УДК 004.056.5

ВИРТУАЛЬНАЯ СРЕДА ДЛЯ ИДЕНТИФИКАЦИИ И НЕЙТРАЛИЗАЦИИ АТАК MAN-IN-THE-MIDDLE

♦♦♦♦♦

VIRTUAL ENVIRONMENT FOR IDENTIFYING AND NEUTRALIZING MAN-IN-THE-MIDDLE ATTACKS

Крячко Никита Александрович
студент,
Уральский государственный экономический университет
tiinkee@yandex.ru

Башарина Ольга Юрьевна
кандидат технических наук,
доцент кафедры бизнес-информатики,
Уральский государственный экономический университет
basharinaolga@mail.ru

Аннотация. В статье описан подход к разработке виртуальной среды, предназначенной для обнаружения и нейтрализации кибератак Man-in-the-Middle (человек посередине). Среда разработана на платформе VM VirtualBox, технология атак типа Man-in-the-Middle реализована с помощью программного инструмента Bettercap. Виртуальная среда позволяет изучать механизмы и технологии кибератак и защиты от них на стороне «злоумышленника» и «жертвы».

Ключевые слова: информационная безопасность, кибератака, «человек посередине», Man-in-the-Middle, MITM.

Kryachko Nikita Aleksandrovich
Student,
Ural State University of Economics
tiinkee@yandex.ru

Basharina Olga Yurievna
Candidate of Technical Sciences,
Associate Professor of the Department of Business Informatics,
Ural State University of Economics
basharinaolga@mail.ru

Annotation. The article describes an approach to developing a virtual environment designed to detect and neutralize Man-in-the-Middle cyberattacks. The environment is developed on the VM VirtualBox platform, the Man-in-the-Middle attack technology is implemented using the Bettercap software tool. The virtual environment allows studying the mechanisms and technologies of cyberattacks and protection against them on the side of the «intruder» and «victim».

Keywords: information security, cyberattack, Man-in-the-Middle, MITM.

В современном мире функционирование как локальных, так и глобальных сетей является неотъемлемой частью повседневной жизни. Каждый день пользователи передают и получают значительные объемы информации через сети. С развитием технологий передачи данных одновременно увеличивается и риск возникновения кибератак.

Кибератака – это враждебные действия, нацеленные на информационную систему с целью использования ее в своих целях, выведения ее из строя, либо с целью получения несанкционированного доступа к конфиденциальной информации для ее хищения, изменения или дополнения [1].

Одним из популярных видов кибератак является атака «человек посередине» (Man-in-the-Middle, MITM) при которой злоумышленник перехватывает и возможно изменяет коммуникации между двумя сторонами, которые полагают, что общаются непосредственно друг с другом [2, 3]. Существуют различные техники осуществления атаки методы и варианты реализации MITM-атак:

ARP-Spoofing – вариант атаки с использованием подделки ARP протокола. Суть данного метода: злоумышленник посылает фальшивые ARP-ответы в локальную сеть, завладевая контролем над сетевым трафиком и делая себя «промежуточным звеном» между жертвой и целевым сервером. Это позволяет злоумышленнику перехватывать и модифицировать сетевой трафик, а также осуществлять атаки на аутентификацию, шифрование и прочие защитные меры [4].

DNS-Spoofing – метод, который основывается на изменении или подмене ответов на запросы, направленные к серверу доменных имен (DNS). Путем создания фальшивых DNS-ответов злоумышленник может перенаправлять жертву на фальшивые веб-страницы, перехватывать учетные данные и конфиденциальную информацию.

SSL-Striping – атака, направленная на снижение уровня безопасности SSL-соединений путем перенаправления пользователей на незащищенные версии сайтов.

Путем подмены HTTPS-ссылок на незащищенные HTTP-ссылки, злоумышленник может обмануть пользователя и заставить его отправлять конфиденциальные данные, такие как пароли, данные кредитных карт и другую чувствительную информацию, по открытым каналам передачи.

Session Hijacking – метод, направленный на перехват идентификаторов сессии для несанкционированного доступа к аккаунтам пользователей или другой конфиденциальной информации. Злоумышленник подменяет идентификатор сеанса между пользователем и веб-сервером, что позволяет ему захватить управление сеансом и продолжить взаимодействие с сервером от имени пользователя.

Целью данного исследования является разработка виртуальной среды для практического изучения технологий и методов обнаружения и нейтрализации MITM-атак.

Для того, чтобы научиться идентифицировать MITM-атаку, необходимо детально изучить принцип ее функционирования и методику проведения. Для реализации данной атаки требуется создать среду, максимально приближенную к реальной, в которой можно будет анализировать MITM-атаку как с позиции злоумышленника, так и с точки зрения жертвы.

Реализация MITM-атак требует несколько основных инструментов, которые в свою очередь могут использоваться комплексно для более удачной атаки. Инструменты делятся на несколько групп по факту своего применения. Чтобы реализовать атаку необходимы инструменты для перехвата трафика, для выполнения ARP-спуфинга, для записи и анализа трафика, и при желании для модификации атаки [5].

Существует специализированное ПО, которое может выполнять как одну задачу, например, перехватывать трафик, так и комплекс, имея в арсенале плагины для дополнительных действий. Приведем обзор наиболее популярных программ данного класса.

Intercepter-NG – это комплексный инструмент, предназначенный имеющий широкий спектр функций такие как пассивный и активный перехват трафика, сниффинг и анализ трафика, различные типы MITM-атак, как например ARP Poisoning и DNS Spoofing. Также данное ПО имеет удобный интерфейс для работы с перехваченными данными. Главным минусом является ограниченная совместимость с некоторыми операционными системами. Intercepter-NG хорошо работает с системами на Android и Windows. Но Windows в свою очередь требует точной настройки для эффективной работы.

Bettercap – это гибкий сетевой универсальный инструмент для провидения различных видов кибератак, включая MITM-атаки. Bettercap может перехватывать и модифицировать трафик, поддерживает ARP-спуфинг, DNS-спуфинг, sniffing и запись трафика для последующего анализа. Данный программный продукт обеспечивает поддержку на различных платформах, включая Linux, macOS и Windows; позволяет автоматизировать задачи с помощью встроенного языка сценариев; регулярно обновляется.

MITMF (Man-In-The-Middle Framework) – это многофункциональный инструмент с открытой модульной архитектурой для выполнения MITM-атак. Благодаря данной архитектуры инструмент является гибким в использовании и имеет возможность расширения функционала дополнительными модулями, но, в то же время, это может вызывать сложности в конфигурировании и настройке модулей.

На основе проведенного анализа для реализации MITM-атаки был выбран Bettercap с интерфейсом командной строки благодаря удобству использования, комплексности в работе и хорошей совместимости с Kali Linux.

Теперь необходимо выбрать платформу, на которой будет развернута виртуальная среда. Были изучены характеристики и системные требования популярных платформ *VMware Workstation, Hyper-V и Oracle VM VirtualBox*. Для решения наших целей была выбрана VM VirtualBox поскольку она предоставляет функциональные возможности, сопоставимые с возможностями конкурирующих решений, и является бесплатной.

Для изучения технологии реализации MITM-атак со стороны злоумышленника и жертвы созданы две виртуальные машины с операционными системами Kali Linux и Windows.

Практическая реализация MITM-атаки, ARP-отравление и перехват трафика были осуществлены инструментом Bettercap. В ходе эксперимента использовались различные способы идентификации MITM-атаки и методы защиты от нее.

Продемонстрируем самый простой метод для распознания атаки ARP-spoof – проверка ARP-таблиц в системе. В случае если на устройство произведена MITM-атака методом ARP-спуфинга, то в данной таблице будет видно изменение MAC-адреса маршрутизатора на MAC-адрес другого устройства, также находящегося в данной сети. Это можно легко заметить так как появляется совпадение MAC-адресов с разными значениями IP-адресов (рис. 1).

```
C:\Users\vboxuser>arp -a

Interface: 172.20.10.3 --- 0x5
  Internet Address      Physical Address      Type
  172.20.10.1           08-00-27-1e-36-4a     dynamic
  172.20.10.4           08-00-27-1e-36-4a     dynamic
  172.20.10.15          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Рисунок 1 – ARP-таблица устройства, находящегося под атакой

Другим способом выявления MITM-атаки является анализ сетевого трафика на наличие аномалий. Это можно сделать с помощью специализированного ПО для чтения трафика – Wireshark. Если в сети наблюдается значительное количество ARP-запросов, направленных к различным IP-адресам в течение короткого временного интервала, существует высокая вероятность того, что кто-то предпринимает попытку выявления активных IP-адресов посредством ARP-спуфинга.

Разработанная виртуальная среда показала свою работоспособность и эффективность. Она представляет интерес для практического изучения методов и технологий обнаружения кибератак и защиты от них.

Литература

1. Яковлев М.А. Анализ кибератак, их типы, признаки и защита / М.А. Яковлев // Инженерные кадры – будущее инновационной экономики России. – 2023. – № 1. – С. 642–647.
2. Особенности атаки «человек посередине» и пути её предотвращения / Д.А. Лысов, А.П. Горлов, В.В. Кузина, В.Д. Медведева // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Сб. материалов и докладов XV межрегион. науч.-практ. конф., Брянск, 28 апреля 2023 года. – Брянск : БГТУ, 2023. – С. 88–93.
3. Beaglesecurity: Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention. – URL : https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html (дата обращения 23.05.2024).
4. Zanero S. ARP Spoofing Defense: Flaw Detection and Prevention Techniques / S. Zanero, A. Basso // International Journal of Advanced Computer Science, 2021. – С. 120–168.
5. Kaspersky: Предотвращение кибератак. – URL : https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-prevent-cyberattacks (date of application 23.05.2024).

References

1. Yakovlev M.A. Analysis of cyber attacks, their types, signs and protection / M.A. Yakovlev // Engineering personnel – the future of the innovative economy of Russia. – 2023. – № 1. – P. 642–647.
2. Features of the «man in the middle» attack and ways to prevent it / D.A. Lysov, A.P. Gorlov, V.V. Kuzina, V.D. Medvedeva // Information security and personal data protection. Problems and ways to solve them: Collection of materials and reports of the XV interregional. scientific and practical. conf., Bryansk, April 28, 2023. – Bryansk : BSTU, 2023. – P. 88–93.
3. Beaglesecurity: Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention. – URL : https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html (дата обращения 23.05.2024).
4. Zanero S. ARP Spoofing Defense: Flaw Detection and Prevention Techniques / S. Zanero, A. Basso // International Journal of Advanced Computer Science, 2021. – С. 120–168.
5. Kaspersky: Предотвращение кибератак. – URL : https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-prevent-cyberattacks (date of application 23.05.2024).