Wifibasic

Asemanator cu wifiland primim 2 fisiere dar acum trebuie sa gasim BSSID,ESSID,PSK din pcap. **BSSID** este adresa MAC a punctului de acces (AP) într-o rețea wireless. Practic, este un identificator unic pentru fiecare punct de acces. **ESSID** este numele unei rețele wireless. Acesta este vizibil pentru utilizatori și este utilizat pentru a identifica rețeaua atunci când se conectează la Wi-Fi.**PSK** este cheia de securitate utilizată într-o rețea Wi -Fi, adică parola care protejează accesul la rețeaua wireless. De obicei, este utilizată într-un tip de criptare **WPA/WPA2.**Din nou o sa folosesc hcxpcapngtool + hashcat pentru a gasi cheia necesara pentru decritare.Comenzile folosite:

hcxpcapngtool wifibasic.pcap -o hit

hashcat -m 22000 hit ../rockyou.txt (va returna parola+numele retelei)

```
TargetHiddenSSID:tinkerbell
```

Intram in pcap si filtram dupa SSID gasit.

wlan.ssid=="TargetHiddenSSID"

```
▸ Frame 852: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
▾ IEEE 802.11 Association Request, Flags: ........
    Type/Subtype: Association Request (0x0000)
  ▸ Frame Control Field: 0x0000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 02:00:00:00:04:00 (02:00:00:00:04:00)
    Destination address: 02:00:00:00:04:00 (02:00:00:00:04:00)
    Transmitter address: 02:00:00:00:0f:00 (02:00:00:00:0f:00)
    Source address: 02:00:00:00:0f:00 (02:00:00:00:0f:00)
    BSS Id: 02:00:00:00:04:00 (02:00:00:00:04:00)
    .... .... .... 0000 = Fragment number: 0
    1000 0010 0001 .... = Sequence number: 2081
```

Avem acum tot la indemana pentru a rula scriptul cu :

BSSID = "02:00:00:00:04:00"
ESSID = "TargetHiddenSSID"
PSK = "tinkerbell"

Rulam scriptul si gasim flagul:

```
┌─[masquerade@parrot]─[~/Downloads]
└──╼ $python3 get_flag.py
CTF{73841584e                    b3df0a27ba8a35388c316d468}
```

Trolled by masquerade8077