Лабораторная работа. Обеспечение безопасности сетевых устройств

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка базовых мер безопасности на маршрутизаторе

Часть 3. Настройка базовых мер безопасности на коммутаторе

Общие сведения/сценарий

Все сетевые устройства рекомендуется настраивать с использованием хотя бы минимального набора эффективных команд обеспечения безопасности. Это относится к устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в топологии таким образом, чтобы разрешать SSH-соединения для удаленного управления. Кроме того, вы должны будете настроить основные эффективные меры обеспечения безопасности через интерфейс командной строки операционной системы Cisco IOS. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они правильно внедрены и работают без ошибок.

Примечание: Маршрутизаторы, используемые в практических лабораторных работах CCNA, - это Cisco 4221 с Cisco IOS XE Release 16.9.4 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.2(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 Маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным).
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.2(2) с образом lanbasek9 или аналогичная модель).
- 1 ПК (под управлением Windows с программой эмуляции терминала, например, Tera Term).
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией.

Инструкции

Часть 1. Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на устройствах.

Шаг 1. Создайте сеть согласно топологии.

Подключите устройства, показанные в топологии, и кабели соответствующим образом.

Шаг 2. Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3. Выполните настройку маршрутизатора и коммутатора.

a. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.

b. Назначьте устройству имя в соответствии с таблицей адресации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

d. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

e. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

f. Назначьте cisco в качестве пароля виртуального терминала и включите вход по паролю.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Настройте и активируйте на маршрутизаторе интерфейс G0/0/1, используя информацию, приведенную в таблице адресации.

i. Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе согласно таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4. Настройте компьютер PC-A.

a. Настройте для PC-A IP-адрес и маску подсети.

b. Настройте для PC-A шлюз по умолчанию.

Шаг 5. Проверьте подключение к сети.

Пошлите с PC-A команду Ping на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2. Настройка базовых мер безопасности на маршрутизаторе

Шаг 1. Меры обеспечения безопасности:

a. Зашифруйте все пароли.

b. Настройте в системе ограничение на минимальный 12-значный пароль.

c. Измените пароли (привилегированный exec, консоль и vty) в соответствии с новым требованием длины.

   1) Установите привилегированный пароль exec на **$cisco!PRIV***

   2) Назначьте пароль консоли «cisco» и настройте вход по паролю **$cisco!!CON***

   3) Установите пароль vty линии **$cisco!! VTY***

d. Настройка маршрутизатора на прием только SSH-подключений из удаленных местоположений

   1) Настройте имя пользователя **SSHadmin** с зашифрованным паролем **55HAdm!n2020**

   2) Доменное имя маршрутизатора должно быть установлено на ccna-lab.com

   3) Длина ключа должна быть 1024 бит.

e. Настройка безопасности и передовых конфигураций на консолях и линиях vty.

   1) Пользователи должны быть отключены через 5 минут бездействия.

   2) Маршрутизатор не должен разрешать вход vty в течение 2 минут, если в течение 1 минуты произойдет 3 неудачных попытки входа в систему.

Часть 3. Меры обеспечения безопасности:

Шаг 1. Убедитесь, что все неиспользуемые порты отключены.

Порты маршрутизатора отключены по умолчанию, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты отключены администратором. Для этого можно воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не отключенные администратором, необходимо отключить с помощью команды **shutdown** в режиме конфигурации интерфейса.

Шаг 2. Убедитесь, что все меры безопасности внедрены правильно.

a. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу Telnet.

   Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.

b. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH.

   Разрешает ли R1 подключение по протоколу SSH?

c. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.

d. Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведенном ниже примере команда **show login** была введена в течение 120-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме Quiet. Маршрутизатор не будет разрешать попытки входа в систему в течение еще 111 секунд.

e. По истечении 120 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя **SSHadmin** и пароль **55HAdm!n2020**.

   Что отобразилось после успешного входа в систему?

f. Войдите в привилегированный режим EXEC и введите в качестве пароля **$cisco!PRIV***.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 60 секунд? Дайте пояснение.

g. Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Часть 4. Настройка базовых мер безопасности на коммутаторе

Шаг 1. Меры обеспечения безопасности:

a. Зашифруйте все пароли.

b. Настройте систему таким образом, чтобы вам требовалось не менее 12 символов пароля

c. Измените пароли (привилегированный exec, консоль и vty) в соответствии с новым требованием длины.

1) Установите привилегированный пароль exec на **$cisco!PRIV***

2) Назначьте пароль консоли «cisco» и настройте вход по паролю **$cisco!!CON***

3) Установите пароль vty линии **$cisco!! VTY***

d. Настройте коммутатор таким образом, чтобы он принимал только SSH-соединения из удаленных местоположений.

1) Настройте имя пользователя **SSHadmin** с зашифрованным паролем **55HAdm!n2020**

2) Имя домена коммутаторов должно быть установлено на ccna-lab.com

3) Длина ключа должна быть 1024 бит.

e. Настройка безопасности и передовых конфигураций на консолях и линиях vty.

1) Пользователи должны быть отключены через 5 минут бездействия.

2) Коммутатор не должен разрешать вход в систему в течение 2 минут, если в течение 1 минуты произойдет 3 неудачных попытки входа в систему.

f. Отключите все неиспользуемые порты.

Шаг 2. Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты.

a. Состояние портов коммутатора можно проверить с помощью команды **show ip interface brief**.

b. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interface range**.

c. Убедитесь, что все неактивные интерфейсы отключены администратором.

Шаг 3. Убедитесь, что все меры безопасности внедрены правильно.

a. Убедитесь, что протокол Telnet на коммутаторе отключен.

b. Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

c. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя **SSHadmin** и пароль **55HAdm!n2020**.

Появился ли баннер после успешного входа в систему?

d. Войдите в привилегированный режим EXEC и введите в качестве пароля **$cisco!PRIV***.

e. Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Вопросы для повторения

1. В части 1 для консоли и линий VTY в вашей базовой конфигурации была введена команда **password cisco**. Когда используется этот пароль после применения наиболее эффективных мер обеспечения безопасности?
2. Распространяется ли команда **security passwords min-length 10** на настроенные ранее пароли, содержащие меньше десяти символов?

Сводная таблица по интерфейсам маршрутизаторов

Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.