МЕТОДИКА ИСПОЛЬЗОВАНИЯ МАТРИЦЫ MITRE ATTACK ДЛЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

Кравченко Е.Д., Буцкевич Е.М. студенты гр.261402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. технических наук, доцент

Аннотация. В статье изучается применение матрицы MITRE ATT&CK в тестировании безопасности корпоративных сетей, с фокусом на технику T1190. Рассматриваются методы компрометации веб-приложений, включая сканирование сети, перебор учетных данных и эксплуатацию уязвимостей. Описаны сценарии атак и их влияние на инфраструктуру, а также предложены меры защиты: ограничение доступа, многофакторная аутентификация и мониторинг активности. Работа предназначена для специалистов в сфере кибербезопасности и исследователей атак по модели MITRE ATT&CK..

Ключевые слова MITRE ATT&CK, T1190, Exploit Public-Facing Application, безопасность корпоративных сетей, тестирование безопасности, моделирование атак, уязвимости веб-приложений.

Структура MITRE ATT&CK охватывает весь жизненный цикл кибератак, начиная с получения нарушителем первоначального доступа к системе и заканчивая эксфильтрацией данных или разрушением инфраструктуры. Понимание этих техник позволяет специалистам по кибербезопасности выявлять потенциальные угрозы и предпринимать проактивные меры защиты.

Модель MITRE ATT&CK – это база знаний, в которой содержится информацию о тактиках, техниках и процедурах, применяемых нарушителями на различных этапах кибератаки. Тактики определяют цель, которой атакующие хотят достичь путём использования определённых техник и процедур, называемых также подтехниками. Всё это вместе обозначается аббревиатурой TTP (Tactics, Techniques and Procedures). Каждая тактика или техника имеет свой уникальный идентификатор, используемый для простоты работы с матрицей.

Цель данной работы заключается в анализе применения модели MITRE ATT&CK для тестирования безопасности корпоративных сетей, выявлении уязвимостей, возникающих в ходе эксплуатации техники T1190, и предложении эффективных методов защиты от возможных атак.

Одним из ключевых этапов тестирования безопасности является анализ наиболее распространенных способов получения нарушителями первоначального доступа к системе. Для получения доступа в инфраструктуру чаще всего используется техника Exploit Public-Facing Application (T1190) – эксплуатация уязвимостей в публично доступных приложениях. Рассмотрим, каким образом атака может быть реализована и какие меры.

В качестве эксплуатируемых приложений чаще всего выступают веб-сайты/веб-серверы, но также могут использоваться базы данных (например, SQL), стандартные службы (например, SMB или SSH), протоколы администрирования и управления сетевыми устройствами (например, SNMP и Smart Install), а также любые другие системы с открытыми сокетами, доступными через Интернет Смоделируем ситуацию, когда обнаруживается уязвимость в веб-приложении, связанная с недостаточной защитой публично доступных директорий и слабой системой аутентификации.

Перед началом кибератаки авторами была развернута среда с Kali Linux в VirtualBox для проведения тестов. В процессе проведения кибератаки, основанной на технике T1190 (Exploit Public-Facing Application), была смоделирована ситуация эксплуатации уязвимого веб-приложения с целью проникновения в корпоративную сеть.

Первоначально с помощью сканирования портов с помощью команды nmap и перебора директорий с помощью команды dirb были обнаружены потенциально уязвимые точки входа, включая /admin, /login, /dashboard, /images и /includes.

В ходе кибератаки была проведена проверка защищенности веб-приложения от Brute-force атак на учетные записи. Для этого использовался инструмент Hydra (рисунок 1), который позволил успешно подобрать пароли администратора и нескольких других учетных записей. Полученный доступ к административной панели /admin открыл возможность выполнения дальнейших кибератак, включая загрузку веб-оболочки (web shell). С ее помощью установили обратное соединение с сервером, что позволило выполнить команды в системе с правами веб-пользователя www-data.

Рисунок 1 – Использование инструмента hydra

После получения доступа к командной оболочке сервера удалось загрузить вредоносный скрипт с использованием команды curl, а затем установить соединение через обратный шелл с помощью команды nc. Действуя от имени пользователя www-data, было произведено изучение файловой системы сервера. В процессе анализа директории /var/www/html/ были обнаружены следующие значимые файлы и папки: config.php, вероятно, содержавший конфигурационные данные; директория /includes, где могли бы находиться дополнительные важные файлы; директория /backup, возможно, содержавшая резервные копии данных. Эта информация позволила продолжить дальнейший анализ системы и потенциально раскрыть дополнительные векторы атаки.

На следующем этапе, исследовав содержимое конфигурационного файла config.php, были обнаружены учётные данные для подключения к базе данных. Используя эту информацию, удалось получить доступ к серверу базы данных MySQL и выполнить авторизацию. Проведение запросов позволило извлечь конфиденциальные данные, включая зашифрованные пароли пользователей и информацию о структуре базы данных, представленных на рисунке 2. Анализ этих данных стал ключевым шагом в изучении системы, предоставив дополнительные возможности для дальнейшего проведения кибератаки.

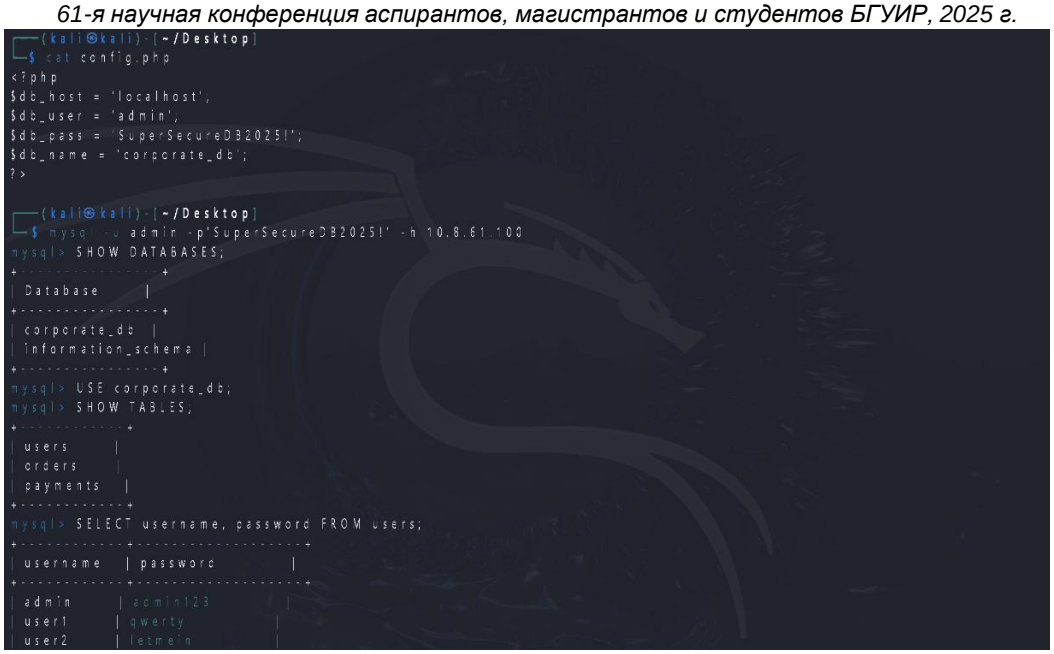

Рисунок 2 – Извлечение конфиденциальных данных

Следующим этапом стало сканирование внутренней сети для выявления дополнительных узлов. С помощью Nmap были обнаружены активные системы в той же подсети. Используя найденные ранее учетные данные, попробовали выполнить подключение к другим серверам по SSH. В результате удалось получить доступ к одному из узлов, используя ту же учетную запись администратора, что указывало на повторное использование паролей внутри корпоративной сети. Это расширило возможности кибератаки, открыв доступ к еще большему количеству системных ресурсов.

На заключительном этапе была проведена эскалация привилегий для получения полного контроля над системой, представленная на рисунке 3. Проверка конфигурации sudo выявила возможность выполнения команд с привилегиями root без запроса пароля. С помощью этого механизма смогли запустить командную оболочку от имени «суперпользователя» и получить полный контроль над сервером. Доступ на уровне root позволит изменять файлы конфигурации, манипулировать учетными записями пользователей и устанавливать постоянные точки доступа для сохранения контроля над системой.

Рисунок 3 – Эскалация привилегий

Для сокрытия следов кибератаки были удалены журналы событий, временные файлы и история выполненных команд, что затруднит последующий анализ инцидента администраторами системы. Проведенная атака продемонстрировала, как эксплуатация уязвимости веб-приложения, связанная с недостаточной защитой публично доступных ресурсов, может привести к компрометации не только

отдельного сервера, но и всей корпоративной сети.

Таким образом доказывается, что эксплуатация уязвимостей веб-приложений может привести к компрометации серверов, утечке данных и развитию кибератаки внутри сети, подчеркивая необходимость их своевременного устранения.

Использование модели MITRE ATT&CK для тестирования безопасности корпоративных сетей, в частности с применением техники T1190, показало высокую эффективность в выявлении уязвимостей в веб-приложениях. Проводя анализ уязвимых точек входа, было продемонстрировано, как нарушители могут воспользоваться уязвимостями для компрометации систем и дальнейшего распространения кибератаки по сети. Результаты работы подтверждают необходимость применения комплексных подходов к защите. Организациям следует активно использовать методы тестирования безопасности, основанные на MITRE ATT&CK, для более эффективного выявления угроз и своевременного реагирования на них.

В заключение, развитие и совершенствование систем защиты необходимо для того, чтобы адаптироваться к быстро меняющимся угрозам в сфере кибербезопасности. Использование моделей, таких как MITRE ATT&CK, позволяет не только тестировать существующие механизмы защиты, но и создавать эффективные стратегии для противодействия новыми атакам, что в итоге способствует повышению общей безопасности корпоративных сетей.

Список использованных источников:

1. Techique T1190 [Электронный ресурс] – 2024. Режим доступа : https://attack.mitre.org/versions/v9/techniques/T1190/

METHODOLOGY OF USING THE MITRE ATTACK MATRIX FOR TESTING THE SECURITY OF CORPORATE NETWORKS

Krauchanka E.D., Butskevich E.M

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), Associate Professor

Annotation. The article examines the application of the MITRE ATT&CK matrix in testing the security of corporate networks, with a focus on the T1190 technique. It considers methods for compromising web applications, including network scanning, brute-force attacks, and exploitation of vulnerabilities. It describes attack scenarios and their impact on the infrastructure, and proposes protective measures: access restrictions, multifactor authentication, and activity monitoring. The work is intended for cybersecurity specialists and researchers of attacks based on the MITRE ATT&CK model.

Keywords. MITRE ATT&CK, T1190, Exploit Public-Facing Application, enterprise network security, security testing, attack modeling, web application vulnerabilities.