TryHackMe Advent of Cyber 2025

Day 2 Challenge Report

Social Engineering & Phishing Attacks

1. Executive Summary

This report documents the completion of Day 2 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on understanding social engineering attacks, specifically phishing techniques, and executing a practical phishing campaign using the Social Engineering Toolkit (SET). Successfully crafted and deployed a phishing email that captured target credentials and gained access to a toy factory management system.

2. Challenge Overview

Objective: Learn about social engineering and phishing attacks, then execute a phishing campaign to capture user credentials and access a protected system.

Target: TBFC (Toy Building Factory Corporation) employee email: factory@wareville.thm

3. Theoretical Foundation

3.1 Social Engineering

Social engineering refers to manipulating users to make mistakes that compromise security. The term 'social' indicates that the attack targets human beings rather than computer systems, relying on psychological manipulation instead of technical vulnerabilities.

Key Psychological Factors:

- Urgency - Creating time pressure to bypass critical thinking
- Curiosity - Exploiting natural human inquisitiveness
- Authority - Impersonating trusted figures or organizations

Social engineering is often referred to as 'human hacking' because it exploits human psychology rather than technical vulnerabilities. Attackers manipulate users into sharing passwords, opening malicious files, or approving fraudulent payments.

3.2 Phishing

Phishing is a subset of social engineering where communication primarily occurs through messages. While email was historically the most common vector, modern phishing has expanded to multiple channels:

- **Email phishing** - Traditional email-based attacks
- **Smishing** - SMS/text message phishing
- **Vishing** - Voice call phishing
- **Quishing** - QR code-based phishing
- **Social media direct messages** - Platform messaging phishing

3.3 S.T.O.P. Anti-Phishing Mnemonics

TBFC cyber security awareness training teaches two S.T.O.P. mnemonics to help users identify and avoid phishing attacks.

First S.T.O.P. - Questions to Ask (from All Things Secured):

- **S**uspicious? - Does this seem unusual or unexpected?
- **T**elling me to click something? - Am I being directed to click a link?
- **O**ffering me an amazing deal? - Is this too good to be true?
- **P**ushing me to do something now? - Is there artificial urgency?

Second S.T.O.P. - Actions to Take:

- **S**low down - Scammers rely on your adrenaline
- **T**ype the address yourself - Don't use links from messages
- **O**pen nothing unexpected - Verify before opening attachments
- **P**rove the sender - Check the real email address, not just the display name

4. Practical Attack Implementation

4.1 Attack Setup

The attack infrastructure consisted of two main components located in ~/Rooms/AoC2025/Day02:

- **index.html** - Fake TBFC portal login page
- **server.py** - Python server to capture compromised credentials

4.2 Social Engineering Toolkit (SET) Configuration

Used the Social Engineering Toolkit to craft and deliver the phishing email. The configuration process involved multiple strategic decisions:

Attack Vector Selection:

1. Selected: Social Engineering Attack
2. Selected: Mass Mailer Attack
3. Selected: E-Mail Attack Single Email Address

Email Configuration Parameters:

- **Target email:** factory@wareville.thm
- **Delivery method:** Use your own server or open relay
- **From address:** updates@flyingdeer.thm

Rationale: The toy factory regularly communicates with Flying Deer shipping company, making this a trusted sender

- **From name:** Flying Deer
- **Username for open-relay:** (blank)
- **Password for open-relay:** (blank)
- **SMTP server:** {VM_IP} - Direct delivery to TBFC mail server
- **SMTP port:** 25 (default)

Message Options:

- **High priority flag:** No (situational decision)
- **Attach file:** No
- **Attach inline file:** No

4.3 Phishing Email Composition

The email was carefully crafted to create urgency and legitimacy while directing the target to the fake login portal.

- **Subject line:** Emergency - crafted to create urgency
- **Message format:** Plain text (default)
- **Phishing link:** http://127.0.0.1:8000 or http://{ATTACKER_IP}:8000

Key Strategy: The message body was designed to be convincing and serious, incorporating the hosted phishing website link. The email ended with 'END' (capitals) to signal completion of the message composition.

Note: *After sending, waited 1-2 minutes monitoring the Python server interface for credential capture.*

4.4 Credential Capture

The Python server successfully captured credentials when the target accessed the fake login page:

```
Starting server on http://0.0.0.0:8000
10.64.138.169 - - [03/Dec/2025 22:03:02] "GET / HTTP/1.1" 200 -
[2025-12-03 22:03:02] Captured -> username: admin    password: unranked-wisdom-anthem    from: 10.64.138.169
```

Captured Credentials:

- **Username:** admin
- **Password:** unranked-wisdom-anthem

4.5 System Access & Intelligence Gathering

Used the captured credentials to access the TBFC portal at http://{VM_IP}.

Login Credentials Used:

- Username: factory
- Password: unranked-wisdom-anthem

Challenge Answer: Total toys expected for delivery: **1984000**

5. Key Skills & Techniques Learned

5.1 Social Engineering Concepts

- Understanding psychological manipulation techniques
- Identifying key factors: urgency, curiosity, and authority
- Recognizing 'human hacking' vs technical exploitation
- Understanding why attackers target human vulnerabilities

5.2 Phishing Attack Methods

- Email phishing techniques and best practices
- Understanding modern phishing variants (smishing, vishing, quishing)
- Crafting convincing phishing messages
- Email spoofing and sender impersonation

5.3 Technical Tools & Infrastructure

- Social Engineering Toolkit (SET) configuration and usage
- SMTP server configuration for email delivery
- Python server setup for credential harvesting
- Fake login page deployment
- Real-time credential monitoring

5.4 Defensive Awareness

- S.T.O.P. mnemonics for phishing detection
- Email verification techniques
- Importance of typing URLs manually
- Sender verification best practices

6. Key Takeaways

- Social engineering exploits human psychology, not technical vulnerabilities
- Phishing attacks are increasingly sophisticated and harder to detect
- Urgency, curiosity, and authority are powerful psychological triggers
- Impersonating trusted entities increases phishing success rates
- Simple tools like SET can execute sophisticated attacks
- The S.T.O.P. mnemonics provide practical defense against phishing
- Even security-aware users can fall victim without proper vigilance

7. Conclusion

Day 2 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in social engineering and phishing attack methodologies. The challenge successfully demonstrated how attackers exploit human psychology to bypass technical security controls.

Through practical implementation of a phishing campaign using the Social Engineering Toolkit, gained hands-on experience in email spoofing, fake portal creation, credential harvesting, and post-exploitation intelligence gathering. The exercise reinforced the critical importance of security awareness training and the S.T.O.P. mnemonics for identifying and preventing phishing attacks.

Challenge Status: **COMPLETED ✓**