PICOCTF WPA-ing Out (Rockyou word list + aircrack-ng)

| 200 points

Tags: picoGym Exclusive Forensics

Author: MistressVampy
Description
I thought that my password was super-secret, but it turns out that passwords passed over the AIR can be CRACKED, especially if I used the same wireless network password as one in the rockyou.txt credential dump. Use this 'pcap file' and the rockyou wordlist. The flag should be entered in the picoCTF{XXXXXX} format.

uhh
bro this took time, not becuase its hard but getting the rock you wordlist was not working on the kali linux wsl install i had. so i just manually downloaded it because BROO i cba if it doesnt wanna work

Pico CTF pcap for this challenge

```
https://artifacts.picoctf.net/c/41/wpa-ing_out.pcap
```

O.o step 1

if you wireshark the whole thing, its impossible to run through

```
sudo apt install aircrack-ng
```

this is what happens when you try to air crack without the wordlist being accessable

```
┌──(naruzkurai㉿YunonZKurai)-[/mnt/a/ctf/WPA-ing Out]
└─$ aircrack-ng -w /usr/share/wordlists/rockyou.txt wpa-ing_out.pcap
ERROR: Opening dictionary /usr/share/wordlists/rockyou.txt failed (No such file or directory)
ERROR: Opening dictionary /usr/share/wordlists/rockyou.txt failed (No such file or directory)
Reading packets, please wait...
Opening wpa-ing_out.pcap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 23523 packets.

   #  BSSID              ESSID                     Encryption

   1  00:5F:67:4F:6A:1A  Gone_Surfing              WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa-ing_out.pcap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 23523 packets.

1 potential targets

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

uhhh ok lets try to install the word-list @~@ (I actually didn't try anything else)

Manual download of wordlist if kali is being stoooopid

```
wget https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz
tar -xzf rockyou.txt.tar.gz
mv rockyou.txt /usr/share/wordlists/
```

Answer

```
┌──(naruzkurai㉿YunonZKurai)-[/mnt/a/ctf/WPA-ing Out]
└─$ aircrack-ng -w /usr/share/wordlists/rockyou.txt wpa-ing_out.pcap
Reading packets, please wait...
Opening wpa-ing_out.pcap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 23523 packets.

   #  BSSID              ESSID                     Encryption

   1  00:5F:67:4F:6A:1A  Gone_Surfing              WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa-ing_out.pcap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 23523 packets.

1 potential targets

                               Aircrack-ng 1.7

      [00:00:00] 1173/10303727 keys tested (20737.79 k/s)

      Time left: 8 minutes, 16 seconds                           0.01%

                          KEY FOUND! [ mickeymouse ]


      Master Key     : 61 64 B9 5E FC 6F 41 70 70 81 F6 40 80 9F AF B1
                       4A 9E C5 C4 E1 67 B8 AB 58 E3 E8 8E E6 66 EB 11

      Transient Key  : 26 85 7B AC DD 2C 44 E6 06 18 03 B0 0F F2 75 A2
                       32 63 F7 35 74 2D 18 10 1C 25 F9 14 BC 41 DA 58
                       52 48 86 B0 D6 14 89 F6 77 00 67 E0 AD 10 1B 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      EAPOL HMAC     : 65 2F 6C 0E 75 F0 49 27 6A AA 6A 06 A7 24 B9 A9
```

answer (if you put things together)

```
picoCTF{mickeymouse}
```

Revision #4
Created 11 November 2023 16:02:57 by naruzkurai
Updated 11 November 2023 16:53:11 by naruzkurai