УДК 004.94:004.056.53
DOI: 10.31673/2412-9070.2024.010913

О. Ю. КОНОВАЛОВ[1], канд. техн. наук, доцент;
Л. О. ХАРЛАЙ[2], канд. техн. наук, доцент;
Л. В. ДАКОВА[3], канд. техн. наук, доцент,
[1] Національна Академія СБ України, Київ
[2] Київський фаховий коледж зв'язку
[3] Державний університет інформаційно-комунікаційних технологій, Київ

ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ЛАБОРАТОРІЇ LABTAINERS ДЛЯ МОДЕЛЮВАННЯ МЕРЕЖНИХ АТАК І ВРАЗЛИВОСТЕЙ

Розглянуто питання використання віртуального середовища Labtainers для організації лабораторного практикуму в процесі підготовлення дисциплін із кібербезпеки. Використовуючи вразливості ARP-протоколу було досліджено принципи та механізми створення атаки типу ARP-Spoofing, здійснено аналіз сучасних інструментів для формування такого типу атак. Наведено порівняльні характеристики потрібного обладнання для різних варіантів упорядкування лабораторного середовища з використанням фізичного обладнання і віртуальних машин.

Запропоновано переваги використання контейнеризації для розгортання тестового мережного середовища на базі контейнерів Docker.

Для дослідження середовища Labtainers як організація лабораторного практикуму було вибрано лабораторну роботу з моделювання атаки типу ARP-Spoofing і аналізом мережного трафіку засобами мережного сніфера Wireshark.

Ключові слова: ARP-Spoofing; Labtainers; моделювання атак; ARP-протокол.

Вступ

Постановка проблеми. Останніми роками кількість кіберзлочинів постійно зростає і сьогодні становить значну загрозу нашому суспільству й економіці. Також внаслідок фінансового шахрайства дедалі збільшується кількість загроз щодо персональних даних та конфіденційності клієнтів, особливо літніх людей.

Отже, за таких умов гостро постає питання наявності спеціалістів із кібербезпеки, а також методик їх підготовки. Кількість дисциплін, пов'язаних із кібербезпекою, стрімко збільшується як у закладах професійно-технічних, так і в закладах вищої освіти. Підготування майбутніх спеціалістів із кібербезпеки є головним пріоритетом національної безпеки, фінансової стабільності та економічного розвитку.

Найбільш відомою атакою на мережні ресурси з перехопленням трафіку між вузлами мережі є атака під назвою ARP-Spoofing (ARP-спуфінг).

Аналіз останніх досліджень. Збільшення кількості атак потребує постійного вдосконалення методів захисту, а також добре навченого персоналу, що дає змогу звести до мінімуму час реагування з моменту виявлення атаки. Для розв'язання такого завдання потрібно мати можливість моделювати атаки і навчати методам реагування на них [1].

Для моделювання атаки типу ARP-Spoofing із використанням комп'ютерної техніки потрібно як мінімум три персональних ПК, що досить витратно з фінансового погляду (рис. 1) [2]. Якщо ж застосовувати віртуальні машини, то на одному хості потрібно розгорнути принаймні три з них. За такого підходу хостова машина має мати значний обсяг пам'яті, потужний процесор і досить місткий жорсткий диск. Оскільки моделювання атак потрібно виконувати у мережному середовищі, то слід також налаштувати і віртуальну мережу для цих віртуальних машин. Розміщення на хостовій машині понад три віртуальні машини, яким потрібна внутрішня мережа, уже є обтяжливим завданням для студентів і вимагає додаткового часу на розгортання і налаштування такої мережі [3].

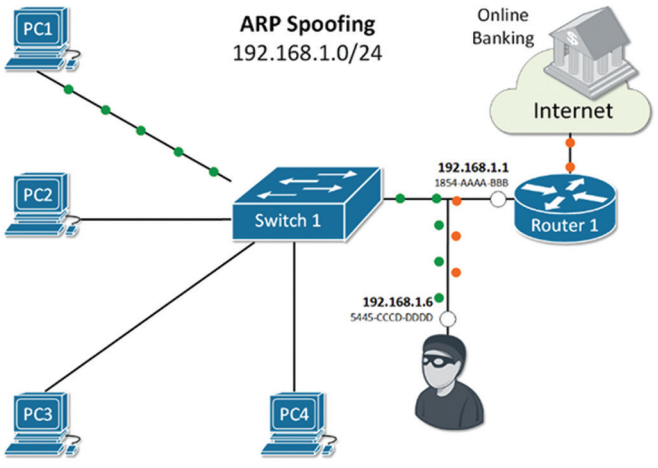

Рис. 1. Атака ARP-Spoofing

Постановка задачі. Проаналізувати методи атаки типу ARP-Spoofing. Дослідити можливості середовища Labtainers для організації лабораторного практикуму з кібербезпеки. Виконати моделювання атаки такого типу на прикладі Labtainers конейнерів для лабораторної роботи ARP-Spoofing.

Основна частина

ARP-спуфінг є різновидом атаки типу MITM, для якої використовують вади протоколу ARP. Механізм атаки засновано на можливості перехоплення зловмисником широкомовного ARP-запиту від користувача, на який він відсилає відповідь про те, що він є тим самим вузлом, котрий потрібен користувачу (зазвичай це шлюз або маршрутизатор). Після цього зловмисник буде контролювати весь трафік, який користувач адресуватиме шлюзу, і навпаки. Таке стає можливим, оскільки в протоколі ARP не передбачена можливість перевірення автентичності трафіку між вузлами мережі [4].

Наприклад, зловмисник (вузол *C*) хоче перехопити трафік вузлів *A* і *B*. Для виконання ARP-спуфінгу потрібно, щоб MAC-адреса зловмисника була прописана в ARP-таблиці вузлів *A* і *B*. Для цього вузол *C* відправляє ARP-відповіді (без отримання запитів):

- вузлу *A* з IP-адресою вузла *B* і MAC-адресою вузла *C*;
- вузлу *B* з IP-адресою вузла *A* і MAC-адресою вузла *C*.

Вузли *A* і *B* змінюють свої ARP-таблиці, записуючи в них замість MAC-адрес комп'ютерів *B* і *A* підміну у вигляді MAC-адреси комп'ютера *C*.

Внаслідок цього вузол *A* під час передавання пакету вузлу *B* знаходить в ARP-таблиці замість MAC-адреси вузла *B* MAC-адресу вузла *C* і відправляє йому пакет для вузла *B*. Відправлений на цю MAC-адресу пакет надходить до вузла *C* замість справжнього одержувача (вузла *B*). Після цього вузол *C* відправляє пакет вузлу *B*. Аналогічно відбувається і передавання зворотних пакетів від вузла *B* вузлу *A*. Увесь трафік в обидва боки перехоплює вузол *C*.

Щоб здійснити атаку в мережі, потрібно відкрити і використовувати далі інструменти таких типів:

- ARPoison — інструмент командного рядка для UNIX-систем [5];
- dsniff — для спуфингу ARP або DNS; dsniff — це набір інструментів для мережного аудиту та тестування на проникнення; dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf і webspy пасивно відстежують мережу на наявність відповідних даних (паролі, електронна пошта, файли тощо) [6];
- Ettercap — за замовчуванням є серед вбудованих інструментів в ОС Kali Linux та інших дистрибутивах аналогічного напряму [7];
- Arpspoof — це попередньо встановлена утиліта Kali Linux, яка дає змогу вилучати трафік до вибраної вами машини з комутованої локальної мережі [8].

Labtainers призначено для розгортання налаштованих контейнерів Docker і має низку переваг у процесі застосування. Для дослідження використання ARP-спуфінгу як засобу перехоплення трафіку локальної мережі в середовищі Labtainers використовуватимемо топологію контейнерів для лабораторної роботи ARP-спуфінгу. Спочатку відкриємо список доступних лабораторних робіт і виберемо потрібну роботу зі списку. Відкриються кілька вікон терміналів запущених контейнерів, із якими працюватимемо далі.

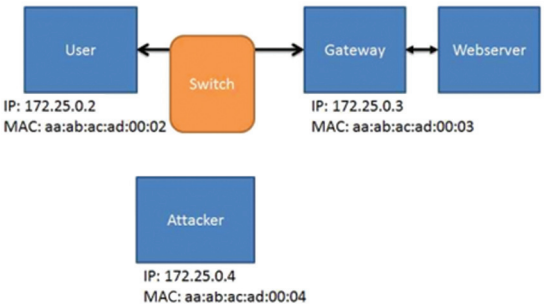

Рис. 2. Шлях трафіку в мережі без зловмисника

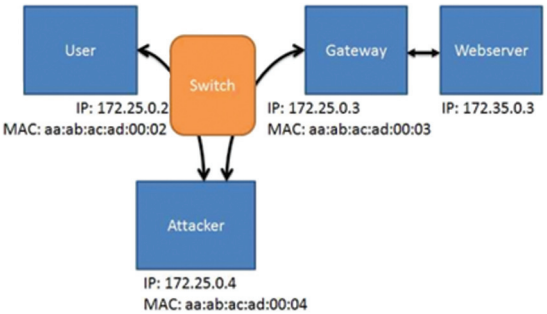

Рис. 3. Шлях трафіку після ініціалізації форвардингу пакетів

Насамперед виконаємо конфігурування мережі. Для дослідження застосування ARP-спуфінгу скористаємося чотирма об'єднаними в мережу віртуальними комп'ютерами (контейнерами середовища Labtainers), як показано на рис. 1, котрий ілюструє запланований потік трафіку між комп'ютером користувача та вебсервером через Gateway.Labtainers (рис. 2).

На комп'ютері зловмисника встановлено інструменти для атаки arpspoof та інструмент для моніторингу трафіку Wireshark. Комп'ютер зловмисника має бути налаштовано для пересилання через себе отриманих IP-пакетів, призначених іншим вузлам (рис. 3).

Ми можемо налаштувати це пересилання, виконавши команду на вузлі зловмисника для форвардингу пакетів від користувача до сервера і навпаки (рис. 4). Це потрібно для того, щоб під час виконання

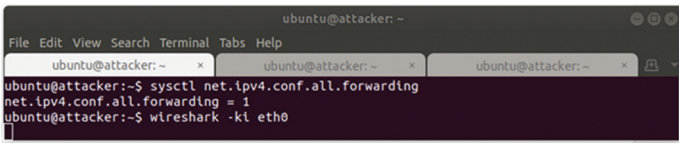

Рис. 4. Запуск форвардингу пакетів на мережній карті зловмисника

атаки користувач не втратив зв'язок із сервером, а отже, машина зловмисника пересилатиме весь трафік через себе:

sysctl net.ipv4.conf.all.forwarding

Потім на мережному інтерфейсі eth0 машини зловмисника для перевірки процесу спостереження за трафіком у мережі (рис. 5) запускаємо Wireshark командою

-wireshark -ki eth0

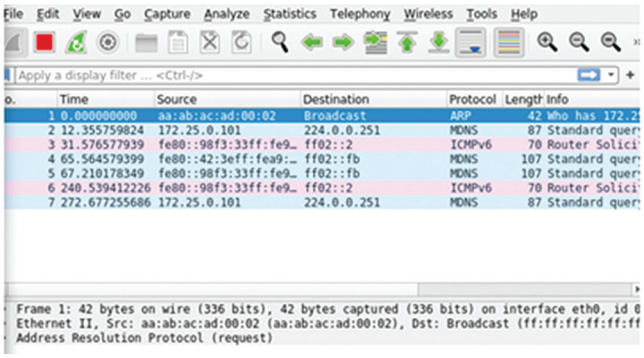

Рис. 5. Вікно мережного сканера Wireshark

У вікні Wireshark на машині зловмисника реєструємо трафік у нашій мережі з конетейнерами (див. рис. 5).

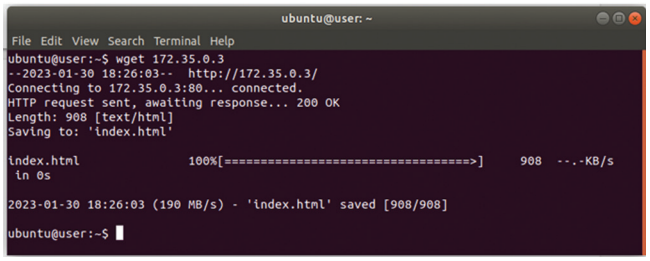

Рис. 6. Запит користувача на скачування файлу

Для перевірки роботи налаштованої системи на машині користувача запускаємо запит до сервера на скачування файлу (рис. 6), бачимо, що процес скачування успішно завершився.

Використовуємо інструмент arpspoof на комп'ютері зловмисника, щоб виконати підробку ARP. Для цього потрібно інфікувати обидва комп'ютери — користувача та шлюзу. Отже, запускаємо програму arpspoof у двох різних віртуальних терміналах у зловмисника (три термінали на машині зловмисника).

Щоб відстежувати пакети від користувача до маршрутизатора, на другому терміналі зловмисника (рис. 7) виконуємо команду формату

sudo arpspoof -t <User IP> <gateway IP> :

sudo arpspoof -t 172.25.0.2 172.25.0.3

Щоб відстежувати пакети від маршрутизатора до користувача, на третьому терміналі зловмисника (рис. 8) виконуємо команду формату

sudo arpspoof -t <gateway IP> <User IP>

sudo arpspoof -t 172.25.0.3 172.25.0.2

Після закінчення цих налаштувань ми вже можемо спостерігати підроблений ARP-трафік у Wireshark, якщо ініціювати процес взаємодії між користувачем і сервером.

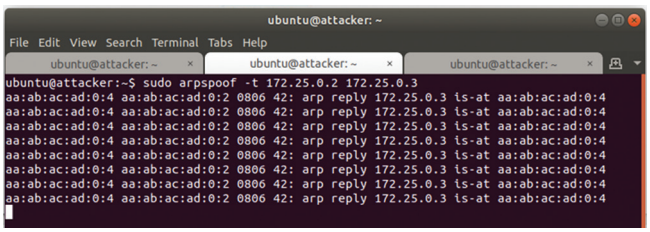

Рис. 7. Запуск arpspoof на другій вкладці

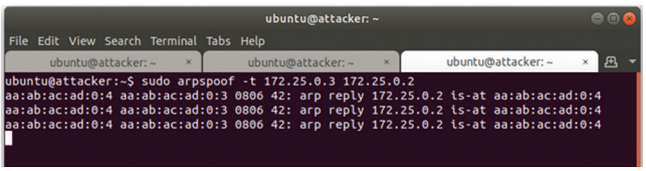

Рис. 8. Запуск arpspoof на третій вкладці

Рис. 9. Запит від користувача до сервера

Проте для захоплення трафіку нам потрібно повернутись до комп'ютера користувача та повторно завантажитити вебсторінку за допомогою команди wget (рис. 9).

У вікні Wireshark ми побачимо трафік TCP. Далі, за потреби, у Wireshark ми можемо зупинити захоплення (червона кнопка) і скористатися меню «Файл/Зберегти», щоб зберегти трафік у файлі під назвою sniff.pcapng у нашому домашньому каталозі (/home/ubuntu).

Потім виконуємо запуск захоплення трафіку у Wireshark, відкриваємо термінал користувача і здійснюємо запит сторінки на сервері (див. рис. 9) командою формату

wget <address of Webserver>

wget 172.35.0.3

Спостерігаємо інфікований TCP-трафік у вікні Wireshark (рис. 10).

Зупиняємо захоплення трафіку у Wireshark і зберігаємо захоплений трафік для подальшого аналізу у файлі sniff.pcapng у потрібній нам папці.

Зупиняємо коректно роботу симулятора командою

stoplab arp-spoof

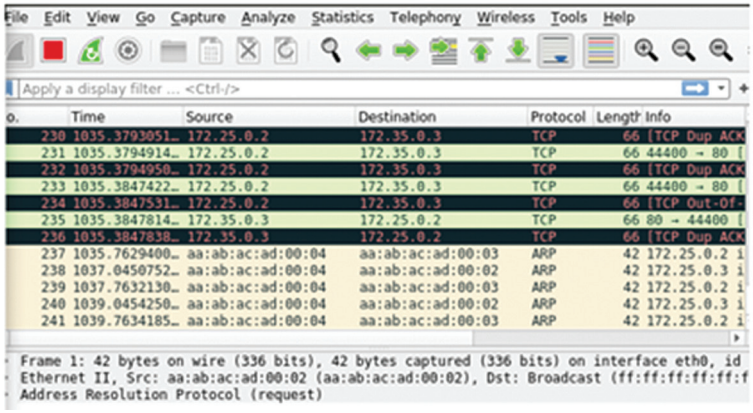

Рис. 10. Інфікований трафік між машиною користувача і сервером

Відкриваємо збережений файл sniff.pcapng для подальшого аналізу.

Висновки

У статті було здійснено аналіз протоколу ARP та механізм виконання атаки типу ARP-Spoofing. Розглянуто виконання лабораторної роботи засобами середовища Labtainers. Для дослідження було взято лабораторну роботу з моделювання атаки типу ARP-спуфінг і аналізом мережного трафіку засобами мережного сніфера Wireshark. За результатами дослідження можна дійти висновків, що здобуті результати наочно демонструють механізм атаки типу ARP-спуфінг, а використання програмного забезпечення Labtainers дало змогу істотно скоротити час на підготовку до проведення лабораторної роботи завдяки готовим до розгортання контейнерам із налаштованими мережними адресами і топологією мережі.

Список використаної літератури

1. ***Jones A.*** *A cloud-based virtual computing laboratory for teaching computer networks. Academia.edu - Share research [Electronic resource]. URL:*
https://www.academia.edu/71430268/A_cloud_based_virtual_computing_laboratory_for_teaching_computer_networks

2. ***ARP Security.*** *NetworkAcademy.io [Electronic resource]. URL:*
https://www.networkacademy.io/ccna/ethernet/arp-security

3. ***Setting Up*** *VirtualBox / Virtual Lab for Penetration Testing in Kali Linux / Backtrack | AmIRootYet. AmIRootYet [Electronic resource]. URL:*
https://www.amirootyet.com/post/setting-up-virtualbox-virtual-lab-for

4. ***RFC 826:*** *An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. IETF Datatracker [Electronic resource]. URL :*
https://datatracker.ietf.org/doc/html/rfc826

5. ***Arpoison*** *- The UNIX Arp Cache Update Utility. Arpoison - The UNIX Arp Cache Update Utility [Electronic resource]. URL:*
http://arpoison.net/

6. ***dsniff.*** *monkey.org:/ [Electronic resource]. URL:*
https://www.monkey.org/~dugsong/dsniff/7

7. ***Ettercap*** *Home Page. Ettercap Home Page [Electronic resource]. URL:*
https://www.ettercap-project.org/

8. ***arpspoof(8):*** *intercept packets on switched LAN - Linux man page. Linux Documentation [Electronic resource]. URL:*
https://linux.die.net/man/8/arpspoof

9. ***Individualizing*** *Cybersecurity Lab Exercises with Labtainers [Electronic resource]. URL:*
https://nps.edu/documents/107523844/117289221/ComputingEdgeArticle.pdf/f7840547-bb94-4d06-9dce-831869a901ac?t=1528477653000

10. ***Labtainers*** *Cyber Exercises: Building and Deploying Fully Provisioned Cyber Labs that Run on a Laptop [Electronic resource]. URL:*
https://nps.edu/documents/107523844/117289221/Labtainers_workshop_guide.pdf/928bc946-df29-6640-4984-deedc723d403?t=1616428917790

O. Konovalov, L. Kharlai, L. Dakova

VIRTUAL MASHINE LABTAINERS FOR EMULATION NETWORK VULNERABILITIES

The number of cybercrimes is constantly increasing and currently poses a significant threat to our society and economy. There is also a growing number of threats to our personal data, confidentiality, children, and the elderly due to financial fraud, which is why cybersecurity specialists are in high demand across all industries.

In such circumstances, the question of the availability of cybersecurity specialists and their training methods. The number of disciplines related to cybersecurity is rapidly increasing in higher education institutions. The training of future cybersecurity specialists is a top priority for our national security, financial stability, and economic development.

The article discusses the utilization of the Labtainers virtual environment for organizing lab sessions in cybersecurity disciplines. It explores ARP protocol vulnerabilities, principles, and mechanisms behind ARP-Spoofing attacks. The analysis delves into existing tools for executing such attacks. The article provides comparative equipment characteristics for setting up lab environments using physical hardware and virtual machines. It highlights the advantages of containerization for deploying test network environments based on Docker containers.

For investigating the Labtainers environment in organizing lab sessions, a lab exercise on simulating ARP-Spoofing attacks and analyzing network traffic using the Wireshark network sniffer was chosen. Labtainers offer over 50 cybersecurity lab exercises and tools for creating custom ones. To perform these exercises on personal equipment, importing a virtual machine for VirtualBox hypervisor or installing Labtainers on a Linux OS is necessary. Subsequently, configurations for specific lab work can be set up and exercises executed according to instructions.

Labtainers is designed for deploying configured Docker containers, allowing the creation of complex network topologies even on modest computers. It automates assessment, enables student performance evaluation, and facilitates lab work execution in an isolated environment.

Students complete lab exercises entirely on their own computers, regardless of the Linux distribution and packages installed. Labtainers operates on a virtual machine with Docker or on any Linux distribution with Docker installed. Additionally, Labtainers' lab exercises are available as cloud-based virtual machines, such as on Azure.

Keywords: ARP-Spoofing; Labtainers; attack modeling; ARP-protocol; Docker; Wireshark; containers.