Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра интеллектуальных информационных технологий

РЕФЕРАТ

По дисциплине

«Современные методы защиты компьютерных систем»

Выполнил:
Студент 4 курса
Группы ИИ-21
Литвинюк Т. В.

Брест 2024

1. POWERSHELL И BASH

PowerShell и Bash — это два популярных инструмента командной строки, широко используемых в различных операционных системах для автоматизации задач, управления системой и работы с файлами. Несмотря на общие цели, они различаются по своему назначению, синтаксису и областям применения.

Основные характеристики PowerShell

PowerShell — это командная оболочка и скриптовый язык, разработанный компанией Microsoft. Она изначально предназначалась для работы в Windows, но с появлением PowerShell Core стала кроссплатформенной. Основные особенности PowerShell:

- Основана на объектной модели .NET, что позволяет работать с объектами, а не просто текстом.
- Удобна для администрирования Windows-систем, включая работу с реестром, службами, и Active Directory.
- Богатый набор встроенных командлетов (cmdlets) для управления системой.
- Расширяемость за счет возможности создания собственных модулей и скриптов.

Основные характеристики Bash

Bash (Bourne Again Shell) — это Unix-оболочка и язык командной строки, который используется в системах на базе Linux и macOS. Основные особенности Bash:

- Основан на текстовых потоках, что делает его мощным инструментом для работы с файлами и текстовыми данными.
- Богатый экосистемный набор утилит для автоматизации задач.
- Простая интеграция с другими языками программирования, такими как Python и Perl.
- Стабильность и повсеместная поддержка в Unix-подобных системах.

Сравнение PowerShell и Bash

1. Синтаксис: PowerShell использует более строгий синтаксис с акцентом на работу с объектами. Bash фокусируется на текстовых данных и использует лаконичный синтаксис, что делает его компактным, но сложным для новичков.
2. Платформы: Bash традиционно используется в Linux и macOS, а PowerShell активно применяется в Windows, хотя и поддерживает кроссплатформенность.
3. Области применения: PowerShell более удобен для управления Windows-системами, в то время как Bash остается стандартом для автоматизации задач в Unix-среде.

PowerShell и Bash — это мощные инструменты для управления системами и автоматизации задач. Выбор между ними зависит от операционной системы и конкретных задач. Для Windows-администраторов PowerShell является естественным выбором, тогда как специалисты по Linux предпочитают Bash. Однако в современном мире, где кроссплатформенные решения становятся стандартом, знание обеих оболочек может стать ценным навыком.

2. CYBER KILL CHAIN

Cyber Kill Chain — это концептуальная модель, созданная компанией Lockheed Martin для описания этапов кибератаки. Этот подход используется для анализа угроз и построения стратегий защиты. Модель помогает организациям понять, как злоумышленники проникают в системы, и разработать эффективные контрмеры.

Модель состоит из семи последовательных этапов, каждый из которых описывает шаги, предпринимаемые злоумышленниками:

1. Разведка (Reconnaissance)
   На этом этапе атакующие собирают информацию о цели. Это может включать изучение инфраструктуры, IP-адресов, уязвимостей и социальных аспектов компании.

2. Вооружение (Weaponization)
   Создается вредоносный инструмент (например, вирус или эксплойт), который будет использоваться для атаки. Этот этап включает объединение собранных данных с уязвимостями цели.

3. Доставка (Delivery)
   Вредоносный код доставляется в систему цели. Для этого могут использоваться фишинговые письма, зараженные вложения, вредоносные ссылки или уязвимости в программном обеспечении.

4. Эксплуатация (Exploitation)
   На этом этапе злоумышленники используют уязвимости в системе для активации вредоносного кода. Это может включать использование слабых паролей, уязвимых протоколов или отсутствия патчей безопасности.

5. Установка (Installation)
   В систему цели устанавливается вредоносное ПО, такое как руткиты или трояны, которое позволяет атакующим закрепить свое присутствие.

6. Командование и управление (Command and Control, C2)
   Злоумышленники устанавливают канал связи с зараженной системой, чтобы управлять ею удаленно. Это может быть через защищенные протоколы или скрытые серверы управления.

7. Действия на объекте (Actions on Objectives)
   На завершающем этапе атакующие достигают своих целей, таких как кража данных, уничтожение систем, шпионаж или финансовая выгода.

Использование Cyber Kill Chain в защите Cyber Kill Chain помогает организациям выявлять угрозы на каждом этапе атаки. Применение модели позволяет:

- Усилить мониторинг подозрительных действий.
- Выявить и нейтрализовать угрозы до их реализации.
- Увеличить осведомленность сотрудников о возможных атаках, например, через обучение противодействию фишингу.

Критика модели
Хотя Cyber Kill Chain широко используется, она имеет свои ограничения:

- Основное внимание уделяется периметру сети и начальным этапам атаки, что делает модель менее эффективной против внутренних угроз.
- Новые технологии, такие как облачные сервисы и Zero Trust-архитектуры, требуют модернизированных подходов.

Cyber Kill Chain — это мощный инструмент для анализа и предотвращения кибератак. Несмотря на свои ограничения, модель остается актуальной для обеспечения безопасности. Организации могут использовать ее для построения многоуровневой защиты, которая минимизирует риск успешной атаки и помогает быстро реагировать на угрозы.

3. MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) — это открытая база знаний о тактиках и техниках, используемых киберпреступниками для проведения атак. Она разработана организацией MITRE для того, чтобы помочь специалистам в области кибербезопасности понять поведение злоумышленников и разработать эффективные меры защиты.

Основная цель MITRE ATT&CK
MITRE ATT&CK направлена на предоставление структурированного и систематизированного описания методов и инструментов, которые используют злоумышленники на различных этапах атаки. База знаний применяется для:

- Анализа угроз и инцидентов.
- Разработки стратегий защиты.
- Тестирования безопасности систем.
- Повышения осведомленности о современных методах атак.

Структура MITRE ATT&CK
MITRE ATT&CK организована в виде матрицы, которая включает:

1. Тактики
    - Тактики представляют собой общие цели атакующих, например, получение доступа, удержание в системе или эксфильтрация данных.
2. Техники
    - Техники описывают конкретные методы, используемые для достижения целей. Например, это могут быть фишинговые атаки, использование уязвимостей или сбор учетных данных.
3. Подтехники
    - Более детализированные методы, которые помогают глубже понять, как злоумышленники достигают своих целей.
4. Соответствующие примеры
    - ATT&CK включает примеры реальных групп угроз, таких как APT (Advanced Persistent Threats), которые используют описанные техники.

Применение MITRE ATT&CK

1. Управление угрозами
    - Матрица помогает анализировать поведение злоумышленников и определять, какие техники наиболее актуальны для конкретной организации.
2. Тестирование безопасности (Red Teaming)
    - Специалисты по тестированию защищенности используют MITRE ATT&CK для симуляции реальных атак и оценки уровня защищенности.
3. Разработка инструментов защиты

- Модель используется для настройки SIEM-систем (систем мониторинга и анализа событий безопасности) и других инструментов защиты.

4. Обучение сотрудников
    - Матрица служит справочником для обучения специалистов в области кибербезопасности и повышения их квалификации.

Преимущества MITRE ATT&CK

- Гибкость: Подходит для анализа угроз в различных средах (Windows, Linux, macOS, облако).
- Обновляемость: Регулярно пополняется новыми данными о современных угрозах.
- Доступность: Открытый доступ делает её полезной для компаний любого уровня.

Критика MITRE ATT&CK

- Матрица предоставляет обширную информацию, что может затруднять её использование для новичков.
- Требуется значительное время и ресурсы для внедрения в процесс защиты.
- Сосредоточенность на известных угрозах делает её менее эффективной против уникальных атак.

MITRE ATT&CK — это мощный инструмент для построения проактивной защиты. Используя матрицу, организации могут лучше понять поведение злоумышленников, предвидеть их действия и реагировать на угрозы быстрее и эффективнее. Несмотря на сложности внедрения, MITRE ATT&CK становится стандартом в сфере кибербезопасности, играя ключевую роль в предотвращении и смягчении атак.

4. SIEM

SIEM (Security Information and Event Management) — это категория решений в области информационной безопасности, которые объединяют функции управления событиями безопасности (SEM) и управления информацией безопасности (SIM). SIEM-системы предоставляют централизованный способ сбора, анализа и реагирования на инциденты безопасности, что делает их неотъемлемой частью современной киберзащиты.

Основные функции SIEM

1. Сбор данных
   SIEM агрегирует данные из множества источников, включая сетевые устройства, серверы, приложения, базы данных, системы аутентификации и средства защиты (антивирусы, IDS/IPS).
2. Корреляция событий
   Система анализирует данные, выявляя связи между событиями, которые могут указывать на потенциальные угрозы. Например, множество неудачных попыток входа может сигнализировать о брутфорс-атаке.
3. Уведомления и оповещения
   SIEM создает предупреждения о подозрительных событиях, позволяя специалистам оперативно реагировать на угрозы.

4. Хранение и управление логами
   Системы SIEM хранят логи, которые могут быть использованы для расследований инцидентов или соблюдения регуляторных требований.

5. Отчеты и аналитика
   SIEM предоставляет подробные отчеты и дашборды, что помогает организациям следить за уровнем безопасности и идентифицировать слабые места.

Применение SIEM

1. Обнаружение угроз
   SIEM помогает выявлять аномалии в работе системы, такие как необычная активность в сети или несанкционированный доступ.

2. Реагирование на инциденты
   Системы SIEM часто интегрируются с SOAR (Security Orchestration, Automation, and Response), автоматизируя процесс реагирования на угрозы.

3. Соблюдение нормативных требований
   SIEM помогает организациям соответствовать стандартам, таким как GDPR, PCI DSS, HIPAA, предоставляя необходимые логи и отчеты.

4. Расследование инцидентов
   Исторические данные из SIEM используются для анализа кибератак и выявления источников угроз.

Преимущества SIEM

- Централизация данных: Упрощает управление безопасностью за счет единой платформы.
- Проактивный подход: Обнаруживает угрозы на ранних стадиях.
- Автоматизация: Уменьшает нагрузку на специалистов, предлагая автоматические оповещения и реакции.

Критика и ограничения

- Высокая стоимость: Внедрение и обслуживание SIEM может быть дорогим.
- Сложность настройки: Для корректной работы требуется точная настройка и регулярное обновление правил корреляции.
- Обилие ложных срабатываний: Некорректные настройки могут привести к многочисленным ложным предупреждениям, отвлекая специалистов от реальных угроз.

Некоторые из самых известных SIEM-платформ:

- Splunk: Известен мощной аналитикой и масштабируемостью.
- IBM QRadar: Отличается глубокой интеграцией с корпоративными системами.
- Microsoft Sentinel: Облачное решение с расширенными функциями искусственного интеллекта.
- ArcSight: Популярен в крупных организациях за надежность и гибкость.

SIEM — это ключевой инструмент для обеспечения безопасности в современных организациях. Он позволяет централизовать управление событиями безопасности, обнаруживать угрозы в реальном времени и минимизировать риски. Несмотря на сложности в внедрении и настройке, SIEM-системы играют важнейшую роль в защите цифровых активов и обеспечении соответствия регуляторным требованиям.