ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Άσκηση 1η
Γρίφος

Περιγραφή

Βρίσκετε ένα USB flash drive στην τσέπη σας, με ένα σημείωμα: "Ξέχνα την άσκηση και λύσε το Γρίφο".

Το drive περιέχει μόνο ένα εκτελέσιμο για Linux/x86-64. Δεν είστε ριψοκίνδυνοι, αλλά είστε περίεργοι: Το τρέχετε σε απομονωμένο περιβάλλον.

Γρήγορα καταλαβαίνετε ότι πρόκειται για σειρά προκλήσεων. Κάθε πρόκληση έχει έκβαση: SUCCESS ή FAIL. Αν λύσετε μια δοκιμασία μπορείτε να δοκιμάσετε την επόμενη (ή και τη μεθεπόμενη, κατά περίπτωση).

Όλες οι δοκιμασίες απαιτούν να μεταβάλετε το περιβάλλον εκτέλεσης του αρχείου, ώστε αυτό να μπορέσει να προχωρήσει παρακάτω.

Για να ρυθμίσετε σωστά το περιβάλλον θα πρέπει

- να παρακολουθήσετε τη δραστηριότητα του εκτελέσιμου
- να κατανοήσετε τη δραστηριότητα και να εξοικειωθείτε με τις αντίστοιχες κλήσεις συστήματος, κλήσεις βιβλιοθηκών και άλλους σχετικούς μηχανισμούς του Unix.
- να γράψετε προγράμματα ή να επέμβετε οι ίδιοι μέσω του φλοιού ώστε το εκτελέσιμο να βρει τις κατάλληλες συνθήκες ώστε να ολοκληρώσει επιτυχώς την εκτέλεση κάθε δοκιμασίας.

Αν πραγματικά τον χρειάζεστε, υπάρχει μηχανισμός παροχής τεχνικών υποδείξεων προς τον επίδοξο λύτη, μένει σε εσάς να ανακαλύψετε τον τρόπο ενεργοποίησής του.

Παραδοτέο

Για να ολοκληρώσετε την άσκηση θα πρέπει να λύσετε με επιτυχία τις προκλήσεις μέχρι να φτάσετε το επίπεδο “Tier2”. Προφανώς η πορεία του challenger δεν τελειώνει εκεί. Από “Tier2” και κάτω, οι προκλήσεις είναι προαιρετικές.

Τελικό παραδοτέο είναι η επίδειξη της σωστής λειτουργίας του εκτελέσιμου, στην οποία θα περιγράφετε τη λειτουργία του προγράμματος σε κάθε μία από τις προκλήσεις, και τη βασική ιδέα στην οποία στηρίχτηκε η λύση σας.

Κανόνες του παιχνιδιού:

- Μπορείτε να κάνετε ό,τι θέλετε για να καταλάβετε πώς λειτουργεί το εκτελέσιμο και τι κάνει κάθε φορά, μπορείτε να χρησιμοποιήσετε οποιονδήποτε μηχανισμό ή περιβάλλον εκτέλεσης σας εξυπηρετεί.
- Παρόλο που ελέγχετε πλήρως το περιβάλλον ανάλυσης, δεν έχετε πρόσβαση στο περιβάλλον εκτέλεσης για την εξέταση.

Για την εξέταση:

- Δεν επιτρέπεται η χρήση μηχανισμού `LD_PRELOAD` για να επιλύσετε τις προκλήσεις.
- Δεν επιτρέπεται η χρήση debugger για να επιλύσετε τις προκλήσεις.
- Δεν επιτρέπεται αλλαγή του binary που έχετε.