Лабораторная работа: обеспечение безопасности сетевых устройств

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-A	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка основных мер обеспечения безопасности на маршрутизаторе

Часть 3. Настройка основных мер обеспечения безопасности на коммуникаторе

Исходные данные/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 принимать SSH-сеансы для удалённого управления. Кроме того, вы настроите основные эффективные меры обеспечения безопасности через интерфейс командной строки IOS CLI. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они реализованы должным образом и работают без ошибок.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA, — Cisco 1941, ПО Cisco IOS версии 15.2(4)M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Необходимые ресурсы

- 1 маршрутизатор (серия Cisco 1941 с программным обеспечением Cisco IOS версии 15.2(4)M3, универсальный или совместимый образ)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 1 ПК (Windows 7, Vista или XP с программой эмулятора терминала, например Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Основные настройки устройства

В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Подключайте отображаемые в топологии устройства, а также кабель по мере необходимости.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

Справку по командам, необходимым для протокола SSH, см. в предыдущей лабораторной работе.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.

b. Войдите в режим конфигурации.

c. Присвойте маршрутизатору имя R1.

d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.

e. Назначьте **class** в качестве пароля привилегированного режима.

f. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

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

h. Зашифруйте пароли, хранящиеся в открытом виде.

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

j. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте коммутатор.

a. Подключите консоль к коммутатору и активируйте привилегированный режим.

b. Войдите в режим конфигурации.

c. Присвойте коммутатору имя S1.

d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введённых команд так, как если бы они были узлами.

e. Назначьте **class** в качестве пароля привилегированного режима.

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

f. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

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

h. Зашифруйте пароли, хранящиеся в открытом виде.

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

j. Присвойте интерфейсу SVI, который используется по умолчанию, IP-адрес из таблицы адресации.

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Настройка основных мер безопасности на маршрутизаторе

Шаг 1: Используйте надёжные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надёжных паролей. Рекомендации могут включать сочетание в пароле букв, цифр и специальных символов и определять его минимальную длину.

Примечание. Согласно рекомендациям по обеспечению эффективной работы в производственной среде необходимо использовать надёжные пароли, такие как приводятся в этой лабораторной работе. Однако для простоты выполнения лабораторных работ в данном курсе используются пароли cisco и class.

a. Чтобы соблюсти рекомендации, измените зашифрованный пароль привилегированного режима.

```
R1(config)# enable secret Enablep@55
```

b. Укажите, что пароль должен включать не менее десяти символов.

```
R1(config)# security passwords min-length 10
```

Шаг 2: Активируйте подключения SSH.

a. В качестве имени домена укажите **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надёжных паролей, а пользователь — иметь права доступа уровня администратора.

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

c. Настройте транспортный ввод для vty-линий таким образом, чтобы они могли принимать подключения SSH, но не разрешайте подключения Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. Для проверки подлинности в vty-линиях должна использоваться база данных локальных пользователей.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Создайте ключ шифрования RSA с длиной 1024 бит.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.CCNA-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

```
[OK] (elapsed time was 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Шаг 3: Обеспечьте защиту консоли и vty-линий.

a. Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения, неактивного в течение указанного времени. Если сетевой администратор вошёл в систему сетевого устройства, а потом был внезапно вызван в другое место, по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведённые ниже команды закрывают линию связи через пять минут неактивности.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. Указанная ниже команда препятствует входу в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введён неверный пароль. На этом таймере установлено низкое значение специально для выполнения данной лабораторной работы.

```
R1(config)# login block-for 30 attempts 2 within 120
```

Что означает **2 within 120** в приведённой выше команде?

Что означает **block-for 30** в приведённой выше команде?

Шаг 4: Убедитесь, что все неиспользуемые порты отключены.

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

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Шаг 5: Убедитесь, что все меры безопасности предприняты должным образом.

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

Принимает ли R1 подключение по протоколу Telnet?

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Поясните свой ответ.

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

Принимает 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.

Что произошло после ввода неправильных данных для входа в систему во второй раз?

d. Из консольной сессии на маршрутизаторе отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведённом ниже примере команда **show login** была отправлена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме «Quiet». Маршрутизатор не будет принимать попытки входа в систему в течение еще 14 секунд.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя **admin** и пароль **Admin15p@55**.

Что отобразилось после успешного входа в систему?

f. Выберите привилегированный режим и укажите в качестве пароля **Enablep@55**.

Если вы неправильно укажете пароль, прервётся ли подключение по протоколу SSH после двух неудачных попыток в течение 120 секунд?

Поясните свой ответ.

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

Часть 3: Настройка основных мер безопасности на коммутаторе

Шаг 1: Выберите более надёжные пароли для коммутатора.

Чтобы соблюсти рекомендации по созданию надёжных паролей, измените зашифрованный пароль привилегированного режима.

```
S1(config)# enable secret Enablep@55
```

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Примечание. Команда безопасности **password min-length** на коммутаторах модели 2960 не используется.

Шаг 2: Активируйте подключения SSH.

a. В качестве имени домена укажите **CCNA-lab.com**.

```
S1(config)# ip domain-name CCNA-lab.com
```

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надёжных паролей, а пользователь — иметь права доступа уровня администратора.

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

c. Настройте транспортный ввод для vty-линий таким образом, чтобы они могли принимать подключения SSH, но не разрешайте подключения Telnet.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. Для проверки подлинности в vty-линиях должна использоваться база данных локальных пользователей.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Создайте ключ шифрования RSA с длиной 1024 бит.

```
S1(config)# crypto key generate rsa modulus 1024
```

Шаг 3: Обеспечьте защиту консоли и vty-линий.

a. Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут отсутствия активности.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа за 120 секунд. На этом таймере установлено низкое значение специально для выполнения данной лабораторной работы.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Шаг 4: 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**.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
```

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

```
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

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

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. Убедитесь, что все неактивные интерфейсы административно отключены.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
```

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

```
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Шаг 5: Убедитесь, что все меры безопасности предприняты должным образом.

a. Убедитесь, что протокол Telnet на коммутаторе отключён.

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 S1 по протоколу SSH и войдите в систему, используя имя пользователя **admin** и пароль **Admin15p@55**.

Появился ли баннер после успешного входа в систему?

d. Выберите привилегированный режим, используя **Enablep@55** в качестве пароля.

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

Вопросы на закрепление

1. В части 1 для консоли и vty-линий в вашей основной конфигурации была введена команда **passwordcisco**. 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?

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Сводная таблица интерфейса маршрутизатора

Общие сведения об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet #1**	**Интерфейс Ethernet #2**	**Последовательный интерфейс #1**	**Последовательный интерфейс #2**
1800	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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.