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

Гузаревич Д.А.

Брест 2024

1. NetFlow

NetFlow — это технология мониторинга и анализа сетевого трафика, разработанная компанией Cisco. Она представляет собой мощный инструмент для изучения и управления сетевыми потоками, что особенно важно для диагностики сети, обеспечения безопасности и повышения производительности.

Основные функции NetFlow

NetFlow позволяет собирать, анализировать и визуализировать данные о сетевом трафике. Основные функции включают:

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

Принципы работы NetFlow

NetFlow собирает данные о каждом сетевом потоке, который проходит через устройство, поддерживающее эту технологию. 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.

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

Компоненты NetFlow

1. NetFlow Exporter — собирает информацию о сетевых потоках и экспортирует её в заданный коллектор.
2. NetFlow Collector — принимает экспортируемые данные, хранит их и подготавливает для анализа.
3. NetFlow Analyzer — предоставляет инструменты для анализа и визуализации собранных данных.

Преимущества NetFlow:

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

Применение NetFlow:

1. Сетевая безопасность: с помощью NetFlow можно обнаруживать вторжения и аномальное поведение.
2. Оптимизация работы сети: позволяет выявлять перегруженные сегменты сети и улучшать 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:

- Объем данных: обработка большого объема данных может требовать 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 существует множество решений для работы с NetFlow, например:

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

Заключение

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

2. WAF (Web Application Firewall)

WAF (Web Application Firewall) — это специализированное программное или аппаратное решение, предназначенное для защиты веб-приложений от различных атак. Основная задача WAF — фильтровать, анализировать и блокировать вредоносный трафик на уровне HTTP/HTTPS, предотвращая эксплойты, направленные на уязвимости в веб-приложениях.

Основные функции WAF:

- Защита от наиболее распространенных угроз веб-приложений, включая OWASP Top 10, такие как SQL-инъекции, XSS (межсайтовый скриптинг), CSRF (межсайтовая подделка запросов).
- Мониторинг HTTP-запросов в реальном времени.
- Обеспечение логирования и отчетности.
- Блокировка ботов и автоматизированных атак.

Принципы работы WAF:

WAF анализирует HTTP/HTTPS-запросы и ответы, проходящие между клиентами и веб-приложением. Основные подходы:

1. Подход на основе сигнатур:
   - Используются заранее определенные шаблоны атак (сигнатуры), чтобы распознать известные угрозы.
   - 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 атаки.
   - Требует настройки и "обучения" нормального поведения.

3. Гибридный подход:

   - Объединяет сигнатурный анализ с поведенческим, что обеспечивает более широкую защиту.

Типы WAF:

1. Облачные WAF:

   - Преимущества: простота настройки, масштабируемость, минимальные затраты на обслуживание.
   - Примеры: Cloudflare WAF, 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:

   - Совмещают преимущества облачных и локальных решений.
   - Предоставляют гибкость и возможность настройки.

Преимущества использования WAF:

- Защита данных: предотвращение утечек и компрометации конфиденциальной информации.
- Соответствие нормативным требованиям: WAF помогает соответствовать стандартам безопасности, таким как PCI DSS, GDPR.
- Легкость управления: возможность централизованного управления и мониторинга.

- Гибкость в настройке: возможность адаптировать политики безопасности под конкретные приложения.

Ограничения WAF:

- Ложные срабатывания: WAF может блокировать легитимные запросы, если политики настроены слишком строго.
- Необходимость обновлений: сигнатурный анализ требует регулярного обновления баз угроз.
- Невозможность устранения уязвимостей: WAF защищает от атак, но не устраняет исходные проблемы в коде приложения.

Популярные решения WAF:

- 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:

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.

4. Path Traversal: защита от атак, направленных на получение доступа к файлам на сервере.

Настройка WAF:

- Определение политик безопасности.
- Обучение системы для распознавания нормального трафика.
- Мониторинг и анализ логов для корректировки правил.

Заключение

WAF является важным элементом комплексной системы защиты веб-приложений. Его использование позволяет минимизировать риски, связанные с современными веб-угрозами, и обеспечивать высокий уровень безопасности данных и приложений. Несмотря на существующие ограничения, грамотная настройка и использование WAF значительно снижают вероятность успешной реализации атак.

3. DCShadow

DCShadow — это продвинутая техника, используемая злоумышленниками для компрометации инфраструктуры Active Directory (AD). Она позволяет злоумышленнику регистрировать фальшивый контроллер домена (Domain Controller, DC) в сети и вносить изменения в базу данных Active Directory без регистрации этих действий в стандартных журналах событий безопасности.

Принципы работы DCShadow:

Основная идея DCShadow заключается в подделке репликации данных Active Directory. Это достигается следующими шагами:

1. Создание ложного контроллера домена: злоумышленник регистрирует фальшивый контроллер домена, 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: так как изменения вносятся через механизм репликации, стандартные инструменты мониторинга безопасности (например, SIEM) не фиксируют эти действия.

Используемые протоколы и механизмы

DCShadow использует 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:

1. Уход от обнаружения: DCShadow позволяет злоумышленникам 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:

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

Обнаружение и защита от DCShadow

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 осведомлённость сотрудников IT-отдела о техниках DCShadow и связанных рисках.

Инструменты, связанные с DCShadow:

- 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 серьёзную 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 данном разделе рассматриваются три важнейших компонента сетевого взаимодействия: протоколы DNS, ICMP и SSH. Каждый из них играет ключевую роль в функционировании компьютерных сетей и, одновременно, может стать целью или инструментом атак.

DNS (Domain Name System)

DNS (система доменных имён) — это распределённая система, предназначенная для преобразования доменных имен в IP-адреса, необходимых для взаимодействия устройств в сети. Благодаря DNS пользователи могут обращаться к ресурсам сети, используя понятные имена, такие как "example.com", вместо 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, содержащихся 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 для обнаружения аномалий в DNS-трафике.
- Ограничение доступа к рекурсивным DNS-серверам.

ICMP (Internet Control Message Protocol)

ICMP — протокол управления передачей данных в сети, 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, приводящее к его перегрузке.
2. Smurf-атака: злоумышленник использует широковещательные ICMP-запросы, чтобы перегрузить целевую систему.
3. Reconnaissance-атаки: ICMP может быть использован для сбора информации о сети, включая её структуру и активные хосты.

Методы защиты ICMP:

- Ограничение ICMP-трафика на маршрутизаторах и файрволах.
- Настройка правил для предотвращения широковещательной передачи ICMP-запросов.
- Мониторинг аномального ICMP-трафика.

SSH (Secure Shell)

SSH (безопасная оболочка) — это 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: при краже приватного SSH-ключа злоумышленник может получить доступ к системе.
3. Слабая конфигурация: использование устаревших алгоритмов шифрования или ненадежных настроек.

Методы защиты SSH:

- Использование двухфакторной аутентификации (2FA).
- Ограничение доступа по IP-адресам (Allow/Deny lists).
- Настройка строгих правил использования SSH-ключей и их регулярная ротация.
- Отключение root-доступа по SSH.
- Включение протоколов современных версий (например, SSHv2).

Сравнение DNS, ICMP и SSH

Характеристика	DNS	ICMP	SSH
Основная функция	Преобразование доменных имен в IP-адреса	Диагностика сетей и сообщения об ошибках	Безопасное удаленное управление системами
Тип данных	Имена доменов, записи (A, MX, CNAME и др.)	Контрольные сообщения, такие как Echo Request и Reply	Команды, файлы, туннели
Уязвимости	Отравление кэша, DNS Tunneling	ICMP Flood, Smurf-атаки	Brute-force, утечка ключей
Защита	DNSSEC, фильтрация аномалий	Ограничение широковещательных запросов, мониторинг	2FA, ротация ключей, ограничение доступа

Тип использования	Преимущественно серверное взаимодействие	Диагностика и мониторинг	Администрирование, управление доступом

Заключение

DNS, ICMP и SSH являются неотъемлемыми частями современных сетей, однако каждая из этих технологий может стать вектором атаки. Понимание их работы, уязвимостей и способов защиты играет ключевую роль в обеспечении безопасности сетевой инфраструктуры. Эффективное управление и регулярный мониторинг помогают минимизировать риски и поддерживать устойчивость сети.