# Emulation and Detection of ARP Attacks in GNS3 Environment: Modelling and Development of a Defense Strategy

Tetiana Vakaliuk[1,2,3], Yelyzaveta Trokoz[1], Oleksandra Pokotylo[1], Viacheslav Osadchyi[4,2], and Viktoriia Bolotina[1]

[1] *Zhytomyr Polytechnic State University, 103 Chudnivsyka str., Zhytomyr, 10005, Ukraine*
[2] *Institute for Digitalisation of Education of the NAES of Ukraine, 9 M. Berlynskoho str., Kyiv, 04060, Ukraine*
[3] *Kryvyi Rih State Pedagogical University, 54 Gagarin ave., Kryvyi Rih, 50086, Ukraine*
[4] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str, Kyiv, 04053, Ukraine*

**Abstract**

The article discusses various types of attacks on the ARP protocol and the tools used to implement and detect them. The principal network vulnerabilities related to the lack of authentication and encryption were identified through modeling, and methods to prevent or reduce the risk were proposed. A network design was created in the GNS3 environment, which is as close to the real environment as possible. Specialized tools such as Nping, Arpspoof, and Ettercap were used to carry out the ARP-Flooding, ARP-Spoofing, and ARP-Poisoning attacks, and XArp software was used for detection.

**Keywords**

ARP, GNS3, attack emulation, ARP-flooding, ARP-spoofing, ARP-poisoning.

## 1. Introduction

Due to the widespread spread of cyber threats and their constant improvement in the modern information environment, the issue of network security is highly relevant. As technologies are constantly evolving, it is essential to ensure appropriate detection and protection against various types of attacks. One of the most common threats to network security is ARP attacks aimed at unauthorized interception and acquiring confidential information. The risk of their impact in the context of the Internet of Things (IoT) expansion is growing due to the constant increase in the number of connected devices in the network [1–3]. Therefore, to avoid vulnerabilities in new environments and effectively manage network infrastructure, it is essential to understand the algorithm of attacks on this protocol, consider methods of detecting them, and develop and implement means of protection against them [4, 5].

### 1.1. Theoretical Background

An analysis of research on this topic has shown that there are many ways to detect and conduct various specialized attacks on network protocols, particularly on ARP, to increase the resilience of network systems.

In particular, the article by Swati Jadhav, Arjun Thakur, Shravani Nalbalwar, Shubham Shah, and Sankalp Chordia [6] proposes various methods for detecting an ARP poisoning attack at both the user and organizational levels. It is noted that after the attack on the client device, the traffic was intercepted and analyzed using a Python algorithm and other software products. The result of the work highlights the options for protecting a computer in the event of potential attacks.

The study by Zhaozhan Chen [7] includes an analysis of the principles of operation and attack modes based on the ARP protocol, IP,

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: tetianavakaliuk@gmail.com (T. Vakaliuk); liza.bailiuk@gmail.com (Y. Trokoz); a.a.polish4uk@gmail.com (O. Pokotylo); v.osadchyi@kubg.edu.ua (V. Osadchyi); viktoriia.polish@gmail.com (V. Bolotina)
ORCID: 0000-0001-6825-4697 (T. Vakaliuk); 0000-0002-4961-7816 (Y. Trokoz); 0000-0002-1587-235X (O. Pokotylo); 0000-0001-5659-4774 (V. Osadchyi 4); 0000-0002-5122-8879(V. Bolotina)

and MAC addresses. The author examines the format of the ARP packet, the process of data exchange during its operation, and the structure of attacks such as Counterfeit gateway, Spoofing gateway, Spoofing user attack, and Man-in-the-middle. The paper proposes a method for improving network security by implementing appropriate security measures based on practical experience.

In the work of Xiaohan Zhang, Lu Cao, Zuojun Meng, and Xiaohui Yao [8], a solution for the SDN (Software Defined Network) network was proposed that allows the accurate detection of ARP attacks by checking the veracity of the IP to MAC address mapping and the MAC address during the ARP packet processing by the controller. The authors have conducted experiments in a simulated SDN network, which confirms the possibility of detecting attacks without affecting the network performance as a whole and reducing the time of ARP interaction between hosts.

In a study by Akinul Islam Jony and Arjun Kumar Bose Arnob [9], Long Short-Term Memory (LSTM) networks are used for intrusion detection as a new strategy to enhance IoT security. The proposed LSTM-based model demonstrates excellent results in detecting both known and novel cyberattack patterns with an accuracy of 98.75% and an F1 score of 98.59% in extensive experimental evaluations using the large CIC-IoT2023 dataset, which represents a diverse set of IoT network traffic scenarios. This research contributes significantly to IoT security by addressing the urgent need for adaptive intrusion detection systems to protect against evolving cyber threats.

In the article by Cristina L. Abad, Rafael I. Bonilla [10] proposed several schemes to mitigate, detect, and prevent attacks on the ARP protocol, but each has its drawbacks. This article will analyze these schemes, identify their strengths and weaknesses, and offer recommendations for developing an alternative and (possibly) better solution to the ARP cache poisoning problem.

Anjana Kawshan [11] found that the ARP protocol is vulnerable to an ARP-spoofing attack, as it lacks authentication. As a result, it can lead to Man-in-the-Middle attacks, denial of service, and others. The author discusses the algorithm of actions in the case of MITM and shows how to detect ARP-spoofing attacks using your code.

The article by Huixing Xi [12] includes a systematization of the current state of research and critical technologies related to the ARP protocol. The author analyses the mechanisms of ARP vulnerability formation and considers possible attack techniques. Based on the generalization of commonly used protection methods, their advantages and disadvantages are presented. Experiments and tests are conducted for each advanced security algorithm.

The study of Mehdi Nobakht, Hadi Mahmoudi, and Omid Rahimzadeh [13] proposes a distributed security mechanism for detecting and counteracting the ARP cache poisoning attack. It can detect a more advanced type of such an attack, in which the attacker leaves a minimum of traces. The prototype of the proposed mechanism is implemented in Python, and its viability and effectiveness are demonstrated through extensive experiments in a local network with 15 hosts. The evaluation results indicate instant detection with millisecond accuracy and minimal impact on network traffic.

During the analysis of publications on this topic, it was found that they pay little attention to the process of modeling threats to the ARP protocol, which is essential for understanding both the specific vulnerability and the algorithm of actions and provides an opportunity to study the network's response to specific actions of attackers. In addition to analyzing the ARP-Flooding, ARP-Spoofing, and ARP-Poisoning attacks, this article discusses their sequential execution in the modeled network, provides an overview of the reactions of network devices and end nodes, and explores the possibility of detecting attacks using the XArp tool. This allows you to identify network vulnerabilities and choose effective methods and means to eliminate them.

## 1.2. Methods

To achieve this goal, this study used analysis and simulation methods. The analysis allowed us to identify vulnerabilities of the ARP protocol, potential attacks on it, and their possible consequences. The simulation was used to model attacks using the Nping, Arpspoof, and Ettercap tools in the GNS3 environment. This made it possible to practically study a network similar to a real one and identify its vulnerabilities to choose an effective method of protection in the future. The object of research is the ARP protocol and its vulnerabilities, and the subject is methods and tools for modeling attacks on the ARP protocol in the GNS3 environment and their detection using XArp.

The purpose of the article is to study various vulnerabilities of the ARP protocol and to simulate ARp-flooding, ARP-Spoofing, and ARp-poisoning attacks on the nodes of a network created in the GNS3 environment using specialized tools Nping, Arpspoof, and Ettercap and detect them using XArp.

## 2. Results

ARP (Address et al.) establishes a correspondence between the logical IP address and the physical MAC address of a device on a local network. It allows for more efficient routing and traffic forwarding, ensuring correct communication and addressing on the network. When one device needs to communicate with another and uses its IP address, ARP makes it possible to determine the corresponding MAC address. If the latter is already known, the device can send data immediately, and if it is unknown, an ARP request is sent to obtain this information.

ARP is an integral part of the network infrastructure, so the growth of threats in the field of network security requires a detailed study of attacks on this protocol and the development of effective methods for detecting and protecting against them. The study of attacks on the ARP protocol is essential in ensuring the privacy of network communications and improving the overall security of computer systems.

The principal vulnerabilities of ARP include the following: lack of authentication and encryption of information, which makes it vulnerable to interception and cache poisoning attacks; the ability to send fake ARP messages, as there are no authentication checks for requests, responses, and ARP tables themselves; ease of cache poisoning, which leads to a violation of the correctness of network interaction.

The peculiarities of the algorithm and the above shortcomings have led to the threat of the following attacks:

1. ARP-Flooding is an attack carried out by creating a broadcast storm, i.e., sending many ARP requests to the network to overflow ARP caches. As a result, network performance decreases, devices fail, incorrect ARP tables are built, which leads to conflicts and incorrect routing, and there is a possibility of traffic interception.
2. ARP-Spoofing is an attack that involves sending fake ARP responses to the network. An attacker impersonates a legitimate device and indicates its own MAC address in response to requests to redirect network traffic through itself. As a result, unauthorized interception of confidential information occurs with its subsequent viewing and modification.
3. ARP-Poisoning is an attack that is a type of ARP-Spoofing aimed at a specific device or a group of them. The logic of its operation is the same, i.e., the attacker sends fake ARP responses to poison the ARP caches of nodes, resulting in incorrect correspondences between IP and MAC addresses and the possibility of redirecting traffic to illegitimate users [14].

These attacks are rarely used in the form described above, usually combining their capabilities and using different implementations.

These potential threats are critical for corporate networks, where reliable and uninterrupted operation is vital. Understanding all the stages of such attacks becomes essential for assessing the possible impact on the network and further determining the necessary measures to protect the network infrastructure.

Various programs and utilities are used to implement attacks on the ARP protocol, including Ettercap, Cain&Abel, BetterCAP, Scapy, Gobbler, Nping, Arpspoof, Arroison, ARPBuilder, and others. Each has its functionality and features, and the choice of a particular tool depends on the user's needs and the goal to be achieved by the attack [15].

In this study, the Nping tool was chosen for the ARP-Flooding attack, Arpspoof for ARP-Spoofing, and Ettercap for ARP-Poisoning, as their functionality is sufficient to achieve the goal.

Detecting the fact of an attack is a necessary element for ensuring information security, so it is essential to monitor the network to identify characteristic signs constantly. In the case of the ARP protocol, it is crucial to monitor whether the device's response time to various network operations increases, whether the ARP activity on the interfaces is too high, whether entries with the same addresses appear in the ARP tables, etc. Specialized software applications can be used for this purpose.

Table 1 compares ArpWatch, XArp, WinARPWatch, ArpStar, ARPScan, NetCut Defender, and Colasoft Capsa by their primary functions and support for different operating systems.

Considering the above comparison, the choice was made to use the XArp software tool to detect ARP attacks planned to be carried out.

The GNS3 (Graphical Network Simulator-3) tool was chosen as the modeling environment, as it allows emulating networks and testing them interactively and using authentic operating system images. An essential factor for using GNS3 is the ability to perform attacks in an isolated environment without affecting the performance of a real network.

**Table 1**
Main characteristics of tools for detecting attacks on the ARP protocol

| Program | Main functions | Support for Windows OSt | Support for Unix/ Linux OS |
|---|---|---|---|
| *ArpWatch* | – Tracking ARP tables<br>– Notification of changes | - | + |
| *XArp* | – ARP attack detection<br>– Notification of attacks | + | - |
| *WinARP Watch* | – Monitoring of ARP tables<br>– Anomaly detection | + | - |
| *ArpStar* | – Protection against ARP attacks<br>– Anomaly detection | - | + |
| *ARPScan* | – Network scan to detect abnormal ARP requests | + | + |
| *NetCut Defender* | – Protection against ARP-spoofing<br>– Access control | + | - |

To emulate attacks on the ARP protocol, we will develop a realistic network topology in the GNS3 environment. We will add network devices and configure them to reproduce the attack scenarios—we will use Nping, Arpspoof, and Ettercap to launch the ARP-Flooding, ARP-Spoofing, and ARP-Poisoning attacks. The next step is to observe the impact of these attacks on the network, detect them with XArp, and develop an effective defense strategy.

To illustrate, it is enough to create a compact network that includes a Cisco router, based on which you can configure a DHCP server for dynamic configuration of endpoint IP addressing parameters, a switch, and four workstations. Three of them will be legitimate Windows workstations (Win10-Admin, Win7-User1, WinXP-User2), and the fourth will be malicious (KaliLinux-Hacker), from which attacks will be carried out using the above tools (Fig. 1).

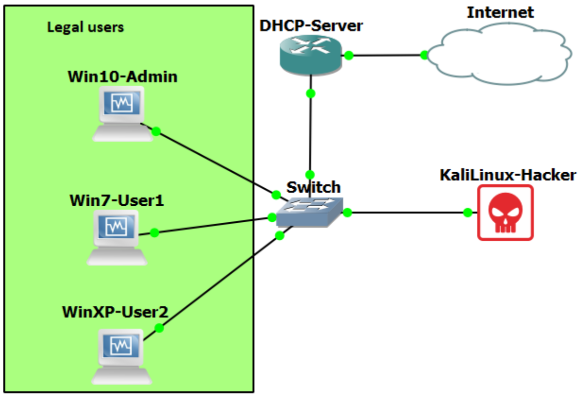


**Figure 1:** Design of the built network

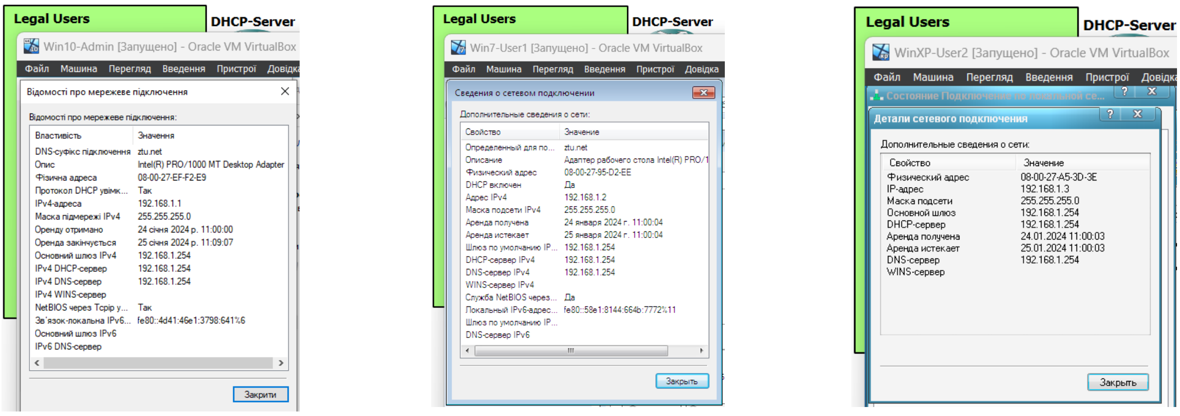
The successful configuration of the DHCP server is confirmed by the end nodes receiving IP addressing parameters (Fig. 2). There is communication between legitimate devices, and the ARP tables of network devices and workstations before the attacks are shown in Fig. 3.

The Win10-Admin workstation has the XArp application installed to detect attacks on the ARP protocol. The KaliLinux-Hacker user received the address 192.168.1.4/24.

Let us start the ARP-Flooding attack using the Nping utility. To do this, execute the corresponding command on the attacker's workstation, which generates many ARP messages and sends them to the same network as the sending device (Fig. 4a). During the attack, the XArp application installed on the Win10-Admin workstation signals the presence of an attack in real-time (Fig. 4b).

During the attack, the switch displays relevant system messages, and the connection between endpoints is either absent or unstable with long delays (Fig. 5).

The next attack that will be modeled is ARP-Spoofing using the Arpspoof utility. We use the corresponding command, in the parameters of which we specify the IP addresses of one of the legal workstations (for example, Win10-Admin) and one of the network devices (for example, a router) (Fig. 6a). The attack is successfully detected using the installed XArp application (Fig. 6b).


Legal Users
DHCP-Server
Win10-Admin [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Закрити
Win7-User1 [Запущено] - Oracle VM VirtualBox
Закрыть
WinXP-User2 [Запущено] - Oracle VM VirtualBox
Состояние Подключение по локальной се...

Відомості про мережеве підключення

Відомості про мережеве підключення:

| Властивість | Значення |
|---|---|
| DNS-суфікс підключення | ztu.net |
| Опис | Intel(R) PRO/1000 MT Desktop Adapter |
| Фізична адреса | 08-00-27-EF-F2-E9 |
| Протокол DHCP увімк... | Так |
| IPv4-адреса | 192.168.1.1 |
| Маска підмережі IPv4 | 255.255.255.0 |
| Оренду отримано | 24 січня 2024 р. 11:00:00 |
| Оренда закінчується | 25 січня 2024 р. 11:09:07 |
| Основний шлюз IPv4 | 192.168.1.254 |
| IPv4 DHCP-сервер | 192.168.1.254 |
| IPv4 DNS-сервер | 192.168.1.254 |
| IPv4 WINS-сервер | |
| NetBIOS через Tcpip у... | Так |
| Зв'язок-локальна IPv6... | fe80::4d41:46e1:3798:641%6 |
| Основний шлюз IPv6 | |
| IPv6 DNS-сервер | |

(a)

Сведения о сетевом подключении

Дополнительные сведения о сети:

| Свойство | Значение |
|---|---|
| Определенный для по... | ztu.net |
| Описание | Адаптер рабочего стола Intel(R) PRO/1 |
| Физический адрес | 08-00-27-95-D2-EE |
| DHCP включен | Да |
| Адрес IPv4 | 192.168.1.2 |
| Маска подсети IPv4 | 255.255.255.0 |
| Аренда получена | 24 января 2024 г. 11:00:04 |
| Аренда истекает | 25 января 2024 г. 11:00:04 |
| Шлюз по умолчанию IP... | 192.168.1.254 |
| DHCP-сервер IPv4 | 192.168.1.254 |
| DNS-сервер IPv4 | 192.168.1.254 |
| WINS-сервер IPv4 | |
| Служба NetBIOS через... | Да |
| Локальный IPv6-адрес... | fe80::58e1:8144:664b:7772%11 |
| Шлюз по умолчанию IP... | |
| DNS-сервер IPv6 | |

(b)

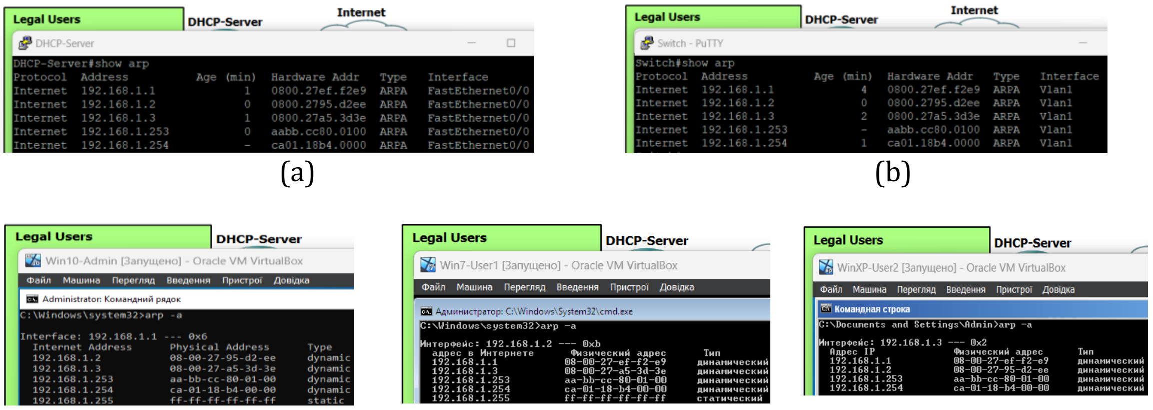
Детали сетевого подключения

Дополнительные сведения о сети:

| Свойство | Значение |
|---|---|
| Физический адрес | 08-00-27-A5-3D-3E |
| IP-адрес | 192.168.1.3 |
| Маска подсети | 255.255.255.0 |
| Основной шлюз | 192.168.1.254 |
| DHCP-сервер | 192.168.1.254 |
| Аренда получена | 24.01.2024 11:00:03 |
| Аренда истекает | 25.01.2024 11:00:03 |
| DNS-сервер | 192.168.1.254 |
| WINS-сервер | |

(c)

**Figure 2:** Dynamic address acquisition by workstations


Legal Users
DHCP-Server
Internet
DHCP-Server
Switch - PuTTY
Win10-Admin [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Administrator: Командний рядок
Win7-User1 [Запущено] - Oracle VM VirtualBox
Администратор: C:\Windows\System32\cmd.exe
WinXP-User2 [Запущено] - Oracle VM VirtualBox
Командная строка

```
DHCP-Server#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             1   0800.27ef.f2e9  ARPA   FastEthernet0/0
Internet  192.168.1.2             0   0800.2795.d2ee  ARPA   FastEthernet0/0
Internet  192.168.1.3             1   0800.27a5.3d3e  ARPA   FastEthernet0/0
Internet  192.168.1.253           0   aabb.cc80.0100  ARPA   FastEthernet0/0
Internet  192.168.1.254           -   ca01.18b4.0000  ARPA   FastEthernet0/0
```

(a)

```
Switch#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             4   0800.27ef.f2e9  ARPA   Vlan1
Internet  192.168.1.2             0   0800.2795.d2ee  ARPA   Vlan1
Internet  192.168.1.3             2   0800.27a5.3d3e  ARPA   Vlan1
Internet  192.168.1.253           -   aabb.cc80.0100  ARPA   Vlan1
Internet  192.168.1.254           1   ca01.18b4.0000  ARPA   Vlan1
```

(b)

```
C:\Windows\system32>arp -a

Interface: 192.168.1.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.2           08-00-27-95-d2-ee     dynamic
  192.168.1.3           08-00-27-a5-3d-3e     dynamic
  192.168.1.253         aa-bb-cc-80-01-00     dynamic
  192.168.1.254         ca-01-18-b4-00-00     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

(c)

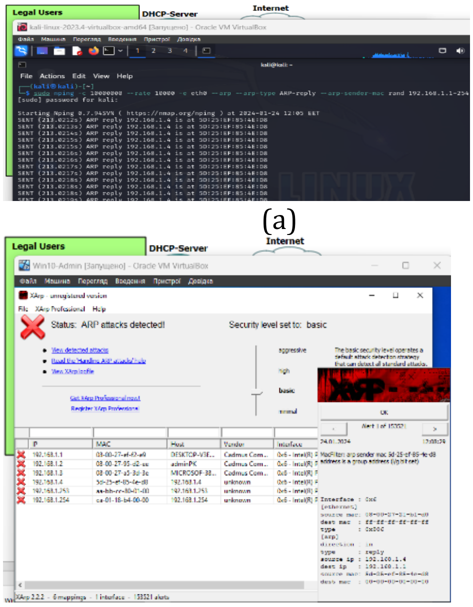
```
C:\Windows\system32>arp -a

Интерфейс: 192.168.1.2 --- 0xb
  адрес в Интернете      Физический адрес      Тип
  192.168.1.1           08-00-27-ef-f2-e9     динамический
  192.168.1.3           08-00-27-a5-3d-3e     динамический
  192.168.1.253         aa-bb-cc-80-01-00     динамический
  192.168.1.254         ca-01-18-b4-00-00     динамический
  192.168.1.255         ff-ff-ff-ff-ff-ff     статический
```

(d)

```
C:\Documents and Settings\Admin>arp -a

Интерфейс: 192.168.1.3 --- 0x2
  Адрес IP              Физический адрес      Тип
  192.168.1.1           08-00-27-ef-f2-e9     динамический
  192.168.1.2           08-00-27-95-d2-ee     динамический
  192.168.1.253         aa-bb-cc-80-01-00     динамический
  192.168.1.254         ca-01-18-b4-00-00     динамический
```

(e)

**Figure 3:** ARP tables of devices before the attack


Legal Users
DHCP-Server
Internet
kali-linux-2023.4-virtualbox-amd64 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
kali@kali: ~
File Actions Edit View Help
Win10-Admin [Запущено] - Oracle VM VirtualBox
XArp - unregistered version
File XArp Professional Help
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal
OK

```
┌──(kali㉿kali)-[~]
└─$ sudo nping -c 10000000 --rate 10000 -e eth0 --arp --arp-type ARP-reply --arp-sender-mac rand 192.168.1.1-254
[sudo] password for kali:

Starting Nping 0.7.94SVN ( https://nmap.org/nping ) at 2024-01-24 12:05 EET
SENT (213.0212s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0213s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0214s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0215s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0215s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0216s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0216s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0217s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0217s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0218s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0218s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0218s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
SENT (213.0219s) ARP reply 192.168.1.4 is at 5D:25:EF:85:4E:D8
```

(a)

Status: ARP attacks detected!

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks.

| IP | MAC | Host | Vendor | Interface |
|---|---|---|---|---|
| 192.168.1.1 | 08-00-27-ef-f2-e9 | DESKTOP-V3E... | Cadmus Com... | 0x6 - Intel(R) P |
| 192.168.1.2 | 08-00-27-95-d2-ee | adminPK | Cadmus Com... | 0x6 - Intel(R) P |
| 192.168.1.3 | 08-00-27-a5-3d-3e | MICROSOF-38... | Cadmus Com... | 0x6 - Intel(R) P |
| 192.168.1.4 | 5d-25-ef-85-4e-d8 | 192.168.1.4 | unknown | 0x6 - Intel(R) P |
| 192.168.1.253 | aa-bb-cc-80-01-00 | 192.168.1.253 | unknown | 0x6 - Intel(R) P |
| 192.168.1.254 | ca-01-18-b4-00-00 | 192.168.1.254 | unknown | 0x6 - Intel(R) P |

Alert 1 of 153521

24.01.2024 12:08:29

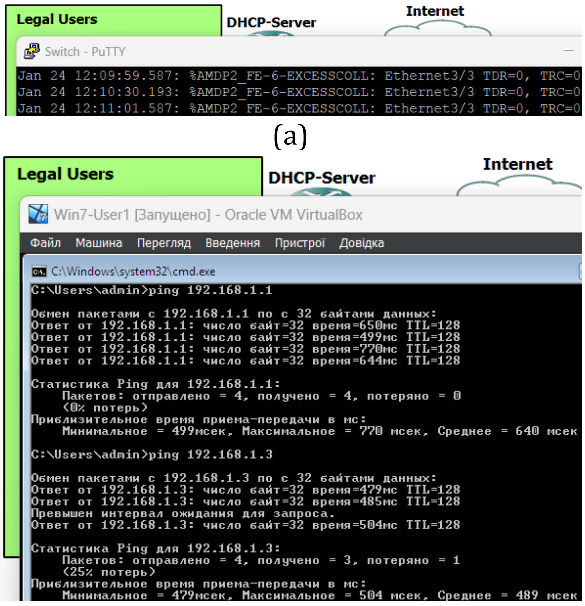
MacFilter: arp sender mac 5d-25-ef-85-4e-d8 address is a group address (I/g bit set)

```
Interface : 0x6
[ethernet]
source mac: 08-00-27-31-b1-d0
dest mac  : ff-ff-ff-ff-ff-ff
type      : 0x806
[arp]
direction : in
type      : reply
source ip : 192.168.1.4
dest ip   : 192.168.1.1
source mac: 5d-25-ef-85-4e-d8
dest mac  : 00-00-00-00-00-00
```

XArp 2.2.2 - 6 mappings - 1 interface - 153521 alerts

(b)

**Figure 4:** ARP-Flooding (a) attack execution (b) attack detection


Legal Users
DHCP-Server
Internet
Switch - PuTTY
Win7-User1 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
C:\Windows\system32\cmd.exe

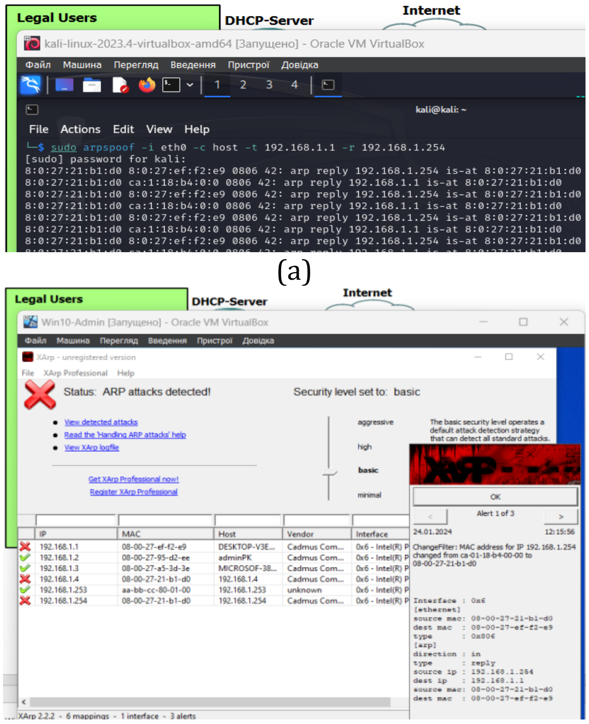
```
Jan 24 12:09:59.587: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
Jan 24 12:10:30.193: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
Jan 24 12:11:01.587: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
```

(a)

```
C:\Users\admin>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=650мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=499мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=770мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=644мс TTL=128

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 499мсек, Максимальное = 770 мсек, Среднее = 640 мсек

C:\Users\admin>ping 192.168.1.3

Обмен пакетами с 192.168.1.3 по с 32 байтами данных:
Ответ от 192.168.1.3: число байт=32 время=479мс TTL=128
Ответ от 192.168.1.3: число байт=32 время=485мс TTL=128
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.3: число байт=32 время=504мс TTL=128

Статистика Ping для 192.168.1.3:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    (25% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 479мсек, Максимальное = 504 мсек, Среднее = 489 мсек
```

(b)

**Figure 5:** Network device response to an ARP-Flooding attack


Legal Users
DHCP-Server
Internet
kali-linux-2023.4-virtualbox-amd64 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
kali@kali: ~
File Actions Edit View Help

```
└─$ sudo arpspoof -i eth0 -c host -t 192.168.1.1 -r 192.168.1.254
[sudo] password for kali:
8:0:27:21:b1:d0 8:0:27:ef:f2:e9 0806 42: arp reply 192.168.1.254 is-at 8:0:27:21:b1:d0
8:0:27:21:b1:d0 ca:1:18:b4:0:0 0806 42: arp reply 192.168.1.1 is-at 8:0:27:21:b1:d0
8:0:27:21:b1:d0 8:0:27:ef:f2:e9 0806 42: arp reply 192.168.1.254 is-at 8:0:27:21:b1:d0
8:0:27:21:b1:d0 ca:1:18:b4:0:0 0806 42: arp reply 192.168.1.1 is-at 8:0:27:21:b1:d0
8:0:27:21:b1:d0 8:0:27:ef:f2:e9 0806 42: arp reply 192.168.1.254 is-at 8:0:27:21:b1:d0
8:0:27:21:b1:d0 ca:1:18:b4:0:0 0806 42: arp reply 192.168.1.1 is-at 8:0:27:21:b1:d0
8:0:27:21:b1:d0 8:0:27:ef:f2:e9 0806 42: arp reply 192.168.1.254 is-at 8:0:27:21:b1:d0
```

(a)

Legal Users
DHCP-Server
Internet
Win10-Admin [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
XArp - unregistered version
File XArp Professional Help
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal
OK
Alert 1 of 3

Status: ARP attacks detected!

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks.

|  | IP | MAC | Host | Vendor | Interface |
|---|---|---|---|---|---|
| ✗ | 192.168.1.1 | 08-00-27-ef-f2-e9 | DESKTOP-V3E... | Cadmus Com... | 0x6 - Intel(R) P |
| ✓ | 192.168.1.2 | 08-00-27-95-d2-ee | adminPK | Cadmus Com... | 0x6 - Intel(R) P |
| ✓ | 192.168.1.3 | 08-00-27-a5-3d-3e | MICROSOF-38... | Cadmus Com... | 0x6 - Intel(R) P |
| ✗ | 192.168.1.4 | 08-00-27-21-b1-d0 | 192.168.1.4 | Cadmus Com... | 0x6 - Intel(R) P |
| ✓ | 192.168.1.253 | aa-bb-cc-80-01-00 | 192.168.1.253 | unknown | 0x6 - Intel(R) P |
| ✗ | 192.168.1.254 | 08-00-27-21-b1-d0 | 192.168.1.254 | Cadmus Com... | 0x6 - Intel(R) P |

24.01.2024 12:15:56

ChangeFilter: MAC address for IP 192.168.1.254 changed from ca-01-18-b4-00-00 to 08-00-27-21-b1-d0

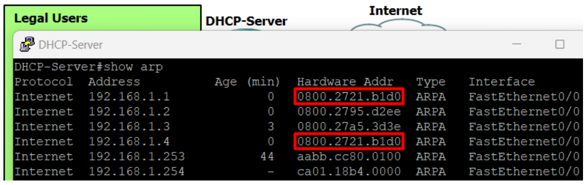
```
Interface : 0x6
[ethernet]
source mac: 08-00-27-21-b1-d0
dest mac  : 08-00-27-ef-f2-e9
type      : 0x806
[arp]
direction : in
type      : reply
source ip : 192.168.1.254
dest ip   : 192.168.1.1
source mac: 08-00-27-21-b1-d0
dest mac  : 08-00-27-ef-f2-e9
```

XArp 2.2.2 - 6 mappings - 1 interface - 3 alerts

(b)

**Figure 6:** ARP-Spoofing (a) carrying out an attack (b) detecting an attack

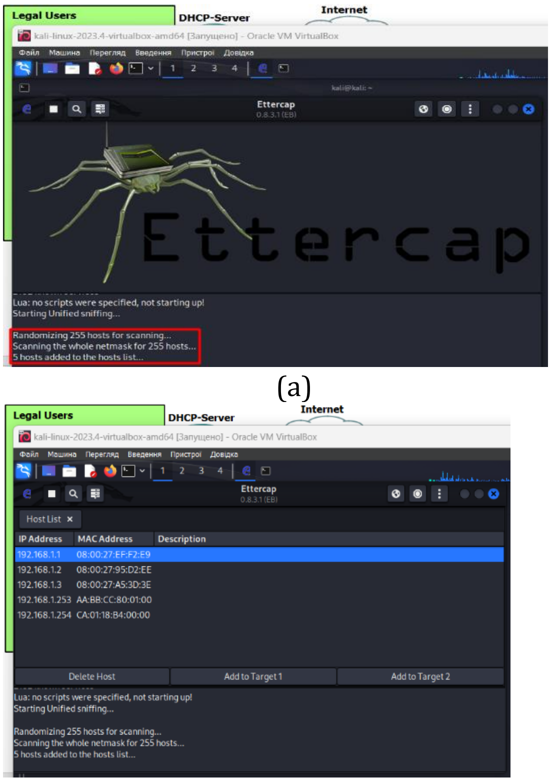
Let us display the router's ARP table (Fig. 7). As you can see, the MAC address of the interface of the legitimate Win10-Admin workstation and the KaliLinux-Hacker workstation are the same (different IP addresses have the same MAC address). The ARP-Spoofing attack was successful. The MAC address of the network interface of the legitimate workstation has been spoofed to the MAC address of the attacker's network interface, which means that the attacker will be able to intercept the network traffic of the legitimate workstation.



```
DHCP-Server#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              0   0800.2721.b1d0  ARPA   FastEthernet0/0
Internet  192.168.1.2              0   0800.2795.d2ee  ARPA   FastEthernet0/0
Internet  192.168.1.3              3   0800.27a5.3d3e  ARPA   FastEthernet0/0
Internet  192.168.1.4              0   0800.2721.b1d0  ARPA   FastEthernet0/0
Internet  192.168.1.253           44   aabb.cc80.0100  ARPA   FastEthernet0/0
Internet  192.168.1.254            -   ca01.18b4.0000  ARPA   FastEthernet0/0
```

**Figure 7:** ARP table of the router after an ARP-Spoofing attack

Let us simulate an ARP-Poisoning attack using the Ettercap utility. To do this, select Hosts in the menu after launching it, then Scan for Hosts. As a result, the hosts are scanned (Fig. 8a). To view them again, select Hosts in the menu and click Host list (Fig. 8b).


Legal Users
DHCP-Server
Internet
kali-linux-2023.4-virtualbox-amd64 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Ettercap
0.8.3.1 (EB)
Ettercap

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
```

(a)

Legal Users
DHCP-Server
Internet
kali-linux-2023.4-virtualbox-amd64 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Ettercap
0.8.3.1 (EB)
Host List ×
Delete Host
Add to Target 1
Add to Target 2

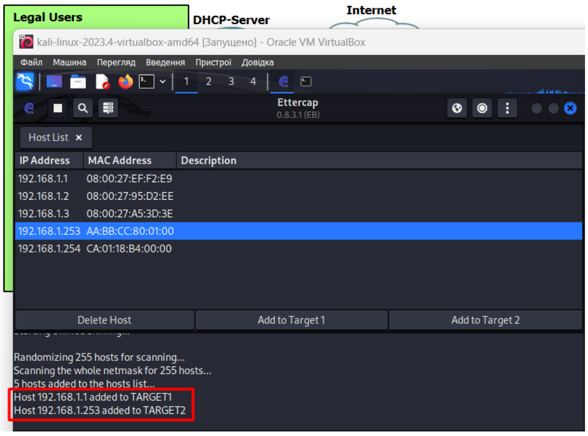
| IP Address | MAC Address | Description |
|---|---|---|
| 192.168.1.1 | 08:00:27:EF:F2:E9 |  |
| 192.168.1.2 | 08:00:27:95:D2:EE |  |
| 192.168.1.3 | 08:00:27:A5:3D:3E |  |
| 192.168.1.253 | AA:BB:CC:80:01:00 |  |
| 192.168.1.254 | CA:01:18:B4:00:00 |  |

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
```

(b)

**Figure 8:** The process of (a) scanning and (b) the result of scanning hosts in Ettercap

From this list, you need to select the hosts that will be attacked. Since the application for detecting ARP attacks is installed on Win10-Admin, select the IP address corresponding to this workstation and add it using Add to Target 1. As the second target address, select, for example, the IP address of the switch interface and add it using Add to Target 2 (Fig. 9).

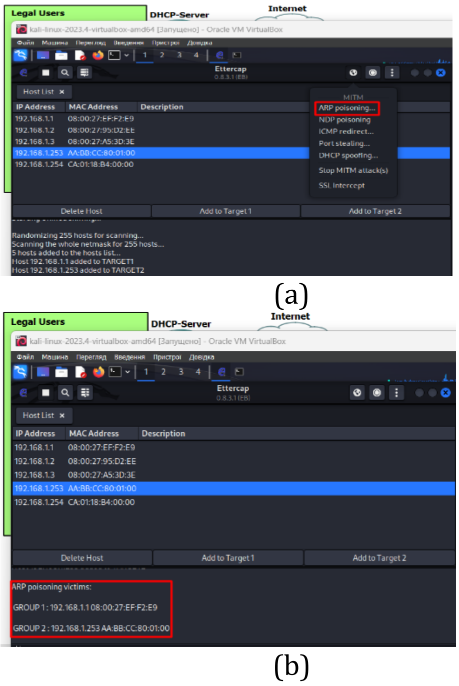

Legal Users
DHCP-Server
Internet
kali-linux-2023.4-virtualbox-amd64 [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Ettercap
0.8.3.1 (EB)
Host List ×
Delete Host
Add to Target 1
Add to Target 2

| IP Address | MAC Address | Description |
|---|---|---|
| 192.168.1.1 | 08:00:27:EF:F2:E9 |  |
| 192.168.1.2 | 08:00:27:95:D2:EE |  |
| 192.168.1.3 | 08:00:27:A5:3D:3E |  |
| 192.168.1.253 | AA:BB:CC:80:01:00 |  |
| 192.168.1.254 | CA:01:18:B4:00:00 |  |

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.253 added to TARGET2
```

**Figure 9:** Selecting target IP addresses for the attack

In the MITM attacks menu, select ARP poisoning, then Sniff remote connections and click OK. The attack process in the Ettercap utility is shown in Fig. 10.



| IP Address | MAC Address | Description |
|---|---|---|
| 192.168.1.1 | 08:00:27:EF:F2:E9 | |
| 192.168.1.2 | 08:00:27:95:D2:EE | |
| 192.168.1.3 | 08:00:27:A5:3D:3E | |
| 192.168.1.253 | AA:BB:CC:80:01:00 | |
| 192.168.1.254 | CA:01:18:B4:00:00 | |

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.253 added to TARGET2
```

(a)

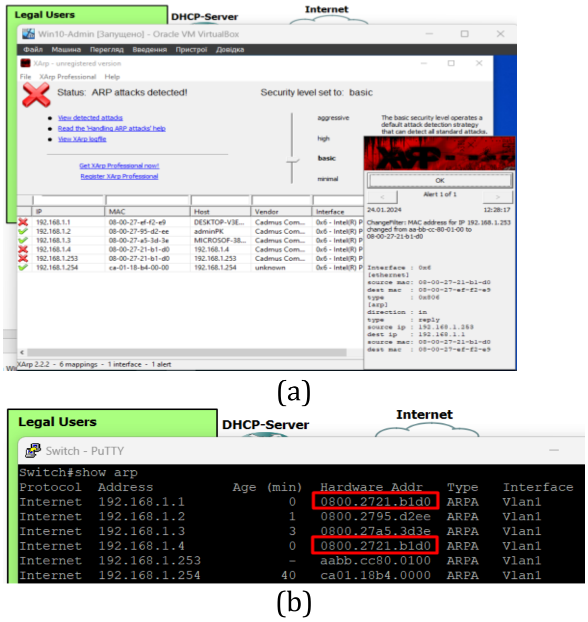
```
ARP poisoning victims:

GROUP 1 : 192.168.1.1 08:00:27:EF:F2:E9

GROUP 2 : 192.168.1.253 AA:BB:CC:80:01:00
```

(b)

**Figure 10:** Performing an ARP-Poisoning attack

The attack is successfully detected by the XArp application (Fig. 11.a). Display the ARP table of the switch (Fig. 11.b).

We can see that the MAC address of the interface of the legitimate Win10-Admin workstation and the KaliLinux-Hacker workstation are the same. The ARP-poisoning attack was successful, and the MAC address was spoofed. The attacker was able to intercept the traffic of a legitimate workstation.


Legal Users
DHCP-Server
Internet
Win10-Admin [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
XArp - unregistered version
File XArp Professional Help
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal
OK
Alert 1 of 1
Switch - PuTTY

Status: ARP attacks detected!

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks.

| | IP | MAC | Host | Vendor | Interface |
|---|---|---|---|---|---|
| ✗ | 192.168.1.1 | 08-00-27-ef-f2-e9 | DESKTOP-V3E... | Cadmus Com... | 0x6 - Intel(R) P |
| ✓ | 192.168.1.2 | 08-00-27-95-d2-ee | adminPK | Cadmus Com... | 0x6 - Intel(R) P |
| ✓ | 192.168.1.3 | 08-00-27-a5-3d-3e | MICROSOF-38... | Cadmus Com... | 0x6 - Intel(R) P |
| ✗ | 192.168.1.4 | 08-00-27-21-b1-d0 | 192.168.1.4 | Cadmus Com... | 0x6 - Intel(R) P |
| ✗ | 192.168.1.253 | 08-00-27-21-b1-d0 | 192.168.1.253 | Cadmus Com... | 0x6 - Intel(R) P |
| ✓ | 192.168.1.254 | ca-01-18-b4-00-00 | 192.168.1.254 | unknown | 0x6 - Intel(R) P |

XArp 2.2.2 - 6 mappings - 1 interface - 1 alert

```
24.01.2024                                    12:28:17
ChangeFilter: MAC address for IP 192.168.1.253
changed from aa-bb-cc-80-01-00 to
08-00-27-21-b1-d0

Interface : 0x6
[ethernet]
source mac: 08-00-27-21-b1-d0
dest mac  : 08-00-27-ef-f2-e9
type      : 0x806
[arp]
direction : in
type      : reply
source ip : 192.168.1.253
dest ip   : 192.168.1.1
source mac: 08-00-27-21-b1-d0
dest mac  : 08-00-27-ef-f2-e9
```

(a)

```
Switch#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             0   0800.2721.b1d0  ARPA   Vlan1
Internet  192.168.1.2             1   0800.2795.d2ee  ARPA   Vlan1
Internet  192.168.1.3             3   0800.27a5.3d3e  ARPA   Vlan1
Internet  192.168.1.4             0   0800.2721.b1d0  ARPA   Vlan1
Internet  192.168.1.253           -   aabb.cc80.0100  ARPA   Vlan1
Internet  192.168.1.254          40   ca01.18b4.0000  ARPA   Vlan1
```

(b)

**Figure 11:** (a) ARP-Poisoning detection (b) ARP table of the switch

After emulating attacks on the ARP protocol, it was determined that they can cause a decrease in network performance, disrupt the correctness of ARP tables of devices, open up the possibility of intercepting network traffic, and lead to devise failures and other negative consequences.

Having identified the weaknesses of the network, it is worth developing a strategy to protect it from this type of attack, which will include the following steps:

1. Use static ARP records to reduce the risk of unauthorized table changes.
2. Install ARP traffic monitoring and filtering systems to detect suspicious activity promptly.
3. Use traffic encryption at the link layer to complicate the analysis of ARP packets.
4. Configuring security mechanisms to protect against attacks (Dynamic ARP Inspection, DHCP Snooping, IP Source Guard).
5. Use VLANs to limit the propagation of ARP traffic.
6. Use personal firewalls on endpoints to block unauthorized ARP packets and changes to ARP tables.

Implementing this strategy will reduce the risk of successful ARP attacks and increase the security of the network infrastructure.

## 3. Conclusion

As a result of step-by-step modeling of attacks on the ARP protocol using the Nping, Arpspoof, and Ettercap utilities, it was found that the built network has specific weaknesses related to insufficient control and security of the internal network infrastructure. The resulting possibility of unauthorized access can cause device malfunctions, MAC address spoofing, and network traffic interception. Following the proposed security strategy, it is essential to consider these risks when designing and configuring the network to prevent unauthorized access. Further research may include analyzing the vulnerabilities of other protocols and developing effective security methods with practical demonstrations of their operation.

## References

[1] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518.

[2] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2.

[3] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922.

[4] O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.

[5] B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76.

[6] S. Jadhav, et al., Detection and Mitigation of ARP Spoofing Attack, International Conference on Innovative Computing and Communications, LNNS (2023) 395–405. doi: 10.1007/978-981-99-3010-4_33.

[7] Z. Chen, Research on ARP Attack Principle and Defense Measures in LAN, International Conference on Computer Network Security and Software Engineering (CNSSE 2023) 12714 (2023) doi: 10.1117/12.2683288.

[8] X. Zhang, et al., A Solution for ARP Attacks in Software Defined Network, The Second International Conference on Artificial Intelligence, Information Processing and Cloud Computing (2021) 1–9. doi: 10.1109/AIIPCC53292.2021.9474466.

[9] A. Jony, A. Arnob, A Long Short-Term Memory Based Approach for Detecting Cyber Attacks in IoT Using CIC-IoT2023 dataset, J. Edge Comput. (2024). doi: 10.55056/jec.648.

[10] C. Abad, R. Bonilla, An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks, 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07) (2007) 60–60. doi: 10.1109/ICDCSW.2007.19.

[11] A. Kawshan, Create ARP Spoofing Attack Using Scapy (2022). doi: 10.13140/RG.2.2.19490.09923.

[12] H. Xi, Research and Application of ARP Protocol Vulnerability Attack and Defense Technology Based on Trusted Network, AIP Conference Proceedings, 1820(1) (2017), 090019. doi: 10.1063/1.4977403.

[13] M. Nobakht, H. Mahmoudi, O. Rahimzadeh, A Distributed Security Approach against ARP Cache Poisoning Attack, ACM Transactions on Internet Technology (TOIT) 22(1) (2022) 1–21. doi: 10.1145/3494108.3522765.

[14] I. Anfalovas, What Is Address Resolution Protocol? A Beginner's Guide to ARP (2024). URL: https://www.ipxo.com/blog/address-resolution-protocol/

[15] T. Vakaliuk, et al., (2023). Modeling Attacks on the DHCP Protocol in the GNS3 Environment and Determining Methods of Security Against Them, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3350 (2023) 209–216.