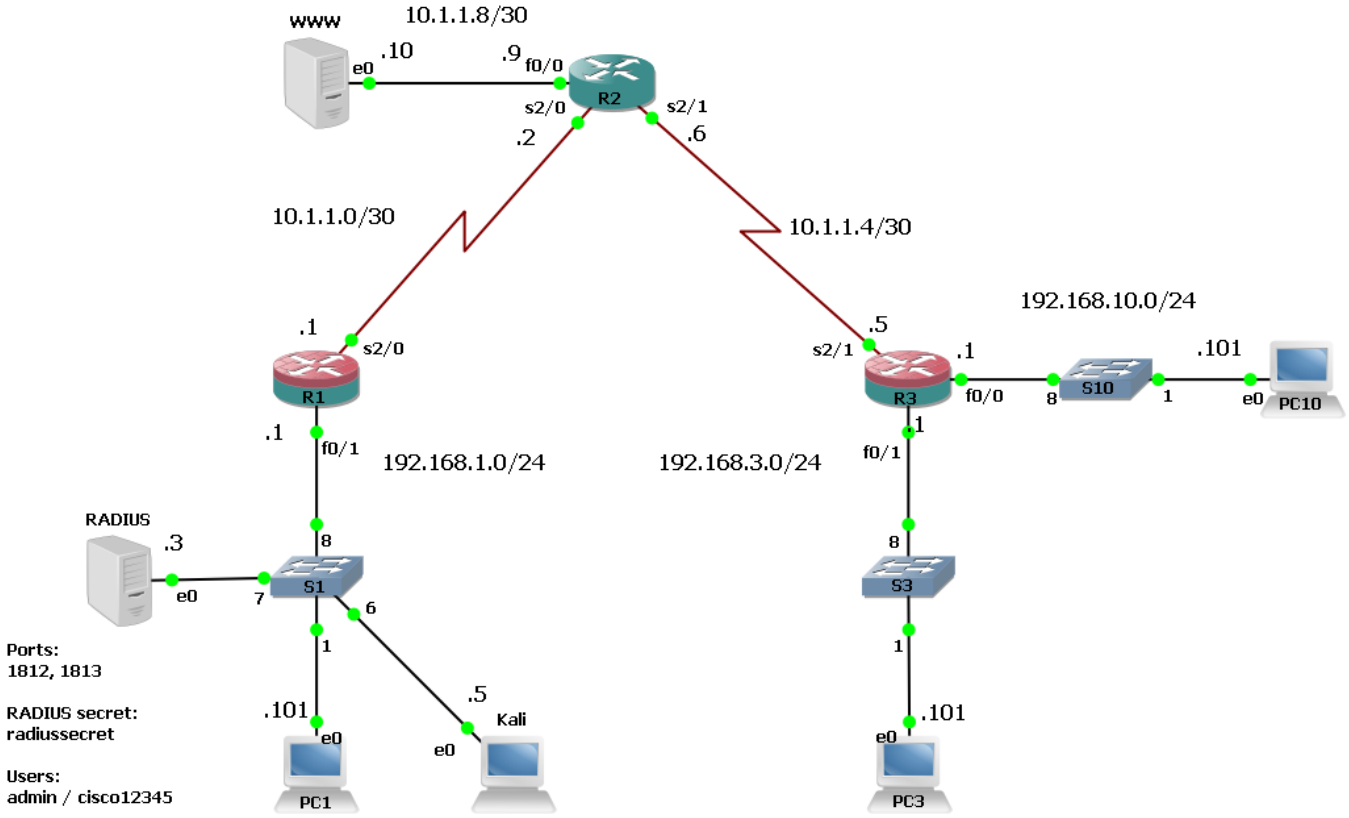
CCNA Security

Лабораторная работа 14

Изучение протокола SCP

Топология



Описание

Хотя новая модель AAA в локальном исполнении не даёт вам существенных преимуществ, её включение – это мостик к внедрению серверной аутентификации. Также локальная модель AAA позволит вам работать с устройством по протоколу SCP для безопасного копирования файлов. Протокол SCP работает внутри протокола SSH, который вы настроили ранее.

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	Описание
R1	Fa0/1	192.168.1.1/24	-	LAN interface
	Se2/0	10.1.1.1/30	-	WAN interface (To R2)
R2	Se2/0	10.1.1.2/30	-	To R1
	Se2/1	10.1.1.6/30	-	To R3
	Fa0/0	10.1.1.9/30	-	To WWW server
R3	Fa0/1	192.168.3.1/24	-	LAN interface
	Fa0/0	192.168.10.1/24	-	Conference Room
	Se2/1	10.1.1.5/30	-	WAN interface (To R2)
PC1	NIC	192.168.1.101/24	192.168.1.1	-
PC2	NIC	192.168.3.101/24	192.168.3.1	-
PC10	NIC	192.168.10.101/24	192.168.10.1	-
Kali	NIC	192.168.1.5/24	192.168.1.1	-
RADIUS	NIC	192.168.1.3/24	192.168.1.1	-
WWW	NIC	10.1.1.10/24	10.1.1.9	-

Имена пользователей и пароли

	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	admin	cisco12345	admin	cisco12345	cisco12345
R2	-	-	-	-	-
R3	admin	cisco12345	admin	cisco12345	cisco12345

Устройство	Имя пользователя	Пароль
PC1	Student1	1
PC2	Student1	1
PC10	Student1	1
Kali	root	toor

Часть 1: Настройка и изучение протокола SCP на маршрутизаторе R1

1. Запустите захват на линке между R1 и S1. Для этого в окне GNS3 щёлкните правой кнопкой мыши по линку между R1 и S1, в контекстном меню выберите **Start Capture**. В открывшемся окне просто нажмите **OK**. Дождитесь открытия Wireshark.

2. Введите в поле Display Filter слово **ssh** и нажмите Enter.

3. Войдите в консоль маршрутизатора R1.

4. Войдите в режим конфигурирования.
   ```
   R1# conf t
   ```

5. Для работы с файлами по протоколу SCP понадобится пользователь с уровнем привилегий 15. Создайте пользователя superadmin с уровнем привилегий 15 и секретным паролем.
   ```
   R1(config)# username superadmin privilege 15 algorithm-type scrypt secret cisco12345
   ```

6. Составьте список методов с именем по умолчанию default для проведения авторизации при выполнении команд на устройстве. Укажите один единственный метод local.
   ```
   R1(config)# aaa authorization exec default local
   ```

7. Включите функционал SCP-сервера.
   ```
   R1(config)# ip scp server enable
   ```

8. Вернитесь в виртуальную машину PC1.

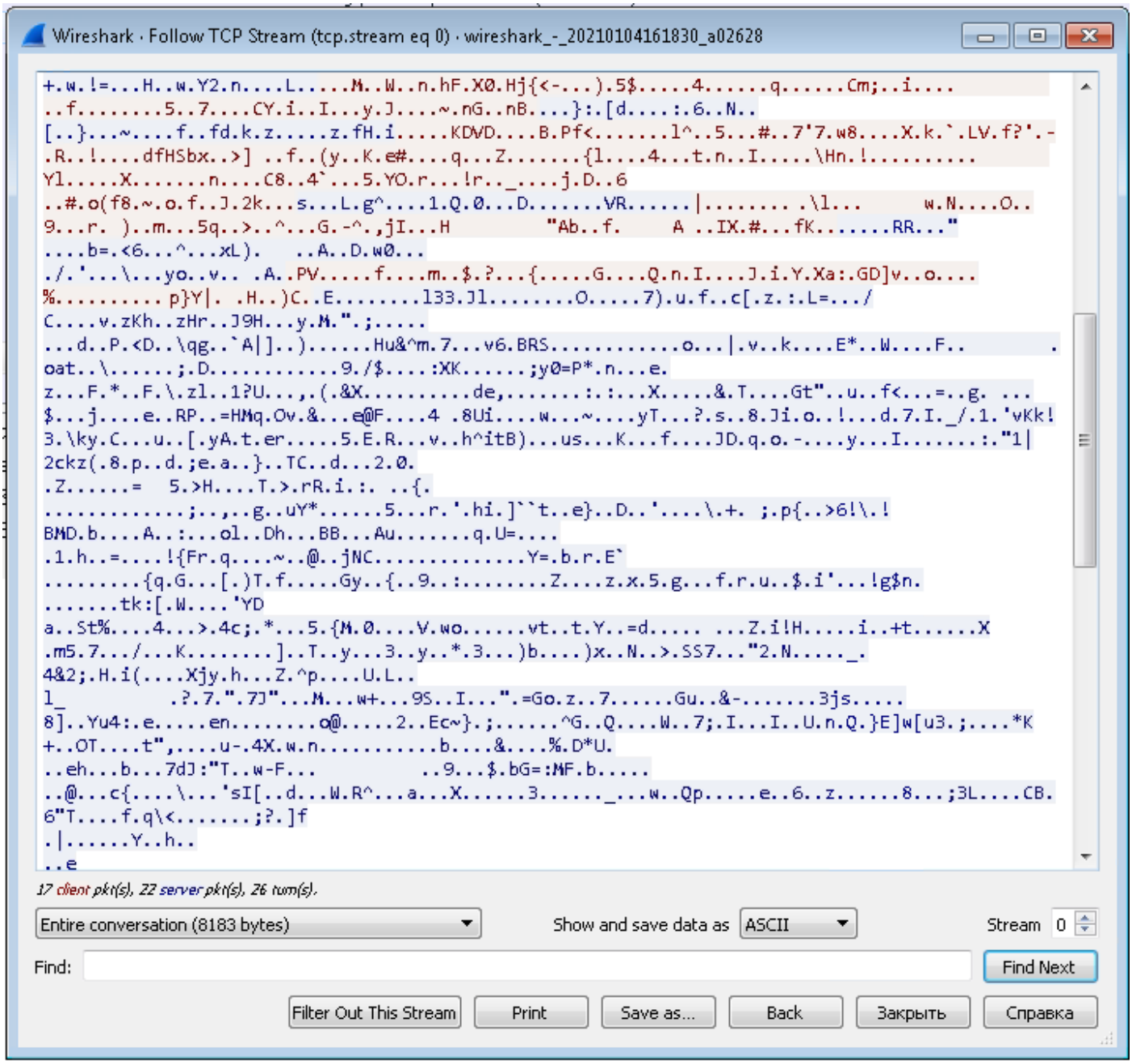
9. Для работы с файлами по протоколу SCP можно воспользоваться ПО pscp, входящем в комплект PuTTY. Если вы знакомы с ПО WinSCP, то расстрою вас, оно не подойдёт. Протокол SCP не имеет возможностей получения списка файлов, поэтому для реализации подобного функционала WinSCP опирается на команды оболочки (sh, bash и т.д.), которые отсутствуют в оболочке Cisco IOS. Откройте командную строку и попробуйте скопировать файл текущей конфигурации с маршрутизатора R1. Параметр **-l** – это маленькая L, сокращение от login, не спутайте с единицей.
   ```
   C:\Users\Student1> pscp -scp -l superadmin 192.168.1.1:running-config r1.cfg
   Using keyboard-interactive authentication.
   Password: < Введите пароль cisco12345 >
   r1.cfg                    | 2 kB |   3.0 kB/s | ETA: 00:00:00 | 100%
   ```

10. Зайдите в папку C:\Users\Student1. Откройте переданный файл r1.cfg в Notepad++. Бегло проверьте, что он похож на текущую конфигурацию маршрутизатора.

11. Вернитесь в Wireshark на основной машине. Хотя вы не подключались к устройству по протоколу SSH, пакеты SSH присутствуют в таблице, т.к. протокол SCP работает внутри протокола SSH.

12. Щёлкните правой кнопкой мыши на любой пакет SSH в таблице. В контекстном меню выберите **Follow -> TCP Stream**.

13. В открывшемся окне будет представлен собранный текст сессии. Видно ли переданные имена пользователей и пароли, другую критичную информацию?



14. Вы убедились, что протокол SCP работает внутри SSH, а стало быть его использование безопасно. Закройте окно Follow TCP Stream, закройте основное окно Wireshark.

Часть 2: Настройка протокола SCP на маршрутизаторе R3

1. Перейдите в консоль маршрутизатора R3.

2. Войдите в режим конфигурирования.
   ```
   R3# conf t
   ```

3. Создайте пользователя superadmin с уровнем привилегий 15 и секретным паролем.
   ```
   R3(config)# username superadmin privilege 15 algorithm-type scrypt secret cisco12345
   ```

4. Составьте список методов с именем по умолчанию default для проведения авторизации при выполнении команд на устройстве. Укажите один единственный метод local.
   ```
   R3(config)# aaa authorization exec default local
   ```

5. Включите функционал SCP-сервера.
   ```
   R3(config)# ip scp server enable
   R3(config)# end
   ```