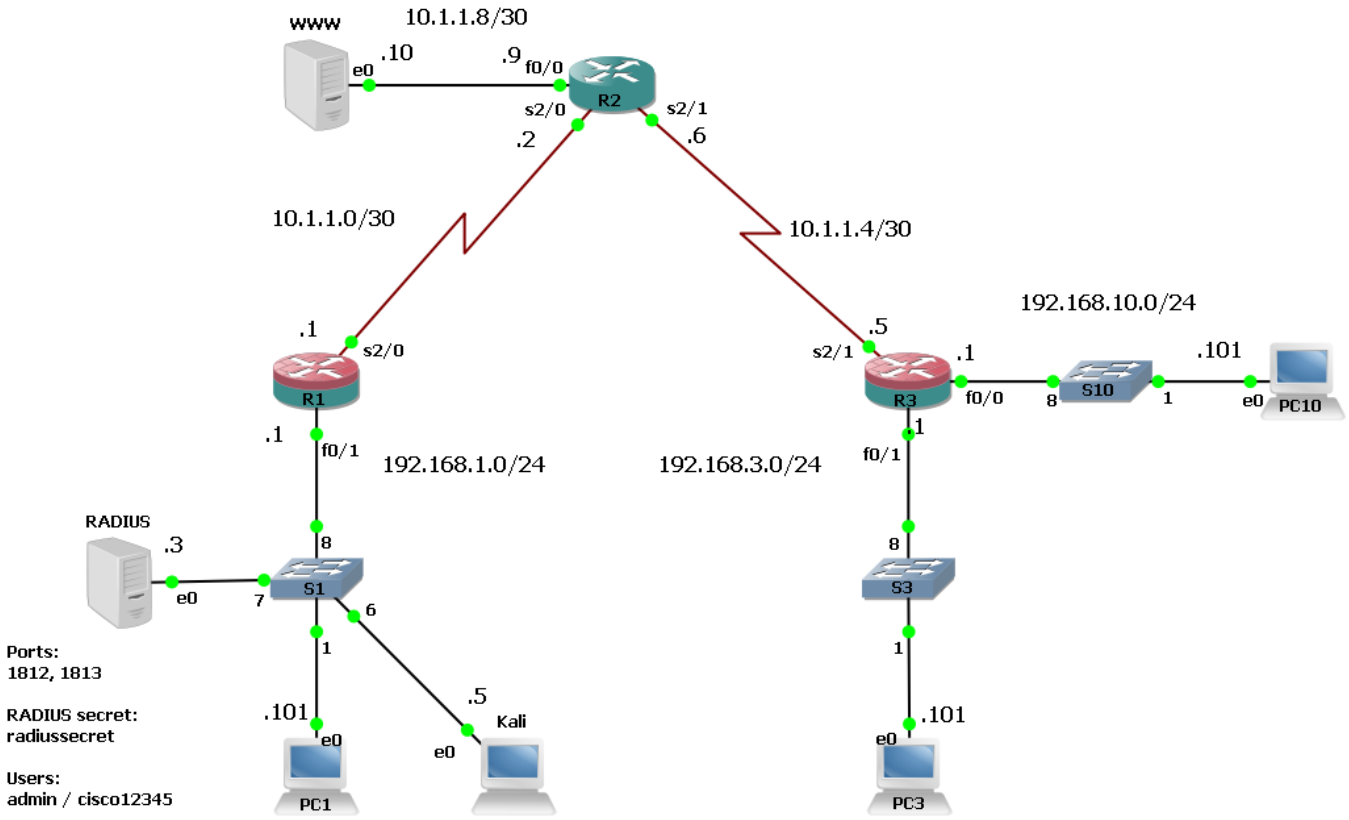
CCNA Security

Лабораторная работа 15

Изучение серверной модели AAA и протокола RADIUS

Топология



Описание

В этой лабораторной работе вы перейдёте от локальной аутентификации к серверной. Аутентификационным сервером будет выступать виртуальная машина RADIUS. Виртуальная машина уже настроена и готова к приёму запросов от маршрутизаторов R1 и R3 по протоколу RADIUS.

В качестве сервера аутентификации можно использовать множество решений. Это и решение от Cisco Systems – Cisco ISE (Identity Service Engine), и решение на базе Microsoft Windows Server с установленной ролью NAP или NPS. В этой лабораторной работе используется ОС FreeBSD с установленным ПО freeRADIUS.

Если вас заинтересует freeRADIUS, то полную документацию всегда можно найти на сайте проекта https://freeradius.org/

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 RADIUS и настройка серверной аутентификации 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 **radius** и нажмите Enter.

3. Перейдите в консоль маршрутизатора R1.

4. Включите вывод отладочных сообщений, связанных с протоколом RADIUS.
```
R1# debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off
```

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

6. Задайте настройки для подключения к RADIUS-серверу: ipv4-адрес, порт для аутентификации и авторизации, порт для учёта, ключ. Настроенный сервер автоматически попадёт в группу всех настроенных RADIUS-серверов.
```
R1(config)# radius server RAD1
R1(config-radius-server)# address ipv4 192.168.1.3 auth-port 1812 acct-port 1813
R1(config-radius-server)# key radiussecret
R1(config-radius-server)# exit
```

7. В качестве адреса отправителя пакетов протокола RADIUS используйте адрес с интерфейса fa0/1.
```
R1(config)# ip radius source-interface fa0/1
```

8. Измените список методов AUTHEN1. Укажите один единственный метод group radius.
```
R1(config)# aaa authentication login AUTHEN1 group radius
R1(config)# exit
```

9. Войдите в виртуальную машину PC1. Запустите PuTTY. Попробуйте подключиться к маршрутизатору R1 по протоколу SSH. На сервере уже создана учётная запись admin с паролем cisco12345. Аутентификация должна пройти успешно.

10. Вернитесь в консоль маршрутизатора R1. Изучите вывод отладочных сообщений. В отладочных сообщениях вы увидите, как маршрутизатор R1 высылает пакет Access-Request, сервер в ответ присылает ответ Access-Accept.

```
RADIUS(0000009B): Config NAS IP: 0.0.0.0
RADIUS(0000009B): Config NAS IPv6: ::
RADIUS/ENCODE(0000009B): acct_session_id: 139
RADIUS(0000009B): sending
RADIUS(0000009B):       Send       Access-Request       to       192.168.1.3:1812
id 1645/1, len 69
RADIUS:     authenticator   AD   36   DC   07   1F   1A   92   59   -   2C   15   E9
2A F1 6E D6 D3
RADIUS:  User-Name            [1]    7    "admin"
RADIUS:  User-Password        [2]    18   *
RADIUS:  NAS-Port             [5]    6    2
RADIUS:  NAS-Port-Id          [87]   6    "tty2"
RADIUS:       NAS-Port-Type                          [61]       6           Virtual
[5]
RADIUS:  NAS-IP-Address       [4]    6    192.168.1.1
RADIUS(0000009B): Sending a IPv4 Radius Packet
RADIUS(0000009B): Started 5 sec timeout
RADIUS(0000009B): Request timed out!
RADIUS:     Retransmit     to     (192.168.1.3:1812,1813)     for     id     1645/
1
RADIUS(0000009B): Started 5 sec timeout
RADIUS: Received from id 1645/1 192.168.1.3:1812, Access-Accept, len 20
RADIUS:     authenticator   88   CD   1C   16   24   15   16   DB   -   21   60   D2
8A 67 1F C7 AA
RADIUS(0000009B): Received from id 1645/1
```

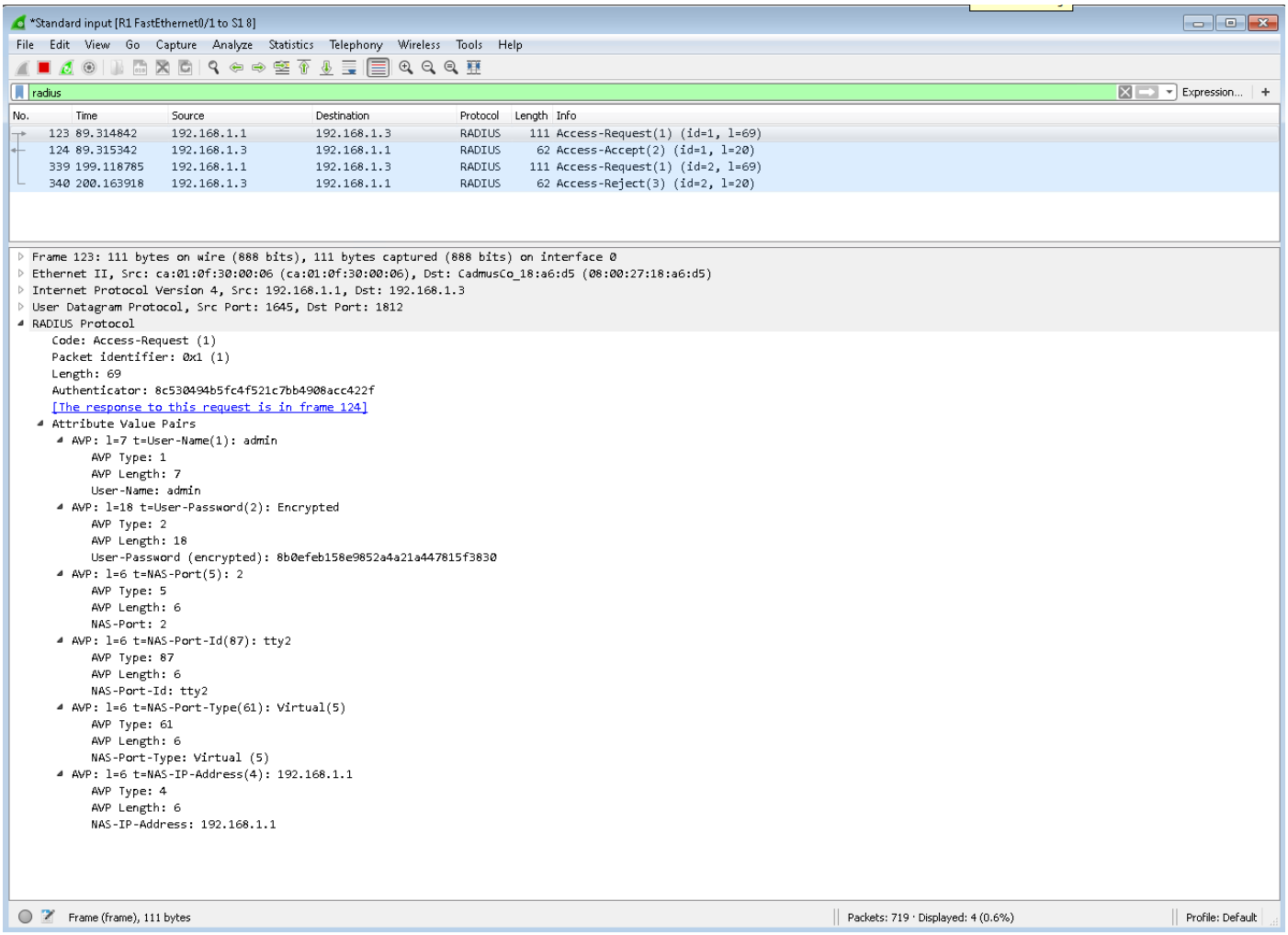
11. Вернитесь в виртуальную машину PC1. Запустите PuTTY. Попробуйте подключиться к маршрутизатору R1 по протоколу SSH с неверным паролем.

12. Вернитесь в консоль маршрутизатора R1. Изучите вывод отладочных сообщений. В отладочных сообщениях вы увидите, как маршрутизатор R1 высылает пакет Access-Request, сервер в ответ присылает ответ Access-Reject.

```
RADIUS(0000009B): Config NAS IP: 0.0.0.0
RADIUS(0000009B): Config NAS IPv6: ::
RADIUS/ENCODE(0000009B): acct_session_id: 139
RADIUS(0000009B): sending
RADIUS(0000009B):       Send       Access-Request       to       192.168.1.3:1812
id 1645/1, len 69
RADIUS:     authenticator   AD   36   DC   07   1F   1A   92   59   -   2C   15   E9
2A F1 6E D6 D3
RADIUS:  User-Name            [1]    7    "admin"
RADIUS:  User-Password        [2]    18   *
RADIUS:  NAS-Port             [5]    6    2
RADIUS:  NAS-Port-Id          [87]   6    "tty2"
RADIUS:       NAS-Port-Type                          [61]       6           Virtual
[5]
RADIUS:  NAS-IP-Address       [4]    6    192.168.1.1
RADIUS(0000009B): Sending a IPv4 Radius Packet
RADIUS(0000009B): Started 5 sec timeout
RADIUS(0000009B): Request timed out!
RADIUS:     Retransmit     to     (192.168.1.3:1812,1813)     for     id     1645/
1
RADIUS(0000009B): Started 5 sec timeout
RADIUS: Received from id 1645/1 192.168.1.3:1812, Access-Reject, len 20
RADIUS:     authenticator   88   CD   1C   16   24   15   16   DB   -   21   60   D2
8A 67 1F C7 AA
```

```
RADIUS(0000009B): Received from id 1645/1
```

13. Вернитесь в Wireshark на основной машине. Вы должны увидеть 4 пакета: Access-Request, Access-Accept, Access-Request, Access-Reject. Изучите содержимое пакетов. Видно ли пароль для общения с сервером? Видно ли имя пользователя? Видно ли пароль пользователя?



14. Закройте основное окно Wireshark.

15. Вернитесь на основную машину и выключите сервер RADIUS. Для этого в окне GNS3 щёлкните правой кнопкой по RADIUS, в контекстном меню выберите **Stop**. Дождитесь, пока закроется окно виртуальной машины RADIUS, и ещё раз щёлкните правой кнопкой по RADIUS, в контекстном меню выберите **Stop**. Линк рядом с виртуальной машиной станет красным.

16. Вернитесь в виртуальную машину PC1. Запустите PuTTY. Попробуйте подключиться к маршрутизатору R1 по протоколу SSH. Подключение будет неуспешно, т.к. в списке методов указан один единственный метод group radius, а все RADIUS-сервера в данный момент недоступны.

17. Вернитесь в консоль маршрутизатора R1. Изучите вывод отладочных сообщений. Маршрутизатор R1 посылает запрос несколько раз, а потом сдаётся.

```
RADIUS(00000043): Config NAS IP: 0.0.0.0
```

```
RADIUS(00000043): Config NAS IPv6: ::
RADIUS/ENCODE(00000043): acct_session_id: 16
RADIUS(00000043): sending
RADIUS(00000043): Send Access-Request to 192.168.1.3:1812 id 1645/3, len 69
RADIUS:  authenticator F4 87 B9 FA CE 91 79 CD - CE FF C7 3E 77 D9 DD 1F
RADIUS:  User-Name           [1]   7   "admin"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port      [5]   6   2
RADIUS:  NAS-Port-Id         [87]  6   "tty2"
RADIUS:  NAS-Port-Type    [61]  6   Virtual                   [5]
RADIUS:  NAS-IP-Address      [4]   6   192.168.1.1
RADIUS(00000043): Sending a IPv4 Radius Packet
RADIUS(00000043): Started 5 sec timeout
RADIUS(00000043): Request timed out!
RADIUS: Retransmit to (192.168.1.3:1812,1813) for id 1645/3
RADIUS(00000043): Started 5 sec timeout
RADIUS(00000043): Request timed out!
RADIUS: Retransmit to (192.168.1.3:1812,1813) for id 1645/3
RADIUS(00000043): Started 5 sec timeout
RADIUS(00000043): Request timed out!
RADIUS: Retransmit to (192.168.1.3:1812,1813) for id 1645/3
RADIUS(00000043): Started 5 sec timeou
RADIUS(00000043): Request timed out!
RADIUS: No response from (192.168.1.3:1812,1813) for id 1645/3
RADIUS/DECODE: No response from radius-server; parse response; FAIL
RADIUS/DECODE: Case error(no response/ bad packet/ op decode);parse response;
FAIL
```

18. Измените список методов AUTHEN1. Укажите дополнительный метод local-case на случай, если все RADIUS-сервера станут недоступны.

```
R1# conf t
R1(config)# aaa authentication login AUTHEN1 group radius local-
case
R1(config)# exit
```

19. Вернитесь в виртуальную машину PC1. Запустите PuTTY. Попробуйте подключиться к маршрутизатору R1 по протоколу SSH. Подключение будет успешно. Сначала маршрутизатор попытается провести аутентификацию с помощью метода group radius, но т.к. все сервера недоступны, переключится на второй метод в списке – local-case. В локальной базе данных пользователей и паролей есть запасная учётная запись на этот случай.

20. Отключите вывод отладочных сообщений.

```
R1# no debug all
All possible debugging has been turned off
```

21. Вернитесь на основную машину и включите сервер RADIUS. Для этого в окне GNS3 щёлкните правой кнопкой по RADIUS, в контекстном меню выберите **Start**.

Часть 2: Настройка серверной аутентификации на маршрутизаторе R3

1. Перейдите в консоль маршрутизатора R3.

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

3. Задайте настройки для подключения к RADIUS-серверу: ipv4-адрес, порт для аутентификации и авторизации, порт для учёта, ключ. Настроенный сервер автоматически попадёт в группу всех настроенных RADIUS-серверов.
   ```
   R3(config)# radius server RAD1
   R3(config-radius-server)# address ipv4 192.168.1.3 auth-port 1812 acct-port 1813
   R3(config-radius-server)# key radiussecret
   R3(config-radius-server)# exit
   ```

4. В качестве адреса отправителя пакетов протокола RADIUS используйте адрес с интерфейса fa0/1.
   ```
   R3(config)# ip radius source-interface fa0/1
   ```

5. Измените список методов AUTHEN1. Укажите методы group radius и local-case.
   ```
   R3(config)# aaa authentication login AUTHEN1 group radius local-case
   R3(config)# end
   ```

6. Для теста связи с RADIUS-сервером и проверки имени пользователя и пароля можно воспользоваться командой **test**. Вместо параметра **legacy** можно использовать параметр **new-code**. Например, вы хотите проверить, пройдёт ли аутентификацию пользователь admin с паролем cisco. Аутентификация не успешна.
   ```
   R3# test aaa group radius admin cisco legacy
   Attempting authentication test to server-group radius using radius
   User authentication request was rejected by server.
   ```

7. А что по поводу пользователя admin с паролем cisco12345? Аутентификация успешна.
   ```
   R3# test aaa group radius admin cisco12345 legacy
   Attempting authentication test to server-group radius using radius
   User was successfully authenticated.
   ```