The Bunny’s Browser Trail

Overview

Room URL: https://tryhackme.com/room/adventofcyberpreptrack

Difficulty: Easy

Category: Prep

Date Completed: 12/1/2025

Objectives

Find the unusual User Agent in the HTTP log.

Table of Contents

Introduction

SOCMAS web servers are experiencing unusual traffic spikes, with one suspicious log entry revealing an unfamiliar User Agent: "BunnyOS/1.0 (HopSecBot)". Analyzing User Agent strings is critical for defenders to identify automated attacks and unauthorized visitors within network logs.

Define User Agent

A client application used by an end user, typically for a network protocol such as HTTP or FTP.

Walk Through

1. Click view site to open the http web log entries
2. Several different user agents accessed this site
    1. `Chrome on Windows`
    2. `Safari on MacOS`
    3. `Firefox on Linux`
    4. `Edge on Windows`
    5. `BunnyOS (HopSecBot)`
    6. `Safari on IoS`
3. Based on this the abnormal agent is `BunnyOS` and they accessed `/admin/panel` according to the log.
   browsertrail.png

Lessons Learned

- Learned to analyze HTTP web logs and identify User Agent strings to detect suspicious or automated traffic patterns
- Successfully identified `BunnyOS (HopSecBot)` as an anomalous User Agent among legitimate browsers, and discovered it accessed the sensitive `/admin/panel` endpoint, demonstrating how User Agent analysis reveals unauthorized system intrusions

---

Resources

TryHackMe

Different User Agents

Revision #1
Created 2025-12-01 18:13:09 UTC by David Rizzo
Updated 2025-12-01 18:20:33 UTC by David Rizzo