Mission Name

The Search

Historical Context

Ethan and Claire are on a mission to uncover the whereabouts of SHAX hideout, a notorious hub for hackers seeking anonymity and security. This quest leads them to a remote location, necessitating a deep dive into a machine believed to hold clues to SHAX's location.

Technical Synopsis

The mission's success hinges on meticulous enumeration and analysis of a given machine. Hidden within its digital confines are the secrets to locating the SHAX hideout. Ethan and Claire must use their technical acuity to sift through data, exploit vulnerabilities, and uncover the hidden information crucial to their quest.

Mission Brief

Ethan, your task is to infiltrate the machine provided and extract any information related to the SHAX hideout. Your skills in enumeration, analysis, and exploitation will be tested as you seek out the digital breadcrumbs that lead to SHAX. Return with evidence of your findings. Good luck!

Detailed Assignment

Amidst the backdrop of the Altai Mountains, Ethan and Claire prepare to dive into the digital depths of a machine, key to unveiling the SHAX hideout. This anonymous hacker sanctuary has eluded many, but with precision and expertise, Ethan and Claire hope to expose its secrets and bring to light the activities within.

Operational Venue

RECON CAR - AIR / ALTAI MOUNTAINS

This mission not only challenges Ethan and Claire's hacking prowess but also their ability to piece together the puzzle of SHAX's location from scattered digital clues. Success could mean a significant blow to the anonymity SHAX has long enjoyed

Tools

- IP

Questions

What kind of technique allow you to open the port 22?

- Port knocking

What is the port knocking sequence?

- 573 835 1243

What is the name of the two series?

- Fibonacci | squares

Hints

1. Fibonacci can help
2. Squares also will help
3. Port knocking

Categories

- Linux Enumeration
- Mathematics

Write Up

The problem presents a sequence that combines elements of both the Fibonacci sequence and the sequence of square numbers, with a hint to use these patterns to find the missing numbers in the given sequence.

Understanding the Sequence

The given sequence is a combination of the Fibonacci sequence and the squares sequence, added together element-wise. Here's how it works:

1. **Fibonacci Sequence:** Starts with two ones, and each subsequent number is the sum of the two preceding ones.
   - Example: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987
2. **Squares Sequence:** Each number is the square of its position in the sequence (starting from 1).
   - **Example:** 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256

Adding these two sequences together gives the sequence you provided, with the last two numbers missing.

Calculating the Missing Numbers

- 14th Numbers in Both Sequences:
  - Fibonacci: 377
  - Squares: 196
  - Sum: 573 (provided)
- 15th Numbers in Both Sequences:
  - Fibonacci: 610
  - Squares: 225
  - Sum: 835
- 16th Numbers in Both Sequences:
  - Fibonacci: 987
  - Squares: 256
  - Sum: 1243

Thus, the missing numbers in your sequence are 835 and 1243.

Accessing the System

With the complete sequence (2, 5, 11, 19, 30, 44, 62, 85, 115, 155, 210, 288, 402, 573, 835, 1243), the last three numbers (573, 835, 1243) are used as a "knock door combination" to gain access, likely through a port knocking sequence. This technique is used to open ports on a firewall by making connection attempts to a series of specified closed ports in a particular order.

Following the instructions in the comment, you'd perform the port knocking with `nmap` and then attempt to SSH into the given address as the `invited` user with the password `auth0r1zed`.

```
# Port knocking sequence
for x in 573 835 1243; do nmap -Pn --host-timeout 201 --max-retries 0 -p $x 35.178.207.239; done

# After knocking, attempt to SSH
ssh invited@18.130.252.225
```

By solving the sequence and following the port knocking sequence, you've demonstrated the ability to decipher complex patterns and apply them in a practical cybersecurity context.

Flag Information

flag{kn0ck_kn0ck_and_you_will_know_the_answer}