Packet Tracer - Безопасность сетевых устройств

Таблица адресации

Устройство	Интерфейс	Адрес	Маска	Шлюз
RTR-A	G0/0/0	192.168.1.1	255.255.255.0	—
	G0/0/1	192.168.2.1	255.255.255.0	—
SW-1	SVI	192.168.1.254	255.255.255.0	192.168.1.1
PC	Сетевой адаптер	192.168.1.2	255.255.255.0	192.168.1.1
Laptop	Сетевой адаптер	192.168.1.10	255.255.255.0	192.168.1.1
Remote PC	NIC	192.168.2.10	255.255.255.0	192.168.2.1

Требования

Примечание. Чтобы сделать это действие кратким и простым в управлении, некоторые параметры конфигурации безопасности не были сделаны. В других случаях рекомендации по обеспечению безопасности не были соблюдены.

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

Инструкция

Шаг 1: Документирование сети

Заполните таблицу адресации недостающей информацией.

Шаг 2. Требования к конфигурации маршрутизатора:

- Предотвращение попыток IOS разрешать неправильно набранные команды для имен доменов.
- Имена узлов должны соответствовать значениям в таблице адресации.
- Требование: вновь созданные пароли должны быть не менее 10 символов.
- Для консольной линии необходим надежный десятизначный пароль. Используйте **@Cons1234!**
- Убедитесь, что сессии консоли и VTY будут закрыть ровно через 7 минут.
- Надежный зашифрованRный десятизначный пароль для привилегированного режима EXEC. Для этого действия допустимо использовать тот же пароль, что и консольной линии.
- Баннер MOTD, предупреждающий о несанкционированном доступе к устройствам.
- ¬\|□⌊®◊⟨∑ для всех паролей.
- Имя пользователя **NETadmin** с зашифрованным паролем **LogAdmin! 9**.
- Активация подключения по SSH.
  - Использование **security.com в** качестве доменного имени.
  - Используйте модуль **1024**.
- Линии VTY должны использовать SSH для входящих подключений.
- Строки VTY должны использовать имя пользователя и пароль, настроенные для аутентификации логины.

- Запретите попытки входа в систему методом грубой силы с помощью команды, которая блокирует попытки входа в систему в течение 45 секунд, если кто-то провалил три попытки в течение 100 секунд.

IOS Command Line Interface

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ip host SW-1 192.168.1.254
Router(config)#ip host PC 192.168.1.2
Router(config)#ip host Laptop 192.168.1.10
Router(config)#ip host Remote PC 192.168.2.10
                               ^
% Invalid input detected at '^' marker.

Router(config)#ip host Remote-PC 192.168.2.10
Router(config)#security passwords min-length 10
Router(config)#line console 0
Router(config-line)#password @Cons1234!
Router(config-line)#login
Router(config-line)#exec 7
Router(config-line)#exit
Router(config)#enable secret @Cons1234!
Router(config)#banner motd "Some"
Router(config)#username yaroslav secret @Cons1234!
Router(config)#username NETadmin secret LogAdmin!9.
Router(config)#ip domain-name security.com
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
Router(config)#hostname RTR-A
RTR-A(config)#crypto key generate rsa
The name for the keys will be: RTR-A.security.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RTR-A(config)#line vty 0 4
*Mar 1 8:24:16.713: %SSH-5-ENABLED: SSH 1.99 has been enabled
RTR-A(config-line)#transport input ssh
RTR-A(config-line)#exec-timeout 7
RTR-A(config-line)#exit
RTR-A(config)#login block-for 45 attempts 3 within 100
RTR-A(config)#
RTR-A(config)#
```

Шаг 3. Требования к конфигурации коммутатора:

- Все неиспользуемые порты коммутатора должны быть административно отключены.
- Интерфейс управления SW-1 по умолчанию должен принимать подключения по сети. Используйте информацию, указанную в таблице адресов. Коммутатор должен быть доступен из удаленных сетей.
- Используйте **@Cons1234!** в качестве пароля привилегированного режима EXEC
- Настройте SSH, как это было сделано для маршрутизатора.
- Создать имя пользователя **NETadmin** с зашифрованным секретным паролем **LogAdmin! 9**
- Линии VTY должны принимать соединения только через SSH.
- Строки VTY должны быть разрешены только для учетной записи администратора сети при доступе к интерфейсу управления коммутатором.
- Узлы в обеих ЛВС должны иметь возможность пропинговать интерфейс управления коммутатором.

```
Switch(config-if-range)#interface range F0/1, F0/3-9,F0/11-24, G0/2
Switch(config-if-range)#shutdown
```

```
Switch(config)#interface VLAN1
Switch(config-if)#ip address 192.168.1.254
% Incomplete command.
Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#ip default-gateway 192.168.1.1
Switch(config)#interface VLAN1
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#enable password @Cons1234!
Switch(config)#enable secret @Cons1234!
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
Switch(config)#enable secret @Cons1234!1
Switch(config)#enable secret @Cons1234!
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
Switch(config)#ip domain-name security.com
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#hostname SW-1
SW-1(config)#crypto key generate rsa
The name for the keys will be: SW-1.security.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-1(config)#username NETadmin secret LogAdmin! 9
*Mar 1 8:41:30.942: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-1(config)#line vty 0 4
SW-1(config-line)#transport input ssh
SW-1(config-line)#login local
SW-1(config-line)#exec-timeout 7
SW-1(config-line)#end
SW-1#
%SYS-5-CONFIG_I: Configured from console by console
```