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-го курса,
ФЭИС,
группы ИИ-22
Любчук И.И.

Брест 2024

1 TEMA 1: netflow

NetFlow — это сетевое решение, созданное компанией Cisco Systems, которое используется для сбора и анализа информации о сетевом трафике. Оно позволяет администраторам мониторить, оптимизировать работу сети и обнаруживать аномалии для обеспечения безопасности.

С момента своего появления в середине 1990-х годов NetFlow быстро стало популярным инструментом, предоставляя возможность детализированного анализа трафика. Идея технологии заключается в разделении трафика на отдельные потоки, каждый из которых представляет собой набор пакетов, объединённых общими характеристиками, такими как IP-адреса, порты и протоколы.

Принципы работы NetFlow

NetFlow анализирует проходящий через сеть трафик, группируя его в потоки на основе следующих ключевых параметров:

1. **IP-адрес источника**.
2. **IP-адрес назначения**.
3. **Порт источника**.
4. **Порт назначения**.
5. **Транспортный протокол** (например, TCP, UDP).
6. **Интерфейс маршрутизатора**, через который проходят пакеты.

Когда поток завершён (например, при завершении сессии или по истечении времени), информация о нём передаётся на серверы для дальнейшего хранения и анализа. Эти данные используются для создания отчетов и визуализаций, помогающих понять, как именно используется сеть.

Компоненты системы NetFlow

1. **Экспортер** — это сетевое устройство, которое собирает данные о потоках и отправляет их на серверы для хранения и анализа.
2. **Коллектор** — система или сервер, который получает данные от экспортера и обрабатывает их.
3. **Анализатор** — это инструмент, который анализирует собранные данные и отображает их в удобном для пользователя виде (графики, отчёты, диаграммы).

Применение NetFlow

1. **Мониторинг сети**: позволяет отслеживать трафик, выявлять перегрузки и узкие места, оптимизировать распределение данных по сети.
2. **Повышение производительности**: анализируя трафик, можно находить способы улучшения маршрутизации и уменьшения задержек.
3. **Обеспечение безопасности**: помогает выявить аномалии в трафике, например, DDoS-атаки или несанкционированные попытки доступа.
4. **Биллинг**: используется для отслеживания использования сети и расчёта стоимости услуг для пользователей.

Альтернативы и развитие технологий

Кроме NetFlow, существуют другие технологии для мониторинга и анализа трафика, такие как **sFlow**, **IPFIX** и **J-Flow**. В последние годы технологии в области сетевого анализа активно развиваются, включая интеграцию с искусственным интеллектом для более точного обнаружения угроз и аномалий.

NetFlow остаётся одним из самых мощных инструментов для мониторинга и анализа трафика в современных сетях, и его роль будет только возрастать с развитием технологий и увеличением объёмов данных.

Преимущества NetFlow

- Предоставляет глубокий уровень анализа без необходимости перехвата пакетов.
- Широкая поддержка на сетевом оборудовании.
- Масштабируемость для работы как с небольшими, так и с крупными сетями.

Недостатки

- Высокая нагрузка на устройства при большом объеме данных.
- Необходимость значительных ресурсов для хранения и обработки информации.

NetFlow остаётся ключевым инструментом для управления сетями. С развитием технологий и увеличением трафика её значимость и востребованность только растут.

2 ТЕМА 2: WAF

WAF (Web Application Firewall) — это брандмауэр для веб-приложений, который защищает их от различных угроз, таких как атаки на уязвимости, попытки взлома и злоупотребление функционалом. WAF работает на уровне HTTP/HTTPS и анализирует входящий, исходящий и межсерверный трафик, чтобы предотвратить потенциально вредоносные действия.

Основные задачи WAF

1. **Защита от уязвимостей приложений**: WAF защищает от атак, таких как SQL-инъекции, XSS (межсайтовый скриптинг), CSRF (межсайтовая подделка запросов), внедрение команд и другие.
2. **Фильтрация вредоносного трафика**: блокирует попытки проникновения злоумышленников или ботов.
3. **Мониторинг и контроль трафика**: WAF анализирует каждую HTTP/HTTPS-запрос и ответ для выявления аномалий или попыток эксплуатации уязвимостей.
4. **Поддержка соответствия стандартам**: помогает организациям соответствовать требованиям стандартов, таких как PCI DSS, для защиты данных.

Принцип работы WAF

WAF размещается между пользователем и веб-приложением. Все запросы и ответы проходят через WAF, который проверяет их на наличие вредоносного содержания.

Основные этапы работы:

1. **Анализ входящего трафика**: проверка запросов по заранее установленным правилам.
2. **Блокировка угроз**: если запрос соответствует шаблону атаки, WAF может его заблокировать.
3. **Журналирование**: запись всех подозрительных действий для дальнейшего анализа.

4. **Отправка безопасного трафика**: разрешённые запросы передаются веб-приложению.

Типы WAF

1. **Сетевой WAF (Network-based)**: устанавливается в сети организации, обеспечивая защиту с минимальными задержками. Обычно это аппаратное решение.
2. **Облачный WAF (Cloud-based)**: управляется поставщиком услуги, что снижает сложность настройки и обслуживания.
3. **Хостовый WAF (Host-based)**: устанавливается на сервере веб-приложения. Предоставляет гибкость настройки, но требует ресурсов сервера.

Преимущества WAF

1. **Быстрая защита**: позволяет оперативно блокировать угрозы без изменений в коде веб-приложения.
2. **Гибкость настройки**: можно адаптировать под специфические требования приложений.
3. **Снижение риска атак**: WAF защищает даже от неизвестных уязвимостей с помощью эвристических методов и анализа поведения.
4. **Улучшение безопасности данных**: предотвращает утечки личной информации пользователей.

Ограничения WAF

1. **Нуждается в настройке**: неправильно настроенный WAF может блокировать легитимные запросы или пропускать угрозы.
2. **Не защищает серверы от всех типов атак**: WAF фокусируется на веб-приложениях, но не защищает инфраструктуру в целом.
3. **Стоимость**: облачные и аппаратные решения могут быть дорогостоящими.

Типичные сценарии применения WAF

1. Защита сайтов и веб-приложений от атак злоумышленников.
2. Снижение вероятности успешной эксплуатации нулевых уязвимостей (Zero-Day).
3. Соответствие стандартам безопасности, таким как PCI DSS.
4. Защита от ботов и автоматизированных атак.

Популярные решения WAF

1. **Cloudflare WAF** — облачный сервис с защитой от DDoS.
2. **AWS WAF** — решение для защиты приложений, размещённых в AWS.
3. **Imperva WAF** — популярное корпоративное решение.
4. **F5 Advanced WAF** — защита с функциями анализа поведения.

WAF — это важный инструмент в современном ландшафте киберугроз, который помогает обеспечивать безопасность веб-приложений и защищать данные пользователей.

1. **SSL/TLS-декриптование**: анализ зашифрованного трафика для обнаружения угроз.

Преимущества использования WAF

- **Защита веб-приложений**: предотвращение атак на уязвимости в коде.
- **Гибкость настройки**: возможность адаптации под специфические требования приложений.
- **Легкость внедрения**: особенно для облачных решений, которые не требуют сложной настройки.

Ограничения WAF

1. **Ложные срабатывания**: некоторые запросы могут быть ошибочно заблокированы.
2. **Ограниченная защита**: WAF не защищает от атак, направленных на сервер или сеть.
3. **Необходимость обновлений**: для эффективной работы требуется регулярное обновление правил.

Примеры использования WAF

- Интернет-магазины используют WAF для защиты платежных данных.
- Финансовые организации применяют WAF для предотвращения утечек информации.
- Социальные сети защищают свои платформы от атак на аккаунты пользователей.

Заключение
Web Application Firewall (WAF) — это важный инструмент для обеспечения безопасности веб-приложений. Он играет ключевую роль в защите от современных угроз и помогает минимизировать риски кибератак. Однако для максимальной эффективности WAF должен быть частью комплексной стратегии информационной безопасности.

3 ТЕМА 3: DCShadow

DCShadow — это техника атак на инфраструктуру Active Directory (AD), которая позволяет злоумышленникам скрытно изменять данные в каталоге, обходя стандартные механизмы безопасности и журналирования. Эта техника была впервые представлена исследователями безопасности из компании Mimikatz и направлена на злоупотребление функционалом Active Directory, предназначенным для синхронизации данных между контроллерами домена.

Суть атаки DCShadow

В нормальной работе Active Directory изменения в каталоге вносятся контроллерами домена (Domain Controllers), которые синхронизируют данные между собой. Техника DCShadow позволяет злоумышленнику:

1. Регистрировать поддельный "контроллер домена" в инфраструктуре AD.
2. Использовать этот поддельный DC для внесения изменений в каталоге, например, изменения прав доступа, добавления учетных записей или модификации привилегий.
3. Изменения выглядят легитимными, так как они исходят от якобы доверенного контроллера домена.

Как работает DCShadow

1. **Имитация контроллера домена**: Злоумышленник использует скомпрометированную учетную запись с высокими привилегиями (например, учетную запись с правами администратора домена) для регистрации поддельного контроллера домена в каталоге.
2. **Репликация данных**: С помощью инструментов, таких как Mimikatz, злоумышленник запускает репликацию изменений в Active Directory, которые выглядят как данные, поступившие от легитимного DC.
3. **Внесение скрытых изменений**: Поддельный DC отправляет изменения в каталог, например:
    - Назначение привилегий пользователям.
    - Изменение атрибутов учетных записей (например, паролей).
    - Создание новых учетных записей или объектов.
4. **Обход стандартного журналирования**: Изменения, внесённые через DCShadow, не фиксируются стандартными журналами безопасности, так как процесс выглядит легитимным с точки зрения AD.

Пререквизиты для успешной атаки

- Злоумышленник должен иметь доступ к учетной записи с привилегиями администратора домена или аналогичными правами.
- Необходимы инструменты, такие как Mimikatz, для реализации техники.
- Доступ к сети организации, в которой развернут Active Directory.

Возможности атак DCShadow

1. **Назначение прав и ролей**: Увеличение привилегий существующим учетным записям или создание новых учетных записей с административными правами.
2. **Модификация политики безопасности**: Изменение групповых политик или конфигурации учетных записей.
3. **Устранение следов**: Откат внесённых изменений после выполнения атаки, что делает её крайне сложной для обнаружения.

Последствия атаки

- **Компрометация инфраструктуры AD**: Полный контроль над доменом, включая учетные записи, устройства и политики.
- **Скрытность**: Атака практически не оставляет следов в стандартных журналах событий.
- **Устойчивость атакующего**: Возможность создавать скрытые бэкдоры в системе.

Как защититься от DCShadow

1. **Минимизация прав доступа**:
    - Используйте принцип минимально необходимых привилегий для учетных записей.
    - Ограничьте доступ к административным учетным записям.
2. **Жёсткий контроль над AD**:
    - Регулярно проверяйте контроллеры домена и их репликации.
    - Используйте мониторинг для отслеживания аномальных изменений в AD.
3. **Внедрение защитных инструментов**:
    - Используйте системы обнаружения угроз (IDS/IPS) и специализированные инструменты для мониторинга AD.
    - Включите защиту от изменений схемы AD, ограничив доступ к соответствующим функциям.
4. **Журналирование и аудит**:
    - Настройте дополнительные средства аудита для контроля изменений в AD.

- Используйте сторонние инструменты, такие как Purple Knight или BloodHound, для анализа уязвимостей AD.

5. **Сегментация сети**:
   - Изолируйте инфраструктуру AD от общедоступных ресурсов.
   - Контролируйте доступ к сети через VPN и двухфакторную аутентификацию.

Итог

DCShadow — это мощная и опасная техника, которая требует от организаций повышенного внимания к безопасности Active Directory. Регулярный аудит инфраструктуры и внедрение современных средств защиты помогут минимизировать риск реализации подобных атак.

4 TEMA 4: DNS ICMP SSH

DNS (Domain Name System)

DNS — это система доменных имен, которая переводит понятные человеку имена доменов (например, `example.com`) в IP-адреса, необходимые для работы сетевых устройств. DNS является важной частью интернета и других сетевых технологий, так как без него пользователи должны были бы запоминать числовые IP-адреса для доступа к веб-сайтам или сервисам.

Основные компоненты DNS:

1. **DNS-клиент (резолвер)**: устройство или программа, которая запрашивает доменное имя и получает соответствующий IP-адрес.
2. **DNS-сервер**: сервер, который обрабатывает запросы и предоставляет информацию о доменных именах.
3. **Зоны и зоны авторитета**:
   - **Авторитетные серверы** — отвечают за конкретные доменные зоны (например, `.com`, `.org`).
   - **Рекурсивные серверы** — осуществляют поиск информации, обращаясь к другим DNS-серверам.

Принцип работы DNS:

1. Пользователь вводит адрес сайта (например, `example.com`) в браузер.
2. Запрос отправляется к локальному DNS-резолверу.
3. Если резолвер не знает IP-адрес, он обращается к рекурсивным DNS-серверам.
4. Рекурсивный сервер передаёт запрос к корневым, TLD и авторитетным серверам, чтобы найти IP-адрес.
5. Полученный IP-адрес возвращается пользователю.

Угрозы и защита:

- **DNS-спуфинг**: атака, при которой злоумышленник подменяет записи DNS, перенаправляя пользователей на фальшивые сайты.
- **DDoS-атаки на DNS**: злоумышленники перегружают серверы большим количеством запросов.
- **Защита**: использование DNSSEC, фильтрация запросов, резервирование серверов.

ICMP (Internet Control Message Protocol)

ICMP — это протокол межсетевых управляющих сообщений, используемый для передачи информации о состоянии сети, диагностики и устранения неполадок. Протокол не используется для передачи данных, но помогает определить работоспособность сетевых узлов и маршрутов.

Основные функции ICMP:

1. **Проверка доступности**:
   - Используется в утилите `ping` для проверки доступности узла.
2. **Диагностика маршрутов**:
   - Утилита `traceroute` показывает путь прохождения пакетов через сеть.
3. **Сообщения об ошибках**:
   - Например, сообщение о том, что узел недоступен или маршрут не найден.

Угрозы и защита:

- **ICMP-флудинг**: злоумышленник посылает большое количество ICMP-запросов, перегружая сеть.
- **ICMP-redirect-атаки**: злоумышленник подменяет маршруты в сети.
- **Защита**: ограничение ICMP-трафика с помощью настроек фаервола.

SSH (Secure Shell)

SSH — это протокол безопасного удалённого управления и передачи данных между устройствами. SSH используется для администрирования серверов, безопасного копирования файлов, туннелирования и шифрования соединений.

Основные компоненты SSH:

1. **SSH-клиент**: программа, установленная на устройстве пользователя, которая инициирует соединение с сервером.
2. **SSH-сервер**: приложение, принимающее запросы от клиента и обеспечивающее доступ.
3. **Шифрование**: использование асимметричной и симметричной криптографии для защиты данных.

Принцип работы SSH:

1. Клиент устанавливает соединение с сервером, передавая свой открытый ключ.
2. Сервер аутентифицирует клиента, используя ключи или пароль.
3. После успешной аутентификации данные передаются в зашифрованном виде.

Угрозы и защита:

- **Брутфорс-атаки**: злоумышленники подбирают пароли к SSH.
- **Угнанные ключи**: если злоумышленник получает доступ к приватному ключу, он может подключиться к серверу.
- **Защита**:
  - Использование сложных паролей или ключей.
  - Ограничение по IP-адресам.
  - Настройка двухфакторной аутентификации.
  - Отключение входа под пользователем `root`.

Сравнение DNS, ICMP и SSH

Характеристика	DNS	ICMP	SSH
Назначение	Разрешение доменных имен	Диагностика сети	Безопасное управление
Тип протокола	Прикладной	Сетевой	Транспортный
Риски	Спуфинг, DDoS	Использование в атаках	Брутфорс, уязвимости
Области применения	Веб-сайты, домены	Ping, Traceroute	Серверное администрирование

DNS, ICMP и SSH — это важнейшие протоколы, обеспечивающие функционирование современных сетей. Каждый из них выполняет уникальные задачи, от разрешения имен до диагностики соединений и безопасного управления устройствами. Для эффективного использования этих протоколов необходимо учитывать их уязвимости и применять меры защиты, такие как шифрование, мониторинг и ограничение прав доступа.