УДК 004.056

Д. Ю. Радзіховський

ОСОБЛИВОСТІ ПІДМІНИ ФАЙЛІВ ПІД ЧАС СПЕЦІАЛІЗОВАНОГО МОНІТОРИНГУ МЕРЕЖІ

Вінницький національний технічний університет

Анотація. *В даній роботі проведено аналіз різних видів MiTM атак. Запропоновано та розроблено модуль для підміни файлів з використанням ARP спуфінгу під час моніторингу мережі, реалізований мовою програмування Python.*

Ключові слова: *Моніторинг, трафік, MiTM атаки, ARP-spoofing, Python.*

Abstract. *This paper analyzes different types of MiTM attacks. A module for replacing files using ARP spoofing during network monitoring, implemented in the Python programming language, has been proposed and developed.*

Keywords: *Monitoring, traffic, MiTM attacks, ARP-spoofing, Python.*

Вступ

У зв'язку з безперервним розвитком мережі Інтернет все більшої актуальності набуває питання безпеки мереж. Атаки відбуваються у всіх можливих векторах, їм піддаються мережі банків, корпоративні мережі, домашні мережі, і загальнодоступні мережі з метою поширення з їх допомогою шкідливого програмного забезпечення.

Найпоширеніший метод, який застосовують зловмисники для отримання доступу у мережі – атака "людина посередині" (Man-in-the-Middle) − це форма кібератаки, при якій для перехоплення даних використовуються методи, що дозволяють впровадитись у існуюче підключення або процес зв'язку. Зловмисник може бути пасивним слухачем, який непомітно збирає інформацію, тобто здійснює пасивну розвідку або активним учасником, змінюючи зміст повідомлень, видаючи себе за людину або систему, з якими користувач може розмовляти.

Результати дослідження

Одним із самих універсальних кібер-загроз на сьогоднішній день є MiTM атака. Охарактеризуємо особливості кібератак під час спеціалізованого моніторингу мережі.А за особливістю кібер-атак під час спеціалізованого моніторингу мережі, їх існує кілька видів:

− ARP-спуфінг – ця атака зв'язує MAC-адресу зловмисника з IP-адресою жертви в локальній мережі за допомогою повідомлень ARP. Будь-які дані, відправлені жертвою в локальну мережу, замість цього перенаправляються на MAC-адресу зловмисника, що дозволяє йому перехоплювати дані та маніпулювати ними за своїм бажанням;

− Шахрайська точка доступу – це точка бездротового доступу, встановлена в законній мережі. Це дозволяє кіберзлочинцям перехоплювати або відстежувати вхідний трафік, часто перенаправляючи його в іншу мережу, щоб спонукати до завантаження шкідливого програмного забезпечення або займатися шахрайськими схемами чи вимаганням;

− DNS-спуфінг: зловмисник заходить на сайт DNS-сервера і змінює запис веб-адреси, після чого змінюється DNS-запис та перенаправляє трафік на сайт зловмисника; [1].

Наприклад, характеристика особливостей ARP-спуфінгу:

ARP-spoofing − це тип кібератаки, що використовує слабкі місця широко поширеного протоколу дозволу адреси (Address Resolution Protocol, ARP) для порушення або перенаправлення мережевого трафіку або стеження за ним [2].

Атака полягає у використанні слабких сторін ARP для порушення призначень MAC-IP для інших пристроїв у мережі. Коли даний протокол був представлений, забезпечення безпеки не було першочерговим завданням, тому розробники протоколу ніколи не використовували механізми автентифікації для перевірки повідомлень ARP. Будь-який пристрій у мережі може відповісти на запит ARP, незалежно від того, чи є адресатом цього запиту. Наприклад, якщо комп'ютер А запитує MAC-адресу комп'ютера В, зловмисник може відповісти на комп'ютері С, і комп'ютер А прийме цю відповідь як достовірну. За рахунок цієї вразливості було проведено величезну кількість атак. Використовуючи

доступні інструменти, зловмисник може «отруїти» кеш ARP інших хостів у локальній мережі, заповнивши його неправильними даними.

Основний наслідок атаки ARP полягає в тому, що трафік, призначений для одного або декількох хостів у локальній мережі, натомість спрямовується на пристрій, обраний зловмисником. Конкретні наслідки атаки залежать від її специфіки. Трафік може прямувати на машину зловмисника або неіснуюче місце. У першому випадку помітного ефекту може і не бути, тоді як у другому – може бути заблокований доступ до мережі.

Саме атака ARP є ключовим кроком для роботи алгоритму підміни файлів, що описаний на рисунку 1.

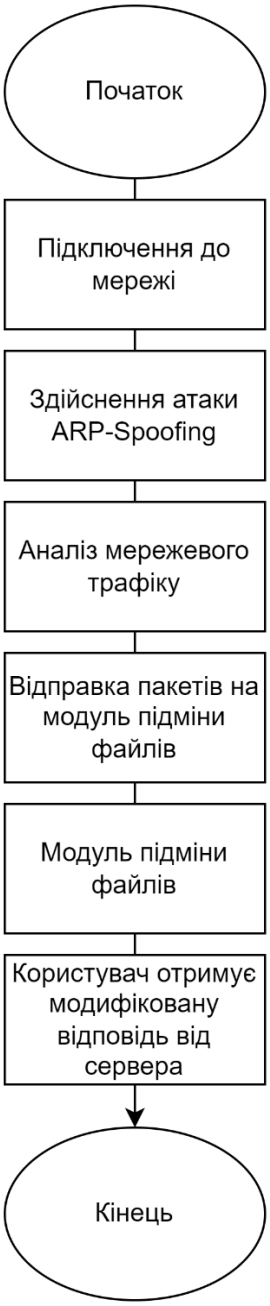

Рисунок 1 – Схема роботи алгоритму для підміни файлів

Іншими словами, для успішного перехоплення і підміни файлів під час спеціалізованого моніторингу мережі необхідно мати такі програмні засоби: ettercap для здійснення атаки ARP spoofing, модуль для моніторингу мережі та аналізу пакетів на відповідні критерії, модуль підміни файлів.

На рисунку 2 наведено готову схему алгоритма для підміни файлів.

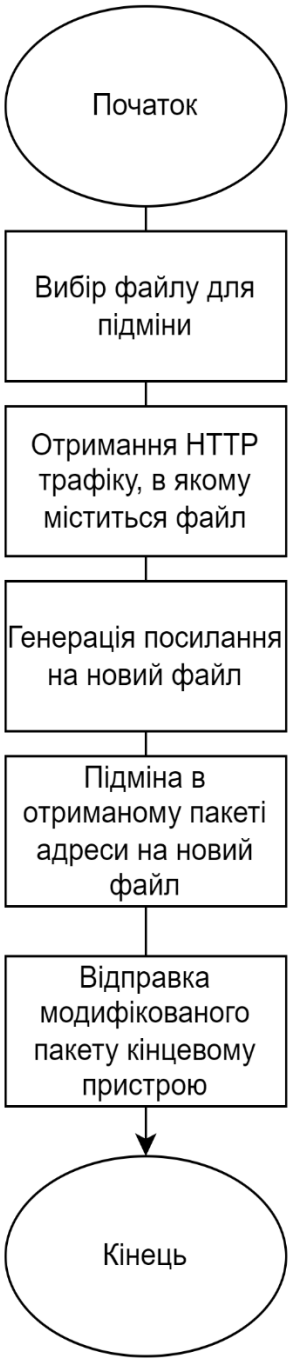

Рисунок 2 – Схема роботи модуля підміни файлів

Схема демонструє процес підміни файлів на основі отриманого HTTP трафіку .

Для початку роботи алгоритму, потрібно вибрати файл необхідного розширення, що буде використовуватись для підміни справжнього істинного файлу. Також на вхід подаються пакети HTTP трафіку, що перевіряються на наявність файла відповідного розширення. У випадку знаходження необхідного пакету, відбувається генерація нового посилання на файл, вибраний на початку роботи програми. Після цього у перехопленому пакеті відбувається підміна посилання на завантаження файлу і в результаті кінцевий користувач отримує змінений файл, на відмінну від того, що йому було потрібно.

Висновки

В результаті виконання роботи проаналізовані деякі існуючі типи MiTM атак. Детально розглянуто один з видів атаки, а саме ARP-spoofing. Саме атака ARP є ключовим кроком для роботи алгоритму підміни файлів. Сам метод підміни файлів під час спеціалізованого моніторингу мережу є комплексним підходом, для роботи якого необхідні відповідні модулі. Один з таких модулів, а саме модуль підміни файлів, був розроблений, використовуючи мову програмування Python. Реалізація даного методу обов'язково потребує наявність всіх інших модулів у комлексі. Основним недоліком даної системи, є те що потрібно перебувати в одній мережі з користувачем, якому потрібно змінити трафік.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is MITM (Man in the Middle) Attack | Imperva. [Електронний ресурс]. – Режим доступу : URL : https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/– Назва з екрану.
2. What is ARP Spoofing | ARP Cache Poisoning Attack Explained. [Електронний ресурс]. – Режим доступу : URL : https://www.imperva.com/learn/application-security/arp-spoofing/ – Назва з екрану.
3. How to Build an ARP Spoofer in Python using Scapy. [Електронний ресурс]. – Режим доступу : URL : https://www.thepythoncode.com/article/building-arp-spoofer-using-scapy – Назва з екрану.

Радзіховський Дмитро Юрійович — студент групи 2БС-18Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: Dimaradvin@gmail.com.

Radzikhovskiy Dmytro Y. — Department of Information Techologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email : Dimaradvin@gmail.com.

Шелепало Галина Василівна — к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Shelepalo Halyna V. — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine..