**Доклад по дисциплине «Современные методы защиты информации»**

Выполнил Кирилович А. А.

**Вариант 1**

**1. Логирование. Изменение журнала логирования. Powershell и Bash.**

Логирование — это процесс записи событий, происходящих в системе, приложении или сети, в специальные файлы или журналы. Эти записи помогают администраторам и специалистам по безопасности отслеживать работу систем, выявлять и устранять ошибки, а также анализировать потенциальные угрозы.

**Изменение журналов логирования**

Внесение изменений в журналы логирования может быть частью административных задач, например, при настройке уровня детализации записей или изменении места хранения логов. Однако несанкционированное изменение или удаление логов может свидетельствовать о попытках скрыть следы вредоносной активности. Поэтому важно обеспечивать целостность и защиту журналов от несанкционированного доступа.

**Логирование в PowerShell**

PowerShell предоставляет встроенные возможности для работы с журналами событий Windows. Командлеты, такие как Get-EventLog и Get-WinEvent, позволяют просматривать и фильтровать записи журналов. Например, чтобы получить последние 100 записей из системного журнала:

Get-EventLog -LogName System -Newest 100

Для включения расширенного логирования, такого как ведение журнала блоков скриптов, можно использовать групповую политику или изменить параметры реестра. Это позволяет записывать содержимое всех обрабатываемых блоков скриптов, что полезно для диагностики и аудита.

**Логирование в Bash**

В системах на базе Linux логирование обычно осуществляется с помощью демона rsyslog, который записывает системные и прикладные сообщения в файлы, расположенные в каталоге /var/log/. Для настройки логирования можно редактировать файл /etc/rsyslog.conf, определяя, какие сообщения и куда должны записываться.

Для логирования в скриптах Bash можно перенаправлять вывод команд в файлы логов. Например, чтобы записать стандартный вывод и ошибки в файл:

#!/bin/bash

exec > >(tee -a /var/log/myscript.log) 2>&1

echo "Начало выполнения скрипта"

# команды скрипта

Это обеспечит сохранение всех сообщений скрипта в указанном файле лога.

**Рекомендации по защите журналов логирования**

* **Ограничение доступа**: установите строгие права доступа к файлам логов, чтобы предотвратить несанкционированное изменение или удаление записей.
* **Ротация логов**: Настройте автоматическую ротацию и архивирование логов, чтобы избежать переполнения диска и сохранить историю событий. В Linux для этого часто используется утилита logrotate.
* **Мониторинг целостности**: Используйте инструменты для контроля целостности файлов логов, чтобы своевременно обнаруживать попытки их изменения.
* **Централизованное логирование**: рассмотрите возможность отправки логов на удаленный сервер или в систему централизованного сбора логов для дополнительной защиты и удобства анализа.

Соблюдение этих рекомендаций поможет обеспечить надежное логирование и защиту ваших систем от потенциальных угроз.

2. Cyber Kill Chain

Модель Cyber Kill Chain, разработанная компанией Lockheed Martin, описывает этапы, через которые проходит кибератака, начиная с разведки и заканчивая достижением целей злоумышленника. Понимание этой последовательности помогает специалистам по безопасности выявлять и предотвращать угрозы на разных стадиях атаки.

**Этапы Cyber Kill Chain:**

1. **Разведка (Reconnaissance):** сбор информации о цели, включая сетевую инфраструктуру, используемые технологии и потенциальные уязвимости.
2. **Вооружение (Weaponization):** создание вредоносного ПО или эксплойтов, которые будут использоваться для компрометации системы.
3. **Доставка (Delivery):** доставка вредоносного кода к цели, например, через фишинговые письма, зараженные веб-сайты или съемные носители.
4. **Эксплуатация (Exploitation):** использование уязвимостей в системе для выполнения вредоносного кода.
5. **Установка (Installation):** установка вредоносного ПО на скомпрометированную систему для обеспечения постоянного доступа.
6. **Управление и контроль (Command and Control):** установление связи между скомпрометированной системой и сервером злоумышленника для дальнейшего управления.
7. **Достижение целей (Actions on Objectives):** выполнение конечных целей атаки, таких как кража данных, разрушение систем или шпионаж.

Понимание этих этапов позволяет организациям разрабатывать стратегии защиты, направленные на обнаружение и прерывание атаки на каждом из этапов, повышая общую кибербезопасность.

3. MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) — это открытая база знаний, систематизирующая тактики и техники, используемые злоумышленниками в кибератаках. Разработанная корпорацией MITRE в 2013 году, она служит руководством для описания и классификации кибератак и вторжений.

**Структура MITRE ATT&CK:**

* **Тактики:** высокоуровневые цели, которых стремится достичь злоумышленник (например, сбор информации, уклонение от обнаружения).
* **Техники:** конкретные методы, используемые для реализации тактик (например, использование скриптовых интерфейсов, внедрение кода).
* **Подтехники:** более детализированные варианты техник, описывающие специфические способы их выполнения.

**Применение MITRE ATT&CK:**

* **Моделирование угроз:** помогает организациям понять, какие тактики и техники могут быть использованы против них, и подготовить соответствующие меры защиты.
* **Оценка безопасности:** используется для проверки эффективности существующих средств защиты и выявления пробелов в безопасности.
* **Обучение и осведомленность:** служит учебным пособием для специалистов по кибербезопасности, помогая им распознавать и реагировать на различные методы атак.
* **Разработка защитных мер:** информирует о создании детекторов и механизмов предотвращения, направленных на конкретные техники атак.

MITRE также предоставляет инструменты, такие как ATT&CK Navigator, для визуализации матриц ATT&CK и анализа покрытия защитными мерами.

Использование MITRE ATT&CK способствует более глубокому пониманию поведения злоумышленников и повышает эффективность стратегий киберзащиты.

4. SIEM (Security information and event management)

SIEM (Security Information and Event Management) — это класс программных решений, предназначенных для сбора, хранения, анализа и корреляции данных о событиях безопасности из различных источников в реальном времени. Основная цель SIEM-систем — предоставление централизованного обзора событий безопасности, что позволяет оперативно обнаруживать, анализировать и реагировать на инциденты, а также обеспечивать соответствие требованиям регуляторов.

**Ключевые функции SIEM:**

* **Сбор данных:** агрегация информации из разнообразных источников, таких как сетевые устройства, серверы, приложения и системы безопасности.
* **Хранение и управление данными:** безопасное хранение собранных данных с возможностью их последующего анализа и аудита.
* **Анализ и корреляция:** обработка и сопоставление событий для выявления аномалий и потенциальных угроз.
* **Мониторинг в реальном времени:** непрерывное наблюдение за событиями безопасности с мгновенным оповещением о подозрительной активности.
* **Отчётность и соответствие требованиям:** генерация отчётов для демонстрации соответствия нормативным требованиям и внутренним политикам безопасности.

**Преимущества использования SIEM:**

* **Быстрое обнаружение угроз:** объединяя данные из различных источников, SIEM-системы позволяют быстрее выявлять сложные атаки и инциденты.
* **Улучшенная реакция на инциденты:** централизованный доступ к информации облегчает расследование и ускоряет реагирование на инциденты.
* **Соответствие нормативным требованиям:** SIEM помогает организациям соблюдать стандарты безопасности и готовить необходимые отчёты для аудита.
* **Повышенная осведомлённость:** предоставляет целостное представление о состоянии безопасности ИТ-инфраструктуры организации.

**Рекомендации по внедрению SIEM:**

* **Определение целей:** чётко сформулируйте, какие задачи должна решать SIEM-система в вашей организации.
* **Выбор подходящего решения:** оцените различные SIEM-продукты с учётом специфики вашей инфраструктуры и требований.
* **Планирование ресурсов:** обеспечьте наличие необходимых ресурсов для установки, настройки и поддержки SIEM-системы.
* **Обучение персонала:** гарантируйте, что сотрудники обладают достаточными знаниями для эффективного использования SIEM.
* **Постоянный мониторинг и оптимизация:** регулярно оценивайте эффективность работы SIEM и вносите необходимые улучшения.

Внедрение SIEM-системы может значительно повысить уровень информационной безопасности организации, обеспечивая проактивный подход к обнаружению и реагированию на киберугрозы.