
ATTACK
DEFENSE
by PentesterAcademy

Name	WEP Cracking Advanced
URL	https://www.attackdefense.com/challengedetails?cid=66
Type	Cracking : Wi-Fi Networks

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Step 1: Use airodump-ng to load the PCAP file.

Command: airodump-ng -r WEP-Advanced.cap

```
CH  0 ][ Elapsed: 12 s ][ 2018-11-03 17:08 ][ Finished reading input file WEP-Advanced.cap.

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:91:D2:8E:25    0        0        1    0   0  -1   WEP  WEP         <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:21:91:D2:8E:25  60:FB:42:D5:E4:01    0    0 - 0      0        1
```

There is one SSID with BSSID 00:21:91:D2:8E:25 and Client 60:FB:42:D5:E4:01. But, there are insufficient data packets to crack the WEP encryption. Hence, we can't use aircrack-ng to crack it.

Step 2: In such cases, we can always try to bruteforce the WEP password by writing a wrapper script around airdecap-ng. We will use the wordlist given to us.

Wrapper code

```
#!/usr/bin/python
```

```
import sys, binascii, re
from subprocess import Popen, PIPE
f = open(sys.argv[1], 'r')
for line in f:
        wepKey = re.sub(r'\W+', '', line)
        if len(wepKey) != 5 :
                continue
        hexKey = binascii.hexlify(wepKey)
        print "Trying with WEP Key: " +wepKey + " Hex: " + hexKey
        p = Popen(['/usr/bin/airdecap-ng', '-w', hexKey, 'WEP-Advanced.cap'], stdout=PIPE)
        output = p.stdout.read()
        finalResult = output.split('\n')[4]
        if finalResult.find('1') != -1 :
                print "Success WEP Key Found: "  + wepKey
                sys.exit(0)
print "Failure! WEP Key Could not be Found with the existing dictionary!"
```

Now, execute the python script and pass wordlist to it.

Command: python cracker.py 1000000-password-seclists.txt

```
Trying with WEP Key: zm182 Hex: 7a6d313832
Trying with WEP Key: zm0rz Hex: 7a6d30727a
Trying with WEP Key: zm0ru Hex: 7a6d307275
Trying with WEP Key: zm007 Hex: 7a6d303037
Trying with WEP Key: zlxhe Hex: 7a6c786865
Trying with WEP Key: zlwz4 Hex: 7a6c777a34
Trying with WEP Key: zLUyc Hex: 7a4c557963
Trying with WEP Key: zluwe Hex: 7a6c757765
Trying with WEP Key: Zlu4k Hex: 5a6c75346b
Trying with WEP Key: tudes Hex: 7475646573
Success WEP Key Found: tudes
student@attackdefense:~$
```

Flag: tudes

References:

1. Aircrack-ng (https://www.aircrack-ng.org/)