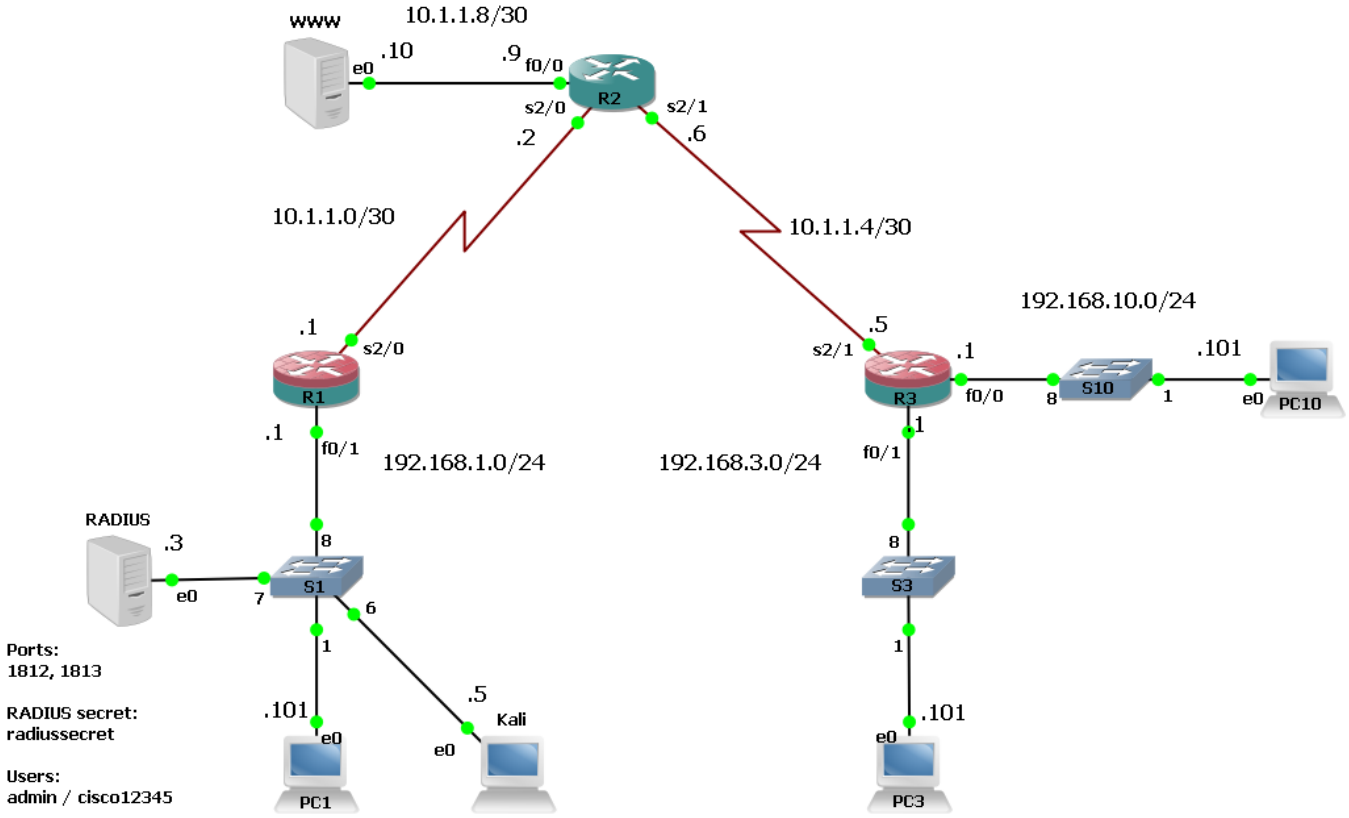
CCNA Security

Лабораторная работа 6

Усиление защиты маршрутизатора от атак на доступ

Топология



Описание

В этой лабораторной работе вы усилите защиту маршрутизатора от атак на доступ с помощью команды login. Хотя мы рассматриваем защиту маршрутизаторов, эти же команды и параметры доступны и для коммутаторов (как третьего уровня, так и второго).

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 маршрутизатора R1

1. Подключитесь к консоли маршрутизатора R1.

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

3. Установите задержку при проверке аутентификационных данных в 10 секунд. Это затруднит попытки взлома методом перебора.
```
R1(config)# login delay 10
```

4. Включите протоколирование всех успешных и неуспешных попыток входа на устройство.
```
R1(config)# login on-success log
R1(config)# login on-failure log
```

5. Включите блокировку попыток входа на устройство на пять минут, если были зафиксированы три неудачные попытки входа в течение двух минут.
```
R1(config)# login block-for 300 attempts 3 within 120
```

6. Во время блокировки все новые попытки входа на устройство будут автоматически неуспешны, но уже открытые сессии продолжат работу. Чтобы оставить возможность удалённого подключения с доверенных узлов или сетей, составьте ACL и прикрепите его к команде login.
```
R1(config)# ip access-list standard ACL-LOGIN-QM
R1(config-std-nacl)# permit host 192.168.1.101
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class ACL-LOGIN-QM
R1(config)# exit
```

7. Проверьте усиленные настройки входа.
```
R1# show login
     A login delay of 10 seconds is applied.
     Quiet-Mode access list ACL-LOGIN-QM is applied.
     All successful login is logged.
     All failed login is logged.

     Router enabled to watch for login Attacks.
     If more than 3 login failures occur in 120 seconds or less,
     logins will be disabled for 300 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 95 seconds.
         Login failures for current window: 0.
     Total login failures: 0.
```

8. Проверьте созданный список контроля доступа. Помимо созданного вами списка ACL-LOGIN-QM в выводе присутствует список sl_def_acl. Этот список был создан автоматически, не трогайте его.

```
R1# show access-list
Standard IP access list ACL-LOGIN-QM
    10 permit 192.168.1.101
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet log
    20 deny tcp any any eq www log
    30 deny tcp any any eq 22 log
    40 permit tcp any any eq 22 log
```

9. Войдите в виртуальную машину PC3.

10. Запустите PuTTY. Попробуйте подключиться несколько раз к маршрутизатору R1 с неверными данными. Обратите внимание на задержку после ввода пароля. После третьей неудачной попытки сессия будет разорвана. Попробуйте подключиться к маршрутизатору R1 ещё раз, сессия сразу будет закрыта.

11. Войдите в виртуальную машину PC1.

12. Запустите PuTTY. Попробуйте подключиться к маршрутизатору R1 с верными данными. Подключение будет успешным несмотря на запрет, т.к. адрес узла R1 попадает в ACL под разрешающую строку.

13. Вернитесь в консоль маршрутизатора R1.

14. Посмотрите на выведенные сообщения о неуспешных и успешных попытках входа, включении «тихого режима».

```
*Dec 22 15:32:11.819: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 192.168.3.101] [localport: 22] [Reason: Login Authentication Failed] at 15:32:11 UTC Tue Dec 22 2020

*Dec 22 15:32:25.003: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 192.168.3.101] [localport: 22] [Reason: Login Authentication Failed] at 15:32:25 UTC Tue Dec 22 2020

*Dec 22 15:32:36.815: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 192.168.3.101] [localport: 22] [Reason: Login Authentication Failed] at 15:32:36 UTC Tue Dec 22 2020

*Dec 22 15:32:36.815: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 95 secs, [user: admin] [Source: 192.168.3.101] [localport: 22] [Reason: Login Authentication Failed] [ACL: ACL-LOGIN] at 15:32:36 UTC Tue Dec 22 2020

*Dec 22 15:33:05.895: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 192.168.1.101] [localport: 22] at 15:33:05 UTC Tue Dec 22 2020
```

15. По умолчанию устройства Cisco не выводят дату и время рядом с лог-сообщениями или отладочными сообщениями, однако в нашей лабораторной работе вывод даты и времени был включён заранее.

```
R1# show run | i service
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

Часть 2: Настройка маршрутизатора R3

1. Проделайте шаги 1-8 из части 1, но в этот раз на маршрутизаторе R3.