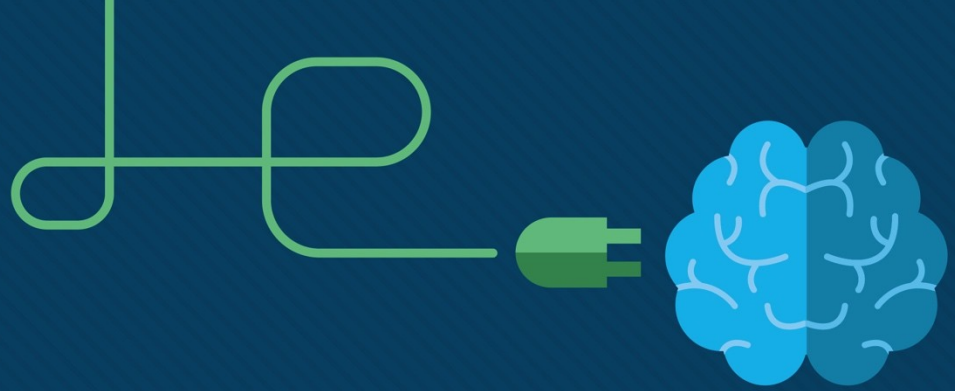


Модуль 16: Принципы обеспечения безопасности сети

Введение в сетевые технологии v7.0 (ITN)

Задачи модуля

Заголовок модуля: Принципы обеспечения безопасности сети

Цель модуля: Выполнить настройку функций, повышающих уровень безопасности, на коммутаторах и маршрутизаторах.

Заголовок темы	Цель темы
Угрозы безопасности и уязвимости	Объяснить необходимость применения базовых мер безопасности на сетевых устройствах.
Сетевые атаки	Определить уязвимости системы безопасности.
Защита от сетевых атак	Перечислить основные методики снижения рисков.
Обеспечение безопасности устройств	Выполнить настройку сетевых устройств с использованием функций дополнительной защиты для отражения угроз безопасности.

16.1. Угрозы и уязвимости безопасности

Типы угроз

Атака на сеть может иметь разрушительные последствия с потерей времени и средств в результате повреждения или хищения важной информации и ресурсов. Злоумышленники могут получить доступ к сети, используя уязвимости программного обеспечения, атаки на аппаратное обеспечение, подбор имени пользователя и пароля. Злоумышленников, которые получают доступ, внося изменения в ПО или используя его уязвимости, называют хакерами.

Хакер, получивший доступ к сети, сразу становится источником четырех видов угроз, как показано на рисунке.

- Кража информации
- Утечка данных и их неправомерное использование
- Кража персональных данных
- Прекращение обслуживания

Типы уязвимостей

Уязвимость — степень незащищенности, свойственная каждой сети и устройству. Некоторая степень уязвимости присуща маршрутизаторам, коммутаторам, настольным компьютерам, серверам и даже устройствам безопасности. Как правило, атакам подвержены такие оконечные устройства, как серверы и настольные компьютеры.

Существует три основных типа уязвимостей:

- Технологические уязвимости могут включать в себя слабости протокола TCP/IP, слабые места операционной системы и слабости сетевого оборудования.
- Уязвимости конфигурации могут включать незащищенные учетные записи пользователей, системные учетные записи с ненадежными паролями, неправильно настроенные интернет-службы, незащищенные параметры по умолчанию и неправильно настроенное сетевое оборудование.
- Уязвимости политики безопасности могут включать в себя отсутствие письменной политики безопасности, политики, отсутствие непрерывности проверки подлинности, неприменение логических элементов управления доступом, установку программного и аппаратного обеспечения и изменения, не соответствующие политике, а также несуществующий план аварийного восстановления.

Все три типа уязвимостей могут быть причиной атак, включая атаки с использованием вредоносного ПО и сетевые атаки.

Физическая безопасность

Злоумышленник может блокировать доступ к сетевым ресурсам, если их можно повредить на физическом уровне. Имеется четыре класса угроз:

- **Угрозы для аппаратного обеспечения** — физическое повреждение серверов, маршрутизаторов, коммутаторов, кабельных линий и рабочих станций.
- **Угрозы со стороны окружающей среды** — предельные температуры (слишком высокие или слишком низкие) или крайние значения влажности (слишком низкая или слишком высокая)
- **Электрические угрозы** — всплески напряжения, недостаточное напряжение в электрической сети (провалы напряжения), колебания напряжения (шум) и полное отключение электропитания
- **Эксплуатационные угрозы** — ненадлежащее обращение с ключевыми электрическими компонентами (электростатический разряд), нехватка важных запасных деталей, неправильная прокладка кабелей и ненадлежащая маркировка.

Для решения этих проблем необходимо разработать и осуществить хороший план обеспечения физической безопасности.

16.2 Сетевые атаки

Типы вредоносных программ

Вредоносное ПО — это вредоносное программное обеспечение (или вредоносный код). Такой код или ПО разрабатывается с целью повредить, разрушить, украсть данные либо причинить вред или совершить незаконные действия в отношении данных, узлов или сетей. Ниже перечислены типы вредоносных программ:

- **Вирус -** это тип вредоносного ПО, который распространяется путем внедрения своей копии в другую программу, заражая ее и становясь ее частью. Вирусы распространяются с одного компьютера на другой, инфицируя все объекты на своем пути.
- **Черви -** Похожи на вирусы тем, что они копируют свои функциональные части и могут нанести не меньший ущерб. В отличие от вирусов, для распространения которых обязательно должен быть зараженный файл, черви - отдельные программы, распространяющиеся без участия программы-носителя или человека.
- **Троянские кони -** Они маскируются под легитимные программы. В отличие от вирусов и червей такие вредоносные программы не распространяются путем заражения других файлов и не реплицируют сами себя. Они самовоспроизводятся. Обязательным условием для их распространения является открытие пользователем почтового вложения или загрузка и запуск файла из Интернета.

Разведывательные атаки

Помимо атак с использованием вредоносного кода сети также могут стать целью различных сетевых атак. Сетевые атаки можно разделить на три основные категории:

- **Разведывательные атаки —** обнаружение и сопоставление систем, служб или уязвимостей.
- **Атаки доступа** — несанкционированные неправомерные действия с данными, доступ к системе или использование прав пользователя
- **Отказ в обслуживании** — отключение или повреждение сетей, систем или служб.

Злоумышленники могут использовать инструменты Интернета, например, программные средства **nslookup** и **whois**, которые позволяют с легкостью определить пространство IP-адресов, назначенное определенной корпорации или юридическому лицу. После определения пространства IP-адресов злоумышленник может отправить команду ping для проверки связи с общедоступными IP-адресами, чтобы выявить активные адреса.

Атаки доступа

Известные уязвимости в сервисах аутентификации, FTP- и веб-сервисах, чтобы получить доступ к учетным записям, базам данных и другой конфиденциальной информации.

Атаки доступа можно разделить на четыре типа:

- **Атаки с паролем -** Реализованы с использованием грубой силы, троянского коня и снифферов пакетов
- **При атаке с злоупотреблением доверия** хакер использует несанкционированные привилегии для получения доступа к системе, что может поставить под угрозу цель.
- **Переадресация портов -** хакер использует взломанную систему в качестве базы для атак на другие целевые объекты. Например, хакер, использующий SSH-протокол (port 22) для подключения к скомпрометированному хосту A. Хост A является доверенным хостом для хоста B, и, следовательно, хакер теперь может использовать для доступа к этому хосту протокол Telnet (port 23).
- **Атака через посредника** хакер располагается между двумя доверяемыми объектами, чтобы читать, изменять или перенаправлять данные, которыми они обмениваются.

Атаки типа «отказ в обслуживании» (DoS-атаки)

Атаки типа DoS-атаки широко распространены, и их последствия устранить труднее всего. Однако ввиду простоты реализации DoS-атак и потенциально существенного вреда от них администраторы безопасности должны уделять таким атакам особое внимание.

- DoS-атаки могут принимать различные формы. Такие атаки, потребляя системные ресурсы, мешают авторизованным пользователям использовать службу. Для предотвращения DoS-атак важно следить, чтобы на компьютере были установлены актуальные обновления для системы безопасности как для ОС, так и для приложений.
- DoS-атаки представляют высокий риск, поскольку могут легко нарушить обмен информацией и вести к крупным потерям времени и средств. Проводить такие атаки относительно несложно, это под силу даже неопытным злоумышленникам.
- Распределенные атаки типа DDoS похожи на DoS-атаки, но проводятся скоординировано из нескольких источников. Например, злоумышленник создает сеть зараженных хостов, известных как зомби. Сеть зомби называется ботнетом. Злоумышленник использует программу командования и управления (CnC), чтобы инструктировать ботнет зомби выполнять DDoS-атаку.

Лабораторная работа. Изучение угроз безопасности сети

В этой лабораторной работе вы выполните следующие задачи.

- Часть 1. Изучение веб-сайта SANS
- Часть 2. Определение новых угроз безопасности сети
- Часть 3. Подробное описание отдельной угрозы безопасности сети

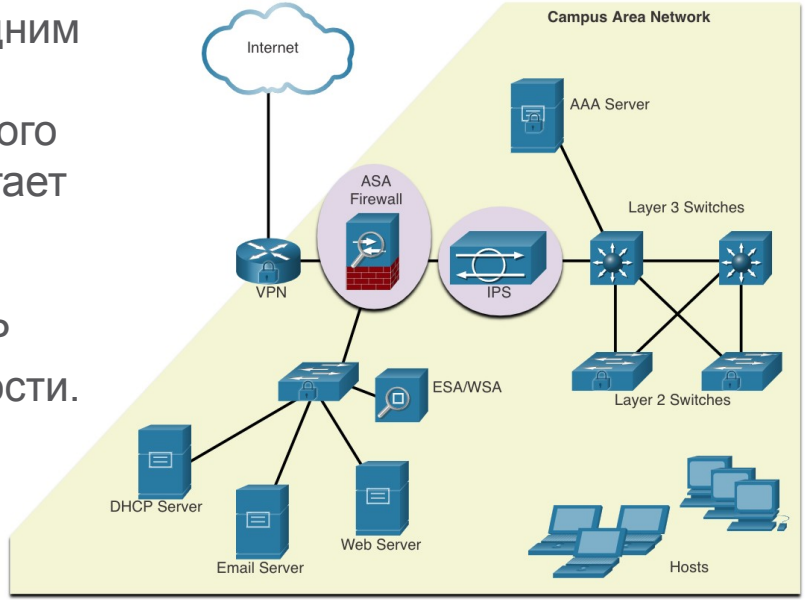
16.3 Защита от сетевых атак

Углубленный подход к защите подход к защите

Чтобы снизить уровень сетевых атак, сначала необходимо обеспечить безопасность устройств, включая маршрутизаторы, коммутаторы, серверы и хосты. Одним из решений является использование углубленного подхода к обеспечению безопасности, также известного как многоуровневый подход. Такой подход предполагает совместную работу сетевых устройств и сервисов.

Для защиты пользователей и активов от угроз TCP/IP реализовано несколько устройств и служб безопасности.

- VPN
- Межсетевой экран ASA
- IPS
- ESA/WSA
- Сервер AAA



Сохранение резервных копий

Резервное копирование данных —эффективный способ защиты данных от потери. Регулярно выполняйте резервное копирование, как определено в политике безопасности. Резервные копии данных обычно хранятся отдельно, чтобы защитить носитель с резервными копиями на случай, если что-либо произойдет в основном помещении.

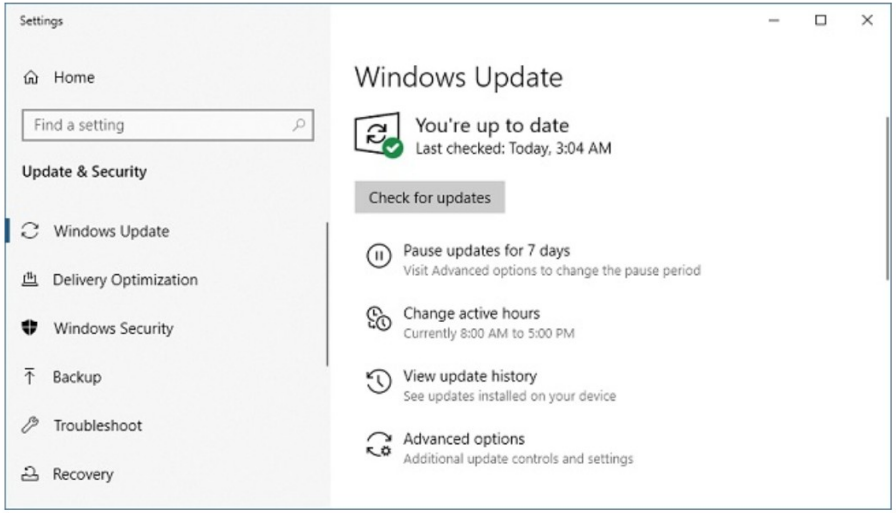
В таблице приведены соображения по резервному копированию и их описания.

Рассмотрение	Описание
Частота	• Регулярно выполняйте резервное копирование, как определено в политике безопасности. • Полное резервное копирование может занять длительное время.
Хранение	• Всегда проверяйте резервные копии, чтобы обеспечить целостность данных и проверить процедуры восстановления файлов.
Безопасность	• Необходимо переносить резервные копии в автономное хранилище ежедневно, еженедельно или ежемесячно в соответствии с политикой безопасности.
Проверка	• Резервные копии должны быть защищены с помощью надежных паролей. Пароль необходим для восстановления данных.

Обновление и установка исправлений

По мере появления нового вредоносного ПО предприятиям рекомендуется постоянно следить за обновлением антивирусного ПО до последних версий.

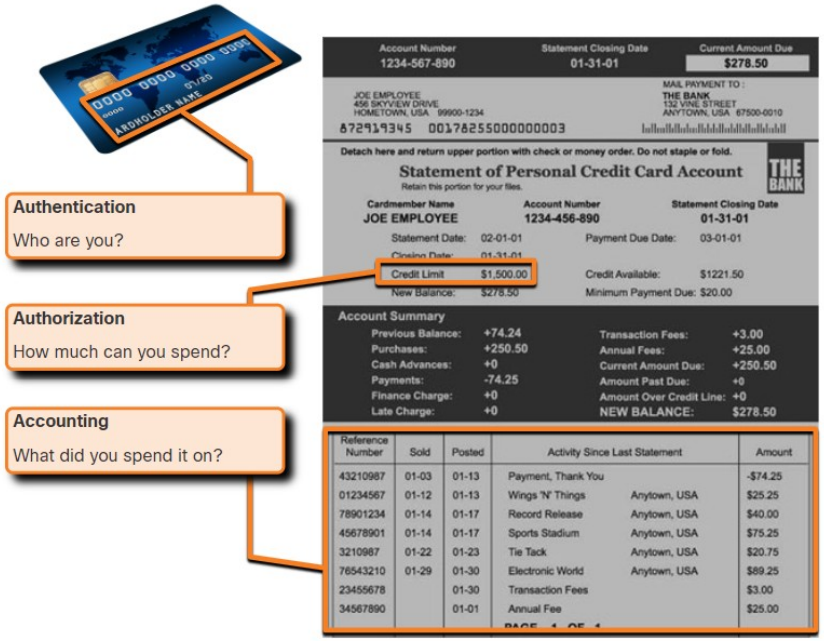
- Наиболее действенный метод минимизации последствий атаки вируса-червя — загрузить обновления для системы безопасности с сайта поставщика ОС и установить соответствующие обновления на все уязвимые копии систем.
- Одно из решений для управления критически важными исправлениями безопасности заключается в том, чтобы убедиться, что все конечные системы автоматически загружают обновления.



Аутентификация, авторизация и учет

Такие службы по обеспечению сетевой безопасности, как аутентификация, авторизация и учет (AAA), являются базовой инфраструктурой, которая устанавливает средства контроля доступа на каком-либо сетевом устройстве.

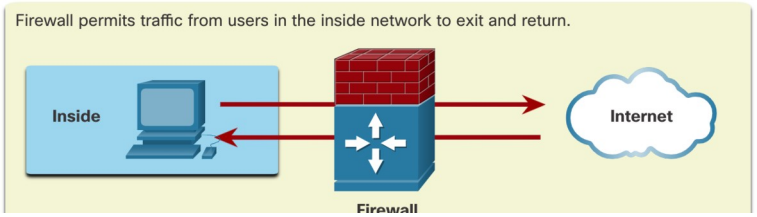
- Сочетание служб аутентификации, авторизации и учета — это метод, позволяющий контролировать вход разрешенных пользователей (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также следить за их действиями во время доступа к сети (учет).
- Концепция служб аутентификации, авторизации и учета (AAA) похожа на использование кредитной карты.

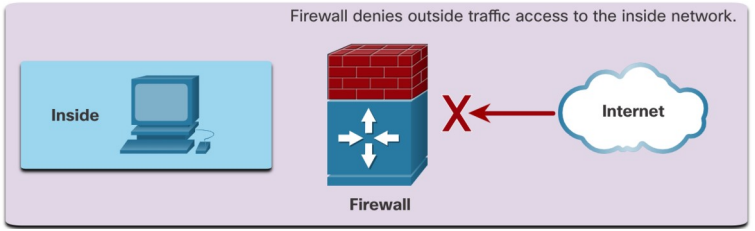


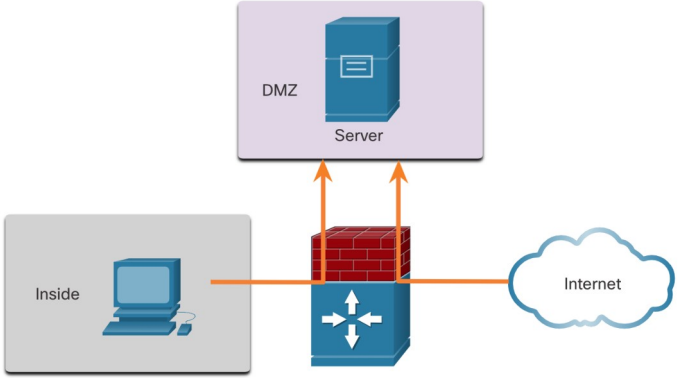
Межсетевые экраны

Межсетевой экран ставится между двумя (или более) сетями и контролирует трафик между ними, а также позволяет предотвратить несанкционированный доступ.

Межсетевой экран может позволить внешним пользователям управлять доступом к определенным службам. Например, серверы, доступные внешним пользователям, обычно размещаются в специальной сети, которая называется демилитаризованной зоной (DMZ). DMZ позволяет администратору применять определенные политики для хостов, подключенных к этой сети.







Типы межсетевых экранов

Решения для межсетевых экранов собраны в различные комплекты. В брандмауэрах используются различные методы для определения разрешения или запрета доступа к сети. В этот список входят следующие продукты:

- **Фильтрация пакетов** — запрет или разрешение доступа на основе IP- или MAC-адресов.
- **Фильтрация по приложениям** — запрет или разрешение доступа для конкретных типов приложений на основе номеров портов.
- **Фильтрация по URL-адресам** — запрет или разрешение доступа к веб-сайтам на основе конкретных URL-адресов или ключевых слов.
- **Анализ пакетов с учетом состояний соединений (SPI)** — входящие пакеты должны представлять собой легитимные отклики на запросы внутренних узлов. Незапрошенные пакеты блокируются, если они не разрешены в явном виде. SPI также предоставляет возможность распознавать и блокировать конкретные типы атак, например атаку типа «отказ в обслуживании» (DoS-атака).

Безопасность оконечных устройств

Оконечное устройство, или узел, представляет собой отдельную компьютерную систему или устройство, которое выступает в роли клиента сети. К наиболее распространенным оконечным устройствам относятся ноутбуки, настольные компьютеры, серверы и смартфоны и планшеты.

Защита оконечных устройств — одна из наиболее сложных задач, входящих в обязанности администратора сети, поскольку в данном случае имеет значение человеческий фактор. Компании необходимо разработать и тщательно задокументировать соответствующие политики и ознакомить с ними сотрудников.

Сотрудников необходимо обучить правильно использовать сеть. Политики зачастую подразумевают использование антивирусного ПО и меры предотвращения несанкционированного вторжения на узел. Комплексные решения для защиты оконечных устройств используют функции контроля доступа к сети.

16.4 Безопасность устройств

Cisco AutoSecure

При установке на устройство новой ОС настройки системы безопасности имеют значения по умолчанию. В большинстве случаев этого недостаточно. В маршрутизаторах Cisco для обеспечения безопасности системы можно использовать функцию Cisco AutoSecure.

Кроме того, существует ряд простых шагов, которые можно применить для большинства ОС:

- Установленные по умолчанию логины и пароли необходимо немедленно изменить.
- Доступом к системным ресурсам должны обладать только лица, наделенные соответствующими правами.
- Все невостребованные службы и приложения при возможности необходимо отключить или удалить.
- Зачастую устройства, полученные от производителя, до отгрузки хранились на складе в течение определенного периода, и поэтому на них не установлены актуальные обновления. Прежде чем внедрять любое ПО, важно сначала его обновить и установить любые имеющиеся обновления для системы безопасности.

Пароли

Для защиты сетевых устройств необходимо использовать надежные пароли. Ниже приведены стандартные рекомендации по выбору пароля.

- Используйте пароль длиной не менее 8 символов (предпочтительно 10 и более символов).
- Выбирайте сложные пароли. Включайте в пароль комбинацию букв в верхнем и нижнем регистре, цифр, специальных символов и пробелов (если допускается их использование).
- Избегайте использования паролей на основе повторений, обычных слов из словаря, последовательностей букв или цифр, имени пользователя, имен родственников и домашних животных, биографических данных (дата рождения, номер паспорта, имена родителей и пр.).
- Допустите в пароле намеренную ошибку. Например, Ivanov = Ivonov = 1vOnov.
- Периодически меняйте пароли.
- Не записывайте пароли на бумаге и не оставляйте их в легко доступных местах.

Маршрутизаторы Cisco игнорируют начальные пробелы в паролях, но пробелы после первого символа учитываются. Таким образом, один из способов создать надежный пароль — использовать пробел в пароле и задать фразу, состоящую из нескольких слов. Это называется парольной фразой. Парольную фразу зачастую проще запомнить, чем обычный пароль. Парольная фраза также имеет большую длину, чем простой пароль, и ее сложнее подобрать.

Расширенная защита пароля

Существует ряд действий, которые можно выполнить, чтобы обеспечить сохранность пароля в тайне на маршрутизаторах и коммутаторах включающих следующее:

- Чтобы зашифровать пароли, используйте команду глобальной конфигурации **service password-encryption**.
- Установите минимально допустимую длину пароля с помощью команды **security password min-length** .
- Обнаружьте атаки с использованием пароля грубой силы с помощью **команды login block for # attempts # within #**
- Отключение доступа к неактивному привилегированному режиму EXEC через определенное время (**exec-timeout)** .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Активация подключения по SSH

Настройка поддержки протокола SSH выполняется в четыре этапа:

1. **Настройте уникальное имя хоста устройства**.
2. **Настройте доменное имя IP** с помощью команды **ip-domain name**.
3. **Создайте ключ для шифрования SSH-трафика**. SSH шифрует трафик между источником и получателем. Однако для этого уникальный ключ проверки подлинности должен быть создан с помощью команды глобальной конфигурации **crypto key generate rsa general-keys modulus** *bits*. Следует лишь отметить, что модуль определяет размер ключа, который может быть в диапазоне от 360 *бит* до 2048 бит. Чем больше значение бита, тем безопаснее ключ. Однако большие значения битов также требовать больше времени для шифрования и расшифровки информации. Минимальная рекомендуемая длина модуля — 1024 бит.
4. **Проверьте или создайте запись локальной базы данных**. Создайте учетную запись пользователя в локальной базе данных с помощью команды **username**.
5. **Пользователи проходят аутентификацию в локальной базе данных.** Используйте команду конфигурации **login local** для проверки подлинности строки vty в локальной базе данных.
6. **Включите входящие сеансы SSH с использованием vty.** По умолчанию сеанс ввода не разрешен на линиях vty. Можно указать несколько протоколов, включая Telnet и SSH, используя команду **transport input [ssh | telnet].**

Отключите неиспользуемые службы.

Маршрутизаторы и коммутаторы Cisco запускаются с большим списком активных служб, которые могут потребоваться или не потребоваться при работе в сети. Отключите все неиспользуемые службы, чтобы сохранить системные ресурсы, такие как ЦП и ОЗУ, и предотвратить использование этих служб злоумышленниками.

- Тип служб, которые по умолчанию включен, зависит от версии IOS. Например, IOS-XE обычно имеет открытые только порты HTTPS и DHCP. Это можно проверить с помощью команды **show ip ports all** .
- В версиях IOS, предшествующих IOS-XE, используется команда **show control-plane host open ports**.

Packet Tracer. Настройка безопасного пароля и протокола SSH

В этом задании Packet Tracer вы будете настраивать пароли и SSH:

- Администратор сети обратился к вам с просьбой подготовить RTA и SW1 для развертывания. Перед его подключением к сети необходимо активировать функции безопасности.

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

В этой лабораторной работе вы выполните следующие задачи.

- Часть 1. Настройка основных параметров устройства
- Часть 2. Настройка маршрутизатора для доступа по протоколу SSH
- Часть 3. Настройка коммутатора для доступа по протоколу SSH
- Часть 4. SSH через интерфейс командной строки (CLI) коммутатора

16.5 Практика и контрольная работа модуля

Packet Tracer — Безопасность сетевых устройств

В этом задании вы будете настраивать маршрутизатор и коммутатор на основе списка требований.

Лабораторная работа — Безопасность сетевых устройств

В этой лабораторной работе вы выполните следующие задачи.

- Настройка основных параметров устройств
- Настройка базовых мер безопасности на маршрутизаторе
- Настройка базовых мер безопасности на коммутаторе

Что я изучил в этом модуле?

- Хакер, получивший доступ в сеть, становится источником хищения информации, хищения данных, потери данных, манипуляций и прекращения обслуживания.
- Три основных уязвимостей: технологии, конфигурация, и политика безопасности
- Четыре класса физических угроз: аппаратный, окружающая среда, электрический и техническое обслуживание.
- Вредоносное ПО. Такой код или ПО разрабатывается с целью повредить, разрушить, украсть данные либо причинить вред или совершить незаконные действия в отношении данных, узлов или сетей. К ним можно отнести вирусы, черви и программы-трояны.
- Сетевые атаки можно разделить на три основные категории: разведывательная атака, атака доступа и атака типа «отказ в обслуживании» (DoS-атака).
- Чтобы снизить уровень сетевых атак, сначала необходимо обеспечить безопасность устройств, включая маршрутизаторы, коммутаторы, серверы и хосты. Организации используют углубленный подход к защите сети.
- Для защиты пользователей и активов организации от угроз TCP/IP реализовано несколько устройств и служб безопасности: VPN-маршрутизатор, межетевой экан ASA, IPS, ESA/WSA и серверы-AAA

Что я изучил в этом модуле? (продолжение)

- Инфраструктурные устройства должны иметь резервные копии файлов конфигурации и образов IOS на FTP или аналогичном файловом сервере.
- Наиболее действенный метод минимизации последствий атаки вируса-червя — загрузить обновления для системы безопасности с сайта поставщика операционной системы и установить соответствующие обновления на все уязвимые копии систем.
- Сочетание служб аутентификации, авторизации и учета — это метод, позволяющий контролировать вход разрешенных пользователей (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также следить за их действиями во время доступа к сети (учет).
- Межсетевой экран ставится между двумя (или более) сетями и контролирует трафик между ними, а также позволяет предотвратить несанкционированный доступ.
- Защита конечных устройств имеет решающее значение для сетевой безопасности. Компания должна иметь хорошо документированные политики, которые могут включать использование антивирусного программного обеспечения и предотвращение вторжения в хост.

Что я изучил в этом модуле? (продолжение)

- В маршрутизаторах Cisco для обеспечения безопасности системы можно использовать функцию Cisco AutoSecure. Для большинства ОС имена пользователей и пароли по умолчанию должны быть изменены немедленно, доступ к системным ресурсам должен быть ограничен только лицами, уполномоченными использовать эти ресурсы, а любые ненужные службы и приложения должны быть отключены и удалены, когда это возможно.
- Для защиты сетевых устройств необходимо использовать надежные пароли. Парольную фразу зачастую проще запомнить, чем обычный пароль. Парольная фраза также имеет большую длину, чем простой пароль, и ее сложнее подобрать.
- Для маршрутизаторов и коммутаторов шифруйте все пароли открытого текста, устанавливая минимально допустимую длину пароля, сдерживайте атаки на взлом паролей методом грубой силы и отключайте неактивный доступ в привилегированный режим EXEC по истечении указанного времени.
- Настройте соответствующие устройства для поддержки SSH и отключите неиспользуемые службы.


CISCO