the methods applied to implement research and development of the final project. Describe about the way of manufacture used, which is based on the flow of researches, problem analysis, and system design.

CHAPTER IV IMPLEMENTATION

This Chapter will explain about the implementation of the final project. Defining the implementation of the topology security towards the CCTV and explaining each step of how the implementation works.

CHAPTER V CONCLUSION

This chapter is a closing chapter which is consists of conclusions from the whole report of this final project, finding all the source from the results of analysis and discussion about network security for CCTV.