Write-Up: Time for darts (Misc)

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

Επισκόπηση Δοκιμασίας

Η δοκιμασία αποτελείται από ένα πρόγραμμα που τρέχει σε κάποιον server.

Ο σκοπός της είναι να βρούμε τον νικητή και την βαθμολογία του σε 40 rounds από ένα παιχνίδι με βελάκια.

Τρέχω το πρόγραμμα με το εργαλείο netcat. Εμφανίζει τα σκορ όλων των παικτών για κάθε γύρο.

Επίλυση

Αρχική ανάλυση

Αρχικά παρατήρησα ότι τα σκορ εμφανίζονται με πολύ μεγάλη ταχύτητα και είναι σχεδόν αδύνατο να υπολογιστούν. Εκτός αυτού όταν μου ζητάει να γράψω τον νικητή και την βαθμολογία του, ο δοσμένος χρόνος είναι πάρα πολύ λίγος.

Η ευπάθεια φαίνεται αρχικά να βρίσκεται στα inputs και στα ζητούμενα αποτελέσματα.

Εκμετάλλευση ευπάθειας

Αρχικά παρατήρησα ότι το όνομα της συγγράφεα στην εκφώνηση της δοκιμασίας μας κάνει redirect σε μία ιστοσελίδα της wikipedia με θέμα τα null devices. Αφού σκέφτηκα τον τρόπο με τον οποίο λειτουργούν αυτά, μου ήρθε η ιδέα ότι μπορώ να πάρω το output από τον server, να κάνω τους απαραίτητους υπολογισμούς και να βρω τον νικητή και το σκορ. Έδωσα την εντολή nc challenges.pmdk.gr 37747 > output.txt. Με αυτή την λογική έφτιαξα ένα πρόγραμμα που να διαβάζει το αρχείο output.txt και να βρίσκει τον παίχτη με το μεγαλύτερο σκορ, όπως και το ίδιο του το σκορ.

Python Κώδικας:

```
import re

with open("output.txt", "r") as file:
        lines = file.readlines()

table = []

for i in range(0, 100):
        table.append(0)

for line in lines:
        if line.startswith("Player"):
```

```
        numbers = re.findall(r'\d+', line)
        table[int(numbers[0])] = table[int(numbers[0])] + int(numbers[1])
max_value = max(table)
max_index = table.index(max_value)
print("Nikitis : Player " + str(max_index))
print("Score : " + str(max_value))
```

Με αυτό το πρόγραμμα όμως δεν μπορούσα να πάρω τα δεδομένα από τον server και αντίστοιχα να δίνω τα σωστά. Για αυτό σκέφτηκα να στείλω τα δεδομένα με ανακατεύθυνση με pipe lines. Αυτό πετυχαίνεται με την εντολή nc challenges.pmdk.gr 37747 | python3 readFile.py.

Python Κώδικας:

```
import re
import sys
table = []
for i in range(0, 100):
    table.append(0)
for line in sys.stdin:
    if line.startswith("Player"):
    items = line.split()
    numbers = re.findall(r'\d+', line)
    table[int(numbers[0])] = table[int(numbers[0])] + int(numbers[1])
max_value = max(table)
max_index = table.index(max_value)
print("Player " + str(max_index))
print(str(max_value))
```

Το πρόγραμμα δούλευε αλλά δεν έβλεπα τα αποτελέσματα. Μου ζητούσε να πληκτρολογήσω χωρίς να μου εμφανίζει τι. Άλλαξα την εντολή ανακατεύθυνσης σε nc challenges.pmdk.gr 37747 | tee >(python3 readFile2.py) και είδα και τα αποτελέσματα.

Το πρόβλημα τώρα ήταν πώς θα πάρω τα αποτελέσματα αυτά και θα τα οδηγήσω πίσω στο πρόγραμμα. Έτσι, πειραματήστηκα με ανακατευθύνσεις είτε απευθείας, είτε με χρήση των Named Pipes, προσπαθώντας πάντα να μου εμφανίζονται και τα μυνήματα για να γνωρίζω που βρίσκομαι (με την εντολή tee). Αφού δεν κατάφερα τίποτα από όλα αυτά, σκέφτηκα να χρησιμοποιήσω το

πρόγραμμα από την δοκιμασία My Rainbow Sorcerer για να συνδεθώ στον server. Οπότε ένωσα το πρόγραμμα από την δοκιμασία My Rainbow Sorcerer και την παραπάνω κώδικα και με μερικές τροποποιήσεις κατάφερα να περάσω στα inputs του server τις σωστές τιμές.

Python Κώδικας:

```
import re

import sys

import json

import socket

# Σύνδεση από την δοκιμασία My Rainbow Sorcerer

HOST = "challenges.pmdk.gr" PORT = 37747

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect((HOST, PORT))

# Αρχικό Πρόγραμμα

table = []

for i in range(0, 100):
        table.append(0)

line="a"

i=0

while line !="":
        line = s.recv(1024).decode()
        line = line.strip("\n")
        print(line)
        if ">" in line and i==0:
                s.sendall(("1 \n").encode())
                i=i+1
        if line.startswith("Player"):
        numbers = re.findall(r'\d+', line)
        table[int(numbers[0])] = table[int(numbers[0])] + int(numbers[1])
        max_value = max(table)
        max_index = table.index(max_value)
        if "Who is the winner" in line and i==1:
                s.sendall(("Player " + str(max_index) +"\n").encode())
```

```
            i=i+1
        if "What was the highest" in line and i==2:
            s.sendall((str(max_value) +"\n").encode())
```

Το πρόγραμμα τρέχει με σύνδεση στον remote server με την εντολή “python3 program.py”

Σημαία

Η σημαία που βρέθηκε:

```
FLAG{N3W-e-D4RT-M4ST3R-1n-Th3-h0use!}
```