The App Trap

Overview

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

Difficulty: Easy

Category: Prep

Date Completed: 12/1/2025

Objective

Find and remove the malicious connected app.

Table of Contents

Introduction

McSkidy's social media account has been compromised and is posting suspicious messages about "EASTMAS." A malicious third-party application may be responsible for the unauthorized access. Learning to review and manage app permissions is essential for preventing data leaks and unauthorized account access.

Walk Through

1. Click view site to launch the simulated enviroment

2. There are 3 applications in the enviroment with the following permissions
    1. Weather Elf
        1. `Location`
        2. `Network Access`
        3. `Notifications`
    2. Gift Tracker
        1. `Contacts`
        2. `Network Access`
        3. `Storage`
    3. Eastmas Scheduler
        1. `Calendar`
        2. `Notifications`
        3. `Passwordvault`
3. Weather Elf and Gift tracker have appropriate apps for their use case. Eastmas Schedular has no reason to have access to `Password Vault`
4. Revoked access to `password vault` apptrap.png

Lessons Learned

- Learned to audit third-party application permissions and identify overprivileged apps that request unnecessary access to sensitive data
- Successfully identified that the **Eastmas Scheduler** app had suspicious access to the `Password Vault` and revoked it, demonstrating proper permission management to prevent unauthorized account compromise

---

Resources

TryHackMe

App Permission

Revision #1

Created 2025-12-01 17:55:38 UTC by David Rizzo

Updated 2025-12-01 18:05:25 UTC by David Rizzo