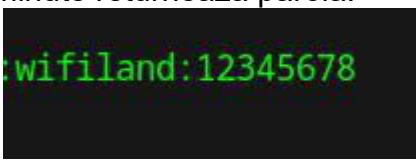
Wifiland

Incepem acest challenge cu 2 fisiere 1 pcap si 1 fisier python.Ca sa gasim flagul avem nevoie de ip la client si target asa ca daca intram in wireshark observam ca avem toate pachetele codate.Deci ar trebui sa folosim tooluri ca aircrack-ng sau hcxpcapngtool.De data aceasta am alex hcxpcapngtool + hashcat pentru a afla cheia pentru decode.Folosesc:

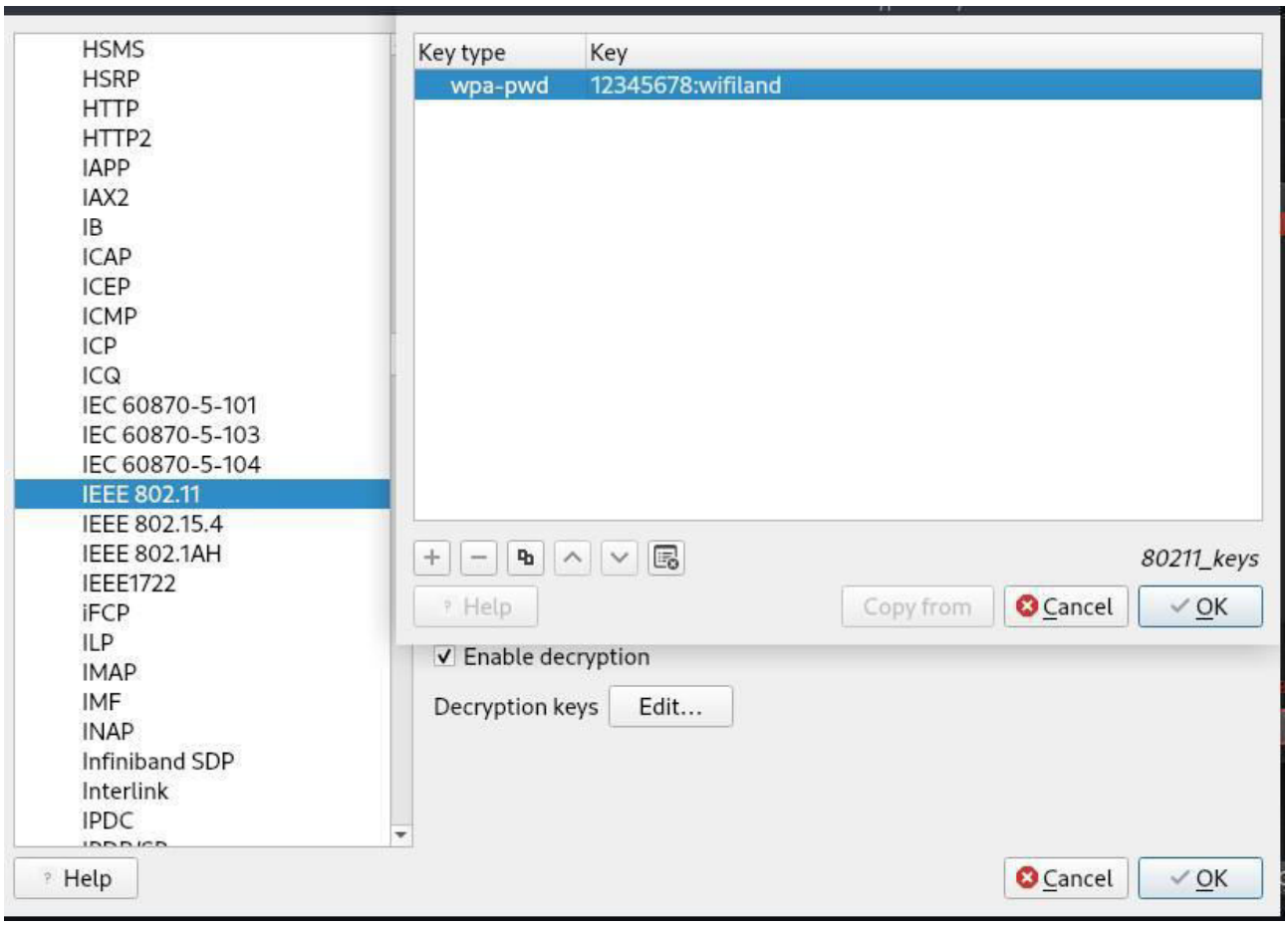
hcxpcapngtool wifiland.pcap -o hit

hashcat -m 22000 hit ../rockyou.txt

Lasam sa ruleze iar dupa 2-3 minute returneaza parola:



Singurul lucru ramas acum este sa introducem parola gasita in Edit>Preferences(ctrl+shift+q)>IEEE 802.11 > Decryption Keys:



Daca verificam acum protocol Hierarchy o sa vedem pachete arp intre 2 calculatoare:

Se observa cele 2 adrese IP daca filtram dupa arp:

```
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
Who has 93.184.216.34? Tell 10.0.3.19
```

Deci le copiem in script si rulam scriptul:

Flag:

CTF{b67842d03eadce036c…….4b4f490f0cb19ccd45c70}

Trolled by masquerade8077