YARA Rules - YARA mean one!

Day 13

Learn how YARA rules can be used to detect anomalies.

- Yara Rules

Yara Rules

Overview

Room URL: https://tryhackme.com/room/yara-aoc2025-q9w1e3y5u7

Difficulty: Medium

Category: Yara

Date Completed: 12/14/20025

Objectives

- Understand the basic concept of YARA.
- Learn when and why we need to use YARA rules.
- Explore different types of YARA rules.
- Learn how to write YARA rules.
- Practically detect malicious indicators using YARA.

Table of Contents

Introduction

As King Malhare's forces tighten their grip on Wareville and McSkidy remains captured, the TBFC SOC team discovers a critical lifeline: hidden messages embedded within the compromised systems. McSkidy, ever resourceful, has left behind encoded clues scattered across the network—fragments of a larger intelligence that could turn the tide of the battle for SOC-mas. To recover these messages and decode McSkidy's urgent warnings, you must master **YARA**, the

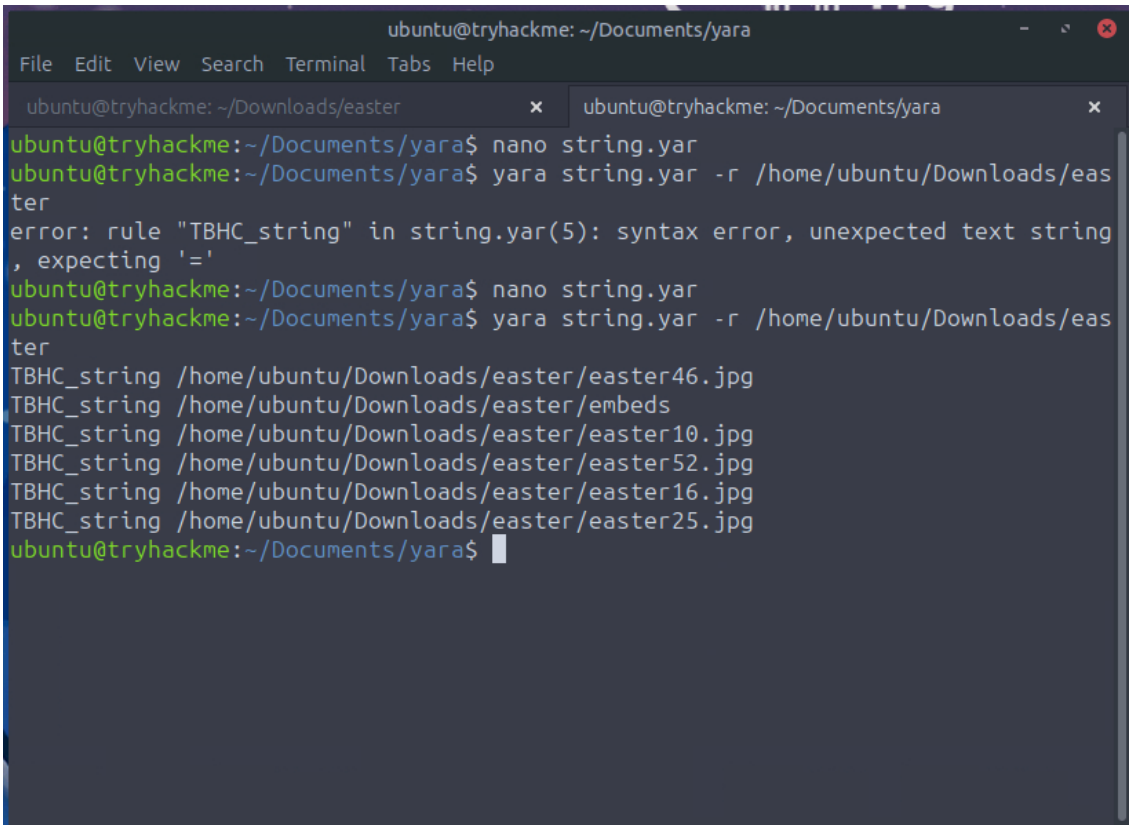
digital detective's most powerful weapon. YARA transforms the chaos of thousands of files into clear, actionable intelligence by searching for unique patterns and signatures that reveal the presence of threats. In this challenge, you'll move beyond theory and into practice, creating your own YARA rules to extract McSkidy's hidden message from the Easter directory. With each rule you craft and each string you match, you're not just finding clues—you're reclaiming control of the network, one forensic discovery at a time.

Walk Through

1. Start the target machine
    1. Folder is in `/home/ubuntu/Downloads/easter`
2. How many images contain the string TBFC?
    1. nano tbfc_string.yara

```
rule TBHC_string
{
meta:
author = "David Rizzo"
description =  "Find TBFC string"
date = "2025-14-12"
strings:
$s1 = "TBFC"
condition:
any of them
}
```

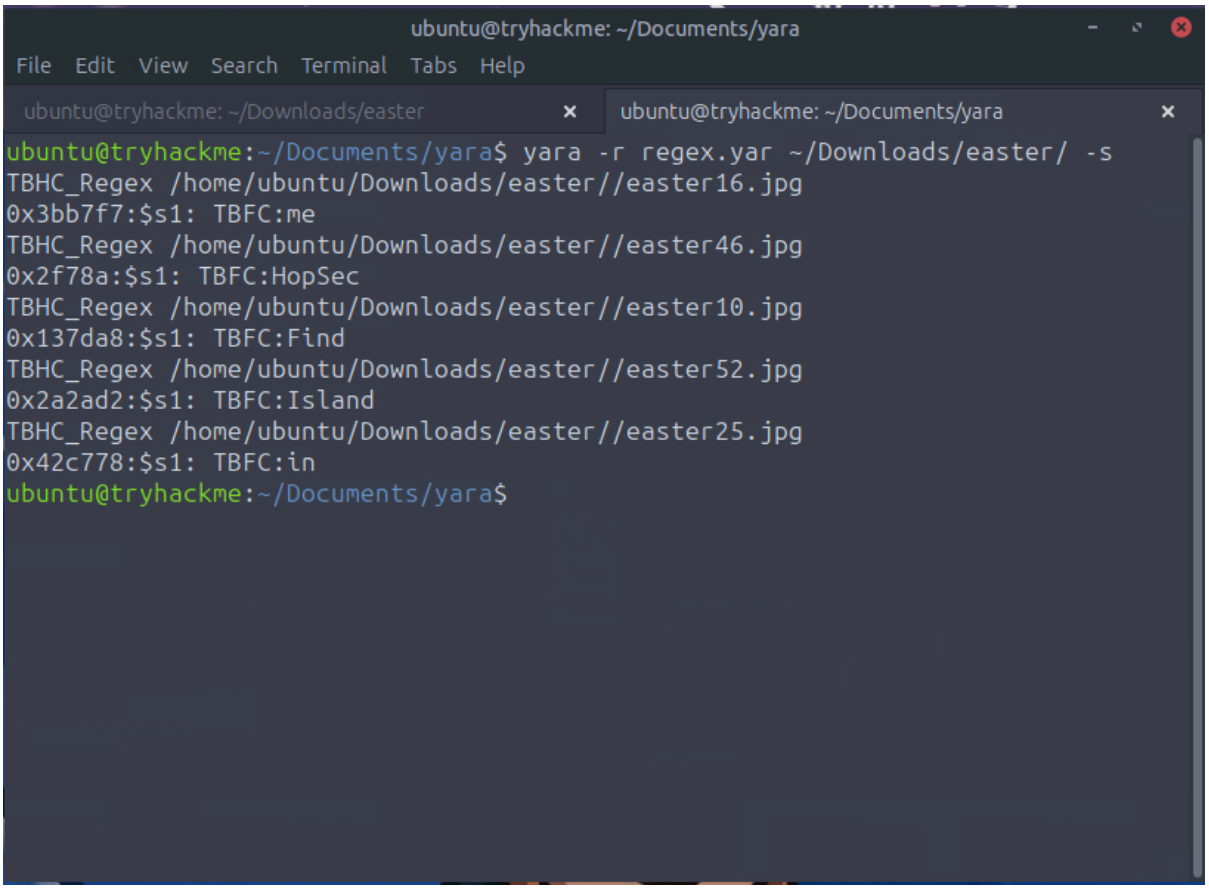
    2. `yara -r tbfc_strin.yara`

1. 

3. What regex would you use to match a string that begins with `TBFC:` followed by one or more alphanumeric ASCII characters?
    1. `/TBFC:[A-Za-z0-0]+/`
4. What is McSkid's message?

```
rule TBHC_Regex
{
    meta:
        author = "David Rizzo"
        description = "Find TBFC string"
        date = "2025-14-12"
    strings:
        $s1 = /TBFC:[A-Za-z0-0]+/
    condition:
        any of them
}
```

    1. Using the regex expression to find TBFC reveals each word of his message
    2. `yara -r regex.yara ~/Downloads/easter -s`

3. 

Lessons Learned

- **YARA rules evolve with your needs**: Starting with simple string matching and progressing to regex patterns demonstrates how defenders can refine their detection capabilities. Basic text searches (`"TBFC"`) provide broad coverage, while regex patterns (`/TBFC:[A-Za-z0-9]+/`) offer surgical precision to extract meaningful intelligence without false positives.
- **Forensic intelligence is a team effort:** By combining metadata documentation, thoughtful string definitions, and logical conditions, you create rules that not only detect threats but also communicate findings to other defenders. McSkidy's hidden message—scattered across multiple files and encoded within file content—represents how real-world incident response requires systematic pattern recognition and collaborative knowledge sharing across the security team.

Resources

TryHackMe YARA Documentation

Regular Expression. Patterns

Malware A. alysis Techniques