THE ATTACKING METHODS INVOLVED IN CURRENT TREND ENVIRONMENT

Rahma Fitria

Sistem Informasi Universitas Malikussaleh Lhokseumawe
Jl. Cot Tgk Nie-Reulet, Aceh Utara, 141 Indonesia
email: *rahmafitria@unimal.ac.id*

Abstract— The use of Common Object Request Broker Architecture (CORBA) has become one of the answer to the requirement for interoperability among the rapidly increasing number of hardware and software products available nowadays. CORBA has been introduced as a mechanism in a distributed computing environment in order to overcome recent interoperability issue. This mechanism allows distributed objects to communicate with each other, whether operate on remote devices or local devices, written in different languages or platforms, or at different locations on a network. In this paper, the concept of CORBA application as a middleware is presented. In order to understand this concept, a simple program to handle auction sale. This system is developed using JAVA programming language. This application is implemented on Windows Operating System (OS) and its method is being invoked by a client from the other machine that also runs in Windows OS. Along with this, the benefits of CORBA and its limitation are discussed in this paper.

Keywords—CORBA concept; client-server; benefits of Corba; Application example

I. INTRODUCTION

Advancement in internet technology growing rapidly nowadays leads to security problems. People have been looking for alternatives of preventing attacks in the network through the development of software and other malicious acts. Recently these attacks have increased to certain point where almost every node and network is exposed to some form of attacks. It might be a shock to others that as we almost twenty four hours daily in order to secure their network from any attacks, the same way goes to an attacker who spends their day altering malicious code and looking for vulnerabilities to be exploit. The technology is constantly evolving and changing fields by new technology and the internet. Awareness of all these network attacks and methods of preventing them helps us in controlling threats and vulnerability. The threat also may ciome from inside organization. These threats may be from a curious person, an angry employee, or from a rival company or a foreign government. There are many research works published on various ways of preventing and protecting computer networks from malicious attacks. This paper will discuss on attacking methods in current environment.

A network will be a medium for attacker to send the attack such as a worm or it could be the medium of attack Denial of Service attack. However, there are few forms of network attacks that do not really attack the computers, but rather attack the network they are attached to. Either by flooding a network stream with unnnecesaary packets which do not attack an individual computer, but cause network down. Although a computer or host may be used to initiate the attack, both the real target and the fake target in the same network. There are few reasons that make intrusion detection system is a necessary part of the entire defense system. In other cases, systems and applications were developed to work in a different environment and may become vulnerable. When deployed, intrusion detection complements these protective mechanisms in order to improve the system security. Internet security is a rapidly evolving field due to the attacks that are catching the headlines can change significantly from one year to the next.

This paper will discuss about the attacking methods that invloved in current environment. This paper will explain about the type of attacks in network security.

II. NETWORK ATTACKS

A network Intrusion Detection System (IDS) is used to monitor networks packets for attacks or intrusion. A large network intrusion detection system server can be implemented on a backbone network when we want to monitor all incoming and outgoing traffic; or smaller systems which can be used to monitor traffic for just particular server, router, switch, or gateway.

When we want to consider network security, it must be ensured that the whole network is secure. Network security does not only concern the security in the nodes at each end of the communication chain. During data transmission, the communication channel should not be vulnerable toany attack. A possible hacker might target the communication channel instead of targeting the nodes, intercept communication and obtain the data, then decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.[2]

The attacks can be launched in times of fast attack or slow attack. Fast attack can be defined as connection within a few seconds[3][4]. Meanwhile, slow attack refers to an attack that takes a few minutes or a few hours to complete[3][4]. Both of the attack gives a great impact to the network environment due to the security breach decade [5]. There several distinct stages that makes up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four (4) main stages:

III. CATEGORIES OF ATTACK

Network and information systems that vulnerable to attacks may attract attackers or hackers. Then, the system must be resistant to attack from any possible threats or attacks. The system also should be able to minimize the damage and recover within short time. Attacks can be categorized into two groups which are passive and active attack monitoring of communication.

A.ACTIVE ATTACK

For active attack, the attacker will try to bypass or break into system. The attack can be launched through stealth, virus, worm or Trojan horses. Active attack can be launched because the attacker wants to introduce malicious code or to steal important information and modify it. The attacks can also be mounted against network backbone, and steal information during data transmission. This type of attack will result in dissemination of data files, DoS, or modification of data.

B.PASSIVE ATTACK

While for passive attack, we will monitor the traffic and find clear text password that can be used in other attack. This type of attack might include analysis traffic and capture the information. In this type of attack, the attacker will not modify the information or data captured. Passive attacks will disclose important information or data files to attacker without user knowing it.

IV. ATTACK METHODS

The vulnerabilities in network can be exploited by attackers in many ways. Attack might happen inside organization or outside organization. Attacks are launched to gain unauthorized access to database and steal confidential data. In this paper, we only focus on six attack methods which are listed below:

A. DOS

In network security, a denial-of-service attack (DOS) is an attempt to make a computer resource unavailable to its intended users. The attackers usually target for high-profile web servers and the hosted web page will be inaccessible on internet. It is a computer crime that violates the Internet proper use policy as indicated by the internet Architecture Board (IAB) [6]. DOS is an attack that happened because of the system received too many requests that the server can handle. All the requests actually come from attacker. when the server cannot handle the requests, then it cannot response to the host that sent request.

After that, the system then consumes resources waiting for the handshake to complete. Actually the system cannot respond to any more requests. In this kind of scenario, it is being rendered useless because it cannot go on with any other services[7].

DOS attack can be categorized into two general forms:

i) Bandwidth depletion
   This method is to congest the network traffic and excessive utilization of the bandwidth which leads to network down.[8]

ii) Resource depletion
   Attacker depletes the key resources such as memory resources and CPU. When server unable to respond to all requests, then the server will down.[8]

In another word, DoS attack is launched to prevent legitimate users from using certain particular services.
Examples of Dos attacks include:

- Flooding a network where preventing legitimate network traffic
- Disrupting service to a specific server or person.
- Attacks can be directed at any network device, routing devices, web, electronic mail, or Domain Name System Servers.
- Consumption of computational resources, such as bandwidth, disk space, or CPU time

The figure 1 below will show how DOS attack is launched.

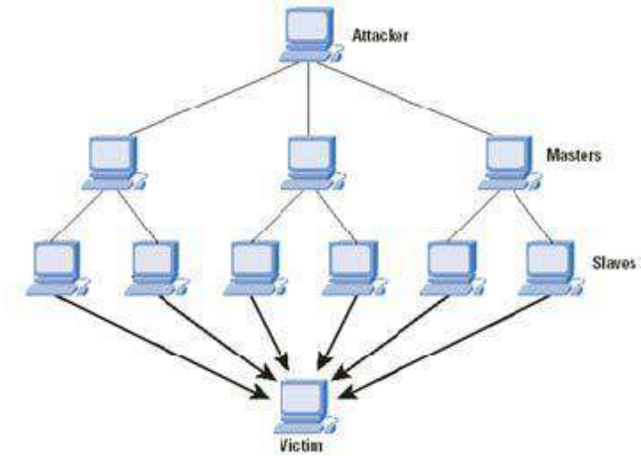

Figure 1: DOS attack flow [9]

B. EAVESDROPPING

Network eavesdropping is network layer attack which contains packet captured from the network. The attacker will search for sensitive information such as passwords, session tokens, or any kind of confidential information. The attack can be launched using certain tools or software which known as packet sniffer. This tool will collect packets transmitted in network and analyze the collected data such as protocol decoders or stream reassembling but it depends on quality of the sniffing tool used.

Eavesdropping attack can be categorized into two types:

1) Active eavesdropping

The malicious host will actively capture the sensitive information through sending queries to sender by disguise themselves as real hosts.[10]

2) Passive eavesdropping

The malicious host will detect the information by listening to the message transmission through wireless medium [10]

Victim tries to access certain web server and then he will send his ID along with his password to the web server for authentication purpose. The packet will pass through hub which will determine destination to route the packet. The packet will be route to web server. Attacker will take this chance to redirect the packet to him. The attacker can analyze the packet to get the sensitive information. Figure 2 will illustrate on how the local eavesdropping launched:

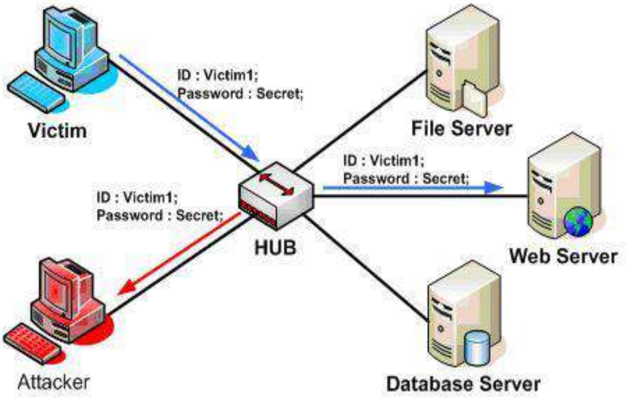

Figure 2: Local Eavesdropping Attack

C. IP SPOOFING

IP Spoofing attack is having IP address of other computer. This is an act of mirroring the address of a trusted computer in order to gain access to a network.[7]. IP spoofing also can be defined as creation of IP packets using somebody else's IP addresses. IP Spoofing also means to imitate or trick someone. Many cyber-attacks happened due to design flaws in the fundamental network designs and packet spoofing also included.

The attack can be done by examining the IP header where first 12 bytes contain various information about the packet. Then the next 8 bytes contains the source and destination IP addresses. By using one or several tools, an attacker can alter these addresses especially the “source address” field. This means that changing the information in the headers of a packet to forge the source IP address. Spoofing can be launched to impersonate other users. This attack is done to avoid detection since source IP address used is belong to the computer spoofed. By spoofing an address that is a trusted port, the attacker can get packets through a firewall.[6] Most of the attacks use spoofed source IP addresses. If the IP address is spoofed a victim is not able to directly trace back the source of the attack or create a firewall.[11]

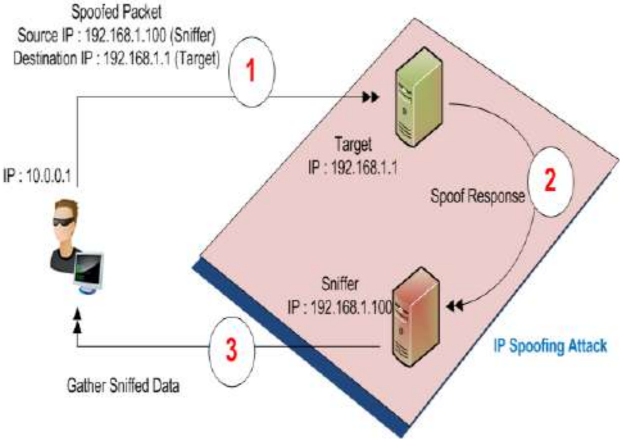

Figure 3: IP Spoofing attack

Based on figure 3, it shows how packet-spoofing attack occurred. The hacker creates IP packets where the source IP field is modified and he will target a destination host, so that it does not have the IP address of the hackers’ computer.

D. HIJACK ATTACK

Hijack attack is easy to be launched and difficult to detect especially for wireless network. Wireless networks do not have specific boundary regions for the packets to be transferred. As the data packets are transferred in air, the chances of sniffing the network packets by the hackers or attackers are high by using the network sniffing tools[12]

For hijack attack, the hijacker takes over a session between sender and receiver and he will interrupt the communication and make one of real user disconnect from network. Then, other user will believe that they are talking to write party and send private and confidential information to the hijacker by accident. The attack can be illustrated in figure 4. The steps are explained below:

i. After login process, victim will send requests to the web application using a cookie (SID) on each request to the web application for authentication purpose.
ii. This request is sent to HTTP, during this process attacker will eavesdrop the request and capture the cookie. The cookie is sent unprotected across the network.
iii. Finally, the attacker can use this cookie to send arbitrary requests to the web application, successfully hijacking the victim’s session. Figure below will show how hijack attack happen.

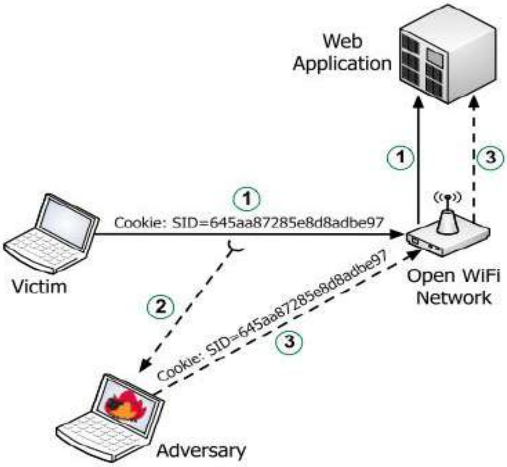
Web
Application
1
3
1
Cookie: SID=645aa87285e8d8adbe97
Victim
Open WiFi
Network
2
Cookie: SID=645aa87285e8d8adbe97
3
Adversary

Figure 4 : Hijacking session[13]

It is important to know that the stolen cookie will remain valid even if the victim logs out from the web application. Cookies are stateless therefore the web application cannot revoke them (the web application could change the key used to create the cookies, but that will revoke the cookies for all users[13].

The other way of session hijacking is exploiting authenticated machine by stealing the cookies stored on that machine or stealing cookies by sniffing the unencrypted network traffic. Then these cookies can be used with the web server to establish an authenticated session.

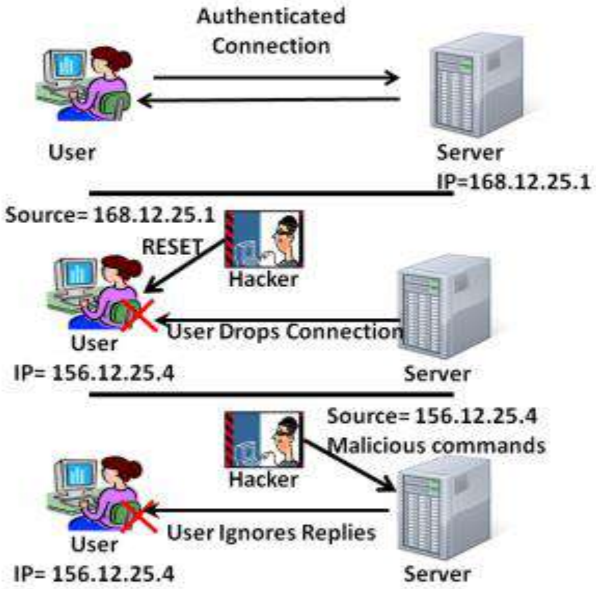

Figure 5 : Hijacking attack[14]

Based on figure 5, we can see that client try to get authentication from server. Then attacker can take this opportunity by sending a reset to client and terminate the connection for client side. Attacker will spoof the real client IP address and continues session with server using that spoofed source address.

E. PHISHING

Phishing is a one of online theft that aims to steal protected information such as credit card information and online banking passwords from users[15]. Phishing attack use fraudulent e-mails designed to fool users into leaking their personal data by stealing the trusted brands of well-known banks, e-commerce and credit card companies[16].

In this attack, the hacker will create a fake website. The website that usually being designed for this attack are bank website where people make online money transaction through website. For example, paypal, maybank2u or CimbClick website. The hacker will create a malicious mail with a hyperlink. The phishing part is when the hacker try to lure users to click a link sent to their email that redirect them to the fake website created by hacker. When the user try to login into system, the information will be sent to hacker's server. Then, the hacker will store the username and pasword. Then they can use it in the real system later.

Phishing can be classified into several types listed below:

1) Clone phishing
   Clone phishing is a type of phishing attack where a cloned website is created. The clone web site usually the site that user always visit. The site usually asks for login credentials[17].

2) Spear phishing
   Spear phishing usually focus at certain group. Instead of sending thousands malicious emails, they will concentrate on a small number of users that share same common. [17]

3) Phone phishing
   This type of phishing refers to text messages or short message system (SMS) that claim to be form a bank asking users to dial a phone number regarding problems with that bank accounts. SMS phishing is one of variation for phone phishing. The end-users receives sms telling him that he has successfully subscribed to a service[17]

The convenience of online commerce has been embraced by consumers and hacker. Phishing has a bad effects on the economy through financial losses experienced by businesses and consumers[18].

V. COUNTERMEASURE OF NETWORK ATTACKS

Countermeasures can be categorized according to the classification of attacks. Most attacks can be prevented using patches and upgrades. This is because by keeping protocols and softwares up-to-date, we can reduce the weaknesses of a computer.

In DoS attack, modification of the system configuration also can reduce possibility of willingly accepting a DoS attack or unwillingly in a DoS attack. User's computer should be aware against illegitimate traffic from or toward the host. Regular scanning also one of alternative to detect any anomalous behavior in the network. Examples of software that can be installed are firewall systems, antivirus, and a reliable intrusion detection systems.

For eavesdropping attack, there are fews alternative to prevent this attack. In this paper, we are going to focus on two prevention ways which are:

i) Signal hiding technique
We can turn off service set identifier (SSID) broadcasting by access point (AP). We also can reduce signal strenght of AP to lower level. Wel also can locate wireless access points in the interior of the building which away from windows.

ii) Encrption
This step involves the use of encryption mechanism in wifi password in order to preserve confidentiality even if the wireless signal is intercepted.

While for IP Spoofing, we can prevent it by installing filter router . It will filter incoming and outgoing packet from and into our network [19], [20].

For hijacking attack, there are several countermeasures can be applied which are listed below:

- Regeneration of Session ID after log in.
- Reduce having remote access.
- Emphasis on Encryption.
- Reduce the life span of session or cookie.

VI. CONCLUSION

Network security is an important field that becomes increasingly important as the internet expands. In this paper, we have presented an overview types of attacks that populars nowadays. Intrusion Detection System (IDS) acts as a mechanism for checking network attacks and the types of attacks that are most likely to be associated with the network. Based on the researchs done, it is shown that DoS attack is more likely preffered by attackers to launch attack.

VII. REFERENCES

[1] R. Anderson, “Network Attack and Defense,” in *Security Engineering : A Guide to Building Dependable Distributed Systems over-long*, 2008, pp. 633–678.

[2] B. Daya, “Network security: History, importance, and future,” *Univ. Florida Dep. Electr. …*.

[3] C. Technology and U. Teknikal, “Statistical Approach for Validating Static Threshold in Fast Attack Detection Faizal, M.A., Zaki, M.M., Shahrin, S., Robiah, Y., Rahayu, S.S.,” *J. Adv. Manuf. Technol.*, vol. 4, no. 1, pp. 53–72, 2010.

[4] O. B. Onuwa, “ORIENTAL JOURNAL OF Improving Network Attack Alarm System : A Proposed Hybrid Intrusion Detection System Model,” 2014.

[5] A. Anand, “An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 8, pp. 94–98, 2012.

[6] M. Gandhi, “Detecting and preventing attacks using network intrusion detection systems,” no. 2, pp. 49–60.

[7] O. Francisca, N. Corresponding, and O. John, “Internet Threat and Attack Hybrid Monitoring System,” vol. 9467, pp. 24–32.

[8] Akash Mittal, A. K. Shrivastava, and Manish Manoria, “A Review of DDOS Attack and its Countermeasures in TCP Based Networks,” *Int. J. Comput. Sci. Eng. Surv.*, vol. 2, no. 4, pp. 177–187, 2011.

[9] A. Sanmorino and S. Yazid, “DDoS Attack detection method and mitigation using pattern of the flow,” *2013 Int. Conf. Inf. Commun. Technol.*, pp. 12–16, 2013.

[10] H. Dai, Q. Wang, D. Li, and R. C. Wong, “On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas,” *Int. J. Distrib. Sens. Networks*, vol. 2013, p. 13, 2013.

[11] M. Vizv, “Mitigation of DDoS Attacks in Software Defined Networks,” no. January, 2015.

[12] S. S. Manivannan and E. Sathiyamoorthy, “A Prevention Model for Session Hijack Attacks in Wireless Networks Using Strong and Encrypted Session ID,” *Cybern. Inf. Technol.*, vol. 14, no. 3, pp. 46–60, 2014.

[13] I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, “One-Time Cookies : Preventing Session Hijacking Attacks with Stateless Authentication Tokens,” pp. 1–31.

[14] A. H. Alqahtani and M. Iftikhar, “TCP / IP Attacks , Defenses and Security Tools,” *Int. J. Sci. Mod. Eng.*, no. 10, pp. 42–47, 2013.

[15] C. K. Engin Kirda, “Parameterized complexity and approximation algorithms,” *Comput. J.*, vol. 51, no. 1, pp. 60–78, 2008.

[16] M. Alkhozae and O. Batarfi, “Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code,” *Int. J. Inf. Commun. Technol. Res.*, vol. 1, no. 6, pp. 283–291, 2011.

[17] M. N. Banu, M. a M. C. Engineering, J. Mohamed, and C. Autonomous, “A Comprehensive Study of Phishing Attacks,” vol. 4, no. 6, pp. 783–786, 2013.

[18] V. Ramakanth, N. Megha, S. Desai, and T. S. Prasad, “A SURVEY ON ATTACKS AND DEFENSE MECHANISMS IN PHISHING,” *Int. J. Res. Appl.*, vol. 1, no. 1, pp. 36–39, 2014.

[19] P. D. Sontakke and P. C. A. Dhote, “Spoofing Attacks Detection and Localizing Multiple Adversaries in Wireless Networks : A Review,” vol. 3, no. 6, pp. 213–220, 2014.

[20] P. V. Subbareddy and Q. I. S. College, “Inter Domain Packet Filters for IP Spoofing,” *Int. J. Comput. Trends Technol. May to June Issue 2011*, 2011.