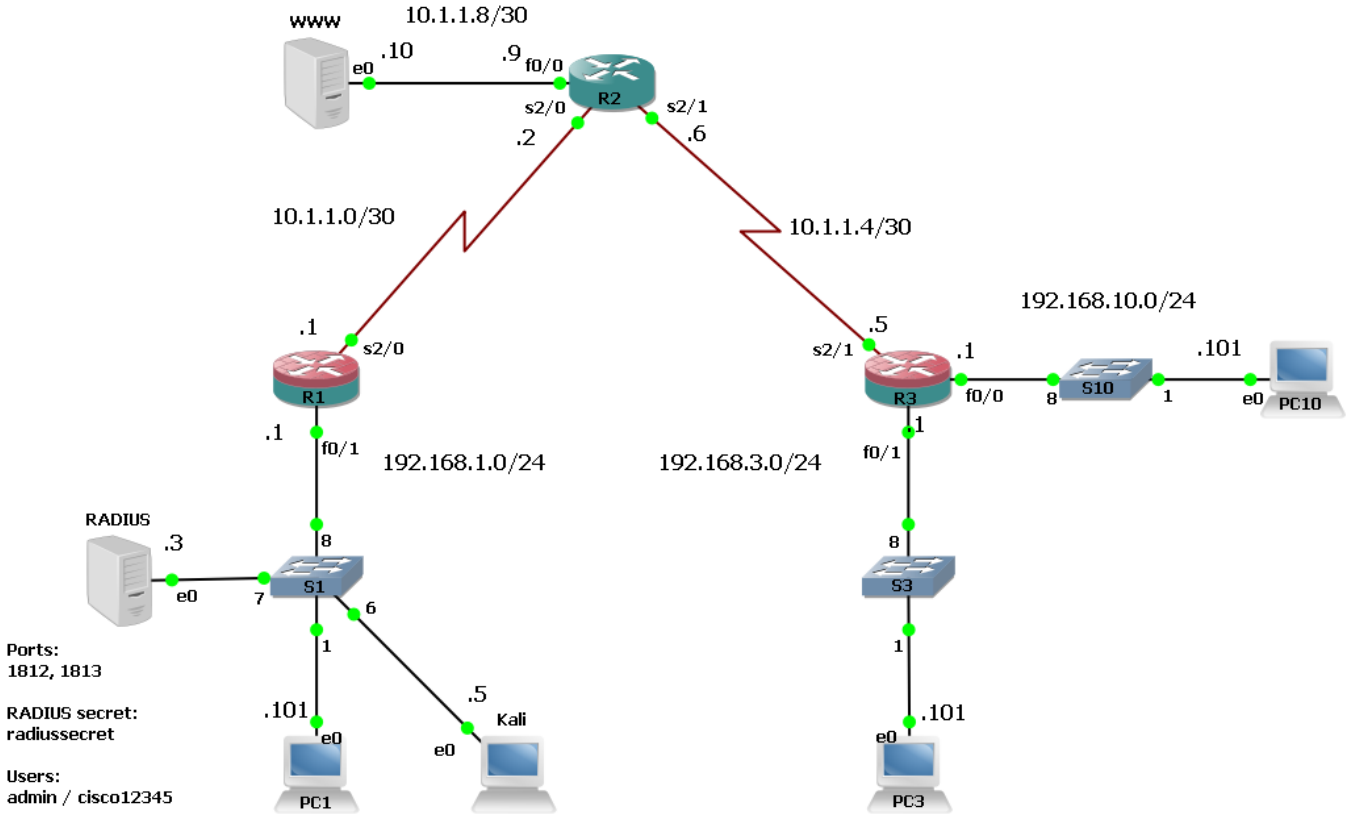
CCNA Security

Лабораторная работа 3

Изучение хранения паролей и варианты взлома

Топология



Описание

В этой лабораторной работы вы изучите хранение паролей (в открытом виде, зашифрованных сервисом шифрования паролей, захешированных с помощью хеш-функции md5 и scrypt), попробуете взломать пароли с помощью сторонних сайтов или взломщика паролей John The Ripper.

Более подробную информацию о John The Ripper можно найти на сайте проекта https://www.openwall.com/john/

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	-	-	-	-	-
R2	-	-	-	-	-
R3	-	-	-	-	-

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

Часть 1: Изучение паролей в открытом виде и сервиса шифрования паролей

1. Подключитесь к консоли маршрутизатора R1.

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

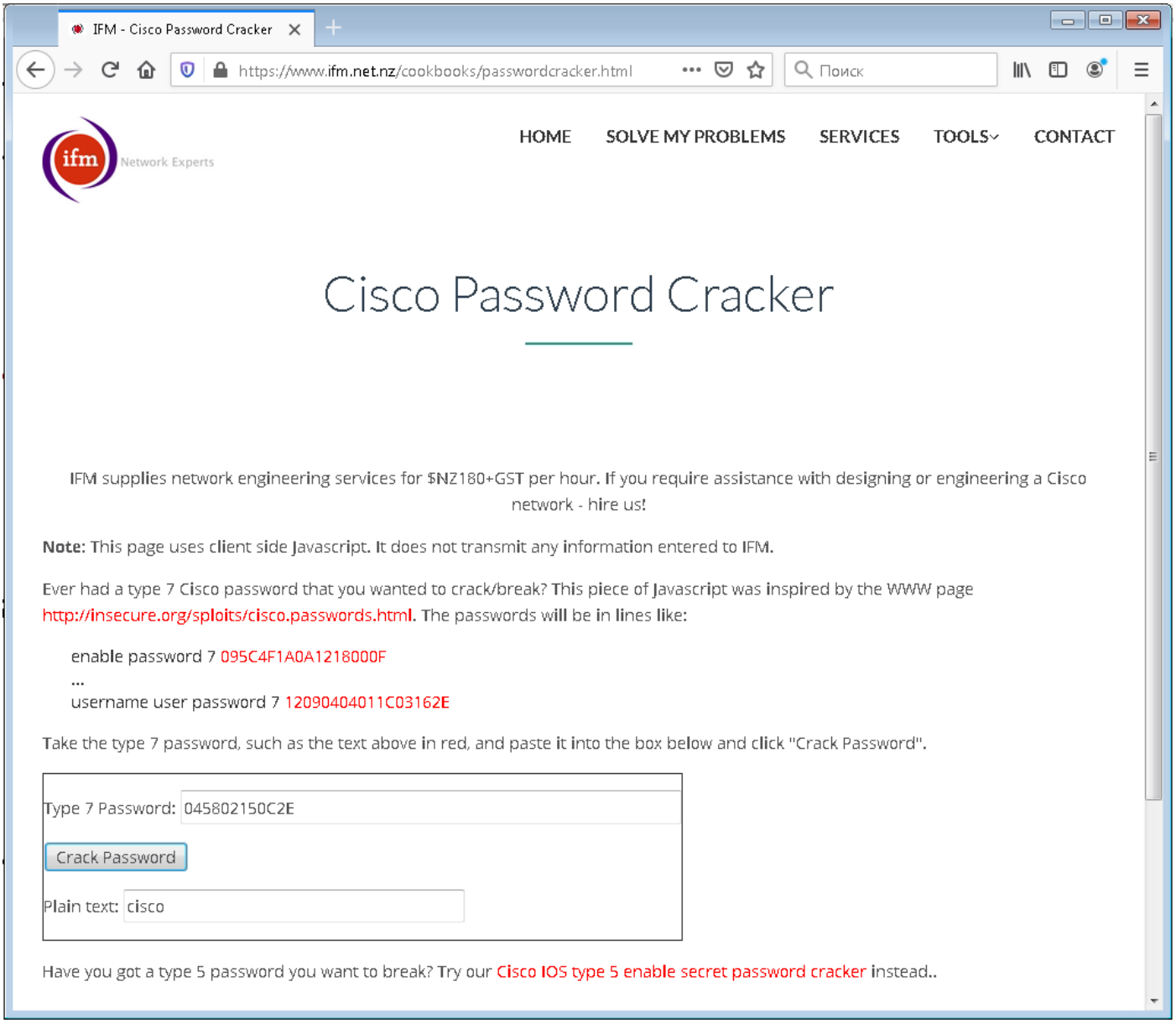
3. Задайте пароль на привилегированный режим.
   ```
   R1(config)# enable password cisco
   ```

4. Выведите кусочек running-config и убедитесь, что пароль хранится в открытом виде.
   ```
   R1(config)# do show run | i password
   no service password-encryption
   enable password cisco
   ```

5. Включите сервис шифрования паролей.
   ```
   R1(config)# service password-encryption
   ```

6. Выведите кусочек running-config и убедитесь, что пароль скрыт. Перед паролем будет стоять тип 7. Тип 7 указывает, что этот пароль был получен с помощью сервиса шифрования паролей. Ваш скрытый пароль может отличаться.
   ```
   R1(config)# do show run | i password
   service password-encryption
   enable password 7 045802150C2E
   ```

7. Скопируйте пароль в буфер обмена. Откройте браузер, зайдите на сайт **google.com** и введите запрос **cisco type 7 password decrypt**. Откройте любой сайт из найденных и попробуйте выполнить дешифровку пароля. Результат работы одного из сайтов представлен ниже.



8. Мы убедились, что пароль, созданный с помощью сервиса шифрования паролей, не даёт полноценной защиты. Стоит рассматривать этот метод только как защиту от подглядывающего через плечо (Shoulder Surfing). Старайтесь никогда не указывать пароли с помощью команды или параметра password. Удалите небезопасные пароли.

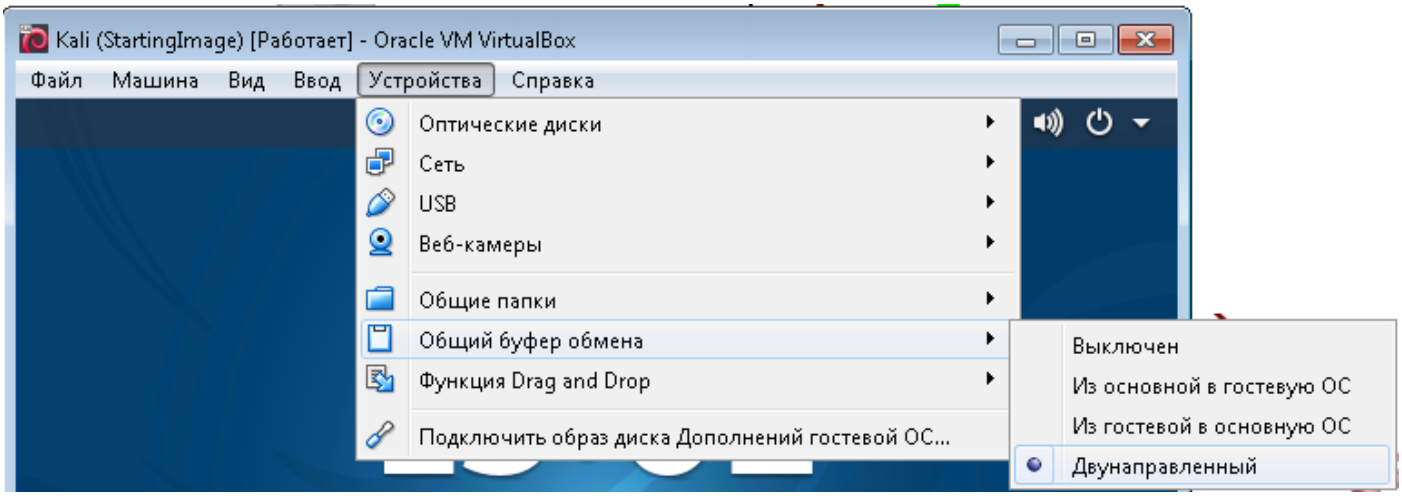
```
R1(config)# no enable password
R1(config)# do show run | i password
service password-encryption
```

Часть 2: Изучение захешированных паролей

1. Задайте секретный пароль на привилегированный режим.
   ```
   R1(config)# enable secret cisco
   ```

2. Выведите кусочек running-config и убедитесь, что пароль захеширован. По умолчанию пароль будет захеширован с помощью хеш-функции md5. Помните, что из-за наличия соли ваш хеш будет отличаться. Из хеша гораздо труднее получить пароль. При должной сложности и длине пароля на перебор могут потребоваться годы, однако наш пароль лёгкий и очень короткий. Скопируйте получившийся хеш в буфер обмена.
   ```
   R1(config)# do show run | i secret
   enable secret 5 $1$2ClI$nmJHyAwXHBT//WzIp4Yo9.
   ```

3. Включите общий буфер обмена между основной машиной и виртуальной машиной Kali. В окне виртуальной машины Kali выберите пункт меню **Устройства -> Общий буфер обмена -> Двунаправленный**.



4. Войдите в виртуальную машину Kali.

5. Откройте **Terminal (Applications -> Favorites -> Terminal).**

6. Создайте текстовый файл pass1, содержащий хэш. Для этого введите команду **echo '**(одинарная прямая кавычка), вставьте хэш, введите **'> pass1**

   ```
   root@kali:~# echo '$1$2ClI$nmJHyAwXHBT//WzIp4Yo9.'> pass1
   ```

7. Запустите взломщик паролей john и дождитесь выполнения работы. В выводе обратите внимание на найденный пароль и скорость перебора.

```
root@kali:~# john pass1
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
cisco            (?)
1g 0:00:00:04 DONE 3/3 (2020-12-20 11:42) 0.2092g/s 42270p/s 42270c/s 42270C/s
cisic..ciscu
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

8. Вернитесь в консоль маршрутизатора R1.

9. Задайте секретный пароль на привилегированный режим, но в этот раз для хранения используйте хеш-функцию scrypt.
   ```
   R1(config)# enable algorithm-type scrypt secret cisco
   ```

10. Выведите кусочек running-config и убедитесь, что пароль захеширован. Обратите внимание на новый тип пароля 9, большую длину соли и самого хеша. Скопируйте получившийся хеш в буфер обмена.

```
R1(config)# do show run | i secret
enable secret 9 $9$nLEhBuWA7zpPvG$9o73vaUY84qcwVgSrbn2oWeFz0L0zp6fqVPciYnklQI
```

11. Вернитесь в виртуальную машину Kali.

12. Создайте текстовый файл pass2, содержащий хэш. Для этого введите команду **echo '**(одинарная прямая кавычка), вставьте хэш, введите **'> pass2**

```
root@kali:~# echo '$9$3mOsLXcTzYrOhm$2ql/r82XMJxp9rFnzZ4bZ8MjMXRHrBUoIwlbw6VRvJE'>
pass2
```

13. Запустите взломщик паролей john и дождитесь выполнения работы. Взлом займёт около 10 минут. Хеш-функция scrypt требует гораздо больше ресурсов, поэтому взлом пароля методом перебора требует гораздо больше времени. В выводе обратите внимание на найденный пароль и скорость перебора. Сравните время работы и скорость перебора с предыдущим запуском.

```
root@kali:~# john pass2
Using default input encoding: UTF-8
Loaded 1 password hash (scrypt [Salsa20/8 128/128 AVX])
Press 'q' or Ctrl-C to abort, almost any other key for status
cisco            (?)
1g 0:00:09:40 DONE 3/3 (2020-12-20 13:50) 0.001721g/s 347.8p/s 347.8c/s 347.8C/s cisco
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

14. Закройте Terminal.

15. Вернитесь в консоль маршрутизатора R1.

16. Удалите пароль на привилегированный режим.
    ```
    R1(config)# no enable secret
    R1(config)# exit
    ```