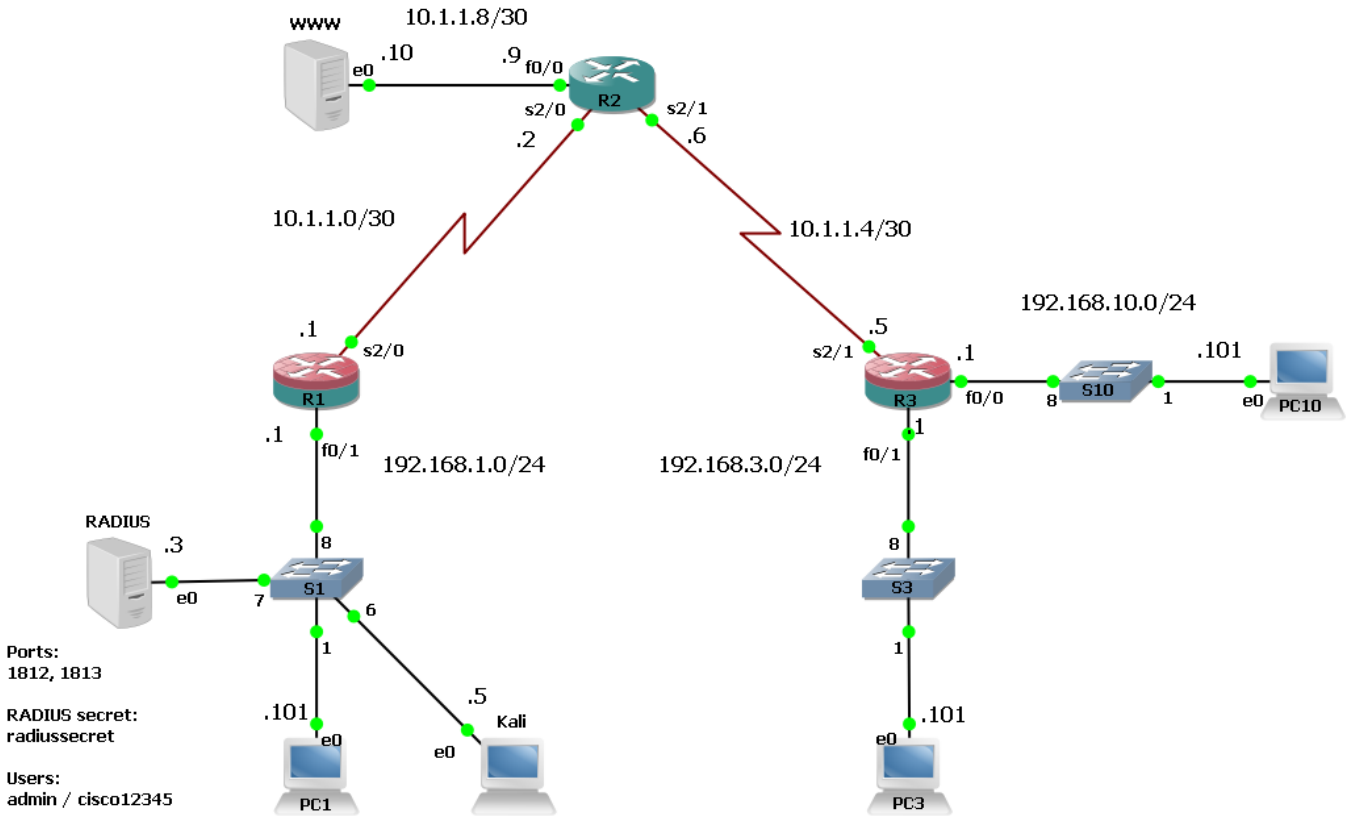
CCNA Security

Лабораторная работа 5

Изучение протоколов Telnet и SSH

Топология



Описание

В этой лабораторной работе вы примерите на себя роль злоумышленника, ставшего человеком посредине (Man-In-The-Middle, MITM). С помощью сниффера Wireshark вы будете отлавливать пакеты, а затем их анализировать. В ходе анализа вы убедитесь в небезопасности протокола Telnet, после чего настроите протокол SSH.

Более подробная информация о Wireshark есть на сайте проекта https://www.wireshark.org/

Также на моём канале в Youtube можно посмотреть видео из проекта «В поисках потерянного пакета», посвящённого изучению сетей с помощью Wireshark. Ссылка: https://youtube.com/playlist?list=PLJ_TFtUlIAJf4qd2M8mnf7W5tLehnyA_N

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	-

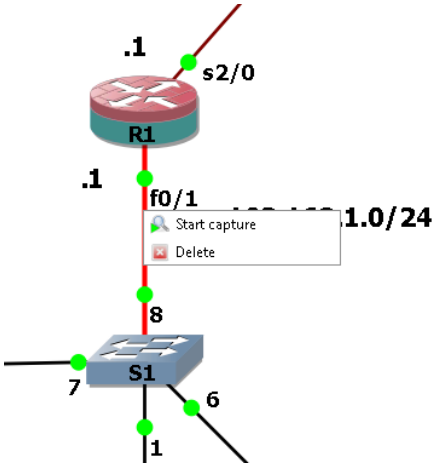
Имена пользователей и пароли

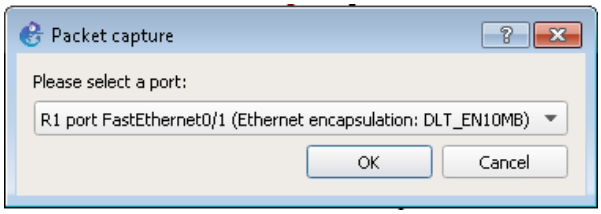
	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	admin	cisco12345	admin	cisco12345	cisco12345
R2	-	-	-	-	-
R3	admin	cisco12345	admin	cisco12345	cisco12345

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

Часть 1: Изучение протокола Telnet

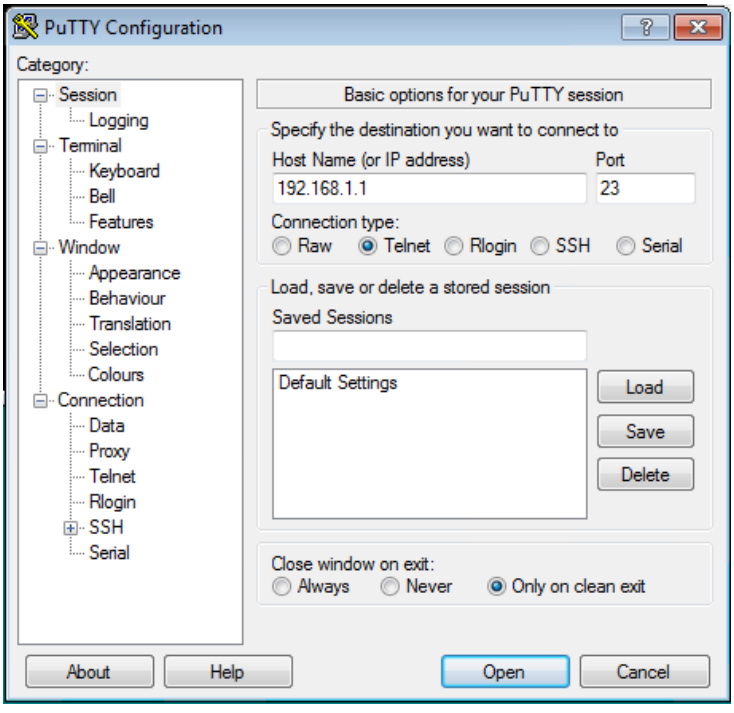
1. Запустите захват на линке между R1 и S1. Для этого на основной машине в окне GNS3 щёлкните правой кнопкой мыши по линку между R1 и S1, в контекстном меню выберите **Start Capture**. В открывшемся окне просто нажмите **OK**. Дождитесь открытия Wireshark.

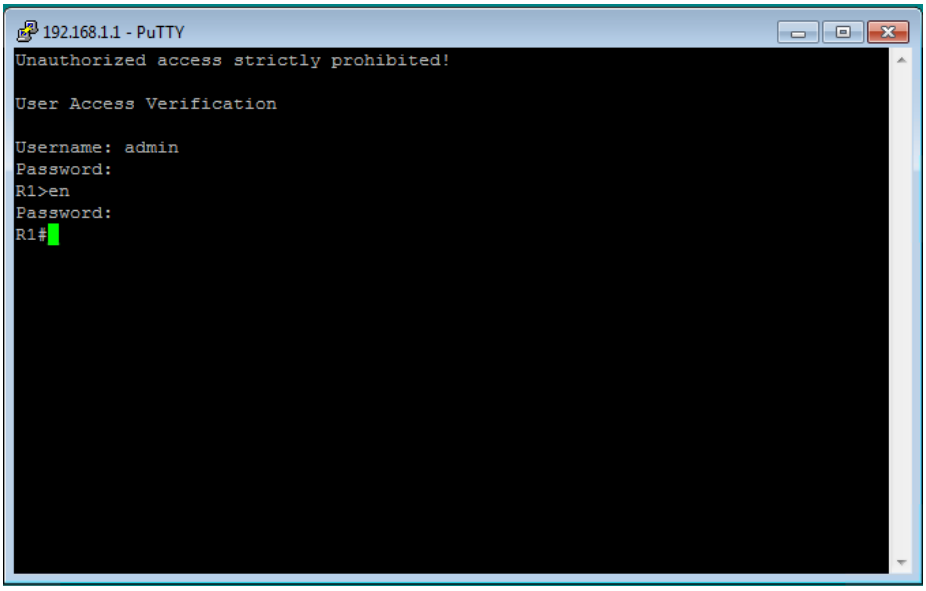




2. Войдите в виртуальную машину PC1.

3. Запустите PuTTY. Подключитесь к маршрутизатору R1 по протоколу Telnet, а затем перейдите в привилегированный режим.

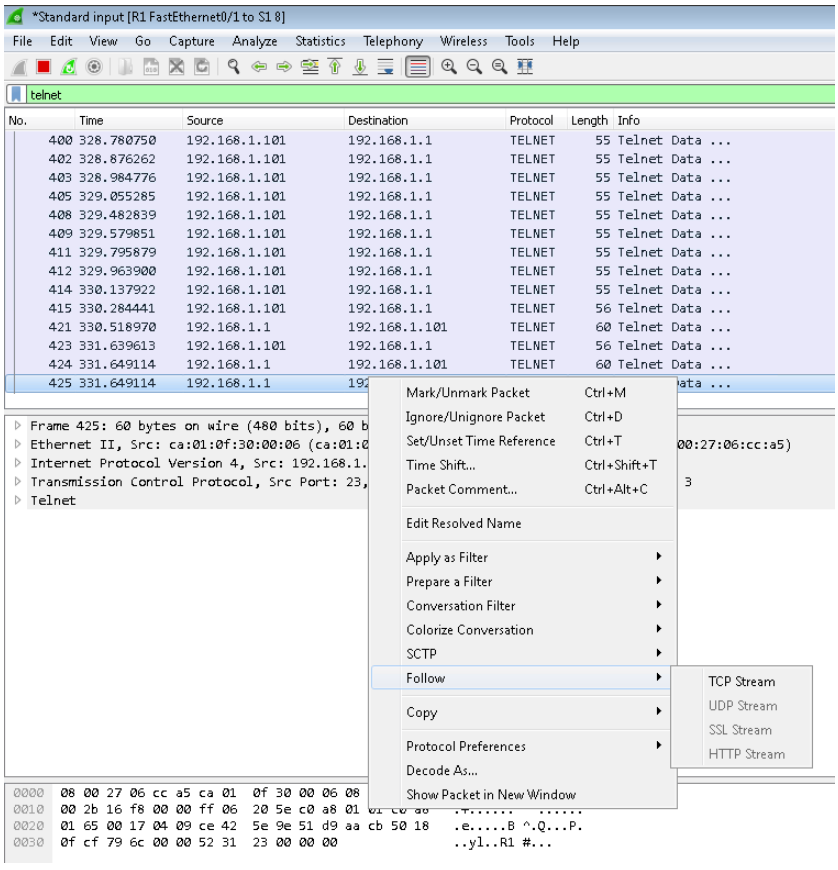




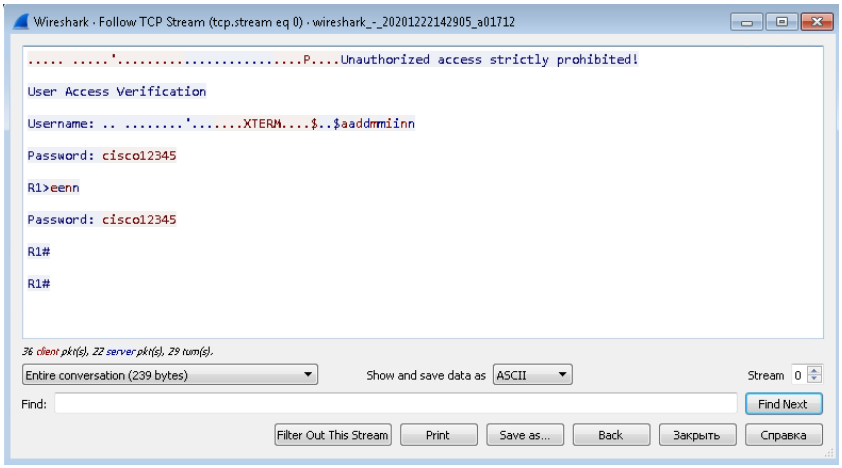
4. Вернитесь в Wireshark.

5. Введите в поле Display Filter слово **telnet** и нажмите Enter. Поле будет подсвечено зелёным, это значит, что применён корректный фильтр. В таблице пакетов теперь будут отображаться только пакеты протокола Telnet.

6. Можно рассматривать каждый пакет отдельно, но проще воспользоваться функционалом Follow Stream, тогда Wireshark объединит все пакеты в указанной сессии и предоставит информацию в отдельном окне. Для этого щёлкните правой кнопкой мыши на последний пакет Telnet в таблице. В контекстном меню выберите **Follow -> TCP Stream**.



7. В открывшемся окне будет представлен собранный текст сессии. Видно ли переданные имена пользователей и пароли?



8. Вы убедились, что протокол Telnet передаёт всю информацию в открытом виде и его использование небезопасно. Закройте окно Follow TCP Stream, сверните основное окно Wireshark.

Часть 2: Настройка и изучение протокола SSH на маршрутизаторе R1

1. Подключитесь к консоли маршрутизатора R1.

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

3. Задайте имя домена acad.local.
```
R1(config)# ip domain-name acad.local
```

4. Сгенерируйте ключи RSA с длиной 2048 бит.
```
R1(config)# crypto key generate rsa general-keys modulus 2048
The name for the keys will be: R1.acad.local

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 34 seconds)
```

5. Разрешите протокол SSH только 2-ой версии.
```
R1(config)# ip ssh version 2
```

6. Разрешите удалённые подключения только по протоколу SSH.
```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# end
```

7. Проверьте настройки протокола SSH.
```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
< Вывод опущен >
```

8. Протокол SSH использует для своей работы транспортный протокол TCP и стандартный порт 22. Проверьте, что на R1 этот порт прослушивается.

```
R1# show control-plane host open-ports
Active internet connections (servers and established)
Prot          Local Address            Foreign Address                 Service    State
 tcp                  *:22                     *:0                  SSH-Server   LISTEN
 tcp                  *:23                     *:0                      Telnet   LISTEN
```

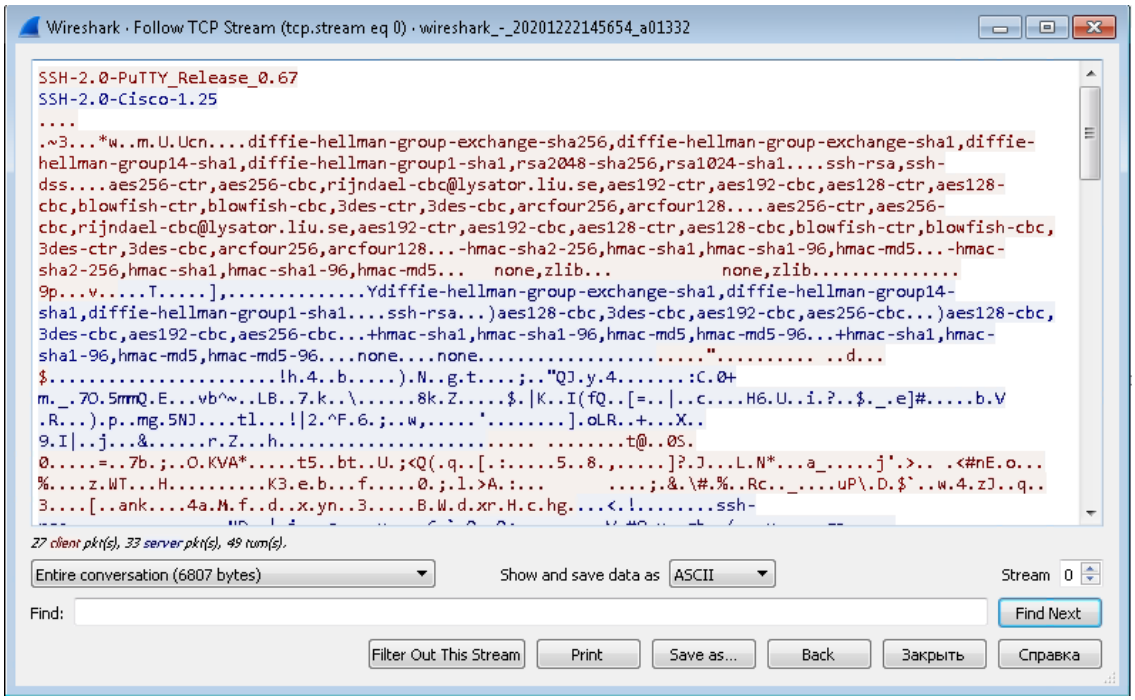
9. Войдите в виртуальную машину PC1.

10. Запустите PuTTY. Подключитесь к маршрутизатору R1 по протоколу SSH, а затем перейдите в привилегированный режим.

11. Вернитесь в Wireshark.

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

13. Щёлкните правой кнопкой мыши на последний пакет SSH в таблице. В контекстном меню выберите **Follow -> TCP Stream**. Попробуйте разобрать что-нибудь в открывшемся окне.



14. Сначала вывод идёт в открытом виде. На этом этапе устройства сообщают свои возможности (поддерживаемые алгоритмы шифрования, хеширования, группы DH и т.д.). После этого начинается безопасный обмен данными. Закройте окно Follow TCP Stream, закройте основное окно Wireshark.

Часть 3: Настройка протокола SSH на маршрутизаторе R3

1. Проделайте шаги 1-10 из части 2, но в этот раз на маршрутизаторе R3.