Практическая работа № 13

ЗАЩИТА СЕТЕВЫХ УСТРОЙСТВ

Цель работы. Изучить способы защиты коммутаторов и маршрутизаторов на примере оборудования Cisco от несанкционированного доступа.

Краткие сведения из теории

Для защиты устройств Cisco от несанкционированного доступа используется несколько видов паролей. К ним относится настройка паролей на консоль, паролей на подключение по telnet и SSH, а так же пароль для доступа в привилегированный режим работы устройства. Пароли настраиваются одинаковым образом для маршрутизаторов и коммутаторов.

Пароль на консоль.

При подключении к устройству через консольный провод необходимо ввести пароль. По умолчанию пароль на консоль отсутствует. Надо понимать, что физическая безопасность устройства наиболее важный аспект защиты, так как имея физический доступ к консольному порту, даже не зная пароля его можно сбросить. Пароль на консоль задаётся следующим образом:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password MyPassword
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
```

Необходимо зайти в режим глобальной конфигурации, зайти в подрежим настройки консоли (line console 0), где 0 – это порядковый номер консоли. Обычно на всех устройствах консольный порт один и он имеет номер 0. В этом подрежиме задаётся пароль с помощью команды password, затем необходимо ввести слово login, чтобы разрешить вход под указанным паролем. После этого при подключении по консоли будет выводиться следующее приглашение:

```
Press RETURN to get started.
User Access Verification
Password:
```

Где требуется ввести указанный пароль. При вводе символы пароля не отображаются.

Пароль на привилегированный режим.

Этот важный пароль используется для перехода из пользовательского режима в привилегированный. При входе на устройство, независимо от того, производится доступ через VTY или через консоль, пользователь попадает в пользовательский режим. Далее можно осуществить переход в привилегированный режим. Если задан пароль на привилегированный режим, то его потребуется ввести, если не задан – то всё зависит от того способа, по которому было произведено подключение к устройству. При подключении по консоли и отсутствующем пароле на enable, переход в привилегированный режим произойдёт без ввода пароля, если же доступ осуществляется через telnet или SSH, то без пароля на enable доступ в этот режим будет отсутствовать. По этой причине начальная настройка маршрутизатора всегда производится через консоль и должна включать в себя задание всех необходимых паролей.

Пароль на enable можно задать двумя разными командами обе из которых вводятся в режиме глобальной конфигурации:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password MyEnablePassword
Router(config)#exit
Router#
```

или

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret SecretPassword
Router(config)#exit
Router#
```

Вводить необходимо одну из команд: enable password, либо enable secret. Разница между ними заключается в том, что вторая команда сохраняет пароль в зашифрованном виде и его нельзя восстановить глядя на файл конфигурации. Если же применять enable password, то пароль храниться в конфиге в открытом виде. Таким образом, лучше всегда использовать enable secret. Если применить обе команды одновременно, то будет работать тот пароль, который задан с помощью команды enable secret.

Для анализа результата установки паролей необходимо просмотреть конфигурацию устройства с помощью команды show running-config:

```
Router#show running-config
```

При этом пароль, заданный enable password виден открытым текстом.

Служба шифрования паролей.

Для того, чтобы скрыть пароли для доступа к сетевому устройству необходимо включить службу шифрования паролей:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#exit
Router#
```

После применения команды service password-encryption, все пароли в конфигурационном файле начинают храниться в зашифрованном виде.

Пароль на telnet и SSH.

Доступ по протоколам telnet или SSH может быть осуществлён только после того как на устройстве настроен IP-адрес, а так же заданы пароли. В этом важное отличие от доступа по консоли. Если пароли не заданы, то по консоли можно зайти без пароля, а по telnet или SSH зайти нельзя – будет выдано сообщение, что пока нет пароля, удалённый вход запрещён.

Для доступа по SSH пароли задаются следующим образом:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password MyPassword
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
```

Процедура аналогична настройке пароля на консоль, только действия выполняются не в режиме конфигурирования консоли (con 0), а в режиме настройки виртуальных терминалов (vty 0 4), где цифры «0» и «4» следует трактовать как «Перейти в подрежим конфигурирования всех виртуальных терминалов с нулевого по четвёртый». Обычно для telnet используются именно эти 5 виртуальных терминалов. Если один терминал занят подключением, то человек подключится к следующему свободному.

Для настройки доступа по протоколу SSH необходимо выполнить следующие команды:

```
Router#configure terminal

Router(config)#hostname Protection
Protection (config)#ip domain-name protection.org
Protection (config)#username username password password
```

Protection (config)#crypto key generate rsa
Protection (config)#login block-for 180 attempts 4 within 120
Protection (config)#line vty 0 4
Protection (config-line)#transport input ssh
Protection (config-line)#login local
Protection (config-line)#exit
Protection (config)#exit
Protection #

Здесь маршрутизатору задается название Protection, доменное имя protection.org. Затем создается пользователь с логином и паролем. Командой **crypto key generate rsa** создается ключи RSA. Длина ключа вводится после выполнения данной команды. Следующая команда будет блокировать на три минуты всех, кто не смог войти в систему, выполнив четыре попытки ввода пароля в течение двух минут. Далее производится настройка линий VTY для доступа по SSH. Здесь задается использование профилей локальных пользователей для аутентификации, а также запрещается использование других протоколов.

Порядок выполнения работы

1 В программе Cisco Packet Tracer собрать сеть, представленную на рисунке 1. Интерфейсу Fast Ethernet компьютера задать IP-адрес 192.168.100.2/24, Default gateway – 192.168.100.1/24. Интерфейсу Gigabit Ethernet маршрутизатора задать IP-адрес 192.168.100.1/24.

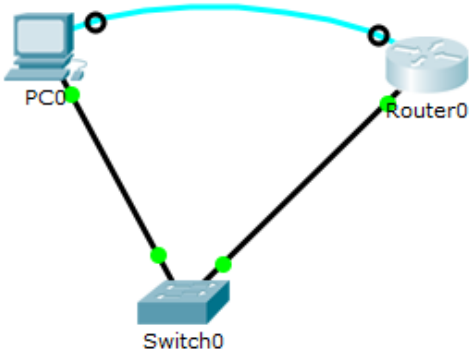

Рисунок 1 – Схема сети

2 Используя консольное подключение через компьютер подключиться к маршрутизатору. Задать разные пароли для привилегированного режима, консольного доступа, доступа по протоколу telnet. Посмотреть конфигурацию маршрутизатора и убедиться в наличии там заданных паролей.

3 Зашифровать пароли и убедиться в наличии зашифрованных паролей в конфигурации маршрутизатора.

4 Организовать подключение к маршрутизатору по протоколу telnet.

5 Настроить на маршрутизаторе протокол SSH, задать имя пользователя и пароль, шифрование алгоритмом RSA с длиной ключа 1024 бит. Подключиться к маршрутизатору по протоколу SSH.

Содержание отчета

1 Цель работы.

2 Схема сети.

3 Конфигурация маршрутизатора до и после шифрования паролей.

4 Мониторинг подключения к маршрутизатору по протоколам telnet и SSH.

5 Вывод по работе.

Контрольные вопросы

1 Что такое привилегированный режим управления сетевым устройством?

2 Как задается пароль на консольное подключение?

3 Как задается пароль на подключение по протоколу telnet?

4 Для чего необходимо шифрование паролей?

5 Как настроить протокол SSH на маршрутизаторе?