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
Полиенко В.Э.

Брест 2024

1 ТЕМА 1: netflow

NetFlow — это технология, разработанная компанией Cisco Systems, которая предоставляет сетевым администраторам возможность сбора и анализа данных о трафике в компьютерных сетях. Она используется для мониторинга, оптимизации сети, а также для выявления аномалий и обеспечения безопасности.

NetFlow была впервые представлена Cisco в середине 1990-х годов как инструмент для маршрутизаторов, позволяющий собирать информацию о потоках данных. Технология быстро завоевала популярность благодаря своей способности детально анализировать трафик. Основная идея NetFlow заключается в том, чтобы разделять сетевой трафик на потоки, где каждый поток представляет собой набор пакетов, имеющих общие атрибуты, такие как IP-адреса источника и назначения, порты, тип протокола и другие параметры.

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

1. IP-адрес источника.
2. IP-адрес назначения.
3. Порт источника.
4. Порт назначения.
5. Протокол транспортного уровня.
6. Интерфейс маршрутизатора.

После завершения потока данные передаются на серверы для хранения и анализа. Эта информация используется для создания отчетов и визуализации, которые помогают понять структуру трафика.

Основные компоненты NetFlow

1. **Экспортер** — устройство, которое собирает данные о потоках и экспортирует их в хранилище.
2. **Коллектор** — система, принимающая данные от экспортера для последующего анализа.
3. **Анализатор** — инструмент, интерпретирующий данные для пользователя, предоставляя графики, диаграммы и статистику.

Области применения NetFlow

1. **Мониторинг сети**: позволяет сетевым администраторам отслеживать объем трафика, определять загруженные участки сети и выявлять узкие места.
2. **Оптимизация производительности**: анализ трафика помогает оптимизировать маршруты передачи данных.
3. **Обеспечение безопасности**: обнаружение аномалий и потенциальных угроз, таких как DDoS-атаки или несанкционированный доступ.
4. **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 технологии анализа трафика развиваются, интегрируясь с искусственным интеллектом для более точного обнаружения угроз.

NetFlow остается одной из самых эффективных технологий для мониторинга и анализа сетевого трафика. Она широко используется во многих организациях благодаря своей универсальности и высокой точности. В будущем, с развитием сетей и увеличением объема данных, роль таких инструментов, как NetFlow, будет только возрастать.

2 ТЕМА 2: WAF

С развитием интернета и увеличением числа веб-приложений растет угроза кибератак, направленных на уязвимости приложений. Одним из ключевых инструментов защиты веб-приложений является Web Application Firewall (WAF) — межсетевой экран для веб-приложений, который обеспечивает защиту от широкого спектра угроз, таких 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 и использует несколько методов для защиты:

1. **Сигнатурный анализ**: сравнение входящих запросов с базой известных атак.
2. **Поведенческий анализ**: определение подозрительной активности на основе поведения пользователей.
3. **Фильтрация по правилам**: настройка специальных правил для блокировки определенных типов запросов.

WAF может работать в одном из следующих режимов:

- **Режим мониторинга (passive mode)**: трафик анализируется, но не блокируется.
- **Режим блокировки (active mode)**: подозрительные запросы блокируются в реальном времени.

Типы WAF

1. **Аппаратные WAF**: представляют собой физические устройства, устанавливаемые в инфраструктуре компании. Пример — F5 Networks.
2. **Программные WAF**: работают как ПО, установленное на сервере. Пример — ModSecurity.
3. **Облачные WAF**: предоставляются как сервисы, такие как AWS WAF, Cloudflare и Imperva.

Основные функции WAF

1. **Защита от OWASP Top 10**: WAF защищает от наиболее распространенных уязвимостей, включая SQL-инъекции, XSS и утечку данных.
2. **Мониторинг и логирование**: WAF регистрирует информацию о подозрительных запросах для анализа и расследования.
3. **Обнаружение и предотвращение DDoS-атак**: фильтрация трафика для предотвращения перегрузки серверов.

4. **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

Введение
В современных корпоративных сетях безопасность Active Directory (AD) играет ключевую роль. Одной из наиболее опасных техник, используемых злоумышленниками для компрометации Active Directory, является атака DCShadow. Эта техника позволяет злоумышленникам изменять критические данные в AD, оставаясь незамеченными для большинства систем мониторинга. В данном реферате рассматриваются 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 выполнения нелегитимных изменений в Active Directory, имитируя поведение легального контроллера домена (Domain Controller, DC). Суть атаки заключается в том, что злоумышленник регистрирует свое устройство как временный контроллер домена и вносит изменения 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:

1. **Получение высоких привилегий**: для выполнения атаки злоумышленнику необходимы права администратора домена.
2. **Регистрация поддельного контроллера домена**: злоумышленник использует инструменты, такие как Mimikatz, чтобы зарегистрировать свое устройство как DC.
3. **Внесение изменений**: злоумышленник отправляет изменения в AD, которые затем реплицируются на легитимные контроллеры домена.
4. **Удаление следов**: после выполнения атаки злоумышленник удаляет запись о поддельном DC, чтобы скрыть свои действия.

Опасности DCShadow

- **Скрытность**: изменения, выполненные через DCShadow, не фиксируются стандартными инструментами мониторинга, такими как журнал событий Windows.
- **Масштаб влияния**: атака затрагивает всю инфраструктуру AD, что делает её чрезвычайно опасной.
- **Изменение критически важных данных**: злоумышленники могут модифицировать права доступа, учетные записи или даже создать "невидимые" учетные записи.

Необходимые условия для атаки
Для успешного выполнения DCShadow злоумышленнику требуются:

1. **Доступ к административным учетным записям**.
2. **Доступ к инструментам, таким как Mimikatz**.
3. **Прямой доступ к контроллеру домена или сетевому соединению с ним**.

Методы защиты от DCShadow

1. **Ограничение прав доступа**: минимизация числа пользователей с правами администратора домена.
2. **Мониторинг изменений в AD**: использование специализированных инструментов, таких как Microsoft Advanced Threat Analytics (ATA) или SIEM-системы.
3. **Обнаружение подозрительных репликаций**: отслеживание вызовов DRSR-протокола.
4. **Усиление аутентификации**: использование многофакторной аутентификации (MFA) для критически важных учетных записей.
5. **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, предназначенная для работы

с учетными данными Windows. В Mimikatz встроен модуль для выполнения DCShadow, который позволяет злоумышленникам выполнять описанные выше действия.

DCShadow — это одна из самых сложных и опасных техник атак на Active Directory. Она требует высокого уровня подготовки, но при этом 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 ТЕМА 4: DNS ICMP SSH

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

---

1. DNS (Domain Name System)

Назначение
DNS — это система доменных имен, которая преобразует понятные человеку доменные имена (например, example.com) в IP-адреса, необходимые для взаимодействия между устройствами в сети.

Принципы работы

1. Пользователь вводит доменное имя в браузере.
2. Запрос отправляется на DNS-сервер, который ищет соответствующий IP-адрес.
3. Если DNS-сервер не знает адрес, он передает запрос на вышестоящие серверы, включая корневые DNS.
4. 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.

---

2. 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

1. **Ping**: проверка доступности устройства.
2. **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.

---

3. 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:

1. Установление соединения между клиентом и сервером.
2. Аутентификация пользователя (по паролю или с использованием ключей).
3. 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 — 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.