All the Space Pirate Challenges:

Context :

- The Space Pirate challenges on Hack The Box use various security tasks, ranging from binary exploitation to web vulnerabilities. Below is a comprehensive write-up on the retired challenges within this category.
- If you require a full write-up i would recommend 7rocky [LINK] Write-up as he did a good job explain each one.

Flag :

1. Space Pirate: Entrypoint

Description

The first challenge introduces players to a sort of game environment. The objective is to get the correct serial number to scan. It is embedded in the compiled binary file.

Steps to Solve

1. **Download the Binary:**
    - Start by downloading the binary file provided in the challenge description.
2. **Analyze with a reverse engineering tool:**
    - Open the binary in any reverse engineering tool to analyze the code.
    - Look for functions that handle user input or any obvious vulnerabilities.
3. **Identify Vulnerabilities:**
    - Pay attention to stack usage, buffer overflows, and any conditions that might lead to an exploit.
4. **Craft Payload:**
    - Based on your findings, create a payload that exploits the identified vulnerability to gain access.
5. **Connect to the Service:**
    - Use a provided script or manually connect to the service, sending the crafted payload / string to gain access to a flag the IP:PORT.

Flag:

- The Flag i gained from this was : **HTB{g4t3_0n3_d4rkn3e55_th3_w0rld_0f_p1r4t35}**

2. Space Pirate: Going Deeper

Description

This challenge builds on the first, requiring players to navigate deeper into the pirate's stronghold. Players must solve more complex problems, often involving additional layers of security.

Steps to Solve

1. **Analyze the Updated Binary:**
    - After completing Entrypoint, download the new binary for this challenge and open it in a reverse engineering tool like Hex-IDA or Binary Ninja.
2. **Identify Changes:**
    - Look for changes in logic or additional security mechanisms that weren't present in the previous challenge.
3. **Find the Key Functionality:**
    - Search for functions that deal with access control or sensitive operations, noting how they differ from the first binary.
4. **Exploit the Vulnerability:**
    - Use similar techniques as before, crafting an appropriate payload to exploit any discovered weaknesses.
5. **Interact with the Service:**
    - Use the provided script to connect and interact with the service, submitting your exploit to progress.

Flag:

- The Flag i gained from this was : **HTB{d1g_1n51d3..u_Cry_cry_cry}**

3. Space Pirate: Retribution

Description

The final challenge in the series represents the climax of the adventure. Players must apply all the skills they have developed to successfully navigate the last hurdles and claim victory.

Steps to Solve

1. **Download and Analyze the Final Binary:**
    - Download the binary associated with Retribution and analyze it in Ghidra.
2. **Comprehensive Review:**
    - Conduct a thorough review of all previous findings and tactics. Look for any lingering vulnerabilities.
3. **Determine the Final Attack Vector:**
    - Identify the best approach to exploit the final defenses. This may involve combining techniques learned from previous challenges.
4. **Execute the Exploit:**
    - Craft and send the final payload that will allow access to the last segment of the pirate's stronghold.
5. **Capture the Flag:**
    - Successfully execute your exploit and retrieve the flag to complete the challenge.

Flag:

- The Flag i gained from this was : **HTB{w3_f1n4lly_m4d3_1t}**
- Here is the python Script to see how to complete this challenge **[**Link**]**