CHAPTER II
LITERATURE REVIEW

2.1 Literature Review

This research is based on the reviews from last literature with the research written by (Habibi, Munadi, & Yovita, 2015) with the title Analysis Secure Socket Layer Protocol with IP Spoofing ,Heartbleed Bug, DDOS , Man-In-The-Middle Attack : Video Hijacking, And Attack Combination describe about how easier access of a IPTV that requires connection uses for video streaming requires secure services to protect data information using 5 type of attacks including Distributed Denial-of-Service(DDoS), IP Spoofing, Man-in-the-Middle Attack: Video Hijacking, with hacker or penetration tester (Pentest), in the final task shows whereas in the attack carried out by the least other than DDoS ,there is no visible impact on the QoS Calculation this is because an attack that occurs other than DDos is not included in the type of attack launching an attack on the network created, or the attack cannot be detected using only the QoS calculation. Thus, it is evident that DDoS attacks are more focused on how security in the network configuration being attacked is made.

The next research written by (Costin, 2016) with the title Security of CCTV and Video Surveillance Systems : Threats, Vulnerabilities, Attacks, and Mitigations explain about a new threat that were targeted especially to CCTV or video surveillance. the main target is to breaching towards the network internet and gain access to where ever the user id type including user and password or QR codes access that were with CCTV to be able to enter the display camera by using a command injection or a malicious firmware upgrade all over the web interface.

The next research written by (Amarudin, Widyawan, & Najib, 2014) with the title Single Sign On (SSO) Network Security with Lightweight Directory Access Protocol (LDAP) using the Man in The Middle Attack (MITMA) method. The research explains that MITMA is a sniffing action that utilizes a switch device weaknesses and ARP cache and TCP/IP handling errors from the operating system. The main idea was to put the hacker position in between of the two computers that were connected so the data packet had to go through the hacker's computer so it could be seen or tapped by hackers. Then hackers direct to the ARP cache computer victims and destination servers (web servers) made to be hackers' computer as a router.

The next research is written by (Adriant, 2015) with the title implementation Wireshark for sniffing packet network data. Explain how cause effect of sniffing technique into Network security using Wireshark software. The way progress sniffing is using capturing technique with the target of stealing the username and password information. The sniffing process is done by using Wireshark software. Wireshark software captures data on the Wireless interface, then observes the capture results that contain POST data that contains HTTP username and password. From the results of the research conducted, it was found that using Wireshark can intercept or retort data passing on computer networks, this results in the loss of one of the security properties of privacy and confidentiality.

The next research written by (Triandi, 2015) with the title Network Security System in Preventing Data Flooding Using IP and Port Blocking Methods explain about how to build a system that can prevent data flooding by blocking IP and ports by creating an active firewall that can define any data that enters the server to detect

whether the data is a flood or data that needed by the user, the detection is done by using TCP,UDP, and ICMP packages.

The next research written by (Arta, Syukur, & Kharisma, 2018) with the title Simulation of Intrusion Prevention system(IPS) with implementation of Mikrotik Router. The research explains about the useful of firewall security to set network administrator as network traffic with the plus of Intrusion Prevention System (IPS) which is increase the safe secure for network from the combination between blocking capabilities and firewall.

Based on the literature review above, the writer will make a research table to compare previous research with author's research (look at table 2.1)

Table 2.1 Literature Review

Authors	Year	Research conclusion
Jafar Alim Habibi, Rendy Munadi, & Leanna Vidya Yovita	2015	Explain about a hacker attacks of video hijacking towards a video streaming. Using an experiment test for analysis in 5 type of attack simultaneously especially Man in the middle attacks target towards web page interface.
Andrei Costin	2016	Over all detail is to describe about the new way of hacker to breach into network goes to the display of CCTV security to do a cybercrime target towards their VSS
Amarudin, Widyawan, Warsun Najib	2014	The Research is describing about a authentication on using hacking tools called Cain and abel in Man in the middle attack method to acquire a targeted information User and Password. For this research is to find out the how useful the network security will be with SSO (Single Sign On) and LDAP (Lightweight Directory Access Protocol), and database server MySQL
Mardianto, Ferdy Adriant	2015	This research is discussing about the technique in sniffing towards network packet data using a Wireshark for getting data post which is include user and password using the capture technique in wireless interface.

Authors	Year	Research conclusion
Budi Triandi	2015	This research is described about a prevent and protect towards IP flooding and port blocking by using an active firewall that detect any available port that can access toward to identify the IP.
Yudhi Arta, Abdul Syukur, Roni Kharisma	2018	The important using between firewall and blocking capability for security network which will manage to monitoring the network traffic with Intrusion Prevention System.

In conclusion according to all the result from all the researches that has been explained, the writer will do as the start to analyse which type cybercrime attacks which mention with the researcher of (Jafar Alim Habibi,Rendy Munadi, Leanna Vidya Yob (2015) and then do a searching to the network and breach which the CCTV were taken from the researcher method of (Andrei Costin, (2016). As we found the access network of the CCTV. Next is where the method of man in middle attacks by using the method of (Amarudin,Widyawan,Warsun Najib, (2014) by using the apps called Cain and Abel to do SSO(Single Sign on) to acquired the following user and password for the targeted information on the website protocol by using LDAP(Lightweight Directory Access Protocol). The next way to acquire information by doing the method of (Maridianto,Adriant,Ferdy (2015) towards the target protocol using sniffing on the targeted traffic by using Wireshark application. After the cybercrime attacks is done with next is to find how to prevent IP flooding and do a port blocking. And also showing how important of capability blocking of firewall security that will manage the monitoring section of the network traffic with intrusion prevention system by using both (Budi Triandi, (2015) (Yudhi Arta, Abdul Syukur, Roni Kharisma, (2018) of the following method.

2.2 Theoretical Basis

In the theory of making a security network to CCTV, writers will be making a theoretical basis. The foundation of the theory is a collection of theories that are used to strengthen the theory in research. The theories used in this study are the following:

2.2.1 Computer Network

Computer network is a telecommunication type of network that allow between computer to exchange data. The purpose of a computer network is to be achieved the way they wanted to obtain, every part of computer network can request and provide Services.(Chandra & Kosdiana, 2018)

Networks can be classified into 3 types, namely Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN)

1) LAN

This network is one of the networks usually takes part as an important role in the network. LAN is stands for local area network. This type of network usually be uses in type of small range area groups in the type building for example to be found is in school, restaurant, campus areas, offices and surrounding building that require connections or connection between two interface or even more in a room. LAN networks are also networks that are greatly influenced by the network topology(Wongkar, Sinsuw, & Najoan, 2015) (Look at figure 2.1)

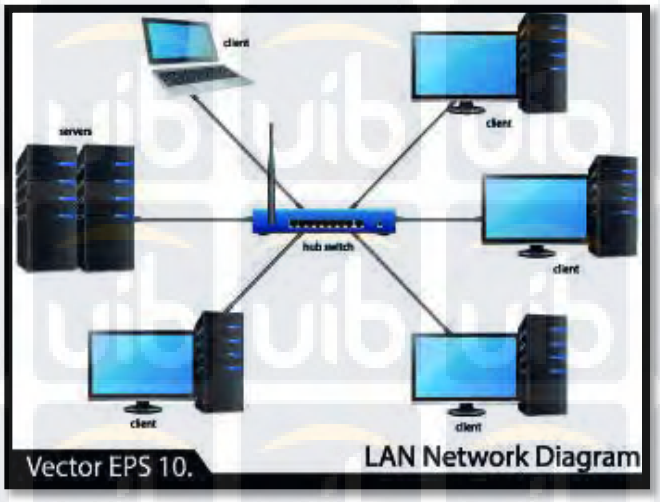

Figure 2.1 Local Area Network (LAN)

2) MAN

MAN stands for Metropolitan Area Network. Basically, MAN has a larger version and usually uses the same technology as LAN. MAN can get an area the size of company offices that are placed adjacent or also a city and can be used for personal (private) or public purposes. MAN is able to support data and sound , it can even relate to cable television networks.(Prayama & Aulia, 2015) (Look at figure 2.2)

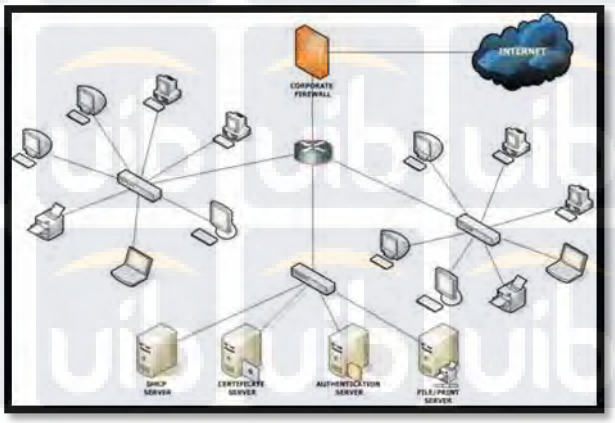

Figure 2.2 Metropolitan Area Network

3) WAN

The definition of WAN network is the concept of relationships between LAN networks, laying areas in different geographical regions. Generally, a WAN network is a concept in connection between LAN networks located at relatively far distances, for example, regions between provinces. Usually in forming a WAN network concept, the role of other parties is needed as well, in this type of the network provider. (Ratnasari, Imansyah, & Pontia, 2017) (Look at figure 2.3)

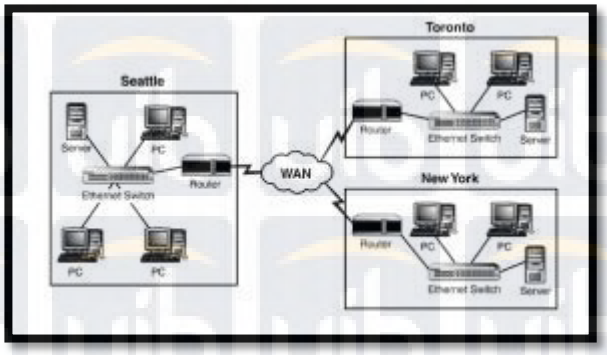

Figure 2.3 Wide Area Network

2.2.2 Network Security

According to (Mutaqin, 2016) Network security is a process to prevent and identify unauthorized uses on the computer networks. Progress to prevent to unauthorized users from accessing any part of a computer network system. Computer network security itself aims to anticipate risks in computer networks in the form of physical and logical threats both direct and indirect threat the ongoing activities in computer networks.

According to (Adrian & Setiyadi, 2018) Network security is one of the important thing for monitoring and preventing unauthorized and inappropriate use

of the network device. The concept for network security has been clarified into 5 parts, as the following:

a. Confidentially

   Confidentiality is a statement who requires information or data that can only be accessed by parties who have been authorize.

b. Integrity

   Integrity is a statement when the information can only be change that can only be change by owner who has the rights.

c. Availability

   Availability is a statement that require some availability information to those who have authority when they needed.

d. Authentication

   Authentication is a statement that the sender of the information can be identified that is correct and to proof the identity obtained is not fake

e. Nonrepudiation

   Nonrepudiation is a statement either the sender or the receiver can't deny the sending and the receiving of the message when it happens.

2.2.3 OSI Layer

This research is written according to (Imam Bayu, Muhammad Yamin, 2017). OSI Layer is one of important network architecture. The OSI layer itself is often used to explain how a computer network works logically. In general, the OSI model divides into 7 layers with various of network functions while the institution that publishes the OS model is the international organization for standard ISO. OSI

model is introduced in 1984. OSI layer model is consists of 7 layers. The seven layers are the following:

1. Application Layer

   This part of the layer deals with the programs computer that usually used by the user. This computer programs related to the only programs that have network access, but the application that doesn't have the network that doesn't mean is not related to OSI. For example, The word processing application. This application is used for text processing program, so it is not related to OSI layer. But if this program is added to the network functions such as sending email with the word application. It can be concluded in the figure 2.4 below.

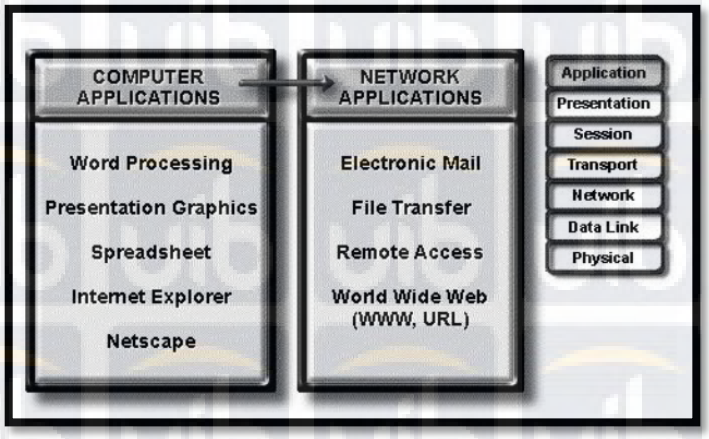

Figure 2.4 Application Layer Summary

2. Presentation Layer

   This part of the layer is task to applying the data format so that it can be understood by various type of media. Other than that, this layer can also convert data formats so that the next layer can understand the format needed for communication. For example: format data that

supported by the presentation layers include: Text, Data, Graphic, Visual Image, Sound, and Video. The description table can be described as in figure 2.5 Below.

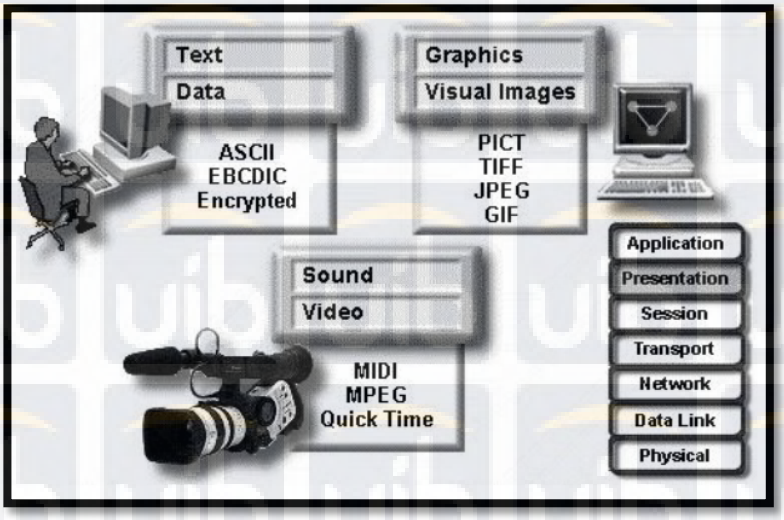

Figure 2.5 Presentation Layer description

3. Session Layer

This layer defines how it will start, control and end a conversation (commonly called a session). List of the examples: NFS, SQL, RPC, ASP, SCP the list is shown in figure 2.6 below.

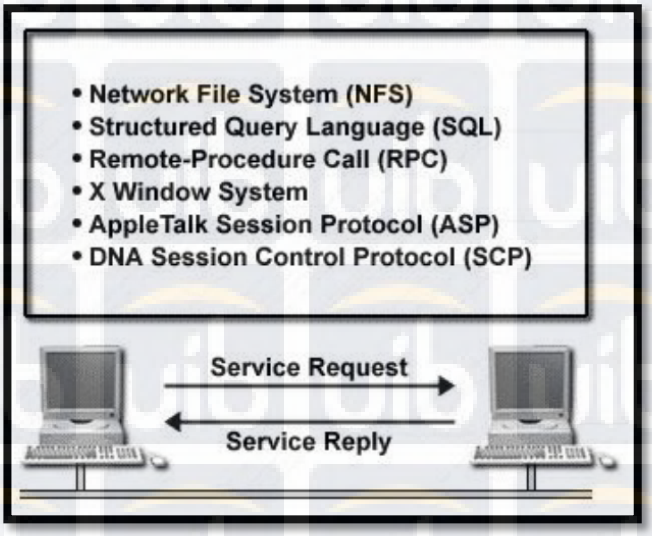

Figure 2.6 Session layer description

4. Transport Layer

In the 4th layer, you can choose whether to use a protocol that supports error recovery or not to. To do a multiplexing of incoming data, sorting data that comes when the arrival is not in order. With this later you can also do end-to-end communication is regulated in several ways, so that the data will be influenced by this 4th layer. The description layer will be shown in figure 2.7 below.

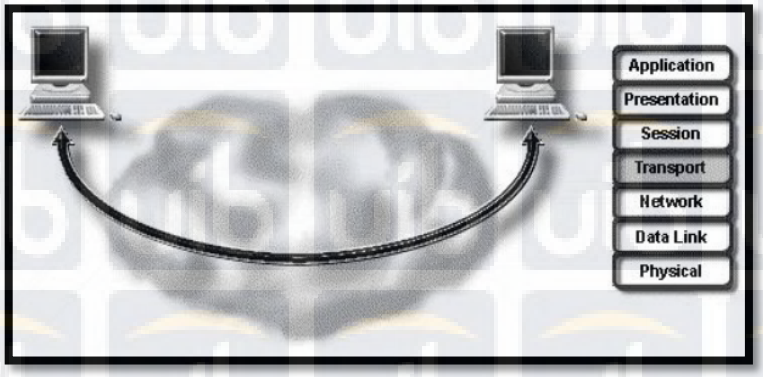

Figure 2.7 Transport layer description

5. Network Layer

The part of the layer is where the connection and network to do transporting. The main function of the network layer is to addressing and routing the network. The addressing for the network is working with logical and systematic. The example in using the IP address is shown in figure 2.8 below.

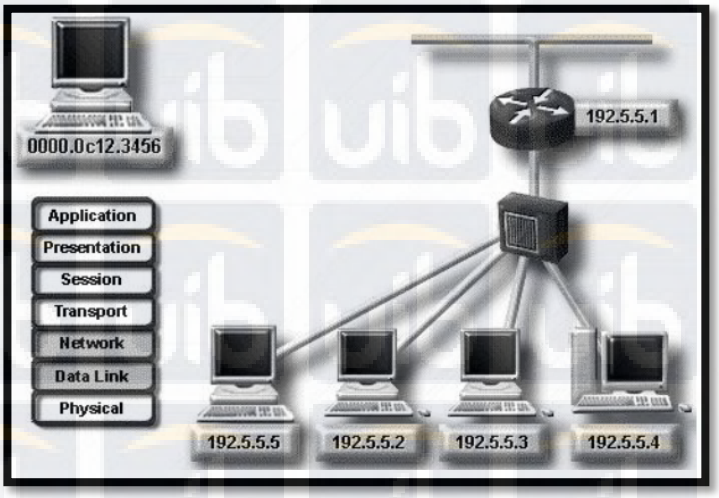

Figure 2.8 Network layer and data link layer description

6. Data link layer

   Data link layer session is often connect with the work of network layer. The functions provided the data link layer as the following:

   a. Arbitration, the selection of physical media
   b. Addressing, physical addressing
   c. Error detection, determine whether the data has been successfully sent
   d. Identify data encapsulation, determine the header pattern in a data.

7. Physical layer

   This layer is sets different definition from other type of layer because this later sets the shape the different interfaces of a transmission media and different specifications most of them were the type of physical external electronic such as connetors, pins, pin usage, electric current passing, encoding, and light sources.

2.2.4 Cybercrime

According to (Fauzan, Riadi, & Fadlil, 2017) on PBB perspective can be consulted in formulated as an illegal act carried out by using an electronic device network as an electronic device or device as an object whether to obtain profit or not, and an act of element that can harm other.

There are many different categories with the deeper explanation Cybercrime itself can be consist into two major groups namely: Violent, potentially violent is the abuse of a computer that will have a physical impact on others. In conclusion it is divided into 3 main groups as the following:

1. Cyber terrorism, which is an activity that leads to terrorist activities by utilizing cyberspace media.
2. Cyber bullying, which is an attempt to a troll in oneself by mocking the other perspective
3. Pornography, this type of crime involves to three groups, namely those involved to create, distribute, and access pornographic material.

Non-Violent is the inappropriate use in computers that are indirect impact on one physical condition but is more systemic. The statement is divided into 5 groups as the following:

1. Cybertrespass, which is an access to computer resources illegally.
2. Cybertheft, is type of activity that being a theft of getting important information or data. A number of activities that can be categorized in cybertheft are:

- Embezzlement, the use of money or company propertly that should not be use to, for example: changing the status of data ownership, illegal transfer,
- Espionage, is an illegal access to important company or organization data

3. Plagiarism, is the recognition of copy others work as an self-made invention.
4. Piracy, illegally claim copyrighted software, music, movies, books.
5. Identity theft, is a statement for stealing personal data such bank accounts, credit cards, e-mails. DNS Cache poisoning, DNS cache manipulation that interferes with network transmission.
6. Cyberfraud, generally in the form of email invitations to work together in investment, social, and relief matters.
7. Destructive crime, which is an activity that can cause damage or loss data such as: viruses, trojans, hacking, and DoS.
8. Other type of crime such as: offering prostitution services, online gambling, drug trafficking, money laundering, unusual items offered in certain type of jurisdictions. For example: the black market of sell buys illegal stuff, rare animal, weapon, and drugs.

2.2.5 Security Threat for IP Camera

There also other threat cybercrime that made especially towards CCTV. this research is according to (Indriyanto & Rahardjo, 2018) :

1. Eavesdropping/disclosure/interception

The videos for CCTV usually are collected or transmitted to DVR/NVR and control servers through public IP networks. In such process of transmitting video is contain secretive information which is not protected from dangerous access. If it caught by an anonymous user can cause serious threats and can also be used in other crimes. This threat must be considered in the development of a surveillance video system.

2. Interruption/Communication Jamming

   These threats interfere with the progress in collecting the video information normally, this causes a denial of service (DoS) for an efficient response.

3. Infection and Modification of Data

   This type of threat modifies video data that is transmitted or stored illegally and injects non-genuine data into it, this reduces the reliability of video information.

4. Unauthorized Access

   Using unauthorized access may damage the authenticity and validity of the videos collected. This also causes violations and misuse of resources from the system.

5. Repudiation

   CCTV or IP camera may sometimes reject the real-time recorded video file / provision except from the granted communication channel between supervisor devices that collect video and video storage devices / control servers.

6. Illegal monitor

The existence of other people who can monitor videos transmitted from CCTV / IP cameras illegally is a statement for violation. Although the administrator has the authority to maintain the collected video information, he is not allowed to monitor directly from the other places personally.

2.2.5.1 Security function

There also a way to prevent the threat from happening. the following researches according to (Indriyanto & Rahardjo, 2018) :

1. Privacy Masking

   As the video collected by multiple IP cameras be able to record at various targeted place, an appropriate technology is needed to protect confidential information and prevent from illegal exposure. Privacy masking consist of two methods, namely static methods and dynamic methods. Static privacy masking is a method protects the ROI (Region of Interest) to remain like a window. In the other side, the dynamic privacy masking method is used for ROI including people, moving vehicles.

2. User/Device Authentication

   As a Video collector device, video storage devices, video control interface, and video service providers consist of a video surveillance system that operates based on public IP networks, a trusted communication channel between the two must be the main consideration. Furthermore, a secure authentication method is needed to fix the user in order access the system.

3. Security Tunnelling

Video information is transmitted through public IP networks, so it is inevitable potential exposure is unauthorized. To resolve problems caused by unauthorize access, therefore is needed to make a channel that can be trusted between entitles that communicate and encrypt video information need to be added.

4. Access Control

   Even though the administrators are involved in the groups that are permitted to maintain and control video information, each admin is given different right access. It guarantees from both security and reliability of the video information.

5. Intrusion Prevention

   This security provides real-time interference detection and the response is mandatory to protect video information from internal / external access attempts, and prevent privacy violations. Disruption prevention technology for video surveillance system can be consisted into two method namely logical and physical methods. Logical interference it protects system resources from attacks that use IP based networks. Other than that, physical interference is to protect system resources from illegal access to physical.

6. Prevention of Forgery

   This security function is to detects the fake copy of video information files

7. Prevention of Misuse

   The information of the collected videos is involving a lot of significant information. That means if there a misuse on the wrong application provided, it can cause several damages.

2.2.6 Closed Circuit Television

CCTV also stands for Closed Circuit Television basically is a digital video camera device that is used to send monitor screen signals in a particular room or a place. It has the main purpose of being able to observe situation and condition in a particular place. In general, CCTV is often used to monitor the area of the public. Generally, the images from the CCTV cameras were only sent via cable to a particular monitor room and also required direct supervision by the operator / security officer with still a low-resolution image. But along with the new development of technology systems. CCTV camera systems can now be operated or controlled with a current smartphone. With this type of gadget u can now monitor anywhere and anytime as long as there is connection with internet or GRPS network access. (Azanuddin & Buulolo, 2017)

2.2.6.1 Type of CCTV

The following research was made by (Nofrida, Hafidudin, & T, 2018) that will describe the type of technology system of CCTV is divided into several, namely :

1) CCTV with Analog camera feature

   The first generation of CCTV on the analog camera system of the device uses standard analog output, namely PAL or NTSC. In the early generation it was recorded only by using a VCR (Video Cassette Recorder). Making the recordings can only be directly seen by connecting with the Television. But with the era of development of CCTV technology can now be installed with integration to computer

networks with the addition of DVR (Digital Video Recorder). (Look at figure 2.9)

Figure 2.9 Analog Camera Architecture

2) IP-Based CCTV

Unlike analog cameras CCTV IP cameras have a type of digital video camera that can transmit and receive data over the internet network. In general, devices are used to monitor the security of the surrounding area. Most of these camera sources are devices called webcam with other terms from "IP camera". The IP CCTV design system is not much different from analog CCTV, the difference is that the device uses a device for the IP camera replaced by NVR and the connection and the camera no longer uses coaxial cable but using an Ethernet cable is compatible with wireless media devices. (Look at figure 2.10)

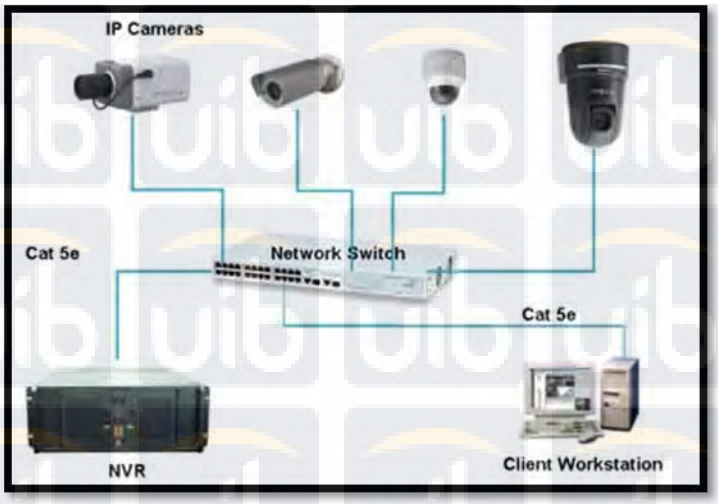

Figure 2.10 Architecture IP Camera CCTV

This type of CCTV is a type of new development. What make different from the ordinary camera with CCTV F-12 is that each camera has their own IP so that we can choose which camera to observe at, IP camera allows home and business owners to view their cameras through an internet connection that is available both through computers and mobile phone that support 3G/4G.(Ade & Yesi, 2018)

2.2.7 Router

According to (Yogyantoro, 2015) Router is a device that works as an traveller data between the two network devices that are currently connected. The router is used to connect between the two active devices so that network communication can be connected from one to an another.

According to (Gustina & Mutiara, 2017) a router is a device that functions for one network with another network with the uses of protocol in different communication. In general routers is a device that sends data packets through a network or internet that goes to its destination, through a process known as obedience. The login process required in layer 3 (network layer such as the

internet protocol) from the seven layers of OSI stack protocol. RouterOS is an operating system software that can be used to make ordinary PC become reliable router networks, including various features made for IP networks and wireless networks.

The researches also using the method of AHP (Analytical Hierarchy Process). The AHP method is a framework to find the effective decision on complex problems, by simplifying and accelerating in making the decision, making process, by solving the problem into its parts, arranging goals, criteria, and alternatives in a hierarchical arrangement, which gives a numerical value to the consideration subjective about the importance of variables and synthesizing these various considerations to determine which variable has the highest priority and acts to influence the outcome of the situation.

The following are the advantages and disadvantages of router with the using of AHP method:

Advantages

1. Having the flexible sense, causing the addition and reduction of criteria in a hierarchy can be done easily and does not screw up or destroy the hierarchy
2. Can enter to personal preferences while accommodating various importance of others in order to obtain objective and non-sectoral assessments.
3. The calculation process is relatively simple because it only requires operation and simple logic.

4. It can quickly show priority, dominance, importance or influence of each element towards other elements.

Weaknesses:

1. The selected participants must have the competency of knowledge and in-depth experience with all aspects of the problem and about the AHP method itself.

2. if there are strong participants it will sure affect the other one.

3. Assessment tends to be subjective because it is strongly influenced by the situation and preferences, perceptions, basic concepts and perspectives of participants.

4. respondents' answers or judgements that are consistent are not always logical in the sense that they are in accordance with existing problems device

2.2.8 Penetration Testing

According to (Yunanri, Riadi, & Yudnana, 2016) Penetration testing is a method of evaluating security on computer systems or networks by identifying weaknesses, vulnerabilities and the absence of patches. Identification in the form of a security hole, firewall configuration and wireless point. Simulation and identification are carried out in internal and remote networks. The goal is to determine and know the types of attacks that might be carried out on the system and the consequences that can occur due to security weaknesses in the computer system or network that is owned.

Description for each stages of the penetration testing execution method standard according to (Adrian & Setiyadi, 2018) as the following :

1. Pre-engagement

   Pre-engagement is the stage where one is the pentester explain the important part of the activities that will be performed on the target.

2. Intelligence Gathering

   This stage is when the pentester trying to collect all the information about the target reference which can be obtained by various media. In this intelligence gathering focuses on wireless networks.

3. Threat Modelling

   Threat Modelling is a definition from the threat modelling approach. Threat modelling is needed for the correct position in penetration testing. The approaching model in this question is the observation of the target which aims to find out the target business process o make it easier to determine the attack.

4. Vulnerability Analysis

   This stage is where the step to look out for security holes based on information that has been gathered previously. Vulnerability aiming to analyse the deficiency in the network system that can be utilized by the pentester.

5. Exploitation

   This stage is where each perspective pentester to attack the target. However, this stage is most likely done by the brute force method without having the element of precision. A pentester will only exploit when he knows exactly

whether the attack was successful or not, but of course there is an unexpected possibility in the target security system. Even so, before committing an attack, the Pentester must know that the target has a security gap that can be used. Doing attacks blindly and hoping for success is not a productive method. one perspective person Pentester has to make an perfect analysis first before making an effective attack

6. Post-Exploitation

   Post exploitation is the stage where each pentester enters into the target network system and then performs the existing infrastructure analysis. At this stage the pentester learns the parts in the system and determines the most critical part of the target. And here a pentester must be able to connect all perspective parts of the system to explain the impact of the attack or the greatest loss that can be hit on the target.

7. Reporting

   Reporting is the stage for most important part in this main activity a pentester use this report for explain to the company tell about the experiment that carried out such as: what has been done, how to do it, the risks that can occur and the most important one is a way to improve the system.

2.2.9 ARP (Address Resolution Protocol)

According to (Nadzirin & Nur, 2017) ARP is a protocol in TCP/IP who is task is to do IP address compress into MAC address. This protocol serves to map the IP address into a MAC address and is a link between the datalink later and the IO layer on TCP/IP. All communication that are ethernet-based is using the ARP protocol. Basically, every computer or device that communicate will definitely

make transactions or exchange information is related to IP and MAC addressesm each transaction will be stored in the following cache operation system.

The following are the functions and roles of the ARP Protocol:

1. ARP protocol role is quite important for network, especially regarding data communication that occurs in the network, especially regarding to data communication that needs of network. Each host that joined or connected in a LAN network communicates with each other using physical address (MAC Address) and using a logical address (IP address)
2. As it is mention in point number one, each host communicates that are using a physical address (MAC Address). So whether like it or not every host that wants to communicates with other hosts must know each other MAC address that is owned by the destination host.
3. At the data transfer stage, before a data that given in a MAC address data must first be given logical address in the form of an IP address. The added IP address is the IP address that are sending host and receiving Host.
4. Then to determine whether is MAC address or physical address of the destination Host. if the physical address is not yet known, it must be sought first. This is where the role of the ARP protocol, by utilizing the IP address information of the existing destination Host, then the sending Host searches by assigning the ARP Protocol.

2.2.9.1 ARP Sniffing and Spoofing

Due to the definition ARP itself of course there a type of network breaching attack to this protocol. This research is according to (Zonggonau & Sajati, 2015)

ARP Sniffing is tapping data on a computer network by diverting data, is an activity that is easily carried out by the hackers. This type of sniffing can be divided into two namely passive sniffing and active sniffing. Passive sniffing intercepts without changing any data or packets on the network, while sniff in actively performs actions or changes to data packets in network. The active sniffing basically modifies the Address Resolution Protocol (ARP) cache so that it deflects the data from the victim's computer to the hacker's computer.

The network attack not only comes from sniffing but there is also an attack by falsifying user identities so that hackers can log into a computer network illegally which is usually called spoofing. Spoofing consists of several types, namely IP spoofing, DNS spoofing, and ARP spoofing. IP spoofing is a complex attack technique that need of several components. This is a security exploit that works by deceiving computers in trusting conversation that you are someone else. DNS spoofing is taking DNS name from another system by jeopardizing the domain name servers of a legitimate domain. ARP spoofing is an act of infiltration using an illegal legal identity by using this identity, the intruder will be able to access everything on the network.

2.2.9.2 ARP poisoning threat with MITM attack

According to (Zonggonau & Sajati, 2015) The ARP protocol works by sending the broadcast ATP request message to all the available computers used

turned out to cause a security hole. During the transaction start it turns out that anyone in the network who is in a broadcast domain can be respond to the ARP broadcast message even though the message content that is intended for him. Not only that anyone on the network who can send the ARP request by pretending to be the host, but with forged physical (MAC) address. Malicious hosts do this by creating fake ARP crafted packets. This security threat is surely known as ARP poisoning

MITM (Man in the Middle) is the follow-up attack that starts from ARP spoofing/poisoning. In the MITM attack, the attacker will position himself in the midst of connection between the two hosts. All forms of communication will go through the attacker's computer. Attacker will easily do snapping(sniffing), manipulate packets (tampering), control communication and all other attacks that are possible with this MITM attack.