





WRITEUP Script

Garbage-Bag

Artur Poetsch







Table des matières

1.	Connexion au port attribué1
2.	Récupération du flag

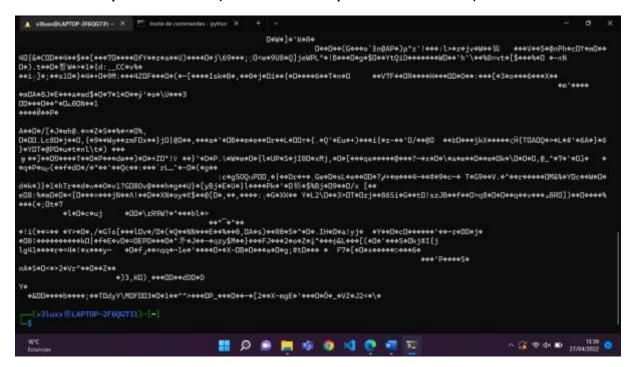






1. Connexion au port attribué :

Dans un premier temps, on nous fourni le port 6667, nous allons donc nous y connecter (ici sur l'exemple en localhost).



On voit qu'après s'être connecter au port avec « nc localhost 6667 », On reçoit un tas de charactères sans suite logique.







2. Lecture des données

Le script du server n'étant pas consultable, on ne peut pas avoir d'information sur la dissimulation du flag, rendant la tache plus compliquée. Cependant il y a toujours la possibilité de lancer une recherche textuelle avec les outils linux (ici avec grep).

Nous connaissons le format du flag HACKYNOV{flag}, nous pouvons donc lancer une recherche avec grep -a HACKYNOV et laisser tourner

Au bout d'un certain temp le flag nous est retourné, et le challenge est réussi!

