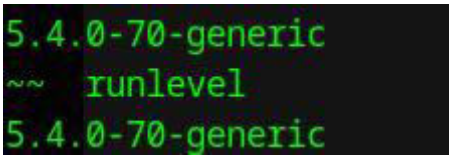
login-view

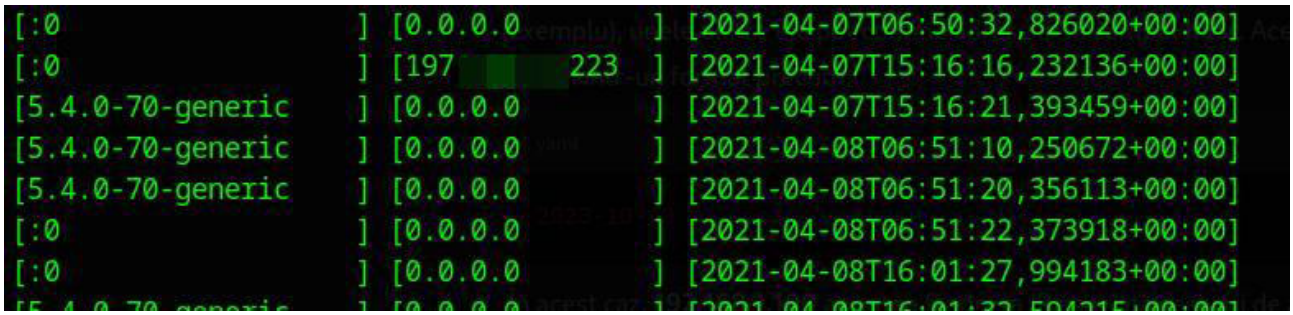
Acest challenge ne cere sa gasim IP dintr-un dump so easy right? Problema este ca la inceput credeam ca trebuie folosit volatility pana sa descopar ca are 2 MB . No dump has so little info right? Daca aplic file pe el nu imi identifica ce tip de fisier este dar daca folosesc strings observ mai multe mesaje de o versiune + generic .



Deci nu este un dump normal ig.Dupa mult timp de cautat am incercat sa iau la rand tooluri pana sa descopar pe un link ca este un utmp dump.Un fișier **utmpdump** provine de obicei dintr-un dump al fișierului de log **utmp** (sau **wtmp**), care este folosit pe sistemele Unix-like pentru a stoca informații despre sesiunile de utilizatori. Aceste fișiere sunt gestionate de către sistem pentru a ține evidența autentificărilor și închiderilor de sesiuni. Instrumentul **utmpdump** este folosit pentru a decoda aceste fișiere, oferindu-ți informații clare despre activitățile utilizatorilor pe sistem.Am observat ce tip de fisier este si datorita faptului ca strings prezenta multi useri repetat.In any case folosim:

utmpdump dump

O sa vedem dupa dumpul decodat iar singurul lucru ramas este sa descoperim adresa IP(este doar 1)



FLAG:

CTF{f50839694983b5ad6ea1……2ff4757dc12259cf1c54c08c}

Trolled by masquerade8077