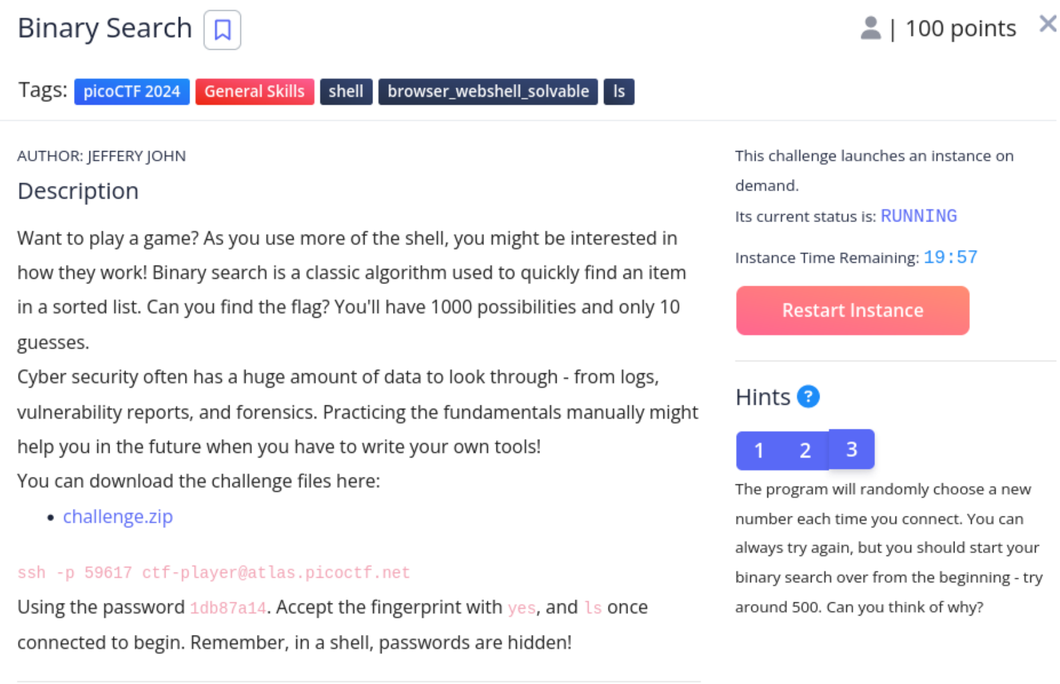
Binary Search



Binary Search

Tags: picoCTF 2024 General Skills shell browser_webshell_solvable ls

AUTHOR: JEFFERY JOHN

Description

Want to play a game? As you use more of the shell, you might be interested in how they work! Binary search is a classic algorithm used to quickly find an item in a sorted list. Can you find the flag? You'll have 1000 possibilities and only 10 guesses.

Cyber security often has a huge amount of data to look through - from logs, vulnerability reports, and forensics. Practicing the fundamentals manually might help you in the future when you have to write your own tools!

You can download the challenge files here:

- challenge.zip

```
ssh -p 59617 ctf-player@atlas.picoctf.net
```

Using the password `1db87a14`. Accept the fingerprint with `yes`, and `ls` once connected to begin. Remember, in a shell, passwords are hidden!

This challenge launches an instance on demand.

Its current status is: RUNNING

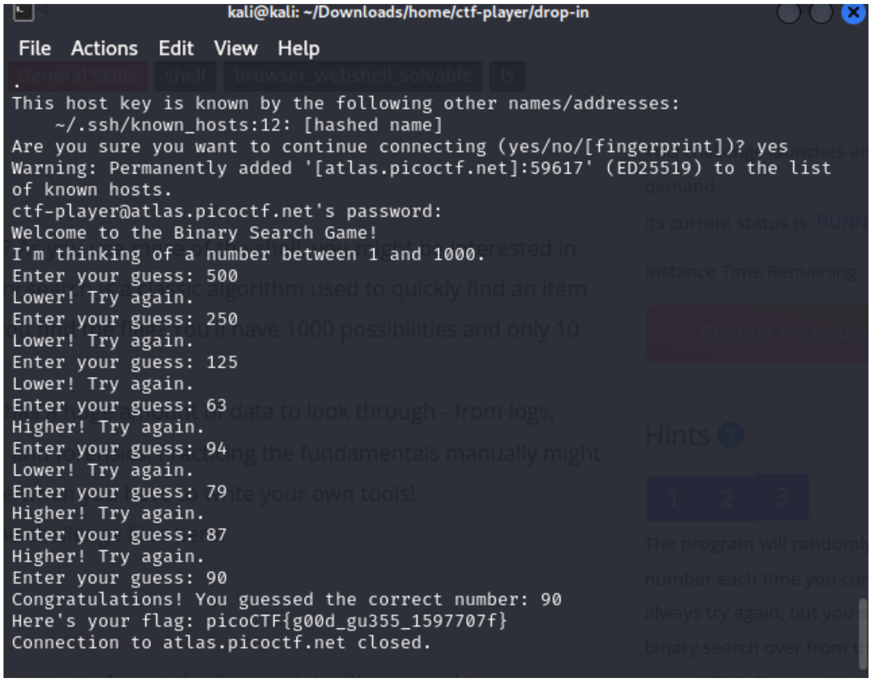
Instance Time Remaining: 19:57

Hints

The program will randomly choose a new number each time you connect. You can always try again, but you should start your binary search over from the beginning - try around 500. Can you think of why?

Binary Search Challenge

This can be done manually by performing the binary search algorithm. Of course you can try to make a python script but it needs to connect over SSH first and be able to write and read through the SSH session. But this can be done manually.



```
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:12: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[atlas.picoctf.net]:59617' (ED25519) to the list
of known hosts.
ctf-player@atlas.picoctf.net's password:
Welcome to the Binary Search Game!
I'm thinking of a number between 1 and 1000.
Enter your guess: 500
Lower! Try again.
Enter your guess: 250
Lower! Try again.
Enter your guess: 125
Lower! Try again.
Enter your guess: 63
Higher! Try again.
Enter your guess: 94
Lower! Try again.
Enter your guess: 79
Higher! Try again.
Enter your guess: 87
Higher! Try again.
Enter your guess: 90
Congratulations! You guessed the correct number: 90
Here's your flag: picoCTF{g00d_gu355_1597707f}
Connection to atlas.picoctf.net closed.
```

The logic for a Binary Search is always using the middle number on a sorted list of number. of course you can divide the sum by half and get the middle and remove the other half where there is no chance of the key/number being there . Do this for some time and you could narrow the number trying to be found quicker.

My case:

1000 - 0 / 2 = 500 (Lower)

500 - 0 / 2 = 250 (Lower)

250 - 0 / 2 = 125 (Lower)

125 - 0 / 2 = 63 (Higher)

(125 - 63) / 2 + 63 = 94 (Lower)

(94 - 63) / 2 + 63 = 79 (Higher)

(94 - 79) / 2 + 79 = 87 (Higher)

(94 - 87) / 2 + 87 = 90 (Correct)