

Attack on Titan CTF Challenge - Solution Writeup

Challenge Overview

This is a reverse engineering CTF challenge themed around the Attack on Titan anime/manga. The challenge presents itself as a "Survey Corps Intelligence System" requiring players to breach three walls (Maria, Rose, and Sheena) by solving cryptographic puzzles and providing the correct titan names.

Initial Analysis

Running the Binary

```
./titan_challenge
```

The program displays a banner and presents the first challenge:

```
=====
SURVEY CORPS INTELLIGENCE SYSTEM v2.0
=====

🏰 Three walls protect humanity's greatest secret.
🔍 Breach each layer to uncover the truth about titans.
🗡️ The fate of humanity rests in your hands, soldier!
```

Static Analysis

Basic reconnaissance with common tools:

```
file titan_challenge
strings titan_challenge | head -20
objdump -d titan_challenge | head -50
```

The `strings` command reveals some interesting clues but notably does NOT reveal the final flag, indicating anti-static-analysis measures.

Wall Maria - Outer Defenses

Challenge Presentation

== WALL MARIA - OUTER DEFENSES ==

📜 wsykoa`yo`afasqwSq~`sW`u`alu`l

💬 The gate was first breached by the tallest of titans...

🔒 Enter the titan's name:

Analysis

The challenge provides:

1. A cryptic string: wsykoa yo afasqwSq~ sW u alu l
2. A hint about "the tallest of titans" who "first broke through the outer wall"

Attack on Titan Knowledge

From the anime/manga lore:

- The first wall breach was at Shiganshina District
- The Colossal Titan (60 meters tall, no skin) kicked a hole in Wall Maria
- This titan is described as the "tallest" in the series

Solution

The answer is: **COLOSSAL**

The cryptic string appears to be a red herring or decorative element. The challenge relies on Attack on Titan knowledge rather than cryptographic analysis of that string.

Verification

```
echo "COLOSSAL" | ./titan_challenge
```

Wall Rose - Middle Defenses

Challenge Presentation


After successfully breaching Wall Maria:

== WALL ROSE - MIDDLE DEFENSES ==

🔒 Intercepted transmission (hex dump):

📡 11 2D 20 65 04 37 28 2A 37 20 21 65

```
16 28 23 36 37 65 21 37 31 24 26 26
65 24 29 31 3B 25 29 65 11 28 22 21
65 06 2F 3F 37 65 34 3E 23 3F 65 37
3F 65 29 28 3D 24 65 29 24 21 26 2C
37 31 3E 21 26 36 65 36 2A 3F 29 65
37 3F 2B 36 22 65 36 31 36 20 2D 75
```

 Decrypted: "=0u'8:'01u83&'u1'!466u49!+59u821u?/'u\$.3/u'/u98-4u9416<'!.16&u&:/9u'/;&2u&!&0=e"

 Reiner's secret identity...

 Enter the titan's name:

Analysis

The hex dump shows encrypted data, and the "decrypted" message is still garbled, suggesting multi-layer encryption. However, the key clue is the hint about "Reiner's secret identity."

Attack on Titan Knowledge

- Reiner Braun is revealed to be the Armored Titan
- The Armored Titan is described as having "impenetrable defense"
- Reiner is the "blonde warrior" mentioned in error messages

Solution

The answer is: **ARMORED**

The encrypted transmission appears to be another thematic element rather than a puzzle requiring actual cryptanalysis.

Wall Sheena - Inner Sanctuary

Challenge Presentation

== WALL SHEENA - INNER SANCTUARY ==

 Final encryption - Titan Cipher:

 Cipher Table:

ATTACK → A	BEAST → B
CART → C	FEMALE → F
EREN → E	FOUNDER → F
JAW → J	WARHAMMER → W

 Encoded message: BEAST EREN ATTACK CART EREN

 Decoded: B E A C E → BEACH → BEAST

 The intelligent titan who can speak and throw...

 Enter the password:

Analysis

This challenge presents a substitution cipher where titan names map to letters. The decoded message spells "BEACH" but the hint suggests this should lead to "BEAST."

The clue mentions "the intelligent titan who can speak and throw," which clearly refers to the Beast Titan (Zeke's titan form).

Attack on Titan Knowledge

- The Beast Titan is known for its intelligence and ability to speak
- It can throw objects with devastating accuracy
- This is Zeke Yeager's titan form

Solution

The answer is: **BEAST**

Final Flag Extraction

After successfully breaching all three walls, the program displays:

 CONGRATULATIONS, SURVEY CORPS MEMBER! 

 You have successfully breached all three walls!

 The truth about the titans is finally revealed:

 FLAG: CTF{THE_RUMBLING_HAS_BEGUN_2000_YEARS_AGO}

Anti-Static Analysis

The flag is constructed character-by-character at runtime, making it invisible to basic strings analysis:

```
strings titan_challenge | grep -i ctf  
# Returns no results
```

This demonstrates an effective anti-static-analysis technique where the flag only exists in memory during execution.

Technical Analysis

Reverse Engineering Approach

For those interested in the binary internals:

1. **Function Analysis:** The main functions are `wall_maria_challenge()`, `wall_rose_challenge()`, and `wall_sheena_challenge()`
2. **Validation Logic:** Each wall uses the `validate_answer()` function with different encryption methods:
 - Method 1 (Wall Maria): XOR with index, XOR with key, subtract 3
 - Method 2 (Wall Rose): Reverse array, XOR operations
 - Method 3 (Wall Sheena): Position-based encryption
3. **Anti-Debugging:** The binary includes several anti-debugging measures:
 - Ptrace detection
 - Timing checks
 - Environment variable analysis
 - Signal handlers

Encryption Details

The password validation uses multi-layered encryption with these keys:

- `KEY_FOUNDING = 0xAA`
- `KEY_CART = 0x45`
- `KEY_FEMALE = 0x55`
- `KEY_WARHAMMER = 0x77`
- `KEY_JAW = 0x33`

Each wall's password is encrypted using a different algorithm, but solving the challenge through Attack on Titan knowledge is more efficient than reverse engineering the crypto.

Summary

This CTF challenge effectively combines:

- **Domain Knowledge:** Attack on Titan lore and character knowledge
- **Reverse Engineering:** Binary analysis and function identification
- **Anti-Analysis:** String obfuscation and runtime construction
- **Thematic Consistency:** All elements tie into the anime's storyline

The solution path prioritizes understanding the source material over complex cryptanalysis, making it accessible to fans while still providing technical depth for reverse engineering enthusiasts.

Final Flag: CTF{THE_RUMBLING_HAS_BEGUN_2000_YEARS_AGO}

Passwords:

- Wall Maria: COLOSSAL
- Wall Rose: ARMORED
- Wall Sheena: BEAST