[Что такое брандмауэр](#_w4nzx5hm1b8s)

[Плюсы и минусы использования брандмауэра](#_egdtso9fx7gs)

[Методы аутентификации:](#_3kdsmkkuqqc3)

[Методы аутентификации](#_yffd1nxqu1m1)

[Протоколы аутентификации](#_8qxme6vihe2i)

[Протокол CHAP](#_bl1k0ngl7rb4)

[Взаимная аутентификация](#_j1gt5lbl3opw)

[IPS (Intrusion Prevention System) — система предотвращения вторжений.](#_xbo739e2z1st)

**ОДИН-ОДИН**

Фундаментальные принципы безопасности сети.

Информационная безопасность - это процесс, в котором обеспечивается "доступность", "целостность" и "конфиденциальность" информации.

Доступность - это обеспечение доступа к информации.

Целостность - это обеспечение достоверности и полноты информации.

Конфиденциальность - это обеспечение доступа лишь авторизованным пользователям

Угроза - возможность тем или иным способом нарушить информационную безопасность.

Атака - попыткареализации угрозы. Атакующий именуется "злоумышленником".

Обычно угроза это следствие наличия в системе защиты уязвимостей. Угрозы ИБ имеют собственную классификацию, по различным критериям:

Угроза самой ИБ(направленнана один из трех пунктов ИБ)

Компоненты, на которые нацелена угроза(данные, программы,инфраструктура)

По способу осуществления(случайные или специальные, природные или техногенного характера)

По расположению источника(внешние и внутренние)

**ОДИН-ДВА**

Принципы построения.

Выделяют 5 основных принципа проектирования Информационной Безопасности на объекте:

- Защита подключенного оборудования. Для защиты используют антивирусы, межсетевые экраны с фильтрацией и другое.

- Оборудование обязано быть отказоустойчивым и иметь возможность быстрого восстановления.

- Частая проверка систем для выявления уязвимостей. Иметь подробную документацию о каждом ПО и оборудовании в системе.

- Мониторинг Пропускной способности сетевого канала. Это позволит своевременно отключить нежелательный трафик.

- Важные узлы должны обеспечивать доступность при атаке или угрозе.

Сетевые атаки разделяютна 2 вида: Активные и Пасивные. Они же бывают внутренними и внешними.

Рекомендуется использовать следующие меры для предотвращения ушроз или атак:

- Прокси-серверы

- Системы выяления угроз

- Средства зищиты от целевых атак

- Системы сетевого мониторинга

- ВПН

**ОДИН-ТРИ**

Конфигурационная информация.

*Делится на Служебную и Предметную.* Служебная (например, пароли пользователей) не относится к определенной области, но раскрытие такой информацию может привести к несанкционированному входу в систему.

Несмотря на то, что информация может хранится на компьютере, ее раскрытие может привести к проблемам вне цифорового мира.

Одна из угроз, с которой сложно бороться - злоупотребление полномочиями. Администратор или другой супер-пользователь может получить доступ к любому(незашифрованному) файлу или информацию о любой почте других пользователей.

Другая - нанесение ущерба при сервисном обслуживании. Инженер обычно получает неограниченный доступ с возможностьюобхода системы защиты.

Для применения оптимальных средств защиты необходимо оценить саму угрозу и возможный ущерб от нее.

**ОДИН-ЧЕТЫРЕ**

*1. Переполнение CAM (Content Address Memory) таблицы*

Злоумышленник флудит таблицу MAC адресов коммутатора ,к которому он подключен, с целью переполнения таблицы. После переполнения CAM таблицы, коммутатор начинает работать в режиме простого хаба.

*2. Hopping.*

Смысл атаки заключается в том, что злоумышленник может получить доступ к другому устройству в сети не из своего VLAN

*3. MAC спуфинг.*

Злоумышленник может подменить MAC адрес, с целью захватить трафик необходимого ему устройства.

*4. Атака на DHCP.*

Злоумышленник может заполнить весь пул DHCP с помощью генерации большого количества запросов с несуществующими MAC адресами. Что приведет к DOS атаке, т.е. отказу в обслуживании, т.к.. так как после заполнения пула сервер не сможет выделять адреса реальным хостам. После чего атакующий может поднять собственный, DHCP сервер и хосты сети будут получать от недоверительного сервера все настройки, которые укажет злоумышленник.

*5. Атака на STP*

Смысл атаки заключается в том, что злоумышленник, с помощью программных средств может отправить коммутатору пакет BPDU, в котором указать высокий приоритет и меньший MAC адрес и тем самым стать «корневым коммутатором» с целью перехвата сетевого трафика.

*6. Переполнение CAM таблицы.*

*Коммутатор имеет CAM таблицу, где содержится "привязка", какие MAC адреса на каком порту принимаются.*

*Разумеется CAM таблица не бесконечна и имеет свои размеры.*

*Стоит подумать, а что же произойдет, когда вся таблица будет занята?*

Новые записи не смогут добавляться, весь трафик будет проходить на все порты.

*Что это даст атакующему вполне очевидно.* Он может "прослушать" весь сетевой трафик и получить конфеденциальную информацию.

*Всё это действенно для VLAN'а, в котором находится злоумышленник.* т.е. после переполнения данной таблицы атакующий не сможет прослушивать весь сетевой трафик, который "ходит" через коммутатор, а лишь своего VLAN, но и это не очень радостно.

*Какие же существуют способы борьбы с данным видом атаки?*

Логика подсказывает, что для подавления такой атаки, нам необходимо указать, что на порте коммутатора, к которому подключен пользователь может быть скажем не больше одного MAC адреса, а в случае если появляется более одного, перевести порт в отключенное состояние и отправить сообщение администратору о нарушении безопасности.

**ДВА-ОДИН**

Конфиденциальность, целостность и доступность данных

Безопасная информационная система — это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, а в-третьих, надежно хранит информацию и гарантирует неизменность данных.

Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

* Конфиденциальность (confidentiality) — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).
* Доступность (availability) — гарантия того, что авторизованные пользователи всегда получат доступ к данным.
* Целостность (integrity) — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Любое действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется угрозой. Реализованная угроза называется атакой. Риск — это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки. Значение риска тем выше, чем более уязвимой является существующая система безопасности и чем выше вероятность реализации атаки.

Классификация угроз

Так, прежде всего угрозы могут быть разделены на умышленные и неумышленные.

Неумышленные угрозы вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности. Кроме того, к такому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы. Так, например, из-за отказа диска, контроллера диска или всего файлового сервера могут оказаться недоступными данные, критически важные для работы предприятия. Поэтому вопросы безопасности так тесно переплетаются с вопросами надежности, отказоустойчивости технических средств. Угрозы безопасности, которые вытекают из ненадежности работы программно-аппаратных средств, предотвращаются путем их совершенствования, использования резервирования на уровне аппаратуры (RAID-массивы, многопроцессорные компьютеры, источники бесперебойного питания, кластерные архитектуры) или на уровне массивов данных (тиражирование файлов, резервное копирование).

**ТРИ-ОДИН**

Особенности защиты информации в компьютерных сетях обусловлены тем, что сети, обладая несомненными преимуществами обработки информации, по сравнению с локальными компьютерами, усложняют организацию защиты, образуя основные проблемные направления:

1. *Разделение совместно используемых ресурсов.*
2. *Расширение зоны контроля.*
3. *Комбинация различных программно-аппаратных средств.*
4. *Неизвестный периметр.*
5. *Множество точек атаки.*
6. *Сложность управления и контроля доступа к системе.*

Сообществом Интернета под эгидой Тематической группы по технологии Интернета (Internet Engineering Task Force, IETF) разработано много рекомендаций по отдельным аспектам сетевой безопасности, тем не менее, целостной концепции или архитектуры безопасности пока не предложено.

Основная идея состоит в том, чтобы средствами оконечных систем обеспечивать сквозную безопасность.

*Экранирование – единственный сервис безопасности, для которого Гостехкомиссия России одной из первых в мире разработала и ввела в действие Руководящий документ, основные идеи которого получили международное признание и фигурируют в профилях защиты, имеющих официальный статус в таких странах, как США.*

Политика безопасности межсетевого экрана базируется на принципе «все, что не разрешено, запрещено».

Межсетевой экран, или **Брандмауэр**– «полупроницаемая мембрана», которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети интранет и контролирует все информационные потоки во внутренний сегмент и из него.

Контроль трафика состоит в его фильтрации, то есть выборочном пропускании через экран.

*Работа брандмауэра заключается в чем?*

В анализе структуры и содержимого информационных пакетов, поступающих из внешней сети, и в зависимости от результатов анализа пропуска пакетов во внутреннюю сеть (сегмент сети) или полное их отфильтровывание.

Эффективность работы межсетевого экрана обусловлена тем, что он полностью переписывает реализуемый стек протоколов TCP/IP, и поэтому нарушить его работу с помощью искажения протоколов внешней сети (что часто делается хакерами) невозможно.

*Межсетевые экраны обычно выполняют следующие функции:*

* физическое отделение рабочих станций и серверов внутреннего сегмента сети (внутренней подсети) от внешних каналов связи;
* многоэтапная идентификация запросов, поступающих в сеть (идентификация серверов, узлов связи и прочих компонентов внешней сети);
* проверка полномочий и прав доступа пользователей к внутренним ресурсам сети;
* регистрация всех запросов к компонентам внутренней подсети извне;
* контроль целостности программного обеспечения и данных;
* экономия адресного пространства сети (во внутренней подсети может использоваться локальная система адресации серверов);
* сокрытие IP-адресов внутренних серверов с целью защиты от хакеров.

*Брандмауэры могут работать на разных уровнях протоколов модели OSI.*

На сетевом уровне выполняется фильтрация поступающих пакетов, основанная на IP-адресах (например, не пропускать пакеты из Интернета, направленные на те серверы, доступ к которым извне не должен осуществляться; не пропускать пакеты с фальшивыми обратными адресами или с IP-адресами, занесенными в «черный список» и т. Д.).

На транспортном уровне фильтрация возможна еще и по номерам портов TCP и флагов, содержащихся в пакетах (например, запросов на установление соединения).

На прикладном уровне может выполняться анализ прикладных протоколов (FTP, HTTP, SMTP и т. Д.) и контроль за содержанием потоков данных (запрет внутренним абонентам на получение каких-либо типов файлов: рекламной информации или исполняемых программных модулей, например).

В брандмауэре возможно наличие экспертной системы, которая, анализируя трафик, диагностирует события, потенциально представляющие угрозу безопасности внутренней сети, извещает об этом администратора сети, а в случае опасности она может автоматически ужесточать условия фильтрации и т. Д.

*Основные компоненты брандмауэра:*

* политика сетевого доступа;
* механизмы усиленной аутентификации;
* фильтрация пакетов;
* прикладные шлюзы.

Еще одним способом сетевой защиты может быть установленное на сервере специальное программное обеспечение, которое позволяет остальным компьютерам сети эмулировать выход в Интернет, оставаясь при этом «невидимым» со стороны глобальной сети. Такой компьютер называют прокси-сервером (proxy – доверенный).

Например, Microsoft Proxy Server 2.0. который, являясь кэширующим сервером (повышает эффективность работы сети – сокращает сетевой трафик), выполняет функции брандмауэра и обеспечивает безопасный доступ в Интернет и имеет два сетевых адаптера – один соединяет его с сетью, другой – с Интернет. Так как локальная сеть «не видна» из Интернет, то легальный IP-адрес имеет только внешний сетевой интерфейс, а IP-адреса внутри сети могут быть выданы из пула, зарезервированного для изолированных сетей.

**ТРИ-ДВА**

# **Что такое брандмауэр**

*Брандмауэр или фаерволл — это системная утилита (сетевой экран) для контроля и фильтрации входящего/исходящего трафика.* Брандмауэр стал неотъемлемой частью операционных систем Windows, начиная с версии XP SP2. В более ранних системах использовался Internet Connection Firewall, который по умолчанию был отключен. Это привело к глобальным атакам червей, таких как Blaster и Sasser, которые суммарно заразили более 350 тысяч компьютеров по всему миру в 2003 и 2004 годах.

Брандмауэр может быть как для отдельного компьютера, так и для всей локальной сети. В общем случае брандмауэр выполняет следующие функции:

* **Защита системы от внешних атак.** В список таких угроз входят сканирование портов, IP-спуффинг, DDoS-атаки, подбор паролей.
* **Блокировка утечек.** Если вредоносное ПО проникло в компьютер через USB или CD, то брандмауэр при соответствующих настройках предотвратит дальнейшее распространение по сети.
* **Контроль приложений.** Брандмауэр позволяет настроить доступ в сеть для каждого отдельного приложения.
* **Зональная защита.** Обеспечение различных уровней доступа в рамках локальной сети.
* **Протоколирование и предупреждение.** Брандмауэр не только собирает статистику, но и предупреждает пользователей о различных действиях.

*Брандмауэр есть не только в операционных системах.* ПО маршрутизаторов также включает встроенный фаерволл, который обычно настраивается через веб-интерфейс.

Брандмауэр способен анализировать абсолютно весь исходящий и входящий трафик, а также динамически открывать порты для конкретных приложений. Что конкретно из трафика будет блокировать брандмауэр, зависит от пользовательских настроек, а также внутренней базы, которая позволяет идентифицировать потенциально нежелательное содержимое.

Фильтры работают на нескольких уровнях модели OSI. Например, брандмауэр способен выполнять фильтрацию пакетов (сетевой уровень), контролировать шлюзы (сеансовый и прикладной уровни). Для каждого уровня используется свой гибкий фильтр. Например, на сетевом уровне брандмауэр анализирует заголовок IP-пакета: адреса получателя и отправителя, информацию о протоколе и приложении, номера портов. Собранная информация сравнивается с таблицей правил, после чего принимается решение — пропустить или отбраковать пакет.

## **Плюсы и минусы использования брандмауэра**

*Главный плюс использования — повышение безопасности.* В корпоративном секторе это обязательная защита, которая предотвратит вторжения извне, ограничит доступ в интернет сотрудникам и сделает безопасным передачу файлов по FTP и другим протоколам. Для обычных пользователей брандмауэр уменьшит шанс заражения червями, а также ограничит деятельность «подозрительных» программ.

Использование брандмауэра в операционной системе сопряжено с несколькими минусами:

* **Падение производительности.** Работающий брандмауэр потребляет ресурс процессора и ОЗУ, а из-за постоянного сканирования трафика пользователи могут столкнуться с незначительным падением скорости доступа в интернет.
* **Ложные срабатывания.** Алгоритмы брандмауэра не совершенны, поэтому он может «ругаться» на работу антивируса, торрента и других доверенных программ.
* **Сложность настройки.** Если вы хотите добиться максимального уровня защиты, то правила для входящих и исходящих соединений придется настраивать вручную.

Если на компьютере множество программ, то пользователям придется добавлять десятки разнообразных правил, но это позволит исключить ложные срабатывания и всецело взять трафик под контроль.

**ЧЕТЫРЕ-ОДИН**

Authentication - аутентификация.

Authorization - авторизация (проверка уровня доступа).

Accounting - учёт, контроль (слежение за потреблением ресурсов пользователем, например, для тарификации (биллинга)).

Представьте организацию (например университет) с множеством систем (серверы, АТС, WI-FI, здания, помещения и т.д.). Необходимо регистрировать в каждой системе одного и того-же пользователя. Чтобы этого не делать, ставится сервер AAA и все пользователи регистрируются только в нем. Все системы организации обращаются к серверу AAA.

**Алгоритм:**

*пользователь посылает запрос на аутентификацию системе (пароль, ключ и т.д)*

*система пересылает его серверу AAA (т.к. не может провести аутентификацию)*

*сервер AAA посылает ответ системе*

*пользователь получает или не получает доступ*

***Основные протоколы AAA:***

*· RADIUS, DIAMETER*

*· TACACS, TACACS+ (компании Cisco)*

Наибольшее распространение получил RADIUS ему на смену создан DIAMETER. Закрытые протоколы не выдерживают конкуренции.

RADIUS (Remote Authentication in Dial-In User Service)

Протокол опубликован в 1997

*Основные особенности:*

*·*

*· поддерживает аутентификацию PAP, CHAP, EAP.*

*· предоставляет более 50 пар атрибут/значение с возможностью создавать специфичные для производителя пары*

*· учетные данные могут хранится локально или во внешних источниках (базы SQL, Kerberos, LDAP, Active Directory)*

*Для протоколов SLIP и PPP могут включаться такие параметры, как*

*· адрес IP*

*· маска подсети*

*· MTU*

*· желательность использования компрессии*

*· идентификаторы желаемых фильтров*

*· Взаимодействие с PAP и CHAP*

*PAP*

*· NAS принимает от пользователя PAP ID (login) и пароль*

*· NAS PAP ID (login) и пароль в запросе Access-Request как атрибуты User-Name и User- Password*

*· сервер RADIUS сверяет User-Name и User- Password со своими значениями*

*CHAP*

*· NAS генерирует случайное число - challenge (предпочтительно 16 октетов) и передает его пользователю*

*· пользователь возвращает CHAP-отклик вместе с CHAP ID и CHAP username*

*· NAS передает запрос Access-Request серверу RADIUS со значением CHAP username для атрибута User-Name и значениями CHAP ID и CHAP-отклик в качестве CHAP-Password.*

*· сервер RADIUS находит пароль для пользователя "User-Name", хэширует (CHAP ID+пароль+CHAP challenge) и сравнивает результат с атрибутом CHAP-Password.*

*LDAP (Lightweight Directory Access Protocol)*

*Облегченный (относительно DAP) протокол для доступа к службе каталогов X.500*

*Cлужба каталогов — это репозитарий, в котором хранится информация о людях, компьютерах, сетевых устройствах и приложениях.*

LDAP можно использовать, например, для web-сайта, для аутентификации. Кроме этого, web-сайт может получить ФИО, email, телефон и д.р. информацию о пользователе из LDAP, что позволяет исключить подмену информации о себе пользователем или допустить ошибку при вводе информации пользователем, а так же уменьшает количество ручной работы по вводу информации.

Протоколы AAA такой информации не дают, но, например, коммутаторы могут работать только с RADIUS, и не могут работать с LDAP.

**ЧЕТЫРЕ-ДВА**

## **Методы аутентификации:**

· парольные (PIN коде и т.д.) - уникальная последовательность символов, которую пользователь должен знать.

· "ключе" - в случае электронных систем это электронный ключ, который хранится на носителе (смарт-карты, электронные таблетки iButton, USB-токены и т. д.)

· биометрические (отпечаток пальца, рисунок радужной оболочки глаза, форма лица, параметры голоса и т. д.)

· криптографические

## **Методы аутентификации**

Аутентификация по многоразовым паролям

Используется один пароль многократно.

Хотя аутентификация может использоваться не только к удаленным системам, методы аутентификации будем рассматривать сразу на примерах к удаленным системам

## **Протоколы аутентификации**

PAP (Password Authentication Protocol)

PAP - аутентификация по имени и паролю пользователя. Протокол PAP ненадежен при использовании в сетях, т.к. пароли можно перехватить.

Алгоритм PAP:

· клиент посылает имя и пароль серверу

· сервер сверяет присланный пароль с паролем в своем хранилище

Преимущества:

· простота

· Недостатки и пути решения:

· подбор паролей

· просмотр паролей в системе

· перехват паролей при передачи

· пароль можно «подсмотреть» при вводе

· человеческий фактор – человек не может запомнить сложные пароли (записывает), диктует открытым способом (по телефону) и т.д.

· каждый раз нужно набирать на клавиатуре

· нужна предварительная регистрация пользователя в системе

Решение проблемы "подбора паролей":

· использовать "сильные" пароли

· блокировка при неправильных попытках (например: 5 раз) ввода пароля

Плохие пароли

Почему эти пароли плохие:

· "2" - один символ, легко перебрать.

· "123456" - один из популярных паролей (еще примеры - 123; 111; qwerty; qazwsx; qazwsxedc; password; "ваш логин"; "номер телефона"; "дата рождения" и т.д.).

· "пароль" - словарное слово, после перебора популярных паролей, перебирают слова из словаря.

· "Gjhs6129dgGF\_9eK\_sj2vc9d" - пароль очень сложный, его не запомнят, а запишут и приклеят к монитору, пароль должен быть только в голове (или в сейфе).

Наиболее хорошим вариантом являются пароли построенные на фразах:

· хорошо запоминаются

· достаточно длинные

· словарные атаки не проходят

Пароли не хранятся в системе, а хранятся их хэши

Пароли в системе не хранятся, при этом пользователь проходит аутентификацию по паролю.

В большинстве современных систем именно так и сделано. Не только в ОС, но и в СУБД, форумах, сайтах и т.д.

Решение проблемы "перехвата паролей при передачи":

· шифровать передаваемые пароли

· использовать алгоритмы без передачи паролей (CHAP)

Шифрование передаваемых паролей

В настоящее время чаще всего для шифрования паролей используется протокол SSL (Secure Sockets Layer — уровень защищённых сокетов

CHAP (Challenge Handshake Authentication Protocol)

CHAP - аутентификация без передачи пароля.

Алгоритм CHAP:

1. пользователь посылает серверу запрос на доступ (login)

2. сервер отправляет клиенту случайное число

3. на основе этого случайного числа и пароля пользователя клиент вычисляет хеш

4. клиент пересылает хеш серверу

5. сервер сверяет присланный хеш со своим вычисленным

6. в случайные промежутки времени сервер отправляет новый и повторяет шаги с 2 по 5.

## **Протокол CHAP**

Основной недостаток - необходимо хранить пароль на сервере.

CRAM - (challenge-response authentication mechanism)

Основан на вычислении имитовставки по алгоритму [HMAC](http://ru.wikipedia.org/wiki/HMAC), роль симметричного ключа выполняет пароль.

В зависимости от алгоритма хэширования - CRAM-MD5, CRAM-MD4, CRAM-SHA1 и т.д.

## **Взаимная аутентификация**

Т.к. сервер может быть ложным, необходимо провести взаимную аутентификацию.

клиент отправляет запрос серверу, содержащий его login и случайное число N1

сервер зашифровывает число N1, генерирует случайное число N2, и отправляет их оба клиенту расшифровывает числа (N1,N2) и сравнивает первое (N1) число с N1. Идентичность означает, что сервер обладает тем же уникальным ключом, что и клиент зашифровывает число N2 и результат отправляет серверу

сервер расшифровывает полученное сообщение. При совпадении результата с исходным числом N2, взаимная аутентификация прошла успешно.

**ШЕСТЬ-ОДИН**

**Vlan Hopping**

Рассмотрим более подробно данный вид атаки, способ реализации и как ее предотвратить.

Цель данной атаки в том, что пользователь может попытаться передать данные в другой vlan.

Давайте рассмотрим, как это сделать. Как подсказывает логика, это возможно когда атакующий может инициировать trunk режим.

В коммутаторах Cisco Catalyst, по умолчанию порт работает не в режиму mode access и не в режиме mode trunk, таким образом на порту работает протокол DTP (Dynamic Trunk Protocol).

В такой ситуации стоит атакующему "претвориться" коммутатором, как между ними будет установленно транковое соединения, и соответсвенно будут доступны vlan'ы сконфигурированные на коммутаторе и после чего передать данные в другой Vlan не составит труда.

Бороться с этим не легко, а очень легко.

Для начала нужно все используемые интерфейсы коммутатора перевести принудительно в режимы access и trunk, где это положено.

Неиспользуемые порты необходимо перевести в shutdown, и перенести их в несуществующий VLAN, который будет известен только данному коммутатору, т.е. не передавался по trunk портам другим коммутаторам.

Атака на STP.

Как известно, STP (Spanning Tree Protocol) это протокол, предназначенный для предотвращения зацикливания пакетов в сети, при наличии дублирующих маршрутов. В кратце как это работает.

Сначала происходит обнаружения коммутаторов которые связаны между собой, Здесь точка. Затем... Выбирается так называемый Root Bridge, т.е. главный «корневой коммутатор» . Далее по специальному алгоритму будут заблокированы порты коммутатора, которые создают петли в получившейся топологии.

Что может сделать атакующий?

Атакующий может так же "претвориться" коммутатором, направить в сторону коммутатора BPDU пакет, в котором может подделать приоритет, mac адрес, для того чтобы стать «корневым коммутатором», и с его помощью перехватить сетевой трафик.

Корневой коммутатор становится тот, у которого самый высокий приоритет. Если приоритет у нескольких коммутаторов одинаковый, то для выбора корневого коммутатора используется MAC адрес, у кого он меньше тот и становится корневым.

Избавиться от этой уязвимости: запретить хождение BPDU пакетов с портов, в которых точно не должно быть никаких коммутаторов. И в случае если такой пакет всё же пришёл, переводить этот порт в shutdown.

Обезопасить наш корневой коммутатор, чтоб не при каких условиях не могу быть выбран другой корневой коммутатор, в том числе и наш атакующий (атакующему не составит труда поставить приортитет лучше чем у настояшего главного коммутатора, и MAC адрес поменьше, что будет гарантировано, что атакующий будет root.)

Для реализации данной идеи на коммутаторе необходимо:

1. на всех портах доступа поставим специальный режим STP, который называется

2. Клиент, подключенный к такому порту, не будет принимать участие в разрешении маршрутов по алгоритму STP и данные будут передаваться ему сразу.

По умолчанию portfast на Cisco Catalyst отключен и это нужно будет сконфигурировать вручную.

**MAC Spoofing.**

MAC Spoofing, это атака, реализуемая путем подделывания MAC адреса, например атакующий может подделать MAC адрес, который использовал другой хост сети. Что это может дать атакующему зависит от политики безопасности сети. Для того чтобы предотвратить данный тип атаки необходимо выполнить следующие меры:

1. Необходимо, указать максимальное количество mac адресов на порту, указать действие, которое будет выполнено в случае нарушения нашей политики (shutdown, restrict, protect).

2. Указать MAC адреса статически, динамически, либо в режиме обучении.

Для указания mac адреса статическим, в режими конфигурирования интерфейса необходимо выполнить:

1. Switch(config-if)# switchport port-security mac-address 3234.2343.fa12

Где, 3234.2343.fa12 mac адрес клиента.

2. Для указания динамического mac адреса, ничего дополнительного не делается, необходимо только включить фурнкцию port-security, как было описано выше.

Чтобы указать режим обучения mac-адресов необходимо выполнить в режиме конфигурирования интерфейса:

switch(config-if-range)#switchport port-security mac-address sticky

Указать время жизни записей arp-таблице

Атака на PVLAN (Private VLAN).

В технологии PVLAN в отличии от VLAN порты могут находиться в трёх режимах:

1. Promiscuous

2. Community

3. Isolated

Порты которые отмечены как Isolated, не могут передавать данные в своем VLAN между клиентами. Данные передаваться могут только между Isolated и Promiscuous портами.

Promiscuous порты это порты в PVLAN, в которые можно передавать данные со всех Isalated и Community портов. как и в обычном VLAN.

Community это группы портов, между членами которых можно передавать данные, можно назвать vlan в vlan'е.

Если атакующему доступно устройство Layer 3 (например маршрутизатор, либо коммутатор третьего уровня), он может установить связь между клиентами, которые находятся в одном PVLAN, между Isolated портами.

Как это можно реализовать?

Пользователь может подделать пакет, в котором IP назначения он укажет необходимое ему устройство (которое находится на другом порту Isolated), источник останется без изменения, т.к. ip атакающего, как и MAC адрес, а вот в качестве MAC адрес назначения он укажет MAC устройства L3. L3 устройство получится данный пакет и может переправить его по указанному адресу. Принимающая сторона может сделать тоже самое, тем самым обеспечив передачу данных между Isolated портами.

Предотвращение такой атаки сводится к тому, что на устройстве L3 создается специальный Access List в котором запрещается прямая передача данных между сегментом сети.