DOI https://doi.org/10.15589/znp2020.1(479).9
УДК 004.056.53

THE "MAN-IN-THE-MIDDLE" ATTACKS ANALYSIS, METHODS OF THEIR DETECTION AND HOW TO PREVENT THEM

АНАЛІЗ АТАК «ЛЮДИНА ПОСЕРЕДИНІ», МЕТОДИ ЇХ ВИЯВЛЕННЯ ТА ЯК ЇХ ПОПЕРЕДИТИ

Yelyzaveta M. Bailiuk
liza.bailiuk@gmail.com
ORCID: 0000-0002-4961-7816
Viktoriia V. Bolotina
viktoriia.polish@gmail.com
ORCID: 0000-0002-5122-8879
Oleksandra A. Pokotylo
a.a.polish4uk@gmail.com
ORCID: 0000-0002-1587-235X

Є. М. Байлюк,
асистент каф. КІ та КБ
В. В. Болотіна,
асистент каф. КІ та КБ
О. А. Покотило,
асистент каф. КІ та КБ

Zhytomyr Polytechnic State University, Zhytomyr
Державний університет «Житомирська політехніка», м. Житомир

Abstract. Purpose. The work raises such an important issue as the rise of cybercrime in today's world. Attackers who commit MITM attacks can access sensitive information, such as logins, passwords, and credit card information. The implementation of such an attack causes great damage to companies and their customers, as evidenced by the large number of successfully conducted attacks. Therefore, the purpose of this study is to analyze all types of "Man in the Middle" attacks, their detection methods and how to prevent them.
Method. For this research it was decided to choose an analysis method and a descriptive method. In order to determine the methods of detection and methods of preventing certain attacks, it is necessary to first analyze the mechanisms of implementation of these attacks and examples of their successful implementation. The analysis and description of the work outlines the methods of detection and methods of preventing attacks "Man in the Middle". The subject of the study is MITM attacks. The subject of the study is the methods of detecting the attacks "Man in the Middle" and determining ways to counter them.
Results. As a result of the conducted researches in this work the unique characteristics of each type of MITM-attacks were singled out and how they can be implemented by the attackers. Methods for identifying attacks of this kind are described and systematized, and an example of a tool to analyze traffic behavior, intercept passive network listening, and analyze web resource and software certificates. It also describes methods for preventing Mid-Man attacks and provides an example of an organization that provides products and services to identify suspicious behavior on the web and prevent this type of attack, and more.
Scientific novelty. The scientific novelty of this research is specifically given examples of tools for detecting MITM attacks and how to prevent this type of attack.
Practical importance. This research enables network security administrators to choose the best method for detecting mid-person attacks and to implement the means of preventing attacks of this kind that are necessary to achieve the required level of security for their organization's computer network. Also, the information in this article can be used to develop more sophisticated software or hardware to improve network security. In addition, the materials of this study are useful for ordinary users. They will take a closer look at the source of the software they are about to install on their computer or gadget, since there are a large number of malware that cybercriminals can access sensitive user data.
Key words: cyberattack; passive and active MITM-attacks; traffic monitoring; verification of certificates; methods of decoding information; preventing MITM attacks.

Анотація. Мета. Робота порушує таке важливе питання, як зростання кіберзлочинності в сучасному світі. Зловмисники, які здійснюють кібератаки типу «Людина посередині» (MITM-атаки), можуть отримати доступ до конфіденційної інформації, такої як логіни, паролі та дані кредитних карток. Реалізація такої атаки завдає великих збитків компаніям та їх клієнтам, про що свідчить велика кількість вдало проведених атак. Отже, метою дослідження є аналіз усіх видів атаки «Людина посередині», методів їх виявлення та способів їх попередження.

Методика. Для проведення дослідження було вирішено вибрати метод аналізу та описовий метод. Для того щоби визначити методи виявлення та способи попередження тих чи інших атак, необхідно спочатку проаналізувати механізми реалізації цих атак та приклади їх вдалої реалізації. За допомогою аналізу та опису в роботі наведено методи виявлення та способи попередження атак «Людина посередині». Об'єктом дослідження є MITM-атаки. Предметом дослідження є методи виявлення атак «Людина посередині» та визначення способів протидії їм.
Результати. В результаті проведених досліджень у роботі виокремлено однозначні характеристики кожного виду MITM-атак та те, яким чином вони можуть бути реалізовані зловмисниками. Описано та систематизовано методи виявлення атак цього виду, наведено приклад інструменту, за допомогою якого можна аналізувати поведінку трафіку, перехопити пасивне прослуховування мережі та проаналізувати сертифікати веб-ресурсів і програмного забезпечення. Описано методи попередження атак «Людина посередині» та наведено приклад організації, що надає продукти та послуги для виявлення підозрілої поведінки трафіку в мережі та запобігання атакам цього виду й не тільки.
Наукова новизна. Наукова новизна дослідження полягає в конкретно наведених прикладах інструментів для виявлення MITM-атак та способів попередження атак цього виду.
Практична значимість. Дослідження дає можливість адміністраторам безпеки мережі вибрати для них найкращий метод для виявлення атак «Людина посередині» та реалізувати ті способи запобігання атакам цього виду, які необхідні для досягнення необхідного рівня безпеки комп'ютерної мережі їхньої організації . Також інформація, наведена у статті, може бути використана для розроблення більш досконалого програмного чи програмно-апаратного забезпечення підвищення рівня безпеки мережі. Крім того, матеріали дослідження корисні для звичайних користувачів. Вони будуть уважніше перевіряти джерело програмного забезпечення, яке вони збираються встановити на свій комп'ютер чи гаджет, оскільки існує велика кількість шкідливих програм, за допомогою яких кіберзлочинці можуть отримати доступ до конфіденційних даних користувачів.
Ключові слова: кібератака; пасивні та активні MITM-атаки; моніторинг трафіку; перевірка сертифікатів; методи розшифрування інформації; попередження MITM-атак.

ПОСТАНОВКА ЗАДАЧІ

Широке використання комп'ютерних мереж у сучасному світі приманює все більше зловмисників до використання вразливості більшості мережних протоколів для досягнення зловмисних цілей, таких як отримання конфіденційної інформації. Під час атаки «Людина посередині» весь трафік, який йде від користувача до сервера (або додатку), проходить через зловмисника. Це дає можливість йому досягти багатьох шкідливих цілей, таких як відмова в обслуговуванні та пасивний моніторинг трафіку. В останньому випадку дуже малоймовірно, що сторони, між якими відбувається передача трафіку, зможуть виявити пасивний моніторинг, оскільки обмін інформацією між ними (з їх точки зору) відбувається без змін. Виявити такі атаки досить складно, тому постає необхідність потурбуватись про їх попередження з використанням відповідного програмного забезпечення та різних методів захисту комп'ютерних мереж.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Під час проведення досліджень з цієї теми було проаналізовано низку публікацій, що стосуються атак «Людина посередині». В роботі таких дослідників, як В. Валліваара, М. Сайліо та К. Халунен [1], було запропоновано метод виявлення MITM-атак з використанням часових позначок заголовків пакетів TCP. Вони показали, що можна знайти та встановити пороговий параметр, який точно визначає атаки «Людина посередині» з низькою ймовірністю помилкових позитивних результатів. Цей метод обмежений немобільними системами, де варіації затримки досить низькі та рівномірні.

В роботі Д. Ал-Абрі [2] зазначено, що більшість задокументованих схем виявлення атак покладається на моніторинг трафіку для виявлення шкідливих пакетів, які можуть бути використані для переадресації трафіку таким чином, що передбачає атаку MITM. В дослідженні представлено схему виявлення, яка зосереджена на виявленні MITM незалежно від схеми, яка використовується для переадресації трафіку. Нова схема, представлена автором роботи, покладається на пошук відповідності між корисними навантаженнями різних кадрів, що передаються в мережі.

Стаття таких авторів, як А. Маллік, А. Ахсан та Дж.-Ч. Цу [3], фактично включає погляд на розуміння терміна «атака «Людина посередині»». Робота була написана для накопичення пов'язаних даних та інформації в одній статті для того, щоби вона могла бути використана для подальшого дослідження цього питання на рівні коледжу/бакалаврату. Автори в цій роботі посилаються на найбільш цитовані дослідження та статті про MITM-атаки в Google-академії. Метою статті є ознайомлення читачів з кібератаками виду «Людина посередині».

ВІДОКРЕМЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Під час аналізу публікацій, присвячених вибраній темі, виявлено, що в них немає чітких рекомендацій щодо захисту комп'ютерних мереж від атак типу «Людина посередині». Крім того, розглянуті в цих

дослідженнях методи виявлення атак цього виду є неоднозначними та обмеженими. У статті, окрім аналізу можливих видів MITM-атак, наведено приклад програмного забезпечення для їх виявлення. Також описано методи попередження атак «Людина посередині» та наведено приклад компанії, яка надає програмні продукти та послуги від кібератак та перебоїв у комп'ютерних мережах.

МЕТА ДОСЛІДЖЕННЯ

Метою дослідження є аналіз усіх можливих видів MITM-атак, способів їх реалізації та визначення методів та інструментів їх виявлення, методів попередження цим атакам у майбутньому на основі проведеного аналізу.

МЕТОДИ, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Для досягнення поставленої мети вибрано такі наукові методи досліджень, як аналіз та описовий метод. За допомогою аналізу визначено всі можливі варіанти атак «Людина посередині» та методи їх реалізації. Крім того, проаналізовано та описано методи виявлення атак цього типу, інструменти, за допомогою яких адміністратори мережевої безпеки можуть виявити аномальну поведінку трафіку мережі та перевірити достовірність сертифікати веб-ресурсів. Також проаналізовано методи попередження MITM-атак та наявні сьогодні аутсорсингові компанії, що надають послуги та інструменти для підвищення мережевої безпеки. Об'єктом дослідження є атаки «Людина посередині». Предметом дослідження є методи виявлення MITM-атак та визначення способів їх попередження.

ОСНОВНИЙ МАТЕРІАЛ

Атака «Людина посередині» (атака посередника, англ. "Man-in-the-middle attack", MITM) – це різновид кібератак, за яких злочинець отримує доступ до обміну інформацією між двома сторонами (користувачами або користувачем і додатком) для її перехоплення або видачі себе за одну зі сторін для підміни інформації (рис. 1). При цьому для легітимних сторін створюється враження нормального обміну інформацією.

Метою цієї атаки є викрадення особистої інформації, такої як реєстраційні дані, дані рахунку та номери кредитних карток. Об'єктами MIMT-атаки є, як правило, користувачі фінансових додатків, компанії SaaS, сайти електронної комерції та інші веб-сайти, де потрібно входити в систему. Інформація, отримана під час атаки, може використовуватися для досягнення багатьох цілей, включаючи крадіжку особистих даних, несанкціоновані перекази коштів або незаконну зміну пароля [4].

Існує багато видів атак «Людина посередині», але загалом вони здійснюються такими чотирма способами:

1) через загальнодоступні мережі (користувач піддається найбільшому ризику під час підключення до будь-якої загальнодоступної мережі, йдеться про загальнодоступні підключення до Wi-Fi в аеропортах, кафе або будь-якої мережі без обмежень доступу; в цьому разі зловмиснику найпростіше здійснити MITM-атаку, тому що багато методів найкраще працюють у локальних мережах та мережах Wi-Fi);

2) на власному комп'ютері (користувач може випадково встановити зловмисне програмне забезпечення, яке відстежує та модифікує інтернет-з'єднання (наприклад, атака "man-in-the-browser"), або може постраждати від фішинг-атаки, як перехоплює з'єднання, заманюючи користувача на сайти зловмисників);

3) через маршрутизатор (маршрутизатори часто постачаються інтернет-провайдерами і мають налаштування безпеки за замовчуванням; це означає, що багато маршрутизаторів мають за замовчуванням облікові дані для входу (наприклад, адміністратор/пароль) або застарілу прошивку, яка могла би мати відому вразливість);

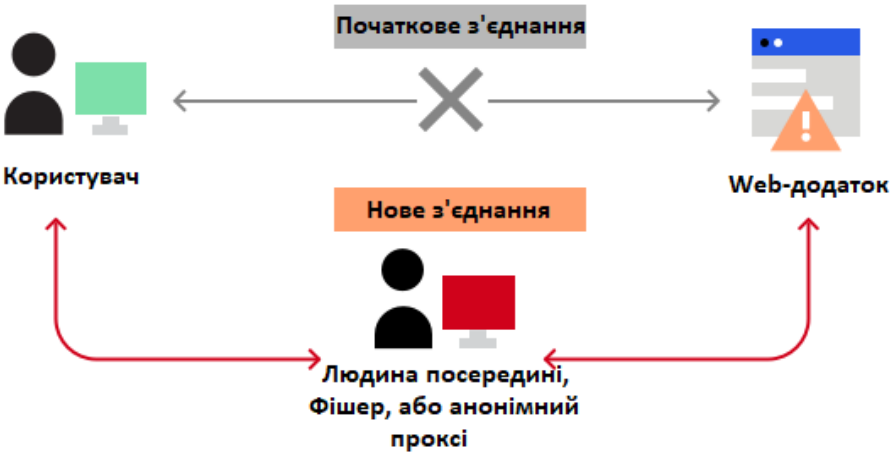

Рис. 1. Принцип атаки «Людина посередині»

4) через веб-сервер (зловмисник отримує доступ до справжнього веб-сервера, до якого мав підключитись користувач-жертва) [5].

Успішне виконання атаки «Людина посередині» поділяється два етапи, а саме перехоплення та розшифрування отриманої інформації.

Перехоплення

На першому етапі відбувається перехоплення користувальницького трафіку через мережу зловмисника до того, як він дійде до призначення. Найпоширенішим (і найпростішим) способом є пасивна атака, за якої зловмисник створює відкриті точки доступу до Wi-Fi. Зазвичай ці точки доступу створюються таким чином, щоб їх назви відповідали місцю їх розташування та здавалися безпечними. Після того як жертва підключається до такої точки доступу, зловмисник отримує повний доступ для будь-якого обміну даними в Інтернеті [6].

Крім пасивних, також є активні атаки для перехоплення інформації.

1) IP-Spoofing (підміна IP-адреси) – атака, за якої зловмисник підмінює IP-адресу в структурі IP-пакета на свою або випадкову. Сам по собі цей вид атаки не належить до MITM-атаки, але може бути її частиною на етапі прослуховування мережі зловмисником. Частіше IP-Spoofing використовується в DDoS-атаках [7].

2) ARP-spoofing (підміна ARP-повідомлень) – це різновид атаки «Людина посередині», за якої зловмисник надсилає фальсифіковані повідомлення ARP через локальну мережу. Це приводить до зв'язку MAC-адреси зловмисника з IP-адресою легітимного комп'ютера або сервера в мережі. Зловмисник використовує основний недолік протоколу ARP, а саме відсутність перевірки ARP-запитів і ARP-відповідей на достовірність. Оскільки мережеві інтерфейси на комп'ютерах підтримують мимовільний ARP (ARP-відповідь надсилається на інтерфейс пристрою без необхідності), то саме в такому разі можлива атака ARP-spoofing [8].

3) DNS-spoofing (підміна DNS-сервера) – це атака, в якій змінені записи DNS використовуються для переспрямування інтернет-трафіку на шахрайський веб-сайт, який нагадує користувачу справжній сайт. Потрапивши туди, користувачі отримують пропозицію увійти в свій обліковий запис, що дає правопорушнику можливість викрасти їхні дані доступу та інші види конфіденційної інформації. Крім того, шкідливий веб-сайт часто використовується для встановлення «хробаків» чи інших вірусів на комп'ютер користувача, надаючи злочинцю тривалий доступ до нього та до даних, які він зберігає [9].

Розшифрування

Останнім етапом атак «Людина посередині» є розшифрування отриманої зловмисником інформації на основі зібраних на етапі прослуховування даних без попередження користувача чи програми. Для досягнення цієї мети існує декілька методів, які також є атаками.

1) HTTPS-spoofing. За допомогою цього методу зловмисник відправляє підроблений сертифікат у браузер жертви, тільки-но відбувається перший запит на підключення до безпечного сайту. Він містить цифровий відбиток, пов'язаний зі скомпрометованим додатком, який браузер перевіряє відповідно до наявного списку довірених сайтів. Потім зловмисник може отримати доступ до будь-яких даних, введених жертвою, перш ніж вони будуть передані легітимному серверу.

2) SSL BEAST (використання браузера щодо SSL/TLS). Цей метод націлений на вразливість TLS версії 1.0 у SSL. Тут комп'ютер жертви заражений шкідливим скриптом, який написаний мовою JavaScript. Цей скрипт перехоплює зашифровані cookie, відправлені веб-додатком. Потім ланцюжок блоків шифрування додатків (CBC) наражається на ризик для розшифровки файлів cookie і токенів аутентифікації.

3) Перехоплення SSL. SSL-з'єднання перехоплюється тоді, коли зловмисник передає підроблені ключі аутентифікації як користувачу, так і з додатку під час початку сеансу TCP (так званого TCP-рукостискання). З точки зору користувача й сервера таке з'єднання здається безпечним, але водночас зловмисник може контролювати весь сеанс.

4) Зачистка SSL. Цей метод понижує HTTPS-з'єднання до HTTP (незашифроване з'єднання), перехоплюючи аутентифікацію TLS, що відправляється з додатку чи сервера користувачу. Тим часом весь сеанс користувача видно зловмиснику в незашифрованому вигляді [6].

Для того щоби виявити атаку «Людина посередині», системний адміністратор та адміністратор безпеки має проводити аналіз мережевого трафіку в реальному часі. Наприклад, для виявлення атаки по SSL необхідно звернути увагу на такі параметри, як IP-адреса сервера, DNS-сервер та X.509-сертифікат сервера. Однією з найвідоміших атак такого типу стала атака на "Comodo", де були створені фальшиві сертифікати для таких популярних доменів, як google.com, yahoo.com, live.com та skype.com. "Comodo" – це центр сертифікації (CA), якому «довіряє» браузер, а це означає, що ці помилкові сертифікати були прийняті більшістю браузерів. Однак напад вдало виявлено, а помилкові сертифікати вже відкликані.

Існує декілька способів виявлення атак MITM, навіть коли на перший погляд здається, що сертифікат підписаний надійним центром сертифікації. Наприклад, плагіни "Firefox" доступні у "Certificate Patrol", а також існують оновлення, які можуть допомогти користувачам, попереджаючи про «нові» сертифікати, які не були відомі раніше. Для перевірки сер-

тифікатів можна використовувати "NetworkMiner", тобто інструмент аналітичного аналізу з відкритим кодом (NFAT) для "Windows" (але також він працює в "Linux", "Mac OS X", "FreeBSD") (рис. 2). Pro-версія цієї програми є платною.

"NetworkMiner" може використовуватися як інструмент перехоплення пасивного прослуховування мережі для виявлення назв операційних систем, сесій, імен хостів, відкритих портів тощо, не створюючи додаткового трафіку для мережі. За допомогою "NetworkMiner" також можна проаналізувати файли PCAP для офлайн-аналізу та відновити/зібрати передані файли та сертифікати з файлів PCAP. "NetworkMiner" дає змогу виконувати розширений аналіз мережевого трафіку (NTA). Спосіб подання даних не тільки робить аналіз більш простим, але й економить цінний час для адміністратора мережевої безпеки. "NetworkMiner" автоматично витягує сертифікати X.509 з SSL-потоків у файли з розширенням ".cer". Ці файли ".cer" можна відкрити в переглядачі сертифікатів для подальшого аналізу. Перше, що потрібно перевірити за можливої атаки MITM, – це правильність імені IP та DNS-сервера. Наступним кроком є ознайомлення із сертифікатом сервера, наприклад, шляхом відкриття необхідного файлу з розширенням ".cer". Сертифікатам, що підписуються самостійно, анульованим сертифікатам та сертифікатам, які підписуються не довіреними центрами сертифікації, не потрібно довіряти. Виявлення таких сертифікатів може свідчити про те, що сталася атака SSL MITM [10].

Виявлення атак типу «Людина посередині» є складним процесом, тому атакам такого виду простіше й надійніше запобігти. Найкращими способами попередження MITM-атак є такі.

1) Використання віртуальної приватної мережі (VPN). VPN шифрує веб-трафік, обмежуючи здатність зловмисника викрасти або змінити інформацію, що передається в мережі.

2) Використання систем виявлення вторгнень в мережу (NIDS). NIDS розміщується у стратегічних точках всередині мережі для контролю трафіку усіх пристроїв мережі. Ця система виконує аналіз трафіку та зіставляє його з бібліотекою відомих атак.

3) Правильне налаштування брандмауера. Правильно налаштований брандмауер може запобігти несанкціонованому доступу.

4) Встановлення антивірусної програми. Антивірусні програми включають сканер, який працює під час завантаження системи, щоби запобігти атакам, які виконуються через встановлення зловмисного програмного забезпечення.

5) Використання двофакторної аутентифікації. Це гарний спосіб запобігти викраденню електронної пошти, який вимагає додаткового вектору аутентифікації поза паролем.

6) Вихід з облікових записів. Для того щоб уникнути викрадення сеансу, необхідно виходити з усіх невикористаних облікових записів, щоб визнати недійсними файли cookie.

7) Усвідомлене встановлення програмного забезпечення. Перед тим як встановлювати додатки

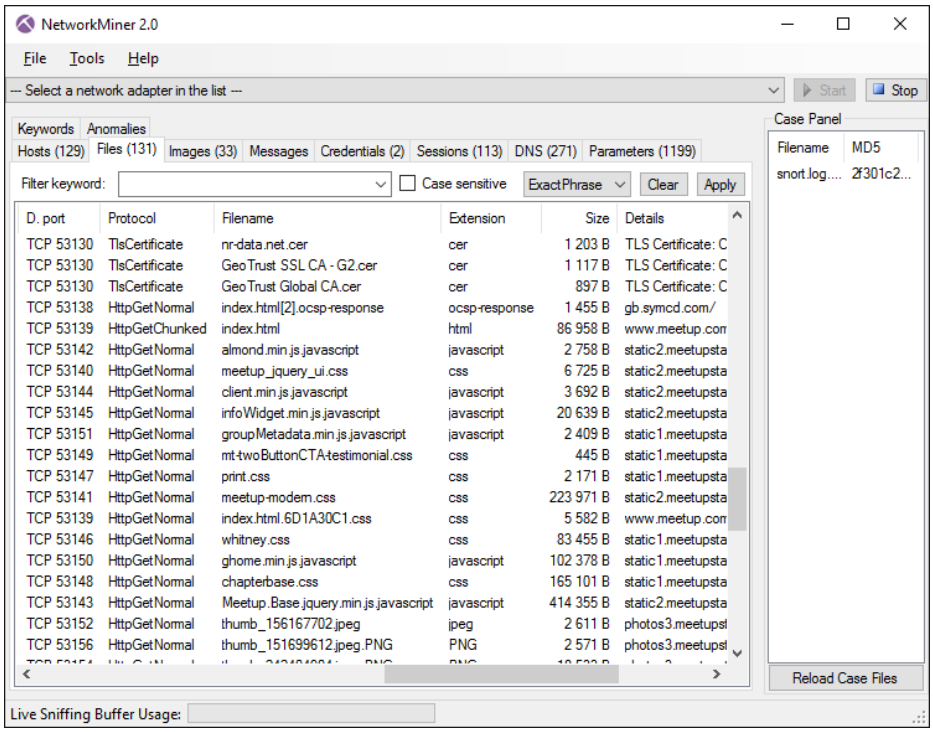

Рис. 2. Вікно програми "NetworkMiner"

та програмне забезпечення для персонального комп'ютера та браузера, необхідно переконатися, що вони завантажені з перевіреного джерела.

8) Використання примусового шифрування. Необхідно уникати обміну будь-якою конфіденційною інформацією на сайтах без HTTPS.

9) Встановлення HTTPS. Це розширення безпеки "Chrome", яке встановлює SSL-з'єднання, де це можливо.

10) Використання протоколу DNS-over-HTTPS. Це протокол для виконання віддаленого дозволу системи доменних імен (DNS) через протокол HTTPS. Метою цього протоколу є підвищення конфіденційності та безпеки користувачів із запобіганням маніпулюванню даними DNS за допомогою атак «Людини посередині» та використанням протоколу HTTPS для шифрування даних між клієнтом та сервером.

11) Використання менеджера паролів. Він має уникати автоматичного заповнення паролів на зловмисних сайтах.

12) Уникання загальнодоступних мереж Wi-Fi. Якщо виникає потреба використовувати загальнодоступний Wi-Fi, свій пристрій необхідно налаштувати так, щоб з'єднання відбувалося вручну.

13) Встановлення патчів (оновлень) програмного та апаратного забезпечення. Необхідно оновлювати свої інструменти для того, щоб уникнути атаки «Людина посередині», яка використовує відомі вразливості.

14) Використання захищених DNS-серверів. Перед тим як використовувати DNS-сервер, необхідно переконатися в тому, що він є захищеним.

15) Захист програм та додатків. Необхідно регулярно тестувати власні веб-сайти або програмне забезпечення на наявність вразливих місць для усунення проблем і підвищення рівня безпеки [5; 11].

Крім того, нині існує низка компаній, які займаються проблемами кібербезпеки, зокрема розробленням програмних продуктів для виявлення атак. Однією з найвідоміших є "UpGuard Inc.", що є австралійською компанією, яка займається кібербезпекою, заснована Аланом Шарп-Полом, Лео Венегасом та Майком Баукесом. "UpGuard" надає продукти та послуги від атак та перебоїв мережі.

Платформа "Cyber Resilience UpGuard" визначає фактори ризику кібербезпеки компанії шляхом сканування як внутрішніх, так і зовнішніх комп'ютерних систем. Платформа автоматично сканує кожен сервер, додаток, мережу та мобільні пристрої в IT-середовищах, щоби створити живу модель їх конфігураційного стану, після чого постійно оцінює цю систему записів щодо вразливості безпеки, зміни конфігурації та процедурних змін. З цієї моделі платформа динамічно отримує уніфіковану оцінку ризику кібербезпеки, CSTAR, яка визначає позицію кібер-ризику IT-активів проти багатофакторних факторів. У продукті використовується інструмент контролю за стійкістю, який інтегрує перевірки на кожен етап технологічного життєвого циклу, одночасно здійснюючи оцінювання факторів ризику, таких як неправильна конфігурація, зміни конфігурації та вразливості процесу. Цей підхід є унікальним, оскільки архітектура платформ дає змогу динамічно фіксувати великі набори даних конфігурації безперервно задля розрізнення, візуалізації та звітності про можливі порушення та відключення. За допомогою програмних продуктів компанії "UpGuard" основна інформація про конфігурацію може бути перетворена на політику безпеки, процедурну перевірку або автоматизацію, щоби забезпечити збереження та перевірку бажаної цілісності IT-середовищ. "UpGuard" поставляє три продукти, які взаємодіють для формування стратегії кібер-стійкості: «Відкрийте, контролюйте та передбачте». Кожна з них має на меті вирішення іншого джерела ризику, пов'язаного з інформаційними технологіями [12].

ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Дослідження показало, що вже запропоновані методи виявлення MITM-атак мають свої обмеження, тому було вирішено описати інші можливі методи виявлення атак «Людина посередині» та навести приклад програмного забезпечення, за допомогою якого це можна зробити. Серед способів попередження MITM-атак можна виділити використання віртуальної приватної мережі (VPN); використання систем виявлення вторгнень в мережу (NIDS); правильне налаштування брандмауера; встановлення антивірусної програми; використання двофакторної аутентифікації; вихід з облікових записів; усвідомлене встановлення програмного забезпечення; використання примусового шифрування; встановлення HTTPS; використання протоколу DNS-over-HTTPS; використання менеджера паролів. Він має уникати автоматичного заповнення паролів на зловмисних сайтах; загальнодоступних мереж Wi-Fi; передбачати встановлення патчів (оновлень) програмного та апаратного забезпечення; використання захищених DNS-серверів; тестування програм та додатків.

ВИСНОВКИ

В ході дослідження проведено глибокий аналіз атак «Людина посередині». Визначені ознаки MITM-атак дають змогу чітко зрозуміти те, яким чином вони можуть бути реалізовані зловмисниками та за допомогою яких методів їх можна виявити. Простий моніторинг трафіку мережі є ефективним методом виявлення атак «Людина посередині», але малоінформативним, тому краще використовувати програмне забезпечення з розширеним набором інструментів, наприклад "NetworkMiner". Описані методи попередження атак «Людина посередині» можуть забезпечити високий рівень безпеки комп'ютерної мережі. Дослідження може бути використане для розроблення програмного забезпечення з виявлення атак на інформаційно-комунікаційні системи або для розроблення політики безпеки організації.

REFERENCES

[1] Vallivaara, V., Sailio, M., Halunen, K. (2014). Detecting Man-in-the-Middle Attacks on Non-Mobile Systems. CODASPY 2014 – Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, pp. 131–134.

[2] Al Abri, D. (2015). Detection of MITM attack in LAN environment using payload matching. IEEE International Conference on Industrial Technology (ICIT), Seville, pp. 1857–1862.

[3] Mallik, A., Ahsan, A., Shahadat, M., Tsou, Jia-Chi. (2019). Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, № 3, pp. 77–92.

[4] Ataky typu Man-In-The-Middle: shcho treba znaty kozhnomu. Retrieved from: https://www.imena.ua/blog/man-in-the-middle (access date 17.02.2020).

[5] What is a Man-in-the-Middle attack and how can it be Prevented. Retrieved from: https://www.upguard.com/blog/man-in-the-middle-attack (access date 17.02.2020).

[6] Man in the middle (MITM) attack. Retrieved from: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm (access date 17.02.2020).

[7] Chto takoe IP-spufing i kak predotvraschat spufing-ataki. Retrieved from: https://le-vpn.com/ru/spoofing-attacks-personal-data-protection (access date 19.02.2020).

[8] ARP-spoofing. Retrieved from: https://www.veracode.com/security/arp-spoofing (access date 20.02.2020).

[9] DNS Spoofing. Retrieved from: https://www.imperva.com/learn/application-security/dns-spoofing (access date 20.02.2020).

[10] Network forensic analysis of SSL MITM attacks. Retrieved from: https://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks (access date 20.02.2020).

[11] What are Man-in-the-Middle attacks & how to prevent MITM-attack with examples. Retrieved from: https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention (access date 21.02.2020).

[12] UpGuard. Retrieved from: https://www.cybersecurityintelligence.com/upguard-2241.html (access date 21.02.2020).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Vallivaara, V., Sailio, M., Halunen, K. (2014). Detecting Man-in-the-Middle Attacks on Non-Mobile Systems. *CODASPY 2014 – Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*. P. 130–133.

[2] Al Abri, D. (2015). Detection of MITM attack in LAN environment using payload matching. I*EEE International Conference on Industrial Technology (ICIT), Seville*. P. 1857–1862.

[3] Mallik, A., Ahsan, A., Shahadat, M., Tsou, Jia-Chi. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*. № 3. P. 77–92.

[4] Атаки типу Man-In-The-Middle: що треба знати кожному. URL: https://www.imena.ua/blog/man-in-the-middle (дата звернення: 17.02.2020).

[5] What is a Man-in-the-Middle attack and how can it be Prevented. URL: https://www.upguard.com/blog/man-in-the-middle-attack (дата звернення: 17.02.2020).

[6] Man in the middle (MITM) attack. URL: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm (дата звернення: 17.02.2020).

[7] Что такое IP-спуфинг и как предотвращать спуфинг-атаки. URL: https://le-vpn.com/ru/spoofing-attacks-personal-data-protection (дата звернення: 19.02.2020).

[8] ARP-spoofing. URL: https://www.veracode.com/security/arp-spoofing (дата звернення: 20.02.2020).

[9] DNS Spoofing. URL: https://www.imperva.com/learn/application-security/dns-spoofing (дата звернення: 20.02.2020).

[10] Network forensic analysis of SSL MITM attacks. URL: https://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks (дата звернення: 20.02.2020).

[11] What are Man-in-the-Middle attacks & how to prevent MITM-attack with examples. URL: https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention (дата звернення: 21.02.2020).

[12] UpGuard. URL: https://www.cybersecurityintelligence.com/upguard-2241.html (дата звернення: 21.02.2020).

Дата надходження статті до редакції: 20.03.2020
Дата затвердження статті до друку: 17.04.2020