

Домашнє завдання до теми "Додаткові атаки на криптографічні системи".

Тема: Злам WEP-пароля для Wi-Fi мережі за допомогою Aircrack-ng


Мета: Навчитись здійснювати злам WEP-ключа на основі перехопленого трафіку за допомогою інструменту Aircrack-ng

Середовище виконання:

- Операційна система: Windows 11
- Інструмент: [Aircrack-ng 1.7](#)
- Файл для аналізу: [crackme.pcap-01.cap](#)
- Інтерфейс: PowerShell

Етапи виконання:

1. Завантаження та встановлення Aircrack-ng

- Завантажено архів  [aircrack-ng-1.7-win.zip](#) [aircrack-ng-1.7-win.zip](#) з офіційного сайту <https://www.aircrack-ng.org>
- Розпаковано в папку [C:\Users\admin\aircrack-ng-1.7-win](#)

Перевірено доступність виконання через PowerShell: `.\aircrack-ng.exe --help`

```
PS C:\Users\admin> cd 'C:\Users\admin\aircrack-ng-1.7-win\bin'
PS C:\Users\admin\aircrack-ng-1.7-win\bin> .\aircrack-ng.exe --help

Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:
  -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
  -t <ssid> : target selection: network identifier
  -b <ssid> : target selection: access point's MAC
  -p <nbcpu> : # of CPU to use (default: all CPU's)
  -q <quiet> : enable quiet mode (no status output)
  -m <macs> : merge the given AP's to a virtual one
  -l <file> : write key to file. Overwrites file.

Static WEP cracking options:
  -c : search alpha-numeric characters only
  -t : search binary coded decimal chr only
  -b : search the numeric key for Fritz!Box
  -d <mask> : use masking of the key (01:XX:CF:V)
  -m <addr> : MAC address to filter usable packets
  -l <bits> : WEP key length: 64/128/152/256/512
  -i <index> : WEP key index (1 to 4), default: any
  -f <fudge> : bruteforce fudge factor, default: 2
  -d <force> : disable one attack method (1 to 10)
  -a <or> <no> : disable bruteforce for last keybytes
  -w1 : last keybyte bruteforcing (default)
  -w2 : enable last 2 keybytes bruteforcing
  -x : disable bruteforce multithreading
  -y : experimental single bruteforce mode
  -k : use only old Korek attacks (pre-PMK)
  -s : show the key in ASCII while cracking
  -n <num> : specify maximum number of IVs to use
  -b <num> : WEP dechunk, skips broken keystreams
  -p <num> : PTW debug: 1: disable Klein, 2: PTW
  -l : run only 1 try to crack key with PTW
  -v : run in visual inspection mode

WEP and WPA-PSK cracking options:
  -w <words> : path to wordlist(s) filename(s)
  -f <file> : path to run session filename
  -e <file> : path to existing session filename

WPA-PSK options:
  -f <file> : create EWSA Project file v3
  -l <str> : PMKID string (hashcat -m 16800)
  -j <file> : create Hashcat v3.6+ file (HCCAPv)
  -c <file> : create Hashcat file (HCCAP)
  -s : WPA cracking speed test
  -z <sec> : WPA cracking speed test length of execution
  -r <db> : path to aircrack-ng database (Cannot be used with -w)

SIMD selection:
  --simd-list : Show a list of the available SIMD architectures, for this machine.
```

2. Завантаження та підготовка .cap-файлу

- Файл `crackme.pcap-01.cap` скопійовано в папку `bin`
- Файл містить перехоплені пакети з Wi-Fi мережі з WEP-шифруванням

3. Визначення доступних мереж

Команда: `.\aircrack-ng.exe crackme.pcap-01.cap`

1. BSSID: 68:7F:74:3E:31:04

ESSID: linksys

Encryption: WEP (41665 IVs)

- Обрана цільова мережа: #1

```
Quitting aircrack-ng...
PS C:\Users\admin\aircrack-ng-1.7-win\bin> .\aircrack-ng.exe crackme.pcap-01.cap
Reading packets, please wait...
Opening crackme.pcap-01.cap
Read 89120 packets.
```

#	BSSID	ESSID	Encryption
1	68:7F:74:3E:31:04	linksys	WEP (41665 IVs)
2	98:DA:C4:BD:13:A6		WPA (0 handshake)
3	9E:DA:C4:BD:18:8E		Unknown

4. Злом WEP-ключа

Команда: `.\aircrack-ng.exe crackme.pcap-01.cap`

→ індекс цілі: 1

Результат:

KEY FOUND! [89:CE:D2:BD:C9]

Decrypted correctly: 100%

Отриманий WEP-ключ:

89:CE:D2:BD:C9

```
KEY FOUND! [ 89:CE:D2:BD:C9 ]
Got 41665 out of 40000 IVsStarting PTW attack with 41665 ivs.
PS C:\Users\admin\aircrack-ng-1.7-win\bin> .\aircrack-ng.exe crackme.pcap-01.cap
Reading packets, please wait...
Opening crackme.pcap-01.cap
PS C:\Users\admin\aircrack-ng-1.7-win\bin>
```

#	BSSID	ESSID	Encryption
1	68:7F:74:3E:31:04	linksys	WEP (41665 IVs)
2	98:DA:C4:BD:13:A6		WPA (0 handshake)
3	9E:DA:C4:BD:18:8E		Unknown

```
Index number of target network ? .\aircrack-ng.exe -b 68:7F:74:3E:31:04 crackme.pcap-01.cap
```

Висновки:

- У ході виконання роботи було виконано повний цикл злому WEP-ключа з використанням Aircrack-ng.
- Результати демонструють вразливість протоколу WEP при наявності достатньої кількості перехоплених пакетів.
- Рекомендовано використовувати сучасніші протоколи — WPA2 або WPA3.