

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.

```
$ nmap 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 21:51 AEST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.040s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
5000/tcp   open  upnp
5001/tcp   open  complex-link
5003/tcp   open  filemaker
8000/tcp   open  http-alt
8080/tcp   open  http-proxy
8888/tcp   open  sun-answerbook
9000/tcp   open  cslistener
9001/tcp   open  tor-orport
9200/tcp   open  wap-wsp
50000/tcp  open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 10.25 seconds
```

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.locat.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.

```
File Actions Edit View Help
Cloning into 'blackeye' ...
remote: Enumerating objects: 590, done.
remote: Total 590 (delta 0), reused 0 (delta 0), pack-reused
0
Receiving objects: 100% (590/590), 10.19 MiB | 540.00 KiB/s,
ne.
Resolving deltas: 100% (126/126), done.
root@kali:~# cd blackeye
root@kali:~/blackeye# ls
```

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.

```
File Actions Edit View Help

99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1

Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email: Exciting Career Opportunity at BrightTech Innovations – Join O
ur Team!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Dear Morgaine Bart
er,

I hope this message finds you well. We came across your impressive background and experience, and
we believe you'd be an excellent fit for an exciting opportunity here at BrightTech Innovations, a
```

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.