Phishing - Merry Clickmas

Day 2

Learn how to use the Social-Engineer Toolkit to send phishing emails.

- Phishing Exercise for TBFC

Phishing Exercise for TBFC

Overview

Room URL: https://tryhackme.com/room/phishing-aoc2025-h2tkye9fzU

Difficulty: Easy

Category: Phishing

Date Completed: 12/2/2025

Objectives

- Understand what social engineering is
- Learn the types of phishing
- Explore how red teams create fake login pages
- Use the Social-Engineer Toolkit to send a phishing email

Table of Contents

Introduction

TBFC's defenses are tested once more, this time through a sophisticated social engineering campaign. The red team orchestrates a phishing attack targeting factory staff, crafting a convincing email from a trusted shipping partner and backing it with a fake login portal designed to harvest credentials. This challenge demonstrates how social engineering exploits human psychology—leveraging urgency, authority, and trust—to bypass even well-intentioned security awareness training. The attack succeeds in capturing working credentials, revealing a critical

vulnerability: no matter how robust technical defenses are, they can be undermined if employees fall victim to carefully crafted phishing schemes. Understanding both the attacker's methodology and the psychological triggers that make phishing effective is essential for building a human-centric defense strategy.

Key Concepts

- **Social Engineering:** Manipulating users into making security mistakes through psychological tactics (urgency, curiosity, authority)
- **Phishing:** Using messages (email, SMS, voice, QR codes) to trick users into clicking malicious links or revealing credentials
- **Credential Harvesting:** Creating fake login pages to capture user credentials when targets are deceived into authenticating
- **Spear-Phishing:** Targeted attacks that research and impersonate trusted entities the victim interacts with

S.T.O.P

- **Suspicious?**
- **Telling me** to click something?
- **Offering me** an amazing deal?
- **Pushing me** to do something now?

S.T.O.P (2)

- **Slow down.** Scammers run on your adrenaline.
- **Type the address yourself.** Don’t use the message’s link.
- **Open nothing unexpected.** Verify first.
- **Prove the sender.** Check the real From address/number, not just the display name.

Walk Through

1. Launch the target machine and the attack box.
    - The attack box is already on the same network as the target machine. No need to mess with vpn configs and troubleshoot.
    - Attackboxwelcome.png

2. **What is the password used to access the TBFC portal?**
    1. There is a script located at `~/Rooms/AoC2025/Day02` to sping up the server to start listening for credentials.
    2. Opened terminal and went to the directory `cd ~/Rooms/AoC2025/Day02`
    3. Launched the script using `./server.py`
    4. Confirmed the webpage is up and running at `http://localhost:8000`
        - fakeportal.png
    5. Using the Social-Engineering-Toolkit (SET) to deliver the link to the victim to collect credentials.
        1. `setoolkit` to launch the toolkit in terminal
        2. Option `1` for *social engineering attacks*
        3. Option `5` for *mass mailer*
        4. Option `1` for *send to single email*
        5. Send To: `factory@wareville.thm`
        6. Option `2` *use your own server or open relay*
        7. From Address: `updates@flyingdeer.thm`
        8. From Name: `Flying Deer`
        9. Username for open relay `` (leave blank)
        10. Password for open relay `` (leave blank)
        11. SMTP Email Server Address `10.64.130.91` (target ip address)
        12. Port Number `25`
        13. Flag as High Priority `no`
        14. Attach a file `n`
        15. Attach an inline file `n`
        16. Email Subject `Shipping Schedule Changes` (should be something convincing)
        17. Send email as `html` or `plaintext` `` (leave blank)
        18. The body of the email line by line. Use `END` to indicate end of email.
            - PhishingBody.png
        19. Email Has been sent
    6. Switch back to terminal with `server.py` running to see if it captured credentials
    7. Username: `admin` Password: `u**********m`
    8. phishingcreds.png
3. Browse to `http://10.64.130.91` from within the AttackBox and try to access the mailbox of the `factory` user to see if the previously harvested `admin` password has been reused on

the email portal. What is the total number of toys expected for delivery?

1. Load `http://10.64.130.91` in web browser to bring up roundcube login
2. See if factory user re-uses password
    1. Username: `factory` Password: `u**********m` was successful
3. `1*****0` expected for delivery
    - toysdeliver.png

Lessons Learned

- **Social engineering attacks succeed through psychological manipulation and credential harvesting:** This challenge demonstrated how a straightforward phishing attack; combining spear-phishing email tactics with a fake login portal; can effectively capture user credentials despite security awareness training. The success of this attack (harvesting the admin credentials) reveals that even basic social engineering techniques leveraging authority and urgency can bypass human defenses. Critically, these foundational concepts are easily escalated into sophisticated attacks: adversaries can deploy the same credential harvesting methodology using cloud infrastructure, legitimate-looking domain names (instead of raw IP addresses), SSL certificates for HTTPS encryption, and professional email infrastructure to create virtually indistinguishable phishing campaigns that are far more difficult to detect and attribute.
- **Credential reuse and lack of multi-factor authentication create cascading security failures:** The challenge exposed a critical vulnerability: users reuse passwords across multiple systems, allowing a single compromised credential to grant access to sensitive operational data. The harvested admin password successfully authenticated the factory user on the email portal, providing immediate access to internal communications and operational details (the toy delivery count). This demonstrates that without multi-factor authentication (MFA), email filtering, and monitoring for unusual access patterns, organizations remain exposed to rapid lateral movement and data exfiltration once an initial credential is compromised; highlighting why defense-in-depth strategies with MFA, anomaly detection, and credential monitoring are essential safeguards against both basic and sophisticated phishing attacks.

Resources

TryHackMe

All Things Secured

Social Engineering Toolkit