Packet Tracer. Настройка протокола SSH

Топология

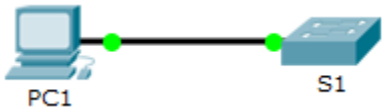

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Цели

Часть 1. Настройка шифрования паролей

Часть 2. Шифрование передачи данных

Часть 3. Проверка реализации SSH

Общие сведения

Для безопасного управления удаленными подключениями Cisco рекомендует заменить протокол Telnet протоколом SSH. В Telnet используется открытый незашифрованный текстовый обмен. Протокол SSH обеспечивает безопасность удалённых соединений, предоставляя надёжное шифрование всех данных, передаваемых между устройствами. В этом упражнении необходимо обеспечить безопасность удалённого коммутатора с использованием зашифрованного пароля и протокола SSH.

Часть 1: Безопасные пароли

a. С помощью командной строки на узле **PC1**, подключитесь к коммутатору **S1** через Telnet. Пароль для пользовательского и привилегированного доступа — **cisco**.

```
PC> telnet 10.10.10.2
Trying 10.10.10.2 ...Open


User Access Verification

Password:
S1>en
Password:
S1#
```

b. Сохраните текущую конфигурацию, чтобы любые допущенные вами ошибки можно было отменить, отключив питание коммутатора **S1**.

```
S1# copy running-config startup-config
Destination filename [startup-config]?
```

```
Building configuration...
[OK]
```

c. Отобразите текущую конфигурацию и обратите внимание на то, что пароли написаны в виде открытого текста. Введите команду, которая шифрует текстовые пароли:

```
S1(config)# service password-encryption
```

d. Убедитесь, что пароли зашифрованы.

Часть 2: Обеспечение защищенной коммуникации

Шаг 1: Настройте имя домена IP и создайте ключи шифрования.

В принципе, использование Telnet небезопасно, поскольку текстовые данные передаются в незашифрованном виде. Поэтому рекомендуется по возможности использовать протокол SSH.

a. Присвойте домену имя **netacad.pka.**

```
S1(config)# ip domain-name netacad.pka
```

b. Для шифрования данных требуются ключи шифрования. Создайте RSA ключи длиной 1024 бит.

```
S1(config)# crypto key generate rsa
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 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]
```

Шаг 2: Создайте пользователя SSH и перенастройте линии VTY на доступ только по протоколу SSH.

a. Создайте пользователя **administrator** с секретным паролем **cisco**.

```
S1(config)# username administrator secret cisco
```

b. Настройте линии VTY для проверки регистрационных данных на основе локальной базы данных имен пользователей, а также для разрешения удаленного доступа только по протоколу SSH. Удалите существующий пароль линии VTY.

```
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# no password cisco
```

Часть 3: Проверка реализации протокола SSH

a. Завершите сеанс Telnet и попробуйте заново войти в систему, используя Telnet. Попытка должна завершиться неудачей.

b. Попробуйте войти в систему через протокол SSH. Введите **ssh** и нажмите **ВВОД**, не добавляя какие-либо параметры, чтобы отобразить инструкции использования команды. Указание. Параметр **-l** — это буква «L», а не цифра 1.

c. После успешного входа перейдите в режим привилегированного доступа EXEC и сохраните конфигурацию. Если вам не удалось получить доступ к коммутатору **S1**, отключите питание и повторите шаги, описанные в части 1.