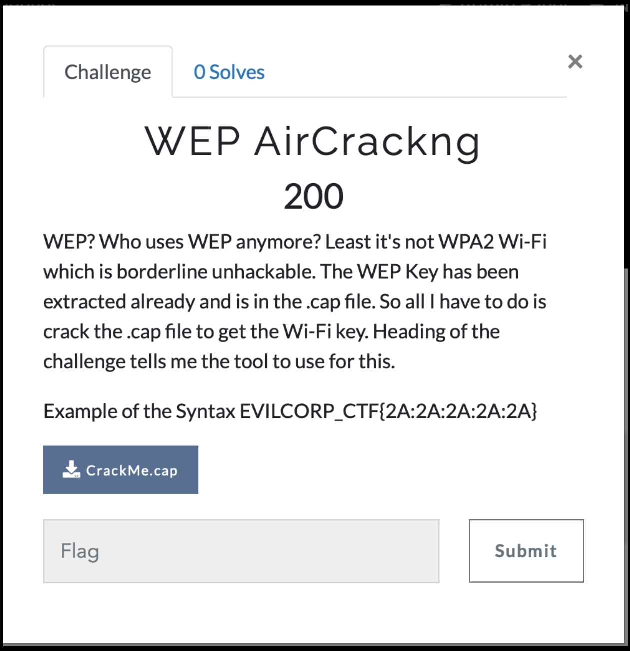
MR. ROBOT

1. The following challenge involves cracking the WEP password for the .cap file provided in the question. This challenge involves using aircrack-ng which the title of the challenge gives away.



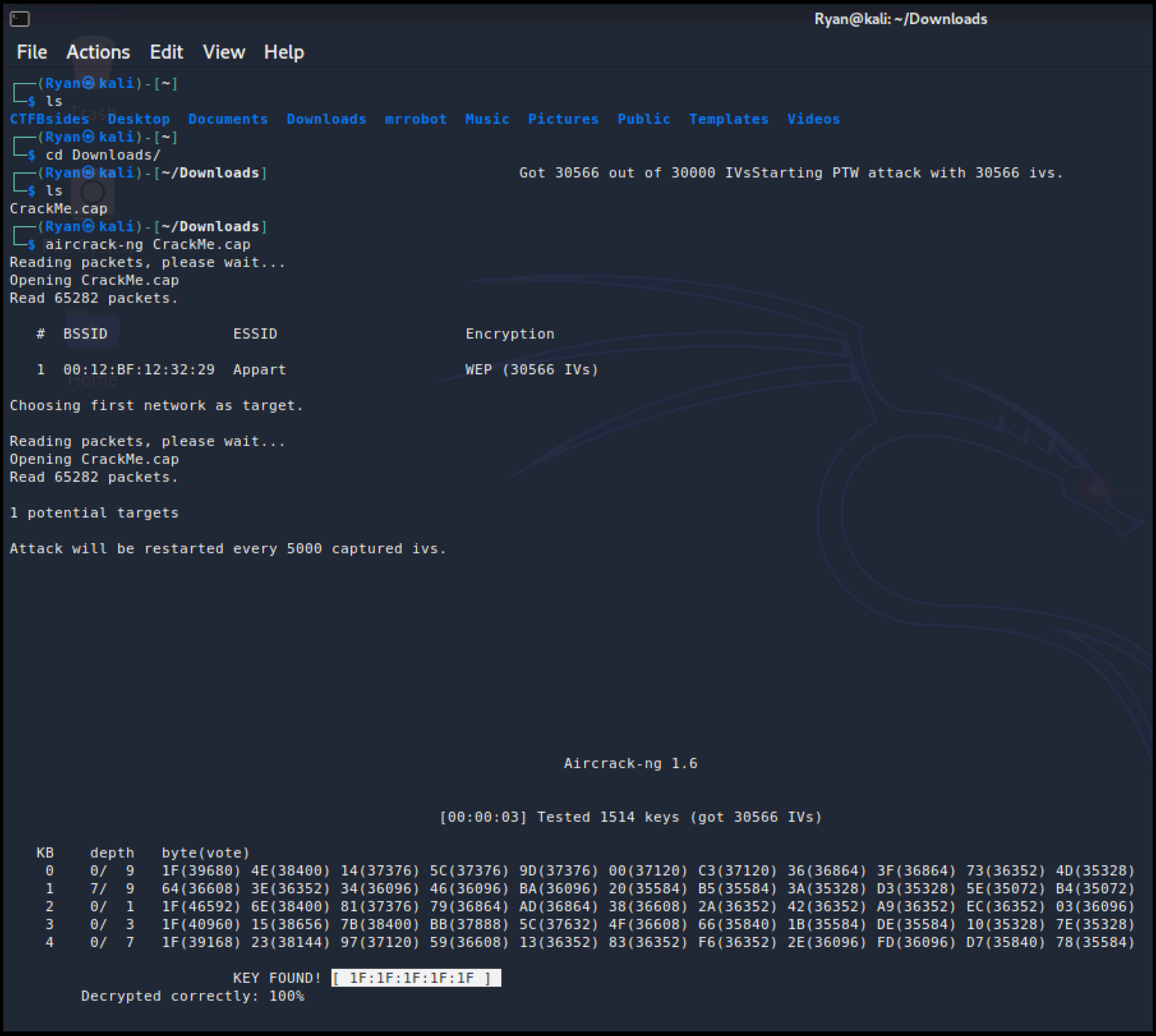
WEP AirCrackng

200

WEP? Who uses WEP anymore? Least it's not WPA2 Wi-Fi which is borderline unhackable. The WEP Key has been extracted already and is in the .cap file. So all I have to do is crack the .cap file to get the Wi-Fi key. Heading of the challenge tells me the tool to use for this.

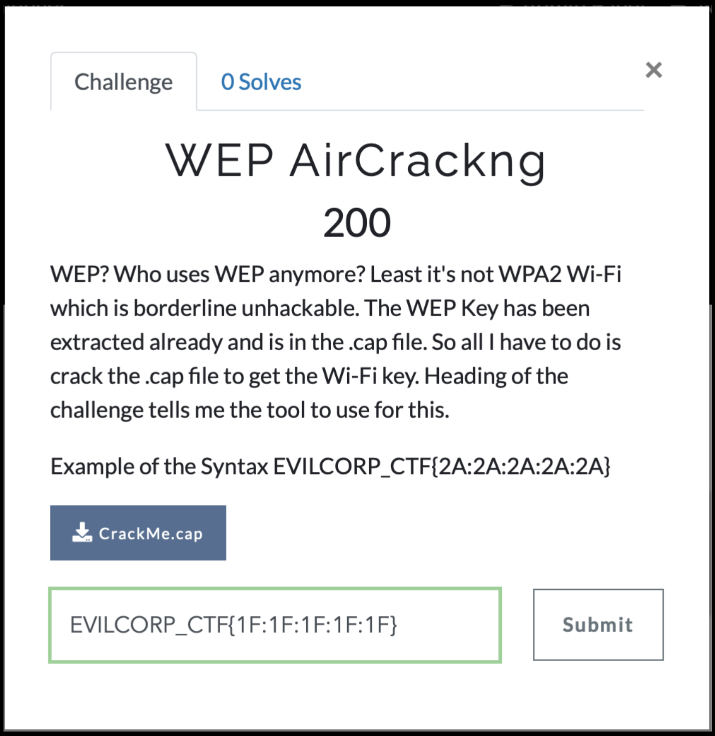
Example of the Syntax EVILCORP_CTF{2A:2A:2A:2A:2A}

2. The .cap file can be found in the downloads when downloaded, then the command aircrack-ng CrackMe.cap should attempt to crack the WEThe following challenge involves cracking the WEP password for the .cap file provided in the question. This challenge involves using aircrack-ng which the title of the challenge gives away. P



```
┌──(Ryan㉿kali)-[~]
└─$ ls
CTFBsides  Desktop  Documents  Downloads  mrrobot  Music  Pictures  Public  Templates  Videos
┌──(Ryan㉿kali)-[~]
└─$ cd Downloads/
┌──(Ryan㉿kali)-[~/Downloads]                         Got 30566 out of 30000 IVsStarting PTW attack with 30566 ivs.
└─$ ls
CrackMe.cap
┌──(Ryan㉿kali)-[~/Downloads]
└─$ aircrack-ng CrackMe.cap
Reading packets, please wait...
Opening CrackMe.cap
Read 65282 packets.

   #  BSSID              ESSID                     Encryption

   1  00:12:BF:12:32:29  Appart                    WEP (30566 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening CrackMe.cap
Read 65282 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.



                                                          Aircrack-ng 1.6


                                            [00:00:03] Tested 1514 keys (got 30566 IVs)

   KB    depth   byte(vote)
    0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376) 00(37120) C3(37120) 36(36864) 3F(36864) 73(36352) 4D(35328)
    1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096) 20(35584) B5(35584) 3A(35328) D3(35328) 5E(35072) B4(35072)
    2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864) 38(36608) 2A(36352) 42(36352) A9(36352) EC(36352) 03(36096)
    3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632) 4F(36608) 66(35840) 1B(35584) DE(35584) 10(35328) 7E(35328)
    4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352) 83(36352) F6(36352) 2E(36096) FD(36096) D7(35840) 78(35584)

                         KEY FOUND! [ 1F:1F:1F:1F:1F ]
        Decrypted correctly: 100%
```

3. Put the WEP key in the brackets and click submit.



WEP AirCrackng

200

WEP? Who uses WEP anymore? Least it's not WPA2 Wi-Fi which is borderline unhackable. The WEP Key has been extracted already and is in the .cap file. So all I have to do is crack the .cap file to get the Wi-Fi key. Heading of the challenge tells me the tool to use for this.

Example of the Syntax EVILCORP_CTF{2A:2A:2A:2A:2A}

EVILCORP_CTF{1F:1F:1F:1F:1F}