RIDDLE

Challenge 0

Πρόβλημα: Openat σε αρχείο που δεν υπάρχει

Λύση: Δημιουργώ το αρχείο, με touch .hello_there

Challenge 1

Πρόβλημα: Δεν θέλουμε να μπορεί κανείς να γράψει στο αρχείο

Λύση: Αφαιρούμε το δικαίωμα με το chmod -w.

Challenge 2

Πρόβλημα: Το riddle καλεί την sigalarm και περιμένει λίγο χρόνο να γίνει κάτι

Λύση: Στέλνουμε SIGCONT με το pkill –18 riddle

Challenge 3

Πρόβλημα: Με ltrace βλέπουμε ότι προσπαθεί να βρει μια μεταβλητή περιβάλλοντος, την ANSWER.

Λύση: Χρησιμοποιούμε export για να ορίσουμε την μεταβλητή και να την θέσουμε στην τιμή που υποδεικνύεται από το hint,

Challenge 4

Πρόβλημα: Θέλουμε να δημιουργήσουμε νέο αρχείο στο οποίο να διαβάζεται ο τελευταίος χαρακτήρας που γράφεται

Λύση: Δημιουργούμε αρχείο fifo με την mkfifo magic_mirror

Challenge 5

Πρόβλημα: Χρειαζόμαστε να υπάρχει αρχείο με fd=99

Λύση: Με το challenge5.c το οποίο το κάνει αυτό μέσω της dup2

Challenge 6

Πρόβλημα: Θέλουμε οι διαδικασίες να στέλνουν ping και pong μέσω ενός κοινού αρχείου που θα λειτουργεί ως pipe

Λύση: Με το challenge.6 δημιουργούμε το pipe

Challenge 7

Πρόβλημα: Θέλουμε δυο αρχεία να έχουν το ίδιο inode

Λύση: Δημιουργούμε λινκ από το ένα στο άλλο, με την ln .hello_there .hey_there

Challenge 8

Πρόβλημα: Θέλουμε να γραφτεί κάτι σε συγκεκριμένη θέση στο αρχείο

Λύση: Challenge8

Challenge 9

Πρόβλημα: Προσπαθούμε να συνδεθούμε σε port που δεν το δέχεται

Λύση: Κάνουμε το συγκεκριμένο port, listening port με την nc -l 49842 και σε παράλληλο terminal τρέχουμε το riddle. Απαντάμε την ερώτηση που έρχεται στο πρώτο port

Challenge 10

Πρόβλημα: Θέλω να διαβάσω ένα αρχείο, αλλά αυτό διαγράφεται

Λύση: Με το challenge10.c δημιουργώ link σε αυτό το αρχείο για να μην διαγραφτεί. Πρώτα κάνω touch not_so_secret, μετά τρέχω το challenge10, μετά το riddle σε άλλο terminal, και μετά σε τρίτο terminal cat not_so_secret, και κάνω copy-paste τον αριθμό στο riddle

Challenge 11

Πρόβλημα: Το ίδιο με το 10, αλλά δεν πρέπει να υπάρχει link στο αρχείο

Λύση: Κάνουμε htop σε καινούριο terminal και κρατάμε το PID του riddle. Μετα το χρησιμοποιούμε στο cd /proc/PID/map_files/. Μετά κάνουμε ls –lia και κάνουμε copy τον αριθμό που αντιστοιχεί στο .hello_there και τέλος sudo cat (αριθμός).

Challenge 12

Πρόβλημα: Θέλω να γράψω σε συγκεκριμένη θέση στην μνήμη

Λύση: Παρατηρώ ότι είναι η 111η θέση από την που γίνεται mmap ένα αρχείο. Τρέχω το challenge12 με ορίσματα το αρχείο και το γράμμα.

Challenge 13

Πρόβλημα: Πάω να διαβάσω σε θέση του αρχείου που δεν υπάρχει

Λύση: Αλλάζω τα δικαώματα με chmod +r+w .hello_there. Επεκτείνω το αρχείο με truncate -s 16385

Challenge 14

Πρόβλημα: Θέλουμε το riddle να πάρει ένα συγκεκριμένο pid

Λύση: Μπαίνω στο proc/sys/kernel κάνω flock ns_last_pid, μετά echo 32766 > ns_last_pid, μετά τρέχω το riddle (σε άλλο terminal), και τέλος πάω και κάνω flock –u ns_last_pid. Μπορεί να χρειαστεί sudo.