Write-Up: Ping me (Pwn)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

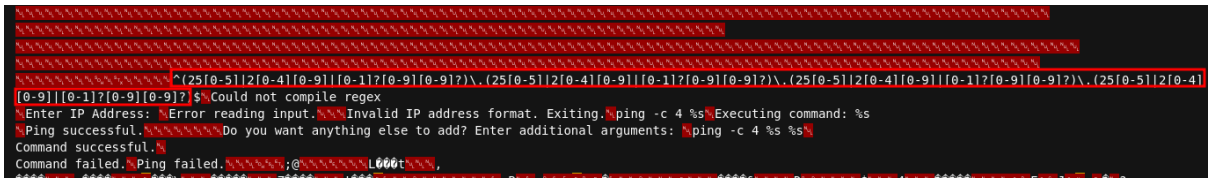
Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα binary αρχείο που ονομάζεται ping-me, το οποίο μπορούμε να το ανοίξουμε με έναν editor.

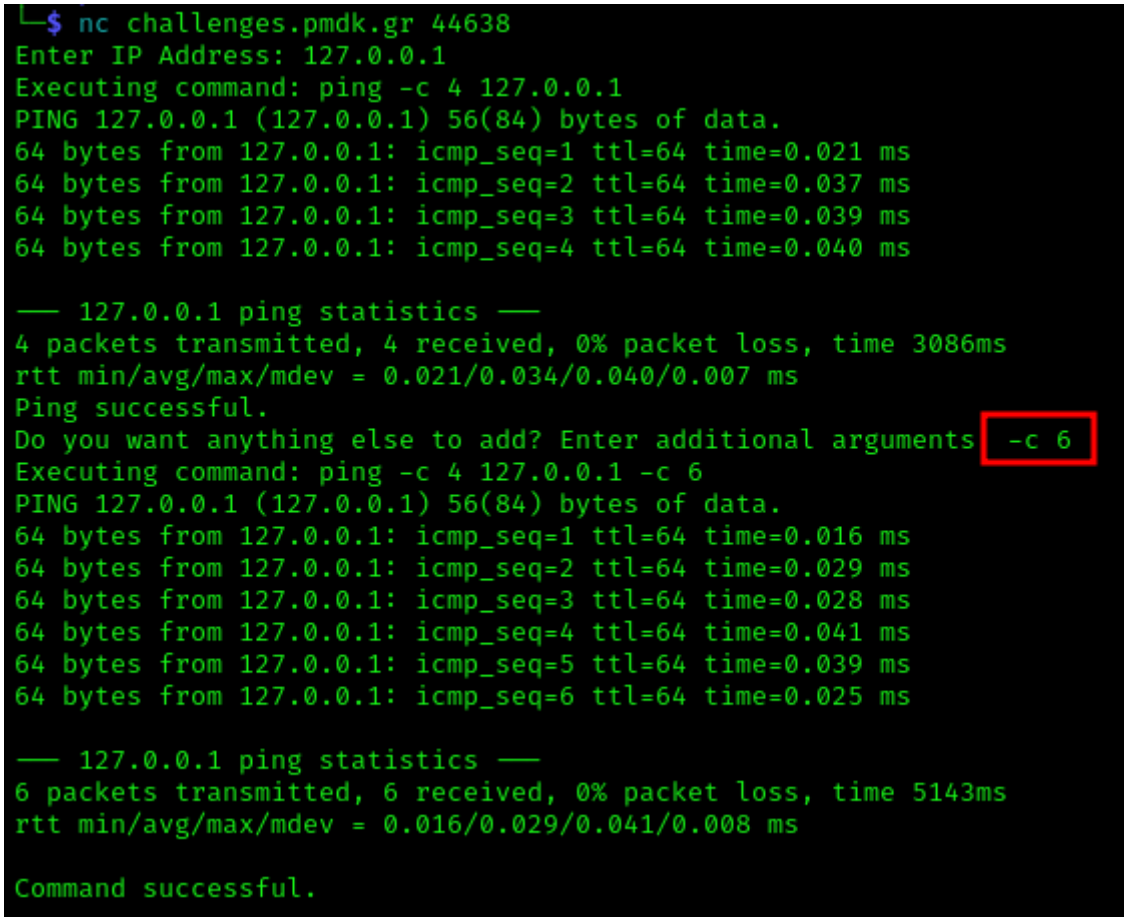
Επίλυση

Αρχική ανάλυση

Στην συγκεκριμένη περίπτωση χρησιμοποιώ το VSCode και το ανοίγω με τον ενσωματωμένο text editor.Με αυτόν τον τρόπο καταφέρνω να δω ένα κομμάτι του κώδικα.



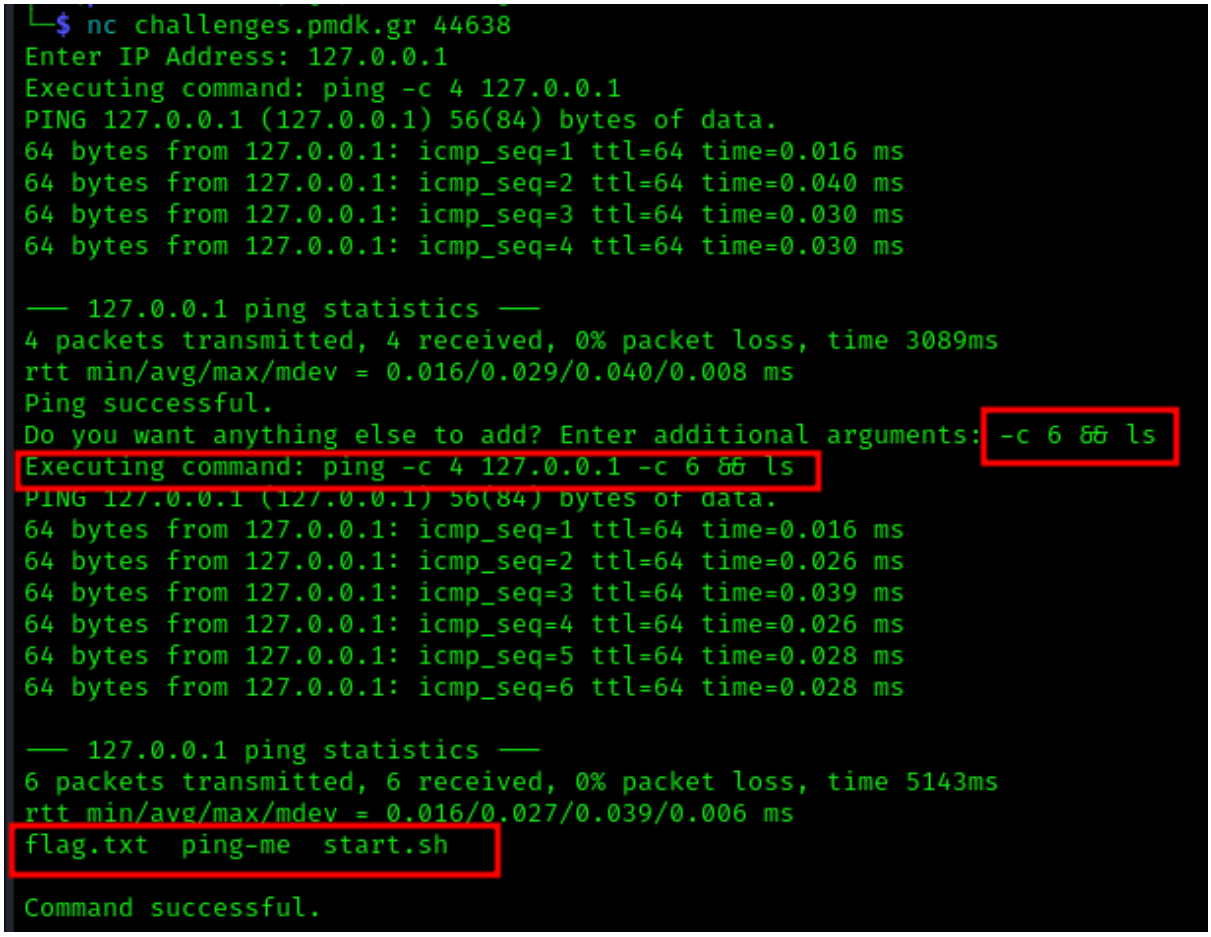
Φαίνεται ότι στο αρχείο ζητείται ένα input για να κάνει ping, άλλα με ένα συγκεκριμένο format. Στο δεύτερο input μου ζητάει να δώσω επιπλέον παραμέτρους για το αρχικό ping.



Σε αυτό το σημείο σκέφτηκα ότι μπορεί να χρειάζεται να χρησιμοποιήσω την τεχνική input injection.

Εκμετάλλευση ευπάθειας

Με την ένωση εντολών κατάφερα να περάσω και δεύτερη εντολή. Στην αρχή έτρεξα την ls για να δω αν δουλεύει και τι θα επιστρέψει αν δουλέψει.



Είδα ότι έτρεξα και μου έβγαλε το flag.txt. Με την εντολή cat πήρα την σημαία της δοκιμασίας.

Σημαία

Η σημαία που βρέθηκε:

```
FLAG{1_d4r3_y0u_t0_p1ng_th3_un1v3rs3_4nd_c0nv1nc3_1t_t0_r3ply}
```