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

Исаенко Н.Д.

Брест 2024

1. NetFlow

NetFlow — это уникальная технология, разработанная компанией Cisco, которая служит мощным инструментом для контроля и анализа сетевого трафика. Она позволяет глубоко исследовать и управлять сетевыми потоками, что особенно важно для диагностики сети, обеспечения безопасности и повышения производительности.

Основные функции NetFlow

NetFlow предлагает обширный набор функций, позволяющих собирать, анализировать и визуализировать данные о сетевом трафике. К основным возможностям относятся:

- Сбор информации о сетевых потоках (flows).
- Экспорт собранных данных для последующего анализа.
- Определение источников и назначения трафика.
- Диагностика проблем в сети.

Принципы работы NetFlow

NetFlow собирает данные о каждом сетевом потоке, который проходит через устройство, поддерживающее эту технологию. Каждый поток в NetFlow определяется сочетанием следующих параметров:

- IP-адрес отправителя.
- IP-адрес получателя.
- Номера портов источника и назначения.
- Протокол уровня транспортного слоя (TCP/UDP).
- Класс обслуживания (ToS).
- Интерфейсы ввода и вывода на устройстве.

Собранные данные потока сохраняются в кэш-памяти устройства и затем экспортируются на сервер для дальнейшего анализа.

Компоненты NetFlow

NetFlow состоит из трех ключевых компонентов:

1. **NetFlow Exporter** — собирает информацию о сетевых потоках и отправляет ее в заданный коллектор.
2. **NetFlow Collector** — принимает экспортируемые данные, сохраняет их и подготавливает для анализа.
3. **NetFlow Analyzer** — предлагает инструменты для анализа и визуализации собранных данных.

Преимущества NetFlow

NetFlow обладает рядом преимуществ, которые делают его незаменимым инструментом для мониторинга и управления сетями:

- **Обнаружение аномалий**: помогает выявлять подозрительные действия, такие как DDoS-атаки и сканирование портов.
- **Мониторинг производительности сети**: позволяет определять узкие места и балансировать нагрузку.
- **Учет и биллинг**: предоставляет данные для анализа использования сети различными пользователями и приложениями.

Применение NetFlow

NetFlow находит широкое применение в различных сферах:

1. **Сетевая безопасность**: помогает обнаруживать вторжения и аномальное поведение.
2. **Оптимизация работы сети**: выявляет перегруженные сегменты и улучшает качество обслуживания (QoS).
3. **Диагностика и устранение неисправностей**: предоставляет информацию для быстрого решения проблем.
4. **Планирование емкости сети**: помогает предсказывать будущие потребности в пропускной способности.

Ограничения NetFlow

Несмотря на все свои преимущества, NetFlow также имеет некоторые ограничения:

- **Объем данных**: обработка большого объема информации может потребовать значительных ресурсов.
- **Задержка анализа**: экспорт данных на сервер может занимать время, что ограничивает использование NetFlow в реальном времени.

- **Зависимость от производителя**: изначально NetFlow был разработан Cisco, но существуют аналоги от других производителей, такие как sFlow и IPFIX.

Инструменты для работы с NetFlow

На рынке представлено множество решений для работы с NetFlow, среди которых выделяются:

- SolarWinds NetFlow Traffic Analyzer.
- PRTG Network Monitor.
- ManageEngine NetFlow Analyzer.
- Cisco Prime Infrastructure.

Заключение

NetFlow — это мощная технология для мониторинга и управления сетями, предоставляющая ценные данные для анализа трафика, диагностики проблем и обеспечения безопасности. Несмотря на некоторые ограничения, ее преимущества делают NetFlow незаменимым инструментом для администраторов и инженеров сетей в современном мире.

2. WAF (Web Application Firewall)

WAF (Web Application Firewall) — это специализированное программное или аппаратное решение, разработанное для защиты веб-приложений от различных угроз. Его основная задача заключается в фильтрации, анализе и блокировке вредоносного трафика на уровне HTTP/HTTPS, что позволяет предотвратить эксплойты, направленные на уязвимости в веб-приложениях.

Основные функции WAF

· **Защита от наиболее распространенных угроз**: WAF предотвращает атаки, включая OWASP Top 10, такие как SQL-инъекции, XSS (межсайтовый скриптинг) и CSRF (межсайтовая подделка запросов).

· **Мониторинг HTTP-запросов в реальном времени**: WAF непрерывно отслеживает все HTTP-запросы, что позволяет оперативно выявлять подозрительную активность и предотвращать потенциальные угрозы.

· **Логирование и отчетность**: WAF обеспечивает запись и анализ событий, что помогает создать детальные отчеты о происходящих угрозах и принимать меры для их устранения.

· **Блокировка ботов и автоматизированных атак**: WAF эффективно защищает от ботнетов и других автоматизированных атак, предотвращая доступ злоумышленников к системам.

Принципы работы WAF

WAF анализирует HTTP/HTTPS-запросы и ответы, которые проходят между клиентами и веб-приложением, используя различные подходы:

1. **Подход на основе сигнатур**:
   – Использует заранее определенные шаблоны атак (сигнатуры) для распознавания известных угроз. Этот подход хорошо подходит для защиты от уже известных атак, но может быть уязвим к новым.
2. **Поведенческий анализ**:
   – WAF отслеживает поведение пользователей и выявляет аномалии, которые могут указывать на возможные атаки. Однако для этого требуется настройка и обучение системы для распознавания нормального поведения.

3. **Гибридный подход**:
   – Объединяет сигнатурный и поведенческий анализ, обеспечивая более широкую защиту.

Типы WAF

Существует несколько типов WAF:

1. **Облачные WAF**:
   – Преимущества: простота настройки, масштабируемость и минимальные затраты на обслуживание.
   – Примеры: Cloudflare WAF и AWS WAF.
2. **Локальные WAF (On-Premises)**:
   – Преимущества: полный контроль над конфигурацией и логами.
   – Используются в корпоративных сетях с высокими требованиями безопасности.
3. **Гибридные WAF**:
   – Сочетают преимущества облачных и локальных решений, предоставляя гибкость и возможность настройки.

Преимущества использования WAF

Использование WAF имеет множество преимуществ:

· **Защита данных**: WAF предотвращает утечки и компрометацию конфиденциальной информации, обеспечивая безопасность пользователей.

· **Соответствие нормативным требованиям**: WAF помогает соответствовать стандартам безопасности, таким как PCI DSS и GDPR.

· **Легкость управления**: WAF предоставляет возможность централизованного управления и мониторинга, что упрощает процессы защиты.

· **Гибкость в настройке**: WAF позволяет адаптировать политики безопасности под конкретные приложения, обеспечивая адаптивную защиту.

Ограничения WAF

Несмотря на множество преимуществ, WAF имеет некоторые ограничения:

· **Ложные срабатывания**: WAF может блокировать легитимные запросы, если политики настроены слишком строго.

· **Необходимость обновлений**: Сигнатурный анализ требует регулярного обновления баз угроз, что может быть затруднительным для небольших организаций.

· **Невозможность устранения уязвимостей**: WAF защищает от атак, но не устраняет исходные проблемы в коде приложения, что может потребовать дополнительных мер.

Популярные решения WAF

На рынке представлено множество популярных решений WAF, среди которых:

- **Cloudflare WAF**: Облачное решение с возможностью интеграции в любой веб-сайт.
- **AWS WAF**: Решение для защиты приложений, работающих в экосистеме AWS.
- **Imperva**: Мощный инструмент с широкими функциями аналитики и защиты.
- **F5 Advanced WAF**: Решение с поддержкой машинного обучения для анализа поведения.

Примеры атак, предотвращаемых WAF

WAF способен предотвратить множество атак, включая:

1. **SQL-инъекции**: Попытки внедрить вредоносные SQL-запросы в приложение для получения несанкционированного доступа к данным.
2. **XSS (межсайтовый скриптинг)**: Внедрение вредоносных скриптов для выполнения на стороне пользователя.
3. **DDoS-атаки**: Фильтрация чрезмерного трафика для предотвращения перегрузки системы.
4. **Path Traversal**: Защита от атак, направленных на получение доступа к файлам на сервере.

Настройка WAF

Настройка WAF включает в себя несколько этапов:

1. **Определение политик безопасности**: Установление правил, определяющих, какие запросы разрешены, а какие блокируются.
2. **Обучение системы**: Обучение системы распознаванию нормального трафика для более точной фильтрации.
3. **Мониторинг и анализ логов**: Постоянный мониторинг и анализ логов позволяет корректировать правила и настройки WAF для обеспечения максимальной защиты.

Заключение

WAF является важным компонентом комплексной системы защиты веб-приложений, позволяя минимизировать риски, связанные с современными веб-угрозами, и обеспечивая высокий уровень безопасности данных и приложений. Несмотря на некоторые ограничения, грамотная настройка и использование WAF значительно снижают вероятность успешной реализации атак.

3. DCShadow

DCShadow представляет собой современную технологию, применяемую злоумышленниками для взлома инфраструктуры Active Directory (AD). С помощью этой техники злоумышленники могут зарегистрировать фальшивый контроллер домена (DC) в сети и вносить изменения в базу данных AD, избегая регистрации в стандартных журналах событий безопасности.

Принципы работы DCShadow

Ключевая идея DCShadow заключается в подделке репликации данных Active Directory. Этот процесс осуществляется в несколько этапов:

1. **Создание ложного контроллера домена**: Злоумышленник регистрирует фальшивый контроллер, который взаимодействует с существующими DC через механизм репликации AD.
2. **Модификация данных AD**: Через ложный контроллер домена злоумышленник вносит изменения в конфигурацию AD, включая добавление учетных записей, изменение привилегий или конфигурации политики безопасности.
3. **Отсутствие логирования**: Поскольку изменения вносятся через механизм репликации, стандартные инструменты мониторинга безопасности, такие как SIEM, не фиксируют эти действия.

Используемые протоколы и механизмы

DCShadow опирается на следующие компоненты и механизмы AD:

- **MS-DRSR (Microsoft Directory Replication Service Remote Protocol)**: Протокол, обеспечивающий репликацию данных между контроллерами домена.
- **LDAP (Lightweight Directory Access Protocol)**: Протокол для доступа и управления объектами в AD.
- **API-интерфейсы Windows**: Используются для выполнения вызовов, необходимых для регистрации ложного DC и проведения операций.

Последствия использования DCShadow

DCShadow имеет серьезные последствия для безопасности:

1. **Уход от обнаружения**: Злоумышленники могут скрыть свои действия, что делает их практически невидимыми для стандартных систем мониторинга.
2. **Повышение привилегий**: Злоумышленники могут изменить права доступа или создать учетные записи с повышенными привилегиями.
3. **Долгосрочный доступ**: Внесенные изменения могут остаться незамеченными длительное время, обеспечивая злоумышленникам постоянный доступ к ресурсам.

Примеры атак с использованием DCShadow

Рассмотрим несколько примеров атак, которые могут быть реализованы с помощью DCShadow:

1. **Добавление учетных записей с привилегиями администратора**: Злоумышленник может создать учетную запись и добавить ее в группу Domain Admins.
2. **Изменение настроек групповой политики (GPO):** В GPO могут быть добавлены вредоносные настройки для выполнения вредоносного кода на компьютерах пользователей.
3. **Изменение атрибутов объектов**: Например, можно изменить атрибут "msDS-AllowedToActOnBehalfOfOtherIdentity", чтобы получить контроль над учетной записью или устройством.

Обнаружение и защита от DCShadow

Для обнаружения и защиты от DCShadow рекомендуется придерживаться следующих мер:

1. **Мониторинг изменений в AD**: Используйте специализированные инструменты, такие как Microsoft Advanced Threat Analytics (ATA) или решения сторонних производителей, для отслеживания изменений в AD.
2. **Ограничение доступа к учетным данным**: DCShadow требует привилегированных учетных данных. Защитите учетные записи администраторов с помощью двухфакторной аутентификации и минимизации привилегий.
3. **Обновление и патчинг**: Регулярно обновляйте операционные системы и применяйте исправления безопасности для уязвимостей, связанных с протоколами репликации.

4. **Использование инструментов безопасности**: PowerShell-модуль "Active Directory" может помочь в обнаружении подозрительных объектов, таких как ложные контроллеры домена.
5. **Обучение сотрудников**: Повышайте осведомленность сотрудников IT-отдела о техниках DCShadow и связанных рисках.

Инструменты, связанные с DCShadow

К инструментам, используемым для реализации DCShadow, относятся:

- **Mimikatz**: Популярный инструмент для выполнения атак на инфраструктуру AD, включая реализацию DCShadow.
- **BloodHound**: Анализирует отношения между объектами AD и может быть использован для выявления потенциальных целей атак DCShadow.

Заключение

DCShadow представляет серьезную угрозу для безопасности Active Directory, особенно в крупных корпоративных сетях. Защита от таких атак требует комплексного подхода, включающего мониторинг, обучение персонала и использование специализированных инструментов безопасности. Понимание принципов работы DCShadow и реализация мер предосторожности помогут минимизировать риски и повысить уровень защиты вашей инфраструктуры.

4. DNS, ICMP, SSH

В этом разделе мы обсудим три ключевых элемента сетевого взаимодействия: протоколы DNS, ICMP и SSH. Каждый из них играет важнейшую роль в работе компьютерных сетей, но в то же время может стать целью или инструментом для атак.

DNS (Domain Name System)

DNS, или система доменных имен, представляет собой распределенную систему, которая преобразует понятные человеку доменные имена в IP-адреса, необходимые для взаимодействия устройств в сети. Благодаря DNS пользователи могут обращаться к сетевым ресурсам, используя удобные имена, такие как "example.com", вместо сложных IP-адресов.

Основные компоненты DNS:

1. **Доменное имя**: читаемая человеком строка, представляющая ресурс (например, "example.com").
2. **DNS-серверы**:
   – **Рекурсивные серверы**: выполняют поиск запрашиваемого имени и возвращают результат пользователю.
   – **Авторитетные серверы**: содержат оригинальную информацию о домене.
3. **Записи DNS**: типы данных, которые содержатся в системе (например, A, AAAA, MX, CNAME).

Уязвимости DNS:

1. **DNS Cache Poisoning (Отравление кэша)**: злоумышленник подставляет поддельные записи в кэш рекурсивного DNS-сервера, перенаправляя пользователей на вредоносные сайты.
2. **DDoS-атаки через DNS**: атаки типа Amplification используют уязвимости DNS для усиления трафика на целевой сервер.
3. **DNS Tunneling**: использование DNS-запросов для передачи данных, обхода файрволов и получения удаленного доступа.

Методы защиты DNS:

- **Использование DNSSEC (DNS Security Extensions)**: предотвращает подделку записей, подписывая их цифровыми подписями.
- **Настройка фильтров и мониторинга**: помогает обнаруживать аномалии в DNS-трафике.
- **Ограничение доступа к рекурсивным DNS-серверам**: обеспечивает безопасность и контроль над использованием этой системы.

ICMP (Internet Control Message Protocol)

ICMP — это протокол управления передачей данных в сети, который используется для диагностики и сообщения об ошибках. Наиболее известной функцией ICMP является команда "ping" для проверки доступности хоста.

Функции ICMP:

1. **Диагностика**: определение доступности узлов и измерение задержек.
2. **Сообщение об ошибках**: уведомление о недостижимости хоста, отказе маршрута и других проблемах.

Уязвимости ICMP:

1. **ICMP Flood**: атака, при которой нацеленный хост получает огромное количество ICMP-запросов, что приводит к его перегрузке.
2. **Smurf-атака**: злоумышленник использует широковещательные ICMP-запросы для перегрузки целевой системы.
3. **Reconnaissance-атаки**: ICMP может быть использован для сбора информации о сети, включая ее структуру и активные хосты.

Методы защиты ICMP:

- **Ограничение ICMP-трафика**: маршрутизаторы и файрволы могут ограничивать ICMP-трафик, защищая сеть от перегрузки.
- **Настройка правил**: правила могут предотвращать широковещательную передачу ICMP-запросов.
- **Мониторинг**: регулярный мониторинг аномального ICMP-трафика помогает выявлять и предотвращать потенциальные угрозы.

SSH (Secure Shell)

SSH, или безопасная оболочка, представляет собой криптографический протокол, обеспечивающий безопасное удаленное управление системами. SSH используется для выполнения команд на удаленных серверах, передачи файлов и туннелирования.

Функции SSH:

1. **Удаленный доступ**: безопасное управление серверами.
2. **Передача файлов**: через SCP или SFTP.
3. **Туннелирование**: шифрование трафика других приложений через SSH.

Уязвимости SSH:

1. **Brute-force атаки**: злоумышленники пытаются подобрать пароль, используя автоматизированные инструменты.
2. **Скомпрометированные ключи**: кража приватного SSH-ключа может позволить злоумышленнику получить доступ к системе.
3. **Слабая конфигурация**: использование устаревших алгоритмов шифрования или ненадежных настроек может привести к уязвимостям.

Методы защиты SSH:

- **Двухфакторная аутентификация (2FA)**: обеспечивает дополнительный уровень защиты, усложняя процесс подбора пароля.
- **Ограничение доступа по IP-адресам**: использование списков "Allow" и "Deny" помогает контролировать доступ к SSH-серверам.
- **Строгие правила использования SSH-ключей**: настройка правил использования и регулярная ротация ключей помогают обеспечить безопасность и надежность.
- **Отключение root-доступа**: отключение доступа по SSH помогает предотвратить несанкционированный доступ к корневым учетным записям.
- **Включение современных версий**: использование протоколов последних версий, таких как SSHv2, обеспечивает повышенную безопасность.

Сравнение DNS, ICMP и SSH

Заключение

DNS, ICMP и SSH являются неотъемлемой частью современных сетей, но каждая из этих технологий может стать потенциальным вектором атаки. Понимание их работы, уязвимостей и методов защиты является ключом к обеспечению безопасности сетевой инфраструктуры. Эффективное управление и регулярный мониторинг помогут минимизировать риски и поддерживать стабильность сети.