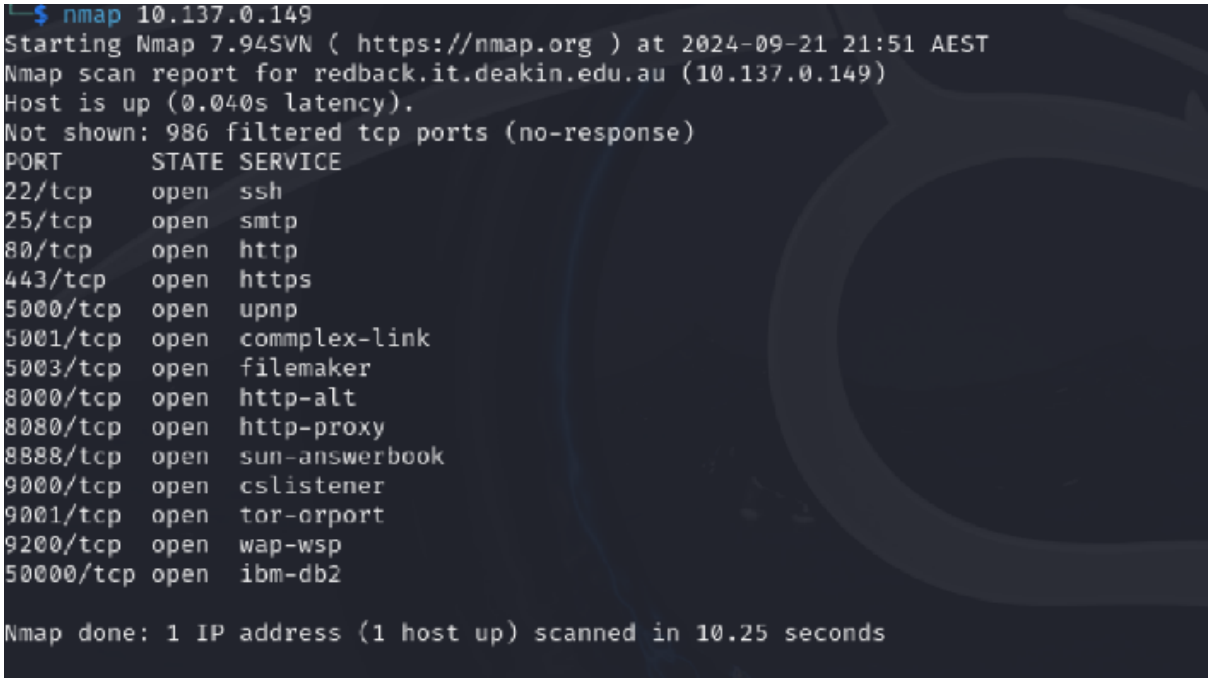
Social Engineering on Candice Smith

Target: Candice Smith

We will target Candice Smith's LinkedIn profile as we have access to her profile details. Our strategy involves creating a fake LinkedIn website to execute a credential harvesting attack.



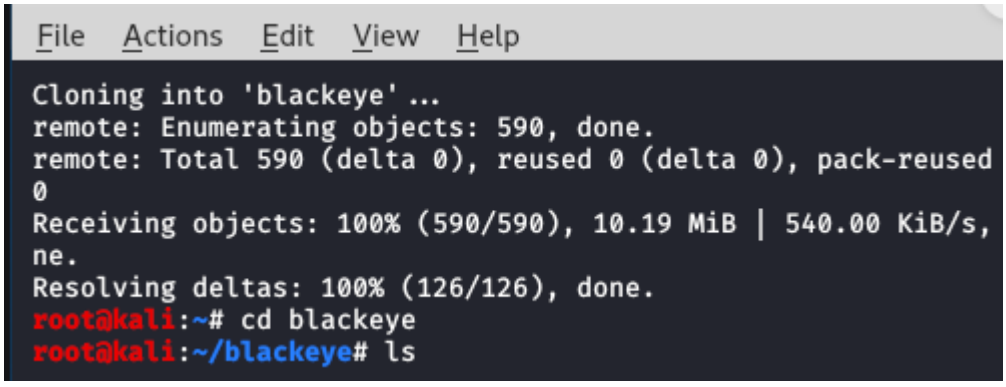
Step 1: Creating a Fake LinkedIn Page

We will use the default Kali tool 'Blackeye' to generate a phishing link that mimics the LinkedIn login page.

Step 2: Phishing Email

We will send an email to Candice Smith offering her a lucrative job opportunity. The email will contain the phishing link: https://wmw-linkedin-com.loca.lt. If Candice falls for it, she will input her credentials into the cloned LinkedIn page, and we will capture her login information.

We will use the Social Engineering Toolkit (SET) to send the phishing email.



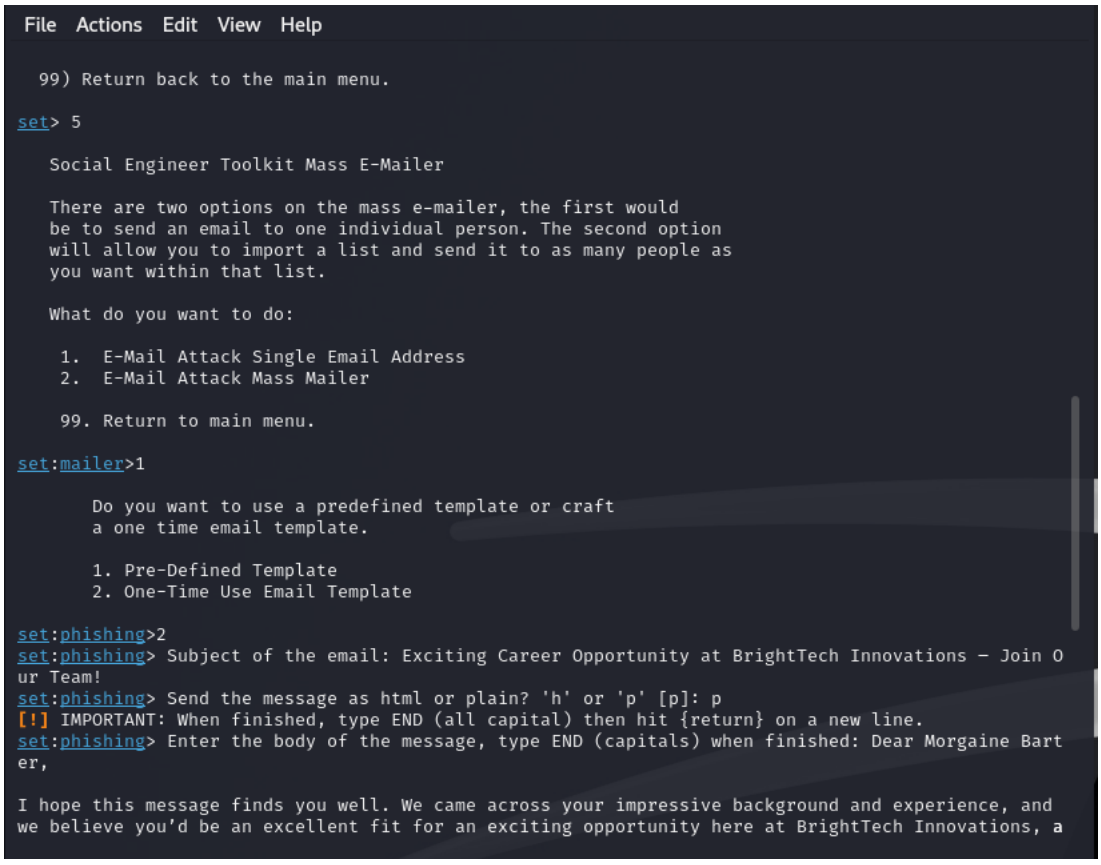
Report

Objective:

The goal of this exercise was to evaluate how aware our team members are of social engineering attacks, particularly phishing attempts involving credential harvesting.

Overview:

In this simulation, we targeted 'Candice Smith' using a common social engineering technique—phishing through LinkedIn job offers. The attack leveraged a fake LinkedIn page designed to capture login credentials.



Matt Mikhail – Red Team

Execution:

1. A fake LinkedIn page was created using Blackeye.
2. A phishing email with a job offer was sent to Candice Smith's email, containing a link to the fake LinkedIn page.
3. The email was crafted to look professional and legitimate, aimed at prompting Candice to click the link and enter her credentials.

Outcome:

Fortunately, Candice did not fall for the attack. She noticed the link looked suspicious and flagged the email as phishing. This shows that Candice, like our broader team, is aware of the dangers posed by social engineering tactics.

Conclusion:

Our team demonstrated strong awareness of phishing attempts and social engineering techniques. Candice's refusal to click on the suspicious link is a testament to the effectiveness of our ongoing security training and awareness campaigns.