NOVA CTF WRITEUP 2023(Forensics)

CHALLENGE NAME : Dump Extraction

CATEGORY : Forensics

DESCRIPTION:

The IMF has received intelligence that a terrorist group is planning a major attack on a major city. The only lead the IMF has is a memory dump obtained from a computer system used by the terrorists.

The player is tasked with analyzing the memory dump to uncover the terrorist's plans and find the flag. The memory dump is heavily protected, and the player must use their advanced decryption skills to decode the data.

Drive link:
https://drive.google.com/file/d/1ngZhC8rKv2efFXdKjcBjO0n3PL9g9VQV/view?usp=sharing

Introduction:

The Memory Dump Analysis Challenge was a fascinating exercise that required players to analyze a memory dump file using tools such as Volatility. The goal was to find suspicious files and uncover a hidden flag encoded in an image.

Analyzing the Memory Dump File :

The first step in the challenge was to analyze the memory dump file using a suitable tool like Volatility. This step required players to have knowledge of memory dump analysis and experience using memory forensics tools.

Identifying Suspicious Files After analyzing the memory dump file:

players had to look for suspicious files that could be related to the flag. This required careful examination of file names, sizes, and content. Players had to rely on their experience and intuition to identify potentially relevant files.

Checking the tmp Directory Once players identified the suspicious files:

They had to check the tmp directory for any additional clues. They discovered that the index.png image was located inside the 0000 named folder within the tmp directory.

Decoding the Image:

To decode the image, players had to use a random online tool that would reveal hidden pixel colors. The image appeared to be random pixels of different colors, but after decoding it, they discovered that the pixel colors contained the final flag: 'NOVA{1_d0n7_8234k_und32_p2355u23}'

Conclusion:

The Memory Dump Analysis Challenge was a complex and intriguing exercise that required players to demonstrate their expertise in memory dump analysis and forensics tools. The challenge also tested their intuition and problem-solving skills. The discovery of the index.png image located inside the 0000 named folder within the tmp directory added an extra layer of complexity to the challenge. Overall, this challenge was an excellent way to learn about memory dump analysis and uncover hidden clues to solve a puzzle.