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
Кузьмич В.Н.

Брест 2024

**1)NetFlow**

NetFlow — технология, разработанная Cisco Systems, которая предоставляет сетевым администраторам возможность собирать и анализировать данные о трафике в компьютерных сетях. Это помогает мониторингу, оптимизации сети, выявлению аномалий и обеспечению безопасности.

Первоначально представленная Cisco в середине 1990-х годов, NetFlow быстро стала популярной благодаря своей способности детально анализировать трафик. Основная концепция NetFlow заключается в разделении сетевого трафика на потоки, где каждый поток представляет собой набор пакетов с общими атрибутами, такими как IP-адреса источника и назначения, порты и тип протокола.

- **Принципы работы NetFlow**

NetFlow анализирует сетевой трафик и группирует его в потоки на основе ключевых параметров:

- IP-адрес источника
- IP-адрес назначения
- Порт источника
- Порт назначения
- Протокол транспортного уровня
- Интерфейс маршрутизатора

Данные о завершенных потоках отправляются на серверы для хранения и анализа, что помогает создавать отчеты и визуализации для понимания структуры трафика.

**Основные компоненты NetFlow**

- Экспортер — устройство, собирающее данные о потоках и отправляющее их в хранилище.
- Коллектор — система, принимающая данные от экспортера для последующего анализа.
- Анализатор — инструмент, интерпретирующий данные, предоставляя графики, диаграммы и статистику.

**Области применения NetFlow**

- Мониторинг сети: отслеживание объема трафика и выявление узких мест.
- Оптимизация производительности: оптимизация маршрутов передачи данных на основе анализа трафика.
- Обеспечение безопасности: выявление аномалий и потенциальных угроз.
- Биллинг: расчет использования сети для выставления счетов пользователям.

**Аналоги и развитие технологии**

Помимо NetFlow, существуют другие технологии для мониторинга сети, такие как sFlow, IPFIX и J-Flow. В последние годы анализ трафика

интегрируется с искусственным интеллектом для более точного обнаружения угроз.

NetFlow остается одной из наиболее эффективных технологий для мониторинга и анализа сетевого трафика, широко применяющейся благодаря своей универсальности и точности. С развитием сетей и увеличением объема данных, роль таких инструментов, как NetFlow, будет только возрастать.

## 2)WAF

С развитием интернета и увеличением числа веб-приложений возрастает угроза кибератак, нацеленных на их уязвимости. Web Application Firewall (WAF) — это важный инструмент защиты веб-приложений, обеспечивающий защиту от таких угроз, как SQL-инъекции, XSS (межсайтовый скриптинг) и атаки на основе HTTP.

**Что такое WAF?**

WAF — это программный или аппаратный инструмент, который анализирует и фильтрует HTTP/HTTPS-трафик между пользователем и веб-приложением. Его основная задача — выявлять и блокировать вредоносные запросы, защищая приложение от известных и неизвестных атак.

**Принципы работы WAF**

WAF работает на уровне HTTP/HTTPS-протоколов, используя несколько методов для защиты:

- Сигнатурный анализ: сравнение запросов с базой известных атак.
- Поведенческий анализ: определение подозрительной активности на основе поведения пользователей.
- Фильтрация по правилам: создание специальных правил для блокировки определенных типов запросов.

**WAF может работать в режимах:**

- Мониторинг (passive mode): анализ трафика без блокировки.
- Блокировка (active mode): блокировка подозрительных запросов в реальном времени.

**Типы WAF**

- Аппаратные WAF: физические устройства, устанавливаемые в инфраструктуре компании. Пример — F5 Networks.
- Программные WAF: работают как ПО на сервере. Пример — ModSecurity.

Облачные WAF: сервисы, такие как AWS WAF, Cloudflare и Imperva.

**Основные функции WAF**

- Защита от OWASP Top 10: защита от распространенных уязвимостей, таких как SQL-инъекции и XSS.
- Мониторинг и логирование: регистрация подозрительных запросов для анализа.
- Обнаружение и предотвращение DDoS-атак: фильтрация трафика для защиты от перегрузок.
- SSL/TLS-декриптование: анализ зашифрованного трафика для выявления угроз.

**Преимущества использования WAF**

- Защита веб-приложений: предотвращение атак на уязвимости в коде.
- Гибкость настройки: адаптация под специфические требования приложений.
- Легкость внедрения: особенно для облачных решений, не требующих сложной настройки.

**Ограничения WAF**

- Ложные срабатывания: вероятность ошибочной блокировки запросов.
- Ограниченная защита: WAF не защищает от атак на сервер или сеть.
- Необходимость обновлений: 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.

**Вывод:**

Web Application Firewall (WAF) — важный инструмент для обеспечения безопасности веб-приложений, играющий ключевую роль в защите от современных угроз. Однако для максимальной эффективности WAF должен быть частью комплексной стратегии информационной безопасности.

**3)DCShadow**

В современных корпоративных сетях безопасность Active Directory (AD) играет важную роль. Одной из наиболее опасных техник, применяемых злоумышленниками для компрометации Active Directory, является атака DCShadow. Она позволяет изменять критически важные данные в AD, оставаясь незамеченной для большинства систем мониторинга. В данном реферате рассмотрены принципы работы DCShadow, риски, связанные с этой техникой, и методы защиты.

**Что такое DCShadow?**

DCShadow — это техника, впервые описанная специалистами по кибербезопасности в 2018 году. Она используется для нелегитимных изменений в Active Directory, имитируя поведение легального контроллера домена (Domain Controller, DC). Атака заключается в регистрации устройства злоумышленника как временного контроллера домена и внесении изменений в реплицируемые данные AD, такие как права пользователей или конфигурация GPO.

**Принципы работы DCShadow**

DCShadow использует протоколы репликации AD, такие как Directory Replication Service Remote Protocol (DRSR), чтобы обойти стандартные механизмы защиты. Основные этапы атаки:

- Получение высоких привилегий: Злоумышленник получает права администратора домена.
- Регистрация поддельного контроллера домена: С помощью инструментов, таких как Mimikatz, злоумышленник регистрирует свое устройство как DC.
- Внесение изменений: Злоумышленник отправляет изменения в AD, которые реплицируются на легитимные контроллеры домена.
- Удаление следов: После атаки злоумышленник удаляет запись о поддельном

DC, чтобы скрыть свои действия.

**Опасности DCShadow**

- Скрытность: Изменения, сделанные через DCShadow, не фиксируются стандартными инструментами мониторинга, такими как журнал событий Windows.
- Масштаб влияния: Атака затрагивает всю инфраструктуру AD.
- Изменение критически важных данных: Злоумышленники могут модифицировать права доступа, учетные записи или создать "невидимые" учетные записи.

**Необходимые условия для атаки**

- Для успешной атаки DCShadow злоумышленнику требуются:
- Доступ к административным учетным записям.
- Доступ к инструментам, таким как Mimikatz.
- Прямой доступ к контроллеру домена или сетевому соединению с ним.

**Методы защиты от DCShadow**

- Ограничение прав доступа: Минимизация числа пользователей с правами администратора домена.
- Мониторинг изменений в AD: Использование специализированных инструментов, таких как Microsoft Advanced Threat Analytics (ATA) или SIEM-системы.
- Обнаружение подозрительных репликаций: Отслеживание вызовов DRSR-протокола.
- Усиление аутентификации: Использование многофакторной аутентификации (MFA) для критически важных учетных записей.
- Периодический аудит AD: Регулярная проверка изменений в конфигурации и правах доступа.

**Инструменты для выполнения DCShadow**

Одним из наиболее известных инструментов, используемых для реализации DCShadow, является Mimikatz — утилита с открытым исходным кодом для работы с учетными данными Windows. В Mimikatz встроен модуль для выполнения DCShadow, который позволяет злоумышленникам выполнять описанные выше действия.

**Вывод:**

DCShadow — одна из самых сложных и опасных техник атак на Active Directory. Она требует высокого уровня подготовки, но предоставляет злоумышленникам практически неограниченные возможности для компрометации инфраструктуры. Для защиты от DCShadow необходимы комплексные меры, включающие усиление контроля доступа, мониторинг активности в сети и регулярный аудит AD.

**4)DNS, ICMP, SSH**

Современные компьютерные сети используют множество протоколов, обеспечивающих их функциональность, производительность и безопасность. Среди наиболее значимых — DNS (Domain Name System), ICMP (Internet Control Message Protocol) и SSH (Secure Shell). Каждый из этих протоколов выполняет свою уникальную задачу: от разрешения доменных имен до безопасного управления устройствами. Рассмотрим основные функции, принципы работы и области применения этих протоколов.

**DNS (Domain Name System)**

Назначение: DNS — это система, которая преобразует доменные имена (например, example.com) в IP-адреса, необходимые для взаимодействия устройств в сети.

**Принципы работы:**

- Пользователь вводит доменное имя в браузере.
- Запрос отправляется на DNS-сервер, который ищет соответствующий IP-адрес.
- Если DNS-сервер не знает адрес, он передает запрос на вышестоящие серверы, включая корневые DNS.
- После нахождения IP-адреса он возвращается клиенту, и начинается соединение с нужным сервером.

**Основные компоненты DNS:**

- Рекурсивные резолверы: обрабатывают запросы от клиентов.
- Авторитетные серверы: хранят информацию о доменных зонах.
- Корневые серверы: содержат информацию о верхних уровнях доменов (например, .com, .org).

**Риски и уязвимости:**

- DNS-спуфинг: подмена ответа DNS-сервера.
- DDoS-атаки на DNS-серверы.
- Утечка данных через DNS-запросы.

**Области применения:**

- Веб-серфинг.
- Корпоративные сети.
- Системы управления доменами.

**ICMP (Internet Control Message Protocol)**

ICMP — это протокол, используемый для диагностики сетей и передачи сообщений об ошибках. Он помогает определять доступность устройств и устранять проблемы с соединением.

ICMP не передает данные пользователя, а используется для обмена служебной информацией. Основные типы ICMP-сообщений:

- Echo Request и Echo Reply: используются в утилите ping для проверки доступности узлов.
- Destination Unreachable: сообщает, что устройство или сеть недоступны.
- Time Exceeded: указывает, что время жизни пакета (TTL) истекло.

**Примеры использования:**

- Ping: Проверка доступности устройства.
- Traceroute: Определение маршрута пакетов до конечного узла.

**Риски и уязвимости:**

- Использование ICMP в DDoS-атаках (например, Ping Flood).
- ICMP-редиректы могут быть использованы для перенаправления трафика на вредоносные узлы.

**SSH (Secure Shell)**

Назначение: SSH — это протокол для безопасного удаленного управления устройствами и передачи данных. Он обеспечивает шифрование соединений, аутентификацию и защиту от атак.

**Принципы работы:** SSH использует криптографические алгоритмы для шифрования данных и аутентификации. Основные этапы работы:

- Установление соединения между клиентом и сервером.
- Аутентификация пользователя (по паролю или с использованием ключей).

- Шифрование передаваемых данных.

**Основные компоненты SSH**:

- SSH-клиент: программа на стороне пользователя.
- SSH-сервер: программа, принимающая соединения.
- SSH-ключи: используются для аутентификации без пароля.

**Области применения:**

- Управление серверами.
- Передача файлов (SCP, SFTP).
- Туннелирование трафика.

**Риски и уязвимости:**

- Брутфорс-атаки на учетные записи.
- Уязвимости в реализации протокола.
- Неправильная конфигурация, позволяющая несанкционированный доступ.

**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 — 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.