

# 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 .

```
5.4.0-70-generic
~~ runlevel
5.4.0-70-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)

```
[ :0 ] [0.0.0.0] [2021-04-07T06:50:32,826020+00:00]
[ :0 ] [197.███.███.223] [2021-04-07T15:16:16,232136+00:00]
[5.4.0-70-generic] [0.0.0.0] [2021-04-07T15:16:21,393459+00:00]
[5.4.0-70-generic] [0.0.0.0] [2021-04-08T06:51:10,250672+00:00]
[5.4.0-70-generic] [0.0.0.0] [2021-04-08T06:51:20,356113+00:00]
[ :0 ] [0.0.0.0] [2021-04-08T06:51:22,373918+00:00]
[ :0 ] [0.0.0.0] [2021-04-08T16:01:27,994183+00:00]
[5.4.0-70-generic] [0.0.0.0] [2021-04-08T16:01:32,504215+00:00]
```

```
[*]-[masquerade@parrot]-[~/Downloads]
$echo -n "197.███.███.223" | sha256sum
f50839694983b5ad6ea███ec49e301a0dcc662ff4757dc12259cf1c54c08c -
```

## FLAG:

CTF{f50839694983b5ad6ea1.....2ff4757dc12259cf1c54c08c}

Trolled by masquerade8077