Project: Rabbit-Hole Forensics

(Hidden Message Extraction)

Overview

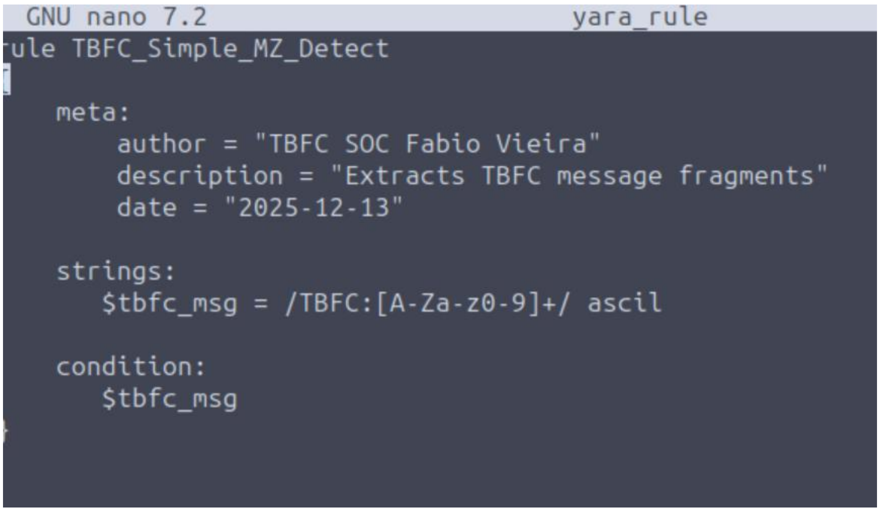
In this forensic challenge, I was tasked with finding a hidden message buried within a dataset of over 50 images of rabbits. Instead of manual inspection, I utilized **YARA**, a tool primarily used for malware research, to automate the identification and extraction of specific data patterns across the entire directory.

The Challenge

The objective was to locate a secret message hidden inside the binary data of multiple image files. This mimics real-world scenarios where malicious actors or "insiders" use basic steganography or data appending to hide exfiltrated information.

The Solution: YARA Rule Implementation

I developed a custom YARA rule named TBFC_Simple_MZ_Detect. The rule uses a regular expression to scan for the "TBFC" prefix followed by alphanumeric characters, ensuring that only relevant message fragments were flagged.

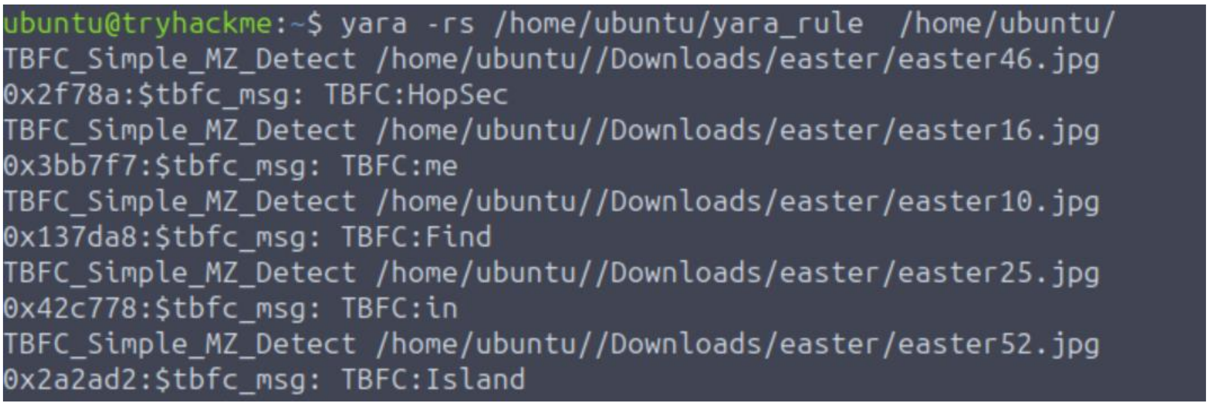


```
  GNU nano 7.2                              yara_rule
rule TBFC_Simple_MZ_Detect
{
   meta:
       author = "TBFC SOC Fabio Vieira"
       description = "Extracts TBFC message fragments"
       date = "2025-12-13"

   strings:
      $tbfc_msg = /TBFC:[A-Za-z0-9]+/ ascil

   condition:
      $tbfc_msg
}
```

Execution & Results

I executed the rule using the YARA command-line tool with the -rs flags (to print strings and scan recursively).

Command: yara -rs /home/ubuntu/yara_rule /home/ubuntu/



```
ubuntu@tryhackme:~$ yara -rs /home/ubuntu/yara_rule  /home/ubuntu/
TBFC_Simple_MZ_Detect /home/ubuntu//Downloads/easter/easter46.jpg
0x2f78a:$tbfc_msg: TBFC:HopSec
TBFC_Simple_MZ_Detect /home/ubuntu//Downloads/easter/easter16.jpg
0x3bb7f7:$tbfc_msg: TBFC:me
TBFC_Simple_MZ_Detect /home/ubuntu//Downloads/easter/easter10.jpg
0x137da8:$tbfc_msg: TBFC:Find
TBFC_Simple_MZ_Detect /home/ubuntu//Downloads/easter/easter25.jpg
0x42c778:$tbfc_msg: TBFC:in
TBFC_Simple_MZ_Detect /home/ubuntu//Downloads/easter/easter52.jpg
0x2a2ad2:$tbfc_msg: TBFC:Island
```

The tool successfully scanned all images in seconds and reconstructed the hidden message:

"Find me in HopSec Island"