Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Реферат
По дисциплине: «Современные методы защиты компьютерных систем»
Вариант 1

Выполнила:
Студентка 4 курса
Группы ИИ-21
Шнур А.А.
Проверил:
Хацкевич М.В.

Брест 2024

Вариант 1 (15 mod 3)

1. Логирование. Изменение журнала логирования. PowerShell&Bash
2. Cyber Kill Chain
3. MITRE ATT&CK
4. SIEM

1.Логирование. Изменение журнала логирования. PowerShell,Bash.

Логирование — это процесс фиксации событий, происходящих в системе или приложении. Журналы логирования помогают администраторам и специалистам по безопасности отслеживать активность, выявлять сбои и обнаруживать следы несанкционированных действий. Изменение или удаление логов может использоваться как для легитимных целей (например, очистка старых записей), так и для сокрытия следов атак.

Логирование в PowerShell

PowerShell предоставляет встроенные инструменты для работы с логами в операционных системах семейства Windows. Логи хранятся в журнале событий Windows и делятся на несколько категорий, таких как Application, Security, System, и др.

Просмотр логов

- Команда **Get-EventLog** позволяет просматривать журналы событий. Например, просмотр журнала системы:

```
Get-EventLog -LogName System -Newest 10
```

- Команда **Get-WinEvent** поддерживает более гибкий подход к работе с логами:

```
Get-WinEvent -LogName Security -MaxEvents 5
```

Изменение и создание логов

- Добавление новой записи в журнал событий:

```
Write-EventLog -LogName Application -Source "MyApp" -EntryType
  Information -EventId 1001 -Message "Тестовая запись в лог"
```

- Создание нового журнала событий:

```
New-EventLog -LogName "MyNewLog" -Source "MyApp"
```

Очистка логов

- Очистка конкретного журнала:

```
Clear-EventLog -LogName System
```

- Удаление журнала событий:

```
Remove-EventLog -LogName "MyNewLog"
```

Логирование в Bash (Linux)

В системах на базе Linux логирование осуществляется через сервисы, такие как syslog и journald. Журналы обычно хранятся в каталоге /var/log.

Просмотр логов

- Просмотр системного журнала:

```
cat /var/log/syslog
```

- Использование команды journalctl для систем с systemd:

```
journalctl -n 20  # Просмотр последних 20 записей
```

Добавление записей в лог

- Запись сообщения в системный лог через logger:

```
logger "Тестовая запись в лог"
```

Очистка и изменение логов

- Очистка файла журнала:

```
> /var/log/syslog
```

- Удаление старых логов с помощью logrotate:

```
logrotate /etc/logrotate.conf
```

Изменение конфигурации логирования

Файл конфигурации для syslog расположен по пути /etc/rsyslog.conf.
Например, для настройки логирования событий ядра можно добавить строку:

```
kern.* /var/log/kern.log
```

После изменения конфигурации необходимо перезапустить сервис:

```
systemctl restart rsyslog
```

Логирование в PowerShell и Bash — это мощный инструмент для контроля за состоянием системы. Возможность изменять и удалять логи может быть полезна как для администрирования, так и для анализа безопасности. Однако изменение логов требует осторожности, так как неправильные действия могут привести к потере важной информации или скрытию следов атак.

2. Cyber Kill Chain

Cyber Kill Chain — это модель, разработанная корпорацией Lockheed Martin для описания этапов, через которые проходят кибератаки. Эта концепция позволяет специалистам по безопасности выявлять угрозы на ранних стадиях и принимать необходимые меры для их предотвращения. Cyber Kill Chain помогает систематизировать подход к анализу атак и разрабатывать эффективные стратегии защиты.

История создания

Модель Cyber Kill Chain была впервые представлена в рамках программы исследований Lockheed Martin по кибербезопасности. Она основана на военной концепции "Kill Chain", которая описывает этапы атаки на физическом поле боя. Lockheed Martin адаптировала эту идею для анализа действий злоумышленников в цифровой среде.

Этапы Cyber Kill Chain

Модель Cyber Kill Chain состоит из семи основных этапов, каждый из которых представляет собой шаг, необходимый злоумышленнику для успешного выполнения атаки. Рассмотрим каждый из этих этапов подробнее.

1. Разведка

На этом этапе злоумышленник собирает информацию о своей цели. Это могут быть данные о сотрудниках компании, сетевой инфраструктуре, программном обеспечении и других уязвимых элементах.

Методы разведки:

- Поиск информации в открытых источниках (OSINT).
- Сканирование сетей для выявления открытых портов и сервисов.
- Фишинговые атаки для получения учетных данных.

2. Вооружение

Злоумышленник создаёт инструмент для атаки, например, вредоносное ПО (вирусы, трояны, эксплойты). Этот инструмент разрабатывается для использования найденных уязвимостей.

Примеры:

- Создание PDF-файла или документа Word с встроенным вредоносным макросом.
- Разработка эксплойта для уязвимости в веб-приложении.

3. Доставка

На этом этапе происходит доставка вредоносного инструмента на целевую систему.

Способы доставки:

- Электронная почта с вложением (фишинг).
- Вредоносные ссылки на веб-сайтах.
- Сетевые атаки с использованием эксплойтов.

4. Эксплуатация

Злоумышленник использует уязвимость для выполнения вредоносного кода на целевой системе. На этом этапе происходит активация доставленного инструмента.

Примеры:

- Уязвимость в веб-приложении, позволяющая выполнить произвольный код.
- Уязвимость в программном обеспечении, запускающая вредоносный скрипт.

5. Установка

После успешной эксплуатации злоумышленник устанавливает вредоносное ПО (например, троян или бекдор) для долгосрочного доступа к системе.
Цели установки:

- Закрепиться на целевом устройстве.
- Установить контроль над системой для дальнейших действий.

6. Управление и контроль

На этом этапе происходит связь между зараженной системой и сервером злоумышленника. Это позволяет атакующему управлять зараженной системой, загружать дополнительные инструменты и выполнять команды.
Методы C2:

- Использование зашифрованного трафика для маскировки команд.
- Управление через поддельные веб-сайты или социальные сети.

7. Действия на цели

Финальный этап, на котором злоумышленник достигает своих целей, будь то:

- Кража данных.
- Шифрование файлов (атака типа ransomware).
- Нарушение работоспособности системы (DDoS-атака).

Применение Cyber Kill Chain для защиты

Модель Cyber Kill Chain позволяет специалистам по безопасности:

1. Идентифицировать и блокировать угрозы на каждом из этапов атаки.
2. Понимать тактику и методы злоумышленников для разработки стратегий защиты.
3. Улучшать процессы реагирования на инциденты за счет систематического анализа атак.

Примеры защитных мер:

- На этапе разведки: Мониторинг публичных источников на предмет утечек информации.
- На этапе доставки: Фильтрация подозрительных вложений и ссылок.
- На этапе установки: Использование антивирусов и систем обнаружения вторжений (IDS).
-

Cyber Kill Chain — это полезный инструмент для понимания и противодействия современным киберугрозам. Разделение атаки на этапы помогает специалистам по безопасности разрабатывать более точные и эффективные меры защиты. Несмотря на то, что злоумышленники совершенствуют свои методы, применение модели Cyber Kill Chain позволяет своевременно выявлять и предотвращать многие виды атак.

3. MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) — это открытая база знаний о тактиках, техниках и процедурах (TTPs), используемых злоумышленниками при проведении кибератак. Она разработана организацией **MITRE Corporation** и служит для документирования и анализа способов атак на информационные системы. MITRE ATT&CK помогает специалистам по кибербезопасности понять, как действуют злоумышленники, и строить более эффективные системы защиты.

История создания

MITRE ATT&CK была представлена в 2013 году в рамках программы **FORTRESS** для анализа поведения угроз в корпоративных сетях. Со временем база знаний расширилась и стала стандартом для оценки угроз и планирования мер защиты. Сегодня MITRE ATT&CK используется во всем мире как инструмент для изучения поведения атакующих и улучшения киберзащиты организаций.

Структура MITRE ATT&CK

MITRE ATT&CK классифицирует атаки по следующим основным категориям:

1. **Тактики (Tactics):** определяют цели, которых злоумышленники хотят достичь (например, получение доступа, перемещение по сети).
2. **Техники (Techniques):** конкретные методы, которые злоумышленники используют для достижения целей.
3. **Подтехники (Sub-Techniques):** более детализированные методы в рамках конкретной техники.
4. **Процедуры (Procedures):** реальные примеры того, как злоумышленники применяют техники на практике.

Матрицы MITRE ATT&CK

MITRE ATT&CK включает несколько матриц для различных типов сред:

1. **ATT&CK для корпоративных сетей (Enterprise):** описывает атаки на операционные системы Windows, macOS и Linux, а также облачные и сетевые технологии.
2. **ATT&CK для мобильных устройств (Mobile):** фокусируется на угрозах для мобильных операционных систем, таких как Android и iOS.
3. **ATT&CK для промышленного интернета вещей (ICS):** анализирует угрозы для промышленных систем управления (SCADA, PLC и др.).

Основные тактики MITRE ATT&CK (Enterprise)

Каждая матрица состоит из множества тактик, которые представляют этапы атаки. Рассмотрим основные тактики:

1. **Разведка (Reconnaissance):** сбор информации о цели до атаки (поиск уязвимостей, сотрудников).

2. **Получение начального доступа (Initial Access):** методы для проникновения в систему (фишинг, эксплуатация уязвимостей).
3. **Исполнение (Execution):** запуск вредоносного кода на целевой системе.
4. **Закрепление (Persistence):** обеспечение долгосрочного доступа к системе (бекдоры, автоматические задачи).
5. **Эскалация привилегий (Privilege Escalation):** получение более высоких прав доступа.
6. **Обход защиты (Defense Evasion):** методы для скрытия следов атаки (изменение логов, маскировка процессов).
7. **Доступ к учетным данным (Credential Access):** кража паролей и других данных для авторизации.
8. **Перемещение по сети (Lateral Movement):** перемещение от одной системы к другой в сети организации.
9. **Сбор данных (Collection):** сбор конфиденциальной информации (файлы, документы).
10. **Передача данных (Exfiltration):** вывод украденных данных из системы.
11. **Воздействие (Impact):** нарушение работы системы (шифрование данных, уничтожение информации).

Примеры техник MITRE ATT&CK

Каждая тактика включает конкретные техники, которые злоумышленники применяют для достижения своих целей. Например:

- **Техника T1078 (Valid Accounts):** использование украденных учетных данных для доступа к системе.
- **Техника T1055 (Process Injection):** внедрение вредоносного кода в процессы для сокрытия активности.
- **Техника T1566 (Phishing):** отправка вредоносных писем для получения доступа.

Применение MITRE ATT&CK в кибербезопасности

MITRE ATT&CK активно используется специалистами для различных целей:

1. **Анализ угроз:** понимание методов атакующих для разработки мер защиты.
2. **Тестирование на проникновение (Pentesting):** имитация атак для оценки защиты организации.
3. **Реагирование на инциденты:** быстрое выявление этапов атаки и принятие мер для её остановки.
4. **Обучение и повышение квалификации:** тренировки для специалистов по безопасности на основе реальных сценариев.

Пример использования:
Компания может сопоставлять свои системы с матрицей MITRE ATT&CK, чтобы выявлять слабые места и усиливать защиту против конкретных техник атак.

Инструменты для работы с MITRE ATT&CK

1. **ATT&CK Navigator:** визуальный инструмент для работы с матрицей и создания пользовательских представлений.
2. **CALDERA:** автоматизированный инструмент для имитации атак на основе MITRE ATT&CK.
3. **MITRE CTI:** информационная платформа для обмена данными о киберугрозах.

MITRE ATT&CK — это мощная база знаний, которая позволяет глубже понять тактики и техники злоумышленников. Она помогает организациям повышать уровень защиты, выявлять угрозы на ранних этапах и эффективно реагировать на инциденты. Благодаря структурированному подходу MITRE ATT&CK стал стандартом в области кибербезопасности, который способствует развитию стратегий защиты от современных киберугроз.

4. SIEM (Security Information and Event Management)

SIEM (Security Information and Event Management) — это система управления информацией и событиями безопасности. Она позволяет организациям собирать, анализировать и интерпретировать данные о безопасности из различных источников для обнаружения угроз и управления инцидентами. SIEM играет ключевую роль в современной кибербезопасности, помогая оперативно выявлять атаки, анализировать их причины и предотвращать возможные угрозы.

История развития SIEM
Концепция SIEM возникла в начале 2000-х годов как комбинация двух технологий:

1. **SIM (Security Information Management):** Системы для долгосрочного хранения и анализа логов безопасности.
2. **SEM (Security Event Management):** Системы для мониторинга и реагирования на события безопасности в реальном времени.

Объединение этих подходов привело к появлению SIEM, способного обрабатывать большие объемы данных, предоставляя как долгосрочный анализ, так и оперативное обнаружение угроз.

Принципы работы SIEM
SIEM-системы работают на основе следующих принципов:

1. **Сбор данных:** Интеграция с различными источниками данных (лог-файлы серверов, сетевых устройств, приложений, антивирусных систем и т.д.).
2. **Агрегация и корреляция:** Объединение данных из разных источников для выявления взаимосвязанных событий и потенциальных угроз.
3. **Анализ данных:** Автоматизированный анализ данных для выявления аномалий и подозрительной активности.
4. **Оповещения:** Генерация уведомлений при обнаружении угроз или аномалий.
5. **Хранение данных:** Архивирование логов для дальнейшего анализа и выполнения требований регуляторов.
6. **Отчеты и визуализация:** Создание отчетов и визуальных представлений для удобства анализа информации.

Основные функции SIEM

1. **Мониторинг в реальном времени:** Непрерывный сбор и анализ данных для выявления угроз в режиме реального времени.
2. **Корреляция событий:** Сопоставление разрозненных событий для выявления сложных атак.
3. **Обнаружение аномалий:** Идентификация необычного поведения на основе заранее определённых правил или моделей поведения.
4. **Управление инцидентами:** Автоматизация процесса реагирования на инциденты и создание уведомлений для специалистов по безопасности.
5. **Отчётность и аудит:** Формирование отчётов для анализа и соответствия требованиям регуляторов.
6. **Долгосрочное хранение данных:** Архивация логов для ретроспективного анализа.

Архитектура SIEM

SIEM-система включает следующие компоненты:

1. **Агенты сбора данных:** Устанавливаются на устройствах и серверах для сбора логов и передачи их в центральный SIEM.
2. **Сервер SIEM:** Центральный компонент, который выполняет анализ данных, корреляцию и генерацию отчетов.
3. **База данных:** Хранит собранные логи и результаты анализа для дальнейшего использования.
4. **Интерфейс пользователя:** Позволяет просматривать отчеты, настраивать правила и управлять системой.

Примеры популярных SIEM-систем

1. **Splunk Enterprise Security:** Мощная платформа для анализа больших объемов данных с интуитивно понятным интерфейсом и гибкими настройками.
2. **IBM QRadar:** Предоставляет функции анализа угроз и корреляции событий, интегрируется с различными источниками данных.
3. **ArcSight ESM (Micro Focus):** Система для мониторинга безопасности и управления инцидентами с возможностью масштабирования.
4. **LogRhythm:** Решение для автоматизации процесса обнаружения и реагирования на угрозы.
5. **OSSIM (Open Source SIEM):** Бесплатная SIEM-система с базовыми функциями для малого и среднего бизнеса.

Преимущества SIEM

1. **Централизованный мониторинг:** Единая точка контроля для всех событий безопасности в организации.
2. **Быстрое обнаружение угроз:** Оперативное выявление инцидентов и реагирование на них.
3. **Соответствие требованиям:** Помощь в соблюдении стандартов и регуляций (например, GDPR, HIPAA, PCI DSS).
4. **Исторический анализ:** Возможность ретроспективного анализа для выявления причин инцидентов.
5. **Автоматизация процессов:** Снижение нагрузки на специалистов по безопасности благодаря автоматизации анализа и реагирования.

Недостатки SIEM

1. **Высокая стоимость внедрения:** Дорогие лицензии и сложность настройки для крупных организаций.
2. **Ложные срабатывания:** Возможность генерации большого количества ложных предупреждений.
3. **Сложность обслуживания:** Требует квалифицированного персонала для эффективного управления и настройки.
4. **Производительность:** Большие объемы данных могут замедлить работу системы.

Применение SIEM в реальной жизни

1. **Корпоративные сети:** Мониторинг активности сотрудников и защита от внутренних угроз.
2. **Финансовые учреждения:** Выявление мошеннических действий и обеспечение соответствия требованиям регуляторов.
3. **Здравоохранение:** Защита медицинских данных и предотвращение утечек информации.

4. **Государственные учреждения:** Обеспечение национальной безопасности и защита критической инфраструктуры.

SIEM является незаменимым инструментом для современных организаций, стремящихся защитить свои информационные активы от киберугроз. Благодаря возможности централизованного сбора, анализа и корреляции данных SIEM помогает оперативно выявлять инциденты и реагировать на них. Несмотря на высокие затраты и сложности внедрения, преимущества SIEM делают его важным компонентом стратегий кибербезопасности в любых организациях.