МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ ЭЛЕКТРОННО-ИНФОРМАЦИОННЫХ СИСТЕМ
Кафедра интеллектуальных информационных технологий

РЕФЕРАТ

по дисциплине:
«Современные методы защиты компьютерных систем»

Выполнил:
студент 4 курса,
ФЭИС,
группы ИИ-22
Клебанович В. Н.

Брест 2024

1 PowerShell и Bash

PowerShell и Bash – это две популярные оболочки командной строки, используемые для управления операционными системами. Несмотря на общую цель – предоставление интерфейса для взаимодействия с системой, они существенно отличаются по архитектуре, синтаксису и возможностям.

Bash (Bourne Again Shell) – это традиционная Unix-подобная оболочка, основанная на текстовых командах. Bash сильно интегрирован с традиционными Unix-утилитами и широко используется в Linux, macOS и других Unix-подобных системах. Его преимущество – широкая распространенность, обширный набор инструментов и большое сообщество пользователей, обеспечивающее массу доступной документации и помощи. Однако, обработка сложных данных и объектов может быть затруднительной, требуя дополнительных утилит.

PowerShell – это современная оболочка от Microsoft, разработанная для управления Windows. В отличие от Bash, PowerShell работает с объектами, а не только с текстом. Это позволяет более эффективно обрабатывать данные, используя встроенные командлеты (cmdlets) – функции, специально разработанные для работы с объектами. PowerShell использует более сложный, но и более мощный синтаксис, основанный на .NET Framework (а теперь и .NET). Это обеспечивает лучшую интеграцию с другими компонентами Windows и возможность автоматизации более сложных задач. PowerShell предоставляет удобные средства для работы с Active Directory, Windows Management Instrumentation (WMI) и другими системами управления Windows.

Bash имеет длительную историю и огромное сообщество, что делает его популярным выбором среди разработчиков и системных администраторов в Unix-подобных системах. PowerShell активно поддерживается Microsoft и имеет растущее сообщество, особенно в корпоративной среде, где востребованы его инструменты для управления инфраструктурой.

В целом, выбор между PowerShell и Bash зависит от операционной системы и задач пользователя. Bash лучше подходит для задач, требующих быстрого и простого выполнения текстовых команд в Unix-подобных системах. PowerShell – более мощный и гибкий инструмент для управления Windows и автоматизации сложных задач, особенно в корпоративной среде. Обе оболочки обладают обширными

возможностями и активно развиваются, предоставляя пользователям эффективные средства взаимодействия с компьютерной системой.

2 Cyber Killchain

Cyber Kill Chain — это концептуальная модель, описывающая последовательность этапов, через которые проходят кибернападения. Разработанная компанией Lockheed Martin, модель представляет собой структуру для понимания и анализа атак, что помогает улучшить защиту информационных систем. Она используется как в кибербезопасности, так и в военных операциях для разработки стратегий защиты.

Модель Cyber Kill Chain делится на семь основных этапов:

– Разведка (Reconnaissance) — на этом этапе атакующие собирают информацию о цели. Это может включать изучение публичных данных, социальных сетей или поиск уязвимостей в IT-инфраструктуре организации. Пример защиты: мониторинг активности в сети, защита публичной информации, использование honeypot-систем для выявления разведывательных действий.

– Оружие (Weaponization) — создается вредоносное ПО, которое будет использоваться для атаки. Это могут быть вирусы, трояны, эксплойты для уязвимостей или файлы-документы с вредоносным кодом. Пример защиты: применение систем предотвращения вторжений (IDS/IPS), анализ подозрительных файлов с помощью песочниц (sandbox).

– Доставка (Delivery) — вредоносное ПО доставляется на цель. Атакующие могут использовать фишинговые письма, зараженные сайты, атаки на цепочку поставок (supply chain attacks) или физические носители, такие как USB-устройства. Пример защиты: фильтрация электронной почты, обучение сотрудников правилам кибербезопасности, безопасная конфигурация веб-серверов.

– Эксплуатация (Exploitation) — атакующие используют уязвимости системы для выполнения своего кода. Это может происходить через ошибки в программном обеспечении, неправильную настройку систем или использование скомпрометированных учетных данных. Пример защиты: регулярное обновление ПО, проведение аудита безопасности, применение принципа минимальных привилегий.

– Установление доступа (Installation) — вредоносное программное обеспечение устанавливается на целевой системе для обеспечения постоянного контроля над ней. Часто используются программы-лоудеры, бекдоры или средства удаленного администрирования (RAT). Пример защиты: использование антивирусных решений, мониторинг системных изменений, контроль запуска приложений (Application Control).

– Командование и контроль (Command and Control) — атакующие устанавливают каналы связи с зараженной системой для получения удаленного управления. Это может быть достигнуто через использование C2-серверов, зашифрованного трафика или скрытых DNS-запросов. Пример защиты: мониторинг сетевого трафика, выявление аномалий в соединениях, применение DNS-фильтров.

– Действия на цели (Actions on Objectives) — последний этап, на котором атакующие выполняют свои цели. Это могут быть кража данных, уничтожение информации, шифрование файлов для выкупа или использование системы для проведения дальнейших атак (например, DDoS). Пример защиты: шифрование данных, сегментация сети, применение систем обнаружения угроз (EDR).

Каждый этап модели предоставляет возможность для обороны, так как можно эффективно идентифицировать и устранить угрозу на любом из этих шагов. Система защиты на основе модели Cyber Kill Chain фокусируется на предотвращении нападений на ранних этапах, что минимизирует последствия атак.

Модель также помогает выявлять и устранять уязвимости в организации, улучшая возможности для реагирования на инциденты и планирования стратегии защиты.

3 MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) — это база знаний, разработанная организацией MITRE, которая описывает методы, тактики и техники, используемые киберпреступниками для атак на информационные системы. ATT&CK помогает профессионалам в области кибербезопасности лучше понимать действия атакующих, эффективно защищать сети и устранять уязвимости.

Основные элементы MITRE ATT&CK:

– Тактики — это цели или намерения атакующего, которые он пытается достичь в ходе атаки. Тактики обычно отражают более высокоуровневые цели, такие как выполнение кода, кража данных, эскалация привилегий и т.д.

– Техники — это конкретные способы, с помощью которых атакующие реализуют свои тактики. Каждая техника описывает метод, используемый для выполнения цели, например, использование фишинговых атак для доставки вредоносного ПО или эксплуатация уязвимостей в программном обеспечении.

– Подтехники — это более детализированные описания техник. Например, техника "Эксплуатация уязвимости" может быть разделена на несколько подтехник, таких как "Эксплуатация уязвимости в браузере" или "Эксплуатация уязвимости в приложении".

– Контрмеры — рекомендации по защите и реагированию на конкретные техники, основанные на опыте атаки. Они помогают организациям улучшить свои системы защиты.

ATT&CK структурирован по нескольким основным категориям:

– Enterprise: Методики для атак, направленных на организационные сети и устройства.

– Cloud: Атаки на облачные инфраструктуры.

– Mobile: Атаки на мобильные устройства.

– Industrial Control Systems (ICS): Атаки на системы управления промышленными процессами.

ATT&CK структурирован по нескольким основным категориям:

– Enterprise: методики для атак, направленных на организационные сети и устройства.

– Cloud: атаки на облачные инфраструктуры.

– Mobile: атаки на мобильные устройства.

– Industrial Control Systems (ICS): атаки на системы управления промышленными процессами.

MITRE ATT&CK была разработана в 2013 году в рамках проекта, направленного на изучение поведения атакующих внутри корпоративных сетей. Изначально база знаний была ориентирована на мониторинг действий атакующих после взлома, но со временем она эволюционировала, охватив весь цикл атаки.

ATT&CK описывает действия атакующих через жизненный цикл атаки, известный как модель "kill chain". Этапы включают:

- начальный доступ;
- выполнение;
- эскалацию привилегий;
- обход механизмов защиты;
- сбор данных;
- эксфильтрацию и др.

Эти этапы позволяют построить целостное понимание атаки и её последствий.

ATT&CK активно используется в области разведки угроз (Threat Intelligence). Это позволяет анализировать действия атакующих и связывать их с известными группами, такими как APT (Advanced Persistent Threat). Например, техники, применяемые атакующими, могут быть сопоставлены с действиями групп APT28 или FIN7, указанных в базе ATT&CK.

MITRE ATT&CK интегрируется с современными инструментами, такими как:

- SIEM (Security Information and Event Management);
- EDR (Endpoint Detection and Response);
- SOAR (Security Orchestration, Automation, and Response).

Эти решения позволяют сопоставлять события в системе с известными техниками атакующих, что ускоряет процесс выявления угроз и реагирования.

ATT&CK помогает организациям:

- проводить оценку зрелости своей защиты, тестируя системы на уязвимости, аналогичные тем, которые используют атакующие;
- анализировать пробелы в защите, используя такие инструменты, как ATT&CK Navigator, чтобы визуализировать угрозы и определить приоритетные области для улучшения.

ATT&CK может быть использован совместно с такими фреймворками, как NIST Cybersecurity Framework, ISO/IEC 27001 и Lockheed Martin Cyber Kill Chain. Это помогает построить комплексный подход к управлению киберугрозами.

Пример использования MITRE ATT&CK в практике:

– Анализ инцидентов: специалисты могут использовать ATT&CK для расследования инцидентов безопасности, выявления техник, которые были использованы атакующими, и планирования ответных действий.

– Усиление защиты: организации могут использовать MITRE ATT&CK для улучшения своих защитных мер, анализируя наиболее вероятные техники, применяемые к их инфраструктуре, и настраивая системы мониторинга.

Одним из ключевых аспектов MITRE ATT&CK является то, что база данных активно обновляется, чтобы учитывать новые угрозы и методы атак. Это позволяет держать защиту на острие современных киберугроз.

4 SIEM

SIEM (Security Information and Event Management) — это система управления информацией и событиями безопасности, которая обеспечивает централизованный сбор, анализ и управление данными, связанными с безопасностью в ИТ-инфраструктуре организации. Основная цель SIEM — улучшение защиты от угроз и инцидентов за счет быстрого обнаружения, анализа и реагирования на потенциальные угрозы.

SIEM-системы собирают данные из различных источников, таких как устройства, приложения, серверы, сети и базы данных. Они обрабатывают информацию в реальном времени, что позволяет оперативно выявлять аномалии, уязвимости и попытки вторжений. Одним из ключевых аспектов является корреляция данных — система сопоставляет различные события и активности, чтобы определить возможные угрозы.

Основные функции SIEM включают:

– Сбор данных: автоматический сбор журналов и событий с различных источников, таких как брандмауэры, антивирусы, системы обнаружения вторжений и другие компоненты безопасности.

– Хранение и анализ: хранятся и анализируются большие объемы данных для выявления угроз, что позволяет быстро идентифицировать инциденты и аномалии.

– Корреляция событий: на основе собранных данных создаются корреляции между событиями, что позволяет выявлять сложные атаки, которые не были бы заметны при анализе отдельных событий.

– Уведомления и оповещения: система генерирует уведомления о подозрительных действиях, позволяя специалистам по безопасности принимать меры для защиты инфраструктуры.

– Отчеты и аудит: предоставление подробных отчетов о событиях и инцидентах для внутреннего аудита и соблюдения нормативных требований.

Использование SIEM помогает организациям повысить уровень безопасности, снизить риски от угроз, ускорить расследование инцидентов и обеспечить соответствие различным нормативным стандартам. Однако для эффективной работы SIEM требуется квалифицированный персонал и правильная настройка системы, а также постоянный мониторинг и обновление.

Важными преимуществами SIEM являются автоматизация процессов обнаружения угроз и реагирования на инциденты, а также улучшение видимости безопасности по всей инфраструктуре. Однако среди недостатков — высокая стоимость внедрения, необходимость в мощных ресурсах для обработки данных и сложности в настройке, особенно для крупных организаций.