neighborhood

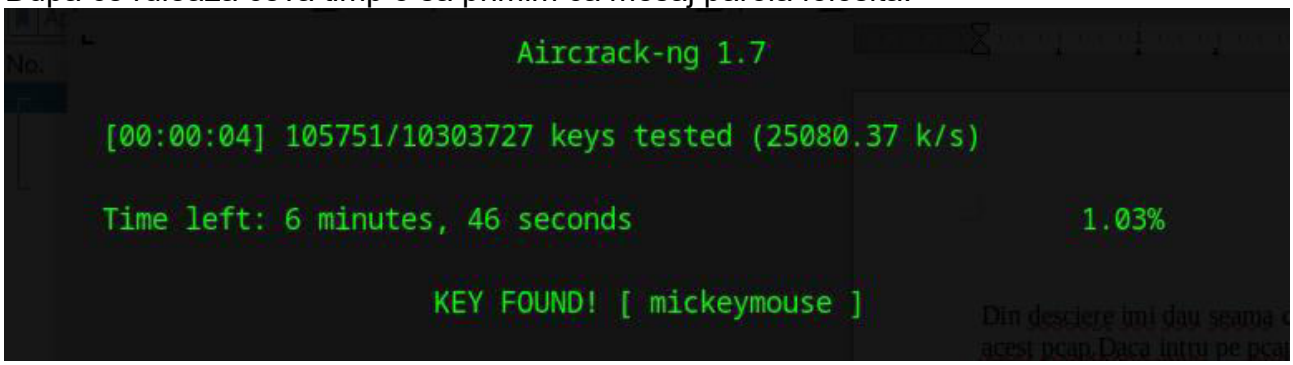
Din desciere imi dau seama ca am nevoie de ceva tool pentru a obtine parola de wifi folosita in acest pcap.Daca intru pe pcap observ 4 pachete care folosesc protocolul EAPOL.

	Time	Source	Destination	Protocol	Length
1	0.000000	Raspberr_ac:da:6b	Raspberr_a1:4b:e1	EAPOL	149
2	-0.016496	Raspberr_ac:da:6b	Broadcast	802.11	152
3	0.002000	Raspberr_a1:4b:e1	Raspberr_ac:da:6b	EAPOL	171
4	0.006943	Raspberr_ac:da:6b	Raspberr_a1:4b:e1	EAPOL	211

EAPOL este un protocol folosit în rețelele **Wi-Fi securizate** (WPA/WPA2) pentru a facilita autentificarea între un client (dispozitiv) și un punct de acces (router).Dacă interceptezi aceste mesaje EAPOL (în special cele din handshake), le poți folosi cu un tool precum **aircrack-ng** pentru a forța parola Wi-Fi printr-un atac de tip **dictionary**.**Aircrack-ng** este o suită de unelte folosită pentru testarea securității rețelelor wireless.Asa ca tot ce avem acum sa facem este sa folosim aircrack-ng pentru a gasi parola cu un payload de genul:

aircrack-ng -w ../rockyou.txt neighborhood.pcap

Dupa ce ruleaza ceva timp o sa primim ca mesaj parola folosita:



Singurul lucru ramas acum este doar sa punem cuvantul folosind sha256
Flag format CTF{sha256(password)}.

Ultima comanda : **echo -n "mickeymouse" | sha256sum**

Flag:

CTF{d0ff2794ec7af8764a654…..f518053fee9629917a5782ad9cf837}

Trolled by masquerade8077