ANALYSIS OF ARP-SPOOFING ATTACK DETECTION METHODS IN THE NETWORK

Mammadov M.
Doctor of philosophy in engineering, associate professor
Azerbaijan State Agricultural University.
AZ 2000, Ataturk av.450, Ganja, Azerbaijan.
Safarova U.
Assistant. Azerbaijan State Agricultural University.
AZ 2000, Ganja, Azerbaijan.
Mammadli T.
Student. Bamberg University, Germany.
Hacili E.
Master. Azerbaijan State Agricultural University.
AZ 2000, Ganja, Azerbaijan.
Ibrahimova G.
Master. Azerbaijan State Agricultural University.
AZ 2000, Ganja, Azerbaijan.
Taghiyeva T.
Master. Azerbaijan State Agricultural University.
AZ 2000, Ganja, Azerbaijan
https://doi.org/10.5281/zenodo.13930713

Abstract

In the era of widespread use of modern computer networks, one of the most important tasks in the infrastructure of a private enterprise is to ensure the security of its computer network. To date, network attacks, especially ARP-spoofing, are particularly relevant. Due to the comprehensive and extensive functionality of modern network systems, it is difficult to detect these types of attacks, and due to the ease of their implementation, these network attacks are considered one of the most dangerous attacks. This article describes the description and detection method of ARP-spoofing attack.

Keywords: ARP-spoofing, network traffic, ARP-table, Mac-address, detection, active detection methods, early detection.

Introduction. In modern times, the biggest criminal area is in the field of information technology. A large part of crimes are cyber-attacks. In parallel with the development of information technologies, the number and quality of cyber-attacks is also developing. Every year, more and more new threats and hacking methods appear. With the increase of information technologies, the risks also increase, the power of information terrorism increases, the amount and methods of propaganda increase. Today, information security is one of the biggest problems of large organizations and all countries. [1]

Among network attacks, ARP-spoofing attack is considered as one of the most pressing problems. In terms of the wide functionality of the modern information and communication system, it is very simple to organize ARP-Spoofing type network attacks, and on the contrary, the detection of this type of attacks is much more complicated. In this regard, such network attacks are among the most dangerous attacks. The nature of ARP-spoofing attack and detection methods are analyzed in our article [2].

The problem. The wide spread of computer networks has brought with it a new problem - the issue of cyber security - a very urgent issue. Currently, people use the Internet widely using various technical and software. One of these tools and the most used one is WI-FI technology. Please note that traffic is not encrypted when using a WI-FI network. For this reason, this information can be intercepted by cyber criminals. Their goal is to trick people into stealing personal information that users send on this network. Therefore, taking measures against cyber attacks in such networks is one of the main problems [4].

A brief review of the research in this area. In the last decades of the 21st century, enough scientific-research works were conducted and articles were published dedicated to the topic of the effects of network attacks in order to obtain information and protect necessary information. Various standards and best protection methods, data transfer processes and security policies, and basic security controls are reviewed. However, despite this, the study of information security, protection means and methods is still very relevant today [3].

Problem selection. Cybercriminals have developed many methods that allow them to intercept network traffic to steal personal information; Interception of TCP connections and organization of data interception for data falsification for the purpose of MITM (Man-in-the-Middle) attack. The concept of this work is to capture information using methods that allow infiltration of an existing connection or communication process. An attacker can be a passive listener in a conversation, quietly stealing sensitive information, or an active participant, changing the content of messages or pretending to be the person or system the person believes they are talking to. A type of cyber-attack that intercepts, redirects and monitors

network traffic in a local network is ARP spoofing [Man-in-the-Middle: советы по ображению и предотвращению [7].

Presentation of the main material. Network attacks have become one of the most important problems in modern society today and can cause significant damage. A study by the University of Maryland's A. James Clark School of Engineering shows that cyberattacks occur with alarming frequency - more than 2,200 times a day - and someone is victimized every 39 seconds.[6]. This relentless pace of cybercrime means that hackers are constantly exploiting vulnerabilities in a variety of sectors, putting both individuals and businesses at significant risk. According to the information of the international company Positive Technologies, the number of incidents increased by 7% in the first quarter of 2024 compared to the previous quarter. A significant proportion of successful cyber-attacks was the leakage of confidential information, with 72% for individual users and 54% for organizations. The number of ARP-spoofing attacks has also increased significantly [11].

In the context of cybersecurity, spoofing is a situation in which an attacker disguises himself as another person, company, or entity in order to gain the user's trust. Typically, the goal of fraud is to gain access to systems, steal data or money, or distribute malware.

Spoofing is a general term for cyberattacks in which a criminal poses as a trusted person or device to gain benefits by harming the user. If an Internet fraudster pretends to be someone else, this can be classified as fraud. [5]

Such attacks can occur in any form of communication on the Internet and can use any means - from simple to technically complex. To increase their chances of success, attackers use social engineering techniques - psychological manipulation techniques that instill fear in the victim, play on their greed or lack of technical knowledge. [10]

The essence of an ARP-spoofing attack is to send an ARP reply with a fake MAC address to redirect network traffic through its own network card. Implementing this attack allows an attacker to eavesdrop on all network traffic without the user suspecting it. That is why it is a priority task to develop a method for detecting ARP-spoofing attacks for scientific research and training of experts using real equipment.

The purpose of developing the method of detecting ARP-spoofing attacks is to increase the level of security of information processes in computer systems through timely detection of this type of attacks.

A feature of the considered attack is the presence of a weakness in the ARP protocol, that is, sending a spontaneous ARP response without authentication. Despite the effectiveness of spontaneous ARP, it is particularly unreliable because it can be used to trick a remote host into believing that the MAC address of any system on the same network has changed and indicate which address to use in the future.

There are several tools to protect against ARP spoofing [12]:

Static ARP entries are the simplest way to protect against ARP spoofing. This entry is entered manually and prevents the device from automatically changing its ARP cache. Note that this method can only be used for certain accesses (e.g. default gateway addresses) and client nodes are still vulnerable to the attack.

A program to inspect ARP requests. It validates IP/MAC addresses and blocks unverified responses. There is another version of this program that notifies the host of changes in the ARP cache.

Firewall with packet filter. They detect attempts by hackers to masquerade as another host by recording packets sent from duplicate addresses [12].

Encryption. This is the most important defense against an ARP attack. This makes ARP cracking more difficult and prevents a hacker from reading messages after they are intercepted.

VPN. When you connect to a VPN, all your data will pass through an encrypted tunnel that guarantees protection from any hacker attacks.

Detection methods.

Arpwatch. Arpwatch is an open source computer program. This software helps monitor Ethernet traffic activity (such as IP and MAC address changes) on the network and maintains a database of MAC/IP addresses. It creates a log of found IP and MAC addresses along with a time stamp, so you can closely monitor any activity occurring on the network. There is also an option to email reports to the network administrator when a pair is added or changed.

The Arpwatch utility is particularly useful for network administrators monitoring ARP activity to detect ARP spoofing or unexpected IP/MAC address changes.

NetCut . NetCut is a program that helps you manage your network using only the ARP protocol. NetCut is a program that helps you manage your network using only the ARP protocol. Calculating the IP-MAC table in seconds, opening and closing the network on any computer on the local network, including routers, switches, etc.

Features:

- IYFT: Obtain the IP addresses of all computers on the local network in seconds.

- High application: work in office network, school network or even internet provider network.

-Safe: TRACE Free, no one will track what happened [8].

Netcut defender is a free software from arcai.com to protect ultra-fast internet speed on your network (including Wi-Fi) and protect your computer and connected devices from network attacks.

TuxCut.TuxCut,

As software written in PyQt is a netcut "on Windows OS".

TuxCut protects Linux computers from the latest attacks

Features: Hide your machine (ip / MAC) from arp scanner utilities. List all live hosts on your local network. disconnect any live host and gateway. Use Wondershaper to monitor upload or download speed [9].

References:

1.Nəbiyev B.R. DDoS hücumların aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodunun tətbiqi.// İnformasiya texnologiyaları problemləri, 2018, №1, 110–120

2.Алиев Р.М. РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ АТАК ТИПА ARP-SPOOFING // Шаг в науку. 2019. №2. URL: https://cyberleninka.ru/article/n/razrabotka-metoda-obnaruzheniya-atak-tipa-arp-spoofing (дата обращения: 17.09.2024).

3.Корнев Д. А. , Лопин В. Н., Лузгин В. Г. активные методы обнаружения SYN-flood атак.// электронный научный журнал Курского государственного университета. 2012. № 4 (24). Т. 2

4.Перехвать и анализ трафика в открытых Wi-Fi [Електронный ресурс] URL:https://hackware.ru/?p=7441

5.Семёнов Ю.А. Ping и Traceroute. // http://citforum.ru/nets/semenov/4/45/ping_451.shtml

6.https://keepnetlabs-website.pages.dev/blog/171- cyber-security-statistics-2024-s-updated-trends-and-data

7. Електронный ресурс] URL: https://habr.com/ru/company/varonis/ blog/526632/

8.https://ruprogi.ru/software/netcut?ysclid=m1grgiywgw318895226

9.https://vertexeng.com/insights/delay-analysis-methods-examining-the-impacted-as-planned-method/].

10.https://www.kaspersky.ru/resource-center/definitions/spoofing

11.https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/

12/https://www.securitylab.ru/analytics/532149.php