About

Campaign Overview

Setting: Wareville, home of The Best Festival Company (TBFC)

Event: SOCMAS - the annual cyber security celebration

Threat Level: Critical

Purpose: Each mission teaches essential cybersecurity skills while uncovering clues about King Malhare's conspiracy to corrupt Christmas into EASTMAS

The Antagonist: King Malhare

Origin: HopSec Island

Motivation: Jealousy over Easter being overlooked; seeks to rebrand Christmas as EAST-mas

Operatives: Sir Carrotbane, Bandit Bunnies, and HopSec Island operatives

Endgame: EASTMAS - a corrupted version of the festival designed to sabotage TBFC operations and hold Wareville hostage

---

Plot Progression

Act 1: The Glitches

- System failures and password issues plague TBFC
- McSkidy detects foul play; King Malhare's name surfaces
- Initial investigations begin on isolated systems

Act 2: Escalation & Kidnapping

- McSkidy is kidnapped by King Malhare's forces
- Wareville's defenses are severely compromised
- Christmas itself becomes at risk
- Ransom demand: 1,000 HopSec Coins for McSkidy's release
- Timeline threat: SOCMAS ends tonight

Act 3: Investigation & Defense

- The TBFC SOC team mobilizes
- Multiple challenges across different attack vectors
- Focus shifts to forensic investigation and incident response

---

Key Investigation Targets & Findings

Primary Investigation: tbfc-web01

System Type: Linux server processing Christmas wishlists

Attack: Eggstrike malware infiltration

Evidence Location: `/home/socmas/2025/eggstrike.sh`

Critical Forensic Techniques:

- Hidden file discovery using `ls -la` to uncover `.guide.txt` and `.bash_history`
- Advanced forensics including user switching and command history analysis
- File decryption to trace attacker movements

Evidence Trail

- McSkidy's last actions before kidnapping
- King Malhare's involvement and operational plans
- Christmas wishlist system compromise details

Challenge Categories

1. Forensic Investigation & Log Analysis

- **Focus:** Splunk SIEM analysis to trace ransomware infiltration
- **Skill:** Understanding attack vectors through log data
- **Objective:** Prevent infrastructure compromise and resolve the hostage situation

2. Red Team & Social Engineering

- **Type:** Authorized penetration testing
- **Team:** Recon McRed, Exploit McRed, Pivot McRed
- **Focus:** Phishing campaigns and employee awareness testing
- **Goal:** Evaluate cybersecurity training effectiveness

3. System Forensics & File Analysis

- **Type:** Linux server investigation
- **Skills:** Hidden file discovery, command history analysis, user switching
- **Goal:** Trace attacker movements and identify compromise vectors

---

Access Credentials

```
Username: mcskidy
Password: AoC2025!
Connection: ssh mcskidy@[machine_ip]
Note: Machine IP changes upon each start
```

Learning Outcomes

Each challenge reinforces essential cybersecurity competencies:

- **Incident Response** - Responding to active threats with time pressure
- **Log Analysis** - Using SIEM tools to identify attack patterns
- **Forensic Investigation** - Tracing evidence and attacker movements
- **Red Team Methodology** - Understanding offensive security tactics
- **Security Awareness** - Identifying social engineering and phishing threats
- **Linux System Administration** - File permissions, command history, user switching

---

The Stakes

- **Missing:** McSkidy (leadership compromised)
- **Threatened:** Christmas and SOCMAS celebration
- **At Risk:** TBFC systems and Wareville infrastructure
- **Timeline:** Demands must be resolved before SOCMAS ends tonight
- **Mission:** Stop King Malhare's EASTMAS plan and save Christmas

---

Revision #8

Created 2025-12-01 16:09:56 UTC by David Rizzo

Updated 2025-12-03 17:02:30 UTC by David Rizzo