Internasional Journal of Integrative Sciences (IJIS)
Vol.2, No.6, 2023: 869-874

Sniffing and Spoofing in Computer Security

Saddam RA[1*], Angga Pranata[2], Sugiono[3], Rizki Zulanggara[4], Nur Halimah[5], Sri Nur H[6], Rosdiana SM[7], Nurhalim[8] Aprina Handayani[9]
Pamulang University
Corresponding Author: Saddam RA saddamrasyidinalfaruk1@gmail.com

A R T I C L E I N F O

Keywords: Sniffing, Spooffing, Computer Security

Received : 8 April
Revised : 18 May
Accepted: 26 June

A B S T R A C T

The development of Information Technology (IT) has changed people's mindset. The presence of the Internet as the main platform for online activity is vulnerable to criminal acts by irresponsible parties. Criminal acts in cyberspace, of course, pose a major threat to the governance of online activities. One of these major threats is the threat of network security. Networks connected to the internet are basically insecure and can always be exploited by hackers, both LAN and wireless networks. The internet network has two data transmission media, namely wired and wireless. what happens is open. Examples of network security threats that often occur are sniffing of activities on the network (sniffing) and also impersonation by other people (spoofing). This resume article aims to identify criminal acts that threaten computer security, namely Sniffing and Spoofing

DOI: https://doi.org/10.55927/ijis.v2i6.4528
ISSN-E: 2985-9050
https://journal.formosapublisher.org/index.php/ijis

INTRODUCTION

The development of technology and information is growing rapidly. Progress in the use of information systems provides many advantages for every human activity. However, the negative impacts of information systems are no less numerous, such as computer crimes in the form of wiretapping of data on computer networks by irresponsible parties. This can happen due to a lack of proper security in the system or ignorance of the general public. Even the victim of this crime does not know and is not aware that he is being bugged by someone who is not known. Not only that, eavesdroppers sometimes commit fraud by pretending to be genuine and trustworthy hosts. In the end, there are still few appropriate solutions to detect or prevent this wiretapping activity. The existing computer network intruder detection system is basically capable of detecting various types of attacks but has not been able to take further action to prevent it.

The purpose of this article is to understand how sniffing and spoofing work (wiretapping and infiltration) can be done to find out how to prevent it by carrying out various kinds of solutions and also to improve and maintain security systems in information systems used and to know the types of software that support sniffing and spoofing.

LITERATURE REVIEW

Computer Security

According to John D. Howard in his book "An Analysis of Security Incidents on The Internet" states that computer security is a precautionary measure from attacks by computer users or irresponsible network accessors.

Security on a computer system is very influential on several factors including the following:

-Social engineering
-Security holes in the operating system and service
-Physical security
-Attacks to the network
-DOS attack
-Attacks via web-based applications
-Trojan, backdoor, rootkit, keylogger
-Virus, worm
-Anatomy of a Hack

Computer Security Aspects

Computer security includes four aspects, among others:

- Authentication

This security method is implemented to ensure that the user requesting data access is the true owner of the data.

- Integrity

Data security and authenticity where data or information sent and received can only be changed by authorized parties.

- Privacy

More towards to personal data.

- Availability

The aspect of availability relates to the availability of information when it is needed. Information systems that are attacked or compromised can hinder or eliminate access to information.

Definition of Sniffing and Spoofing

Sniffing is tapping data on a computer network by deflecting data, which is an activity that is easily carried out by hackers. Sniffing can be divided into two, namely passive sniffing and active sniffing. Passive sniffing performs wiretapping without changing any data or packets on the network, while active sniffing performs actions or changes to data packets on the network. This active sniffing essentially modifies the Address Resolution Protocol (ARP) cache so that it diverts data from the victim's computer to the hacker's computer. ARP is a protocol in the TCP/IP Protocol Suite which is responsible for resolving IP addresses into Media Access Control (MAC Address) addresses. ARP is defined in RFC 826.

Attacks do not only come from sniffing but there are also attacks 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 Identify spoofing. IP spoofing is a technically complex attack consisting of several components. This is a security exploit that works by tricking the computer into believing that you are someone else. DNS spoofing is taking DNS names from other systems by compromising the domain name server of a legitimate domain. Identify spoofing is an act of infiltration using an official identity illegally. By using that identity, the intruder will be able to access everything in the network.

METHODOLOGY

Aspects of Security Threats

Aspects of security threats that occur to information are:

a) Interruption, is a threat to the availability of information, data in the computer system is damaged or deleted so that if the data or information is needed, the owner will have difficulty accessing it, maybe even the information is lost. An example is the destruction/modification of hardware or network channels.

b) Interception, constitutes a threat to confidentiality. Information is intercepted so that unauthorized persons can access the computer where the information is stored. An example is wiretapping of data in a network.

c) Modification, is a threat to integrity. Unsuccessful people intercept traffic information that is being sent and then change it according to that person's wishes. Examples are changing values in data files, modifying programs so that they run improperly, and modifying messages that are being transmitted over a network.

d) Fabrication, is a threat to integrity. People who are not entitled to succeed in imitating or falsifying information so that the person receiving the information thinks that the information comes from the person the recipient of the information wants. An example is sending fake messages to other people.

RESULT

Impact of Spoofing

Spoofing is an attack in the form of cyber that should not be underestimated, because the impact of the attack can be very bad, especially for us.

Prevention of Sniffing and Spoofing

In terms of prevention, of course there are several ways to prevent threats or sniffing and spoofing attacks, including the following:

a) Use of SSL Certificates

Before browsing, or transmitting other data, the simple thing you have to do is ensure that the page you are visiting has an SSL (Secure Socket Layer) certificate.

SSL is an encryption-based internet security protocol that is commonly used for website security systems, website pages that already use an SSL certificate can be sure of their security. Usually marked with the HTTPS:// link prefix or a green padlock as shown below.

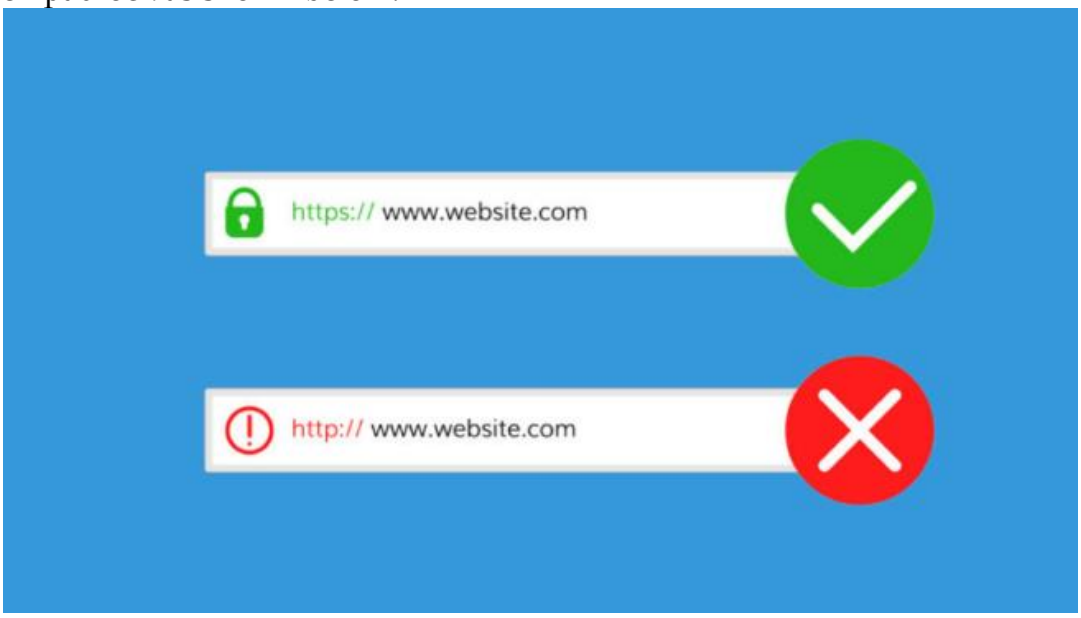

Figure 1. HTTPS dan HTTP

b) Use of filters on router devices

Using filters on router devices can certainly reduce the occurrence of Sniffing and Spoofing, by filtering IPs that you think are suspicious.

Apart from doing IP filtering, you can also activate a spam filter on an email address, so that suspicious incoming emails can be filtered and entered automatically on the spam check menu.

CONCLUSION

Based on the results of data processing and discussion in this study, the authors can draw the following conclusions

a) Interruption, is a threat to the availability of information
b) Interception, constitutes a threat to confidentiality.
c) Modification, is a threat to integrity.
d) Fabrication, is a threat to integrity.

FURTHER STUDY

This research still has many shortcomings such as the influence of variables that may be less influential and need to be added, so further research is still needed

REFERENCES

S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M.

John D.Howard "computer security" An Analysis of Security Incidents on The Internet.

J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

https://sslindonesia.com/sniffing-dan-spoffing-pada-keamanan-website-ssl-indonesia/

Buyung Dwi Permana "Implementasi Sniffing Pada Jaringan HTTP Menggunakan Wireshark" Universitas Perjuangan Tasikmalaya.

E. Kumara, "Analisis Paket Data dengan Mengunakan Wireshark dan Command Prompt," 2017.

Marselina Liren "Kajian Software Penyadap: Sniffing" https://cbn.ac.id/my/blog/view/265/kajian-software-penyadap-sniffing