Testing Your Organization's Social Media Awareness

Contents

- Social Media
- Why is it important
- Why we should be testing it
- How we can test it
    - Social Mapper
    - Social Attacker

# id –un jacob-wilkin

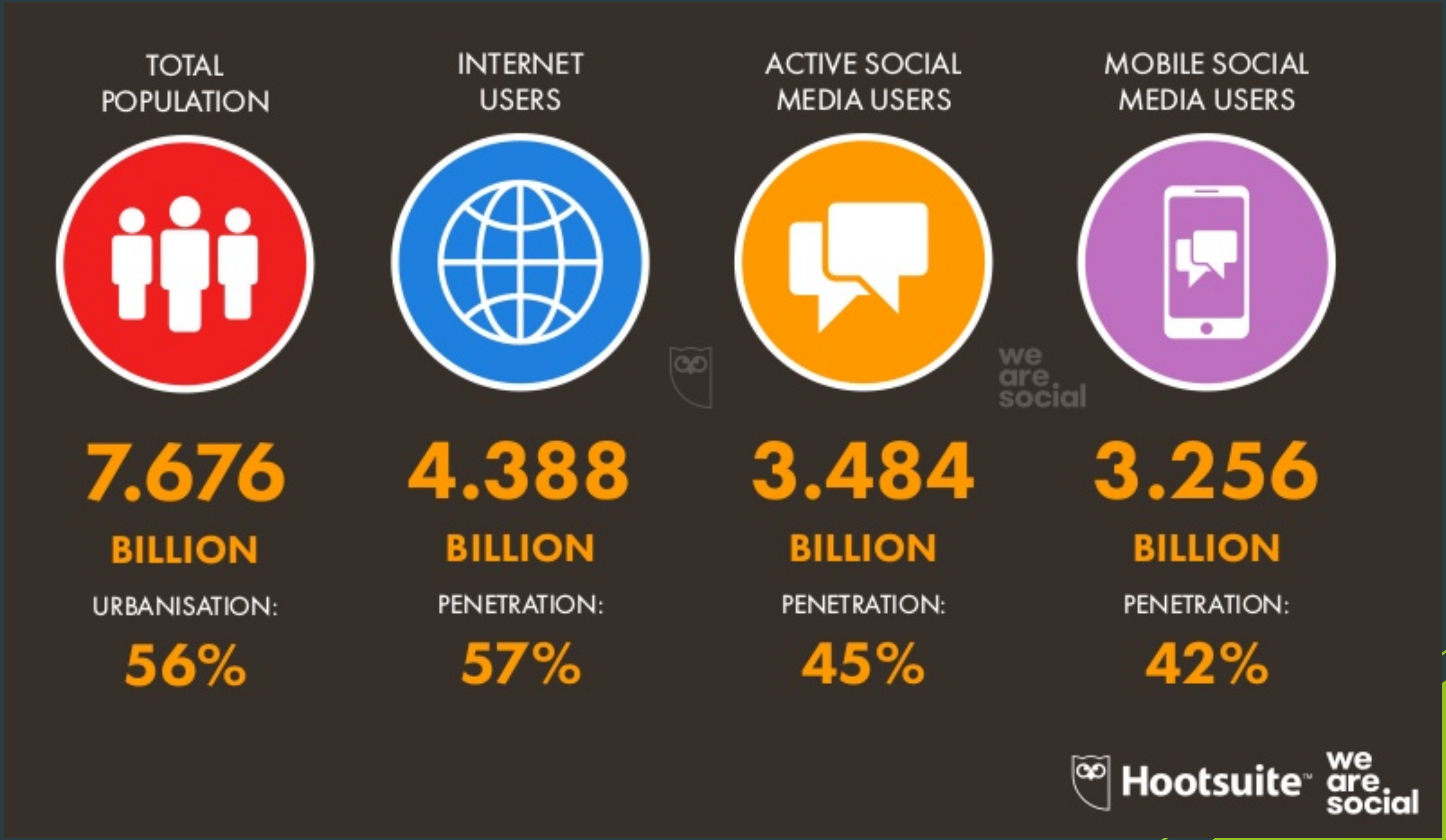
- Security Consultant, Penetration Tester,
  Red Teamer, Hacker
- Performed 100s of Penetration Tests
- Hacked Multiple Banks (with permission)
- Creator of Spray & Social Mapper
- British (☕🇬🇧)

Social Media Sites Hate Him

Security Consultant discovers how to scrape social media sites without an API Key

JUST USING THIS ONE DUMB TRICK!

Social Media



TOTAL POPULATION
7.676 BILLION
URBANISATION: 56%

INTERNET USERS
4.388 BILLION
PENETRATION: 57%

ACTIVE SOCIAL MEDIA USERS
3.484 BILLION
PENETRATION: 45%

MOBILE SOCIAL MEDIA USERS
3.256 BILLION
PENETRATION: 42%

Hootsuite™ we are social

How does it affect security?

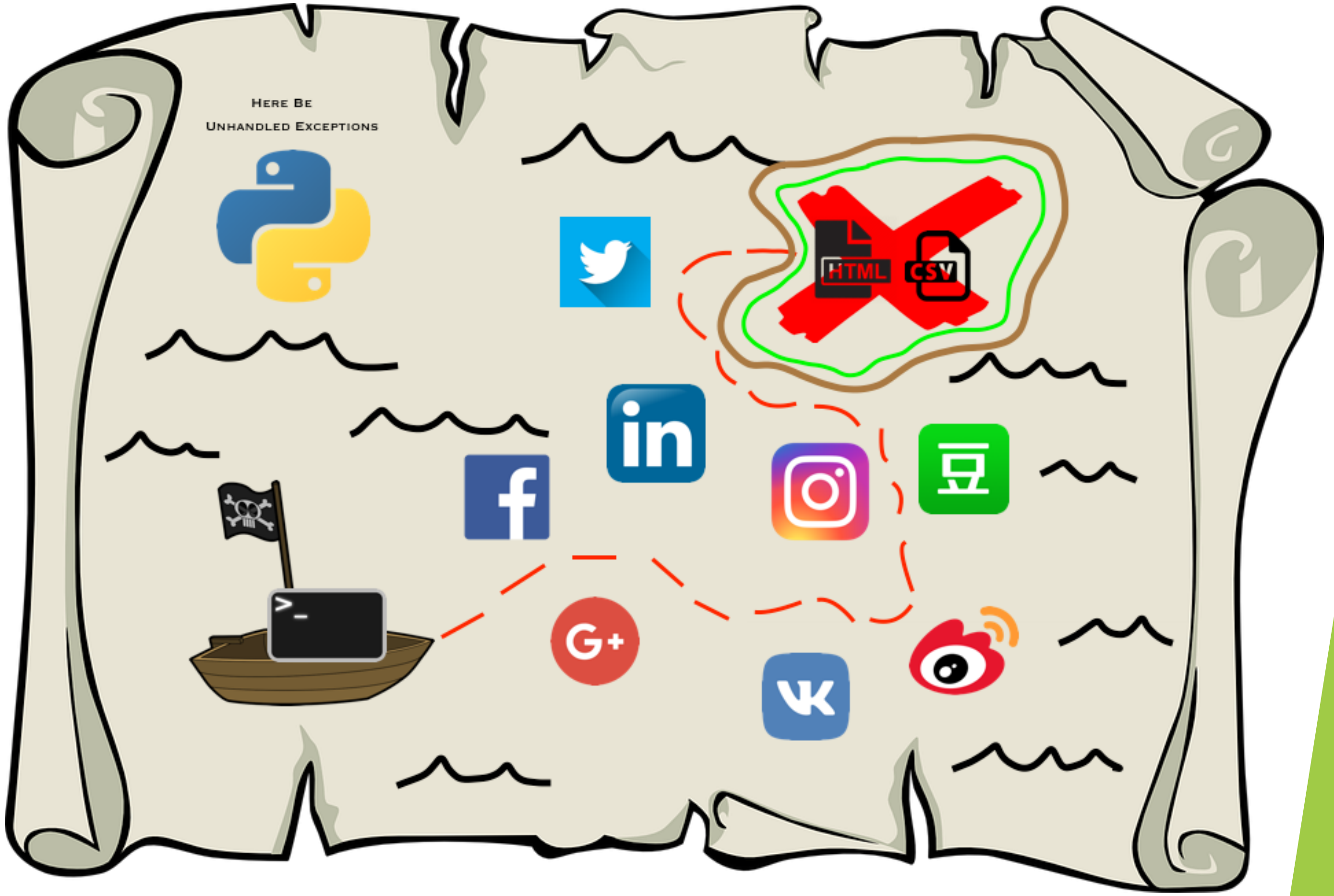
- Social Media Phishing is on the rise
  - Preferred Vector for attackers
  - 33% click rates vs 11% for business email
- Bring your own device
- Access from work devices
- Alternatives attack vectors
  - Credential based phished – shared work credentials
  - Malicious file download
  - Browser exploitation

How do we address this?

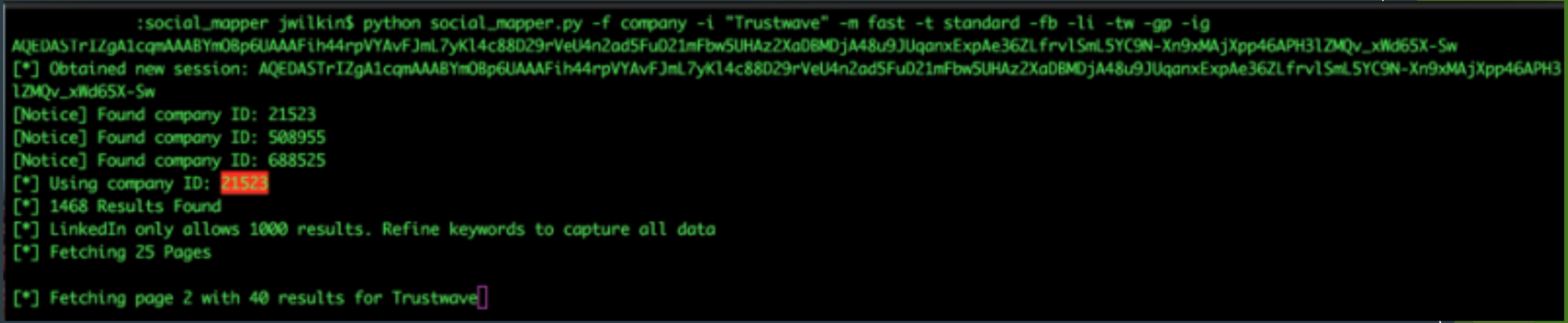
- Improving Awareness
- Mock Campaigns
- Identify who is at risk
- Two types of test:
  - Passive
  - Active

Passive Testing with Social Mapper

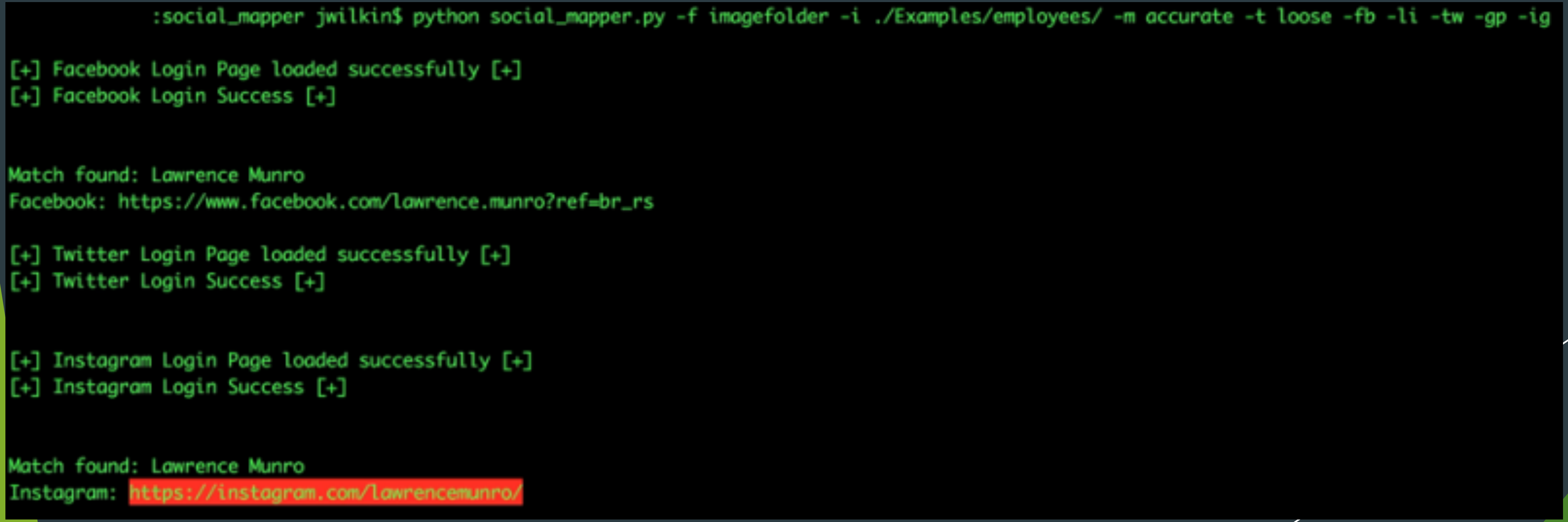
- Feed in LinkedIn Company or list of enumerated employees
- Logs into Social Media sites with provided credentials
- Searches based on name, and identifies via Facial Recognition
- Pros:
  - Quicker
  - Less Intrusive
- Cons:
  - Identification only, no evaluation



Running Social Mapper



```
            :social_mapper jwilkin$ python social_mapper.py -f company -i "Trustwave" -m fast -t standard -fb -li -tw -gp -ig
AQEDASTrIZgA1cqmAAABYmOBp6UAAAFih44rpVYAvFJmL7yKl4c88D29rVeU4n2ad5FuD21mFbw5UHAz2XaDBMDjA48u9JUqanxExpAe36ZLfrvlSmL5YC9N-Xn9xMAjXpp46APH3lZMQv_xWd65X-Sw
[*] Obtained new session: AQEDASTrIZgA1cqmAAABYmOBp6UAAAFih44rpVYAvFJmL7yKl4c88D29rVeU4n2ad5FuD21mFbw5UHAz2XaDBMDjA48u9JUqanxExpAe36ZLfrvlSmL5YC9N-Xn9xMAjXpp46APH3
lZMQv_xWd65X-Sw
[Notice] Found company ID: 21523
[Notice] Found company ID: 508955
[Notice] Found company ID: 688525
[*] Using company ID: 21523
[*] 1468 Results Found
[*] LinkedIn only allows 1000 results. Refine keywords to capture all data
[*] Fetching 25 Pages

[*] Fetching page 2 with 40 results for Trustwave
```



```
           :social_mapper jwilkin$ python social_mapper.py -f imagefolder -i ./Examples/employees/ -m accurate -t loose -fb -li -tw -gp -ig

[+] Facebook Login Page loaded successfully [+]
[+] Facebook Login Success [+]


Match found: Lawrence Munro
Facebook: https://www.facebook.com/lawrence.munro?ref=br_rs

[+] Twitter Login Page loaded successfully [+]
[+] Twitter Login Success [+]


[+] Instagram Login Page loaded successfully [+]
[+] Instagram Login Success [+]


Match found: Lawrence Munro
Instagram: https://instagram.com/lawrencemunro/
```

Example Social Mapper Report

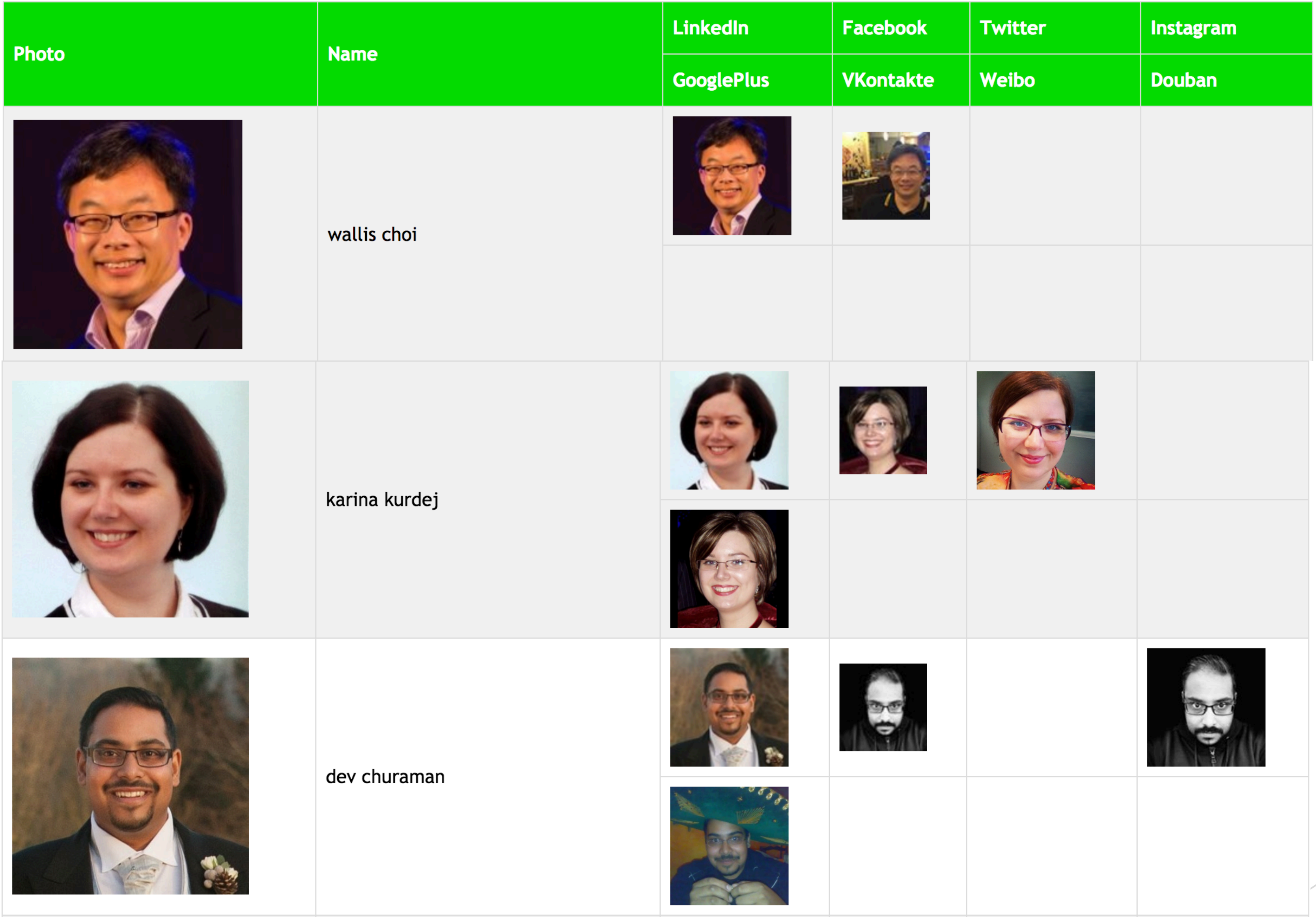
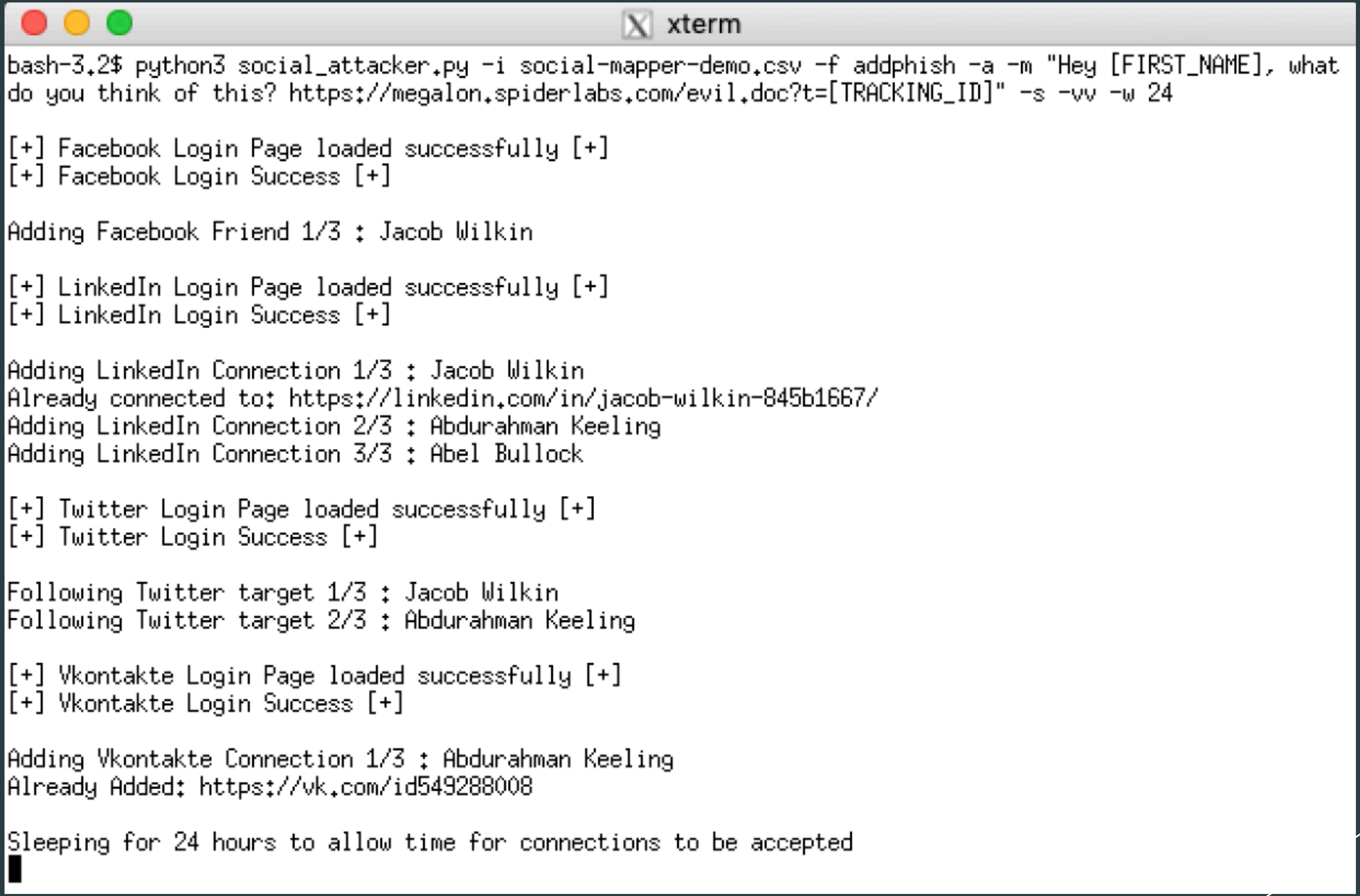


Photo	Name	LinkedIn	Facebook	Twitter	Instagram
		GooglePlus	VKontakte	Weibo	Douban
	wallis choi				
	karina kurdej				
	dev churaman				

Active Testing with Social Attacker

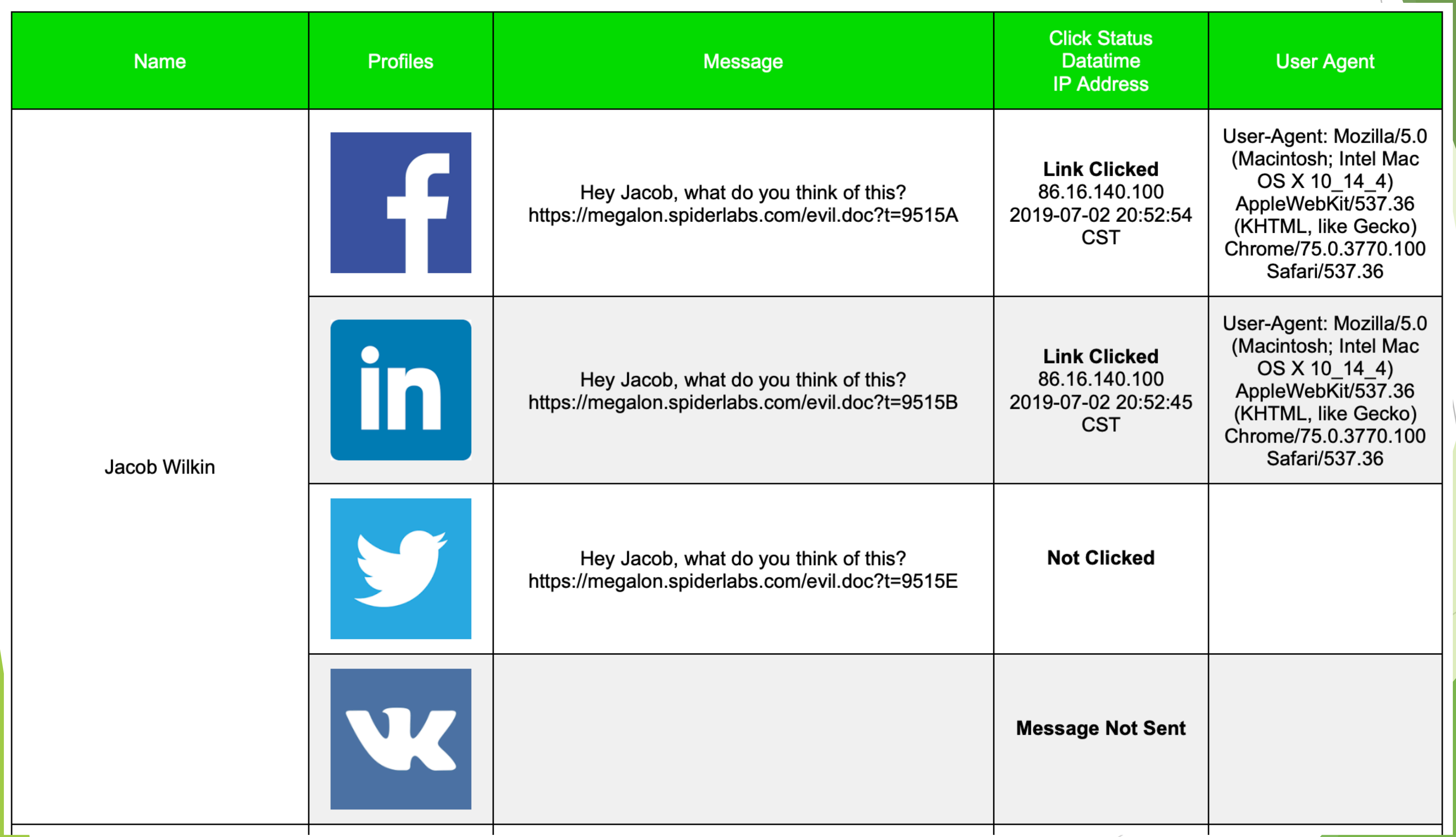
- Feed in Social Mapper output of targets social media profiles.
- Logs into Social Media sites with provided credentials
- Initiates connections to targets
- Sends phishing messages/links to users which accept.
- Pros:
  - Full testing, identifies at risk users
- Cons:
  - Slower
  - Intrusive on private profiles

Running Social Attacker



```
bash-3.2$ python3 social_attacker.py -i social-mapper-demo.csv -f addphish -a -m "Hey [FIRST_NAME], what
do you think of this? https://megalon.spiderlabs.com/evil.doc?t=[TRACKING_ID]" -s -vv -w 24

[+] Facebook Login Page loaded successfully [+]
[+] Facebook Login Success [+]

Adding Facebook Friend 1/3 : Jacob Wilkin

[+] LinkedIn Login Page loaded successfully [+]
[+] LinkedIn Login Success [+]

Adding LinkedIn Connection 1/3 : Jacob Wilkin
Already connected to: https://linkedin.com/in/jacob-wilkin-845b1667/
Adding LinkedIn Connection 2/3 : Abdurahman Keeling
Adding LinkedIn Connection 3/3 : Abel Bullock

[+] Twitter Login Page loaded successfully [+]
[+] Twitter Login Success [+]

Following Twitter target 1/3 : Jacob Wilkin
Following Twitter target 2/3 : Abdurahman Keeling

[+] Vkontakte Login Page loaded successfully [+]
[+] Vkontakte Login Success [+]

Adding Vkontakte Connection 1/3 : Abdurahman Keeling
Already Added: https://vk.com/id549288008

Sleeping for 24 hours to allow time for connections to be accepted
█
```

Example Social Attacker Report



Name	Profiles	Message	Click Status Datatime IP Address	User Agent
Jacob Wilkin	f	Hey Jacob, what do you think of this? https://megalon.spiderlabs.com/evil.doc?t=9515A	**Link Clicked** 86.16.140.100 2019-07-02 20:52:54 CST	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
	in	Hey Jacob, what do you think of this? https://megalon.spiderlabs.com/evil.doc?t=9515B	**Link Clicked** 86.16.140.100 2019-07-02 20:52:45 CST	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
	🐦	Hey Jacob, what do you think of this? https://megalon.spiderlabs.com/evil.doc?t=9515E	**Not Clicked**	
	VK		**Message Not Sent**	

- Defenses

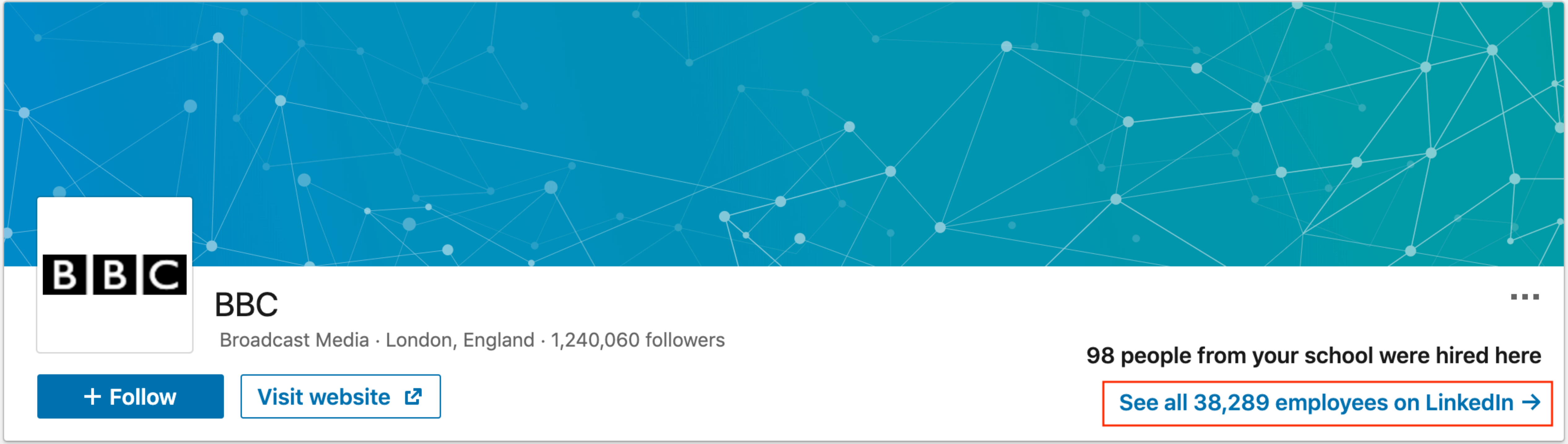
Protecting Yourself

- Don’t use the same name/username across sites.
- Don’t accept connections from people you don’t know.
- Don’t click on links from people you don’t know.
- Don’t show your face in your profile picture.

Jacob Wilkin
Timeline ▾
About

Protecting Your Organization

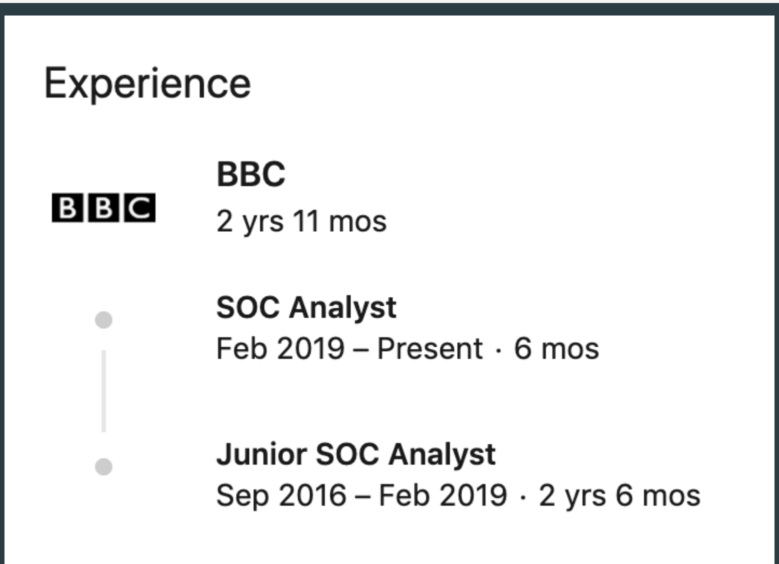
- Run Social Media Awareness testing.
- At least Social Mapper to identify employees linked to your company online.
- Warn employees about Social Media Phishing.
- Add additional slides/information to standard phishing awareness trainings.
- Ask Employees not to link themselves to your organization on LinkedIn



BBC

Broadcast Media · London, England · 1,240,060 followers

98 people from your school were hired here

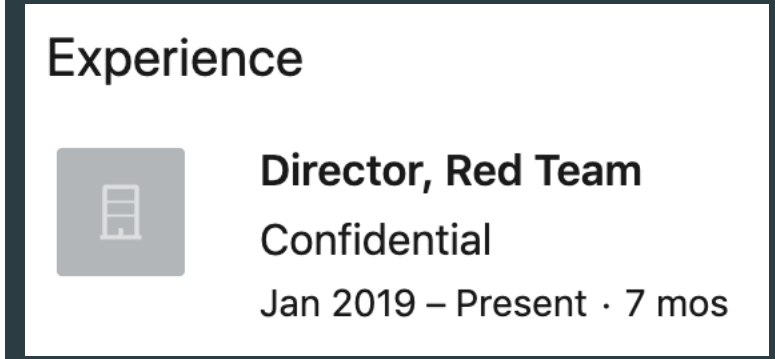


Experience

BBC
2 yrs 11 mos

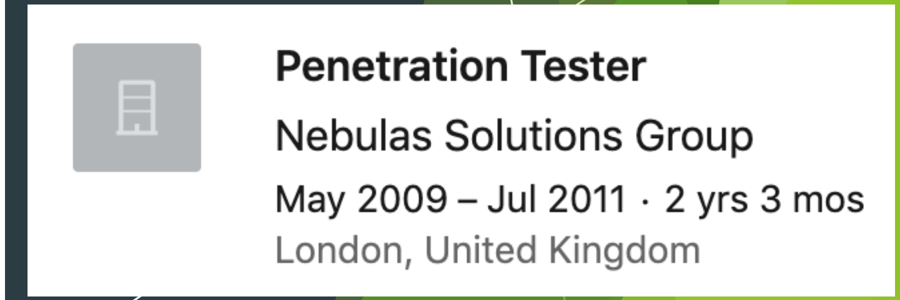
SOC Analyst
Feb 2019 – Present · 6 mos

Junior SOC Analyst
Sep 2016 – Feb 2019 · 2 yrs 6 mos



Experience

Director, Red Team
Confidential
Jan 2019 – Present · 7 mos



Penetration Tester
Nebulas Solutions Group
May 2009 – Jul 2011 · 2 yrs 3 mos
London, United Kingdom

Advice to Social Media Sites

- Work on detecting browser instrumentation bots that use selenium.
- Move away from name based searches
- Require additional proof of connection such as phone number
  - (like WhatsApp & WeChat)

Disclaimer

- Targeting employees private social media accounts may be illegal in some countries. Check local laws before running any tests.
- Don’t target organizations you don’t have permission to target.
- Running this tool will likely break Social Media Sites Terms and Conditions. Your accounts may be banned.

- Summary

Q&A

- Thanks for listening
- Any Questions? AMA
  - via email/twitter is fine too!

✉ jacobwilkin123@outlook.com

https://github.com/Greenwolf/social_mapper

https://github.com/Greenwolf/social_attacker

@Jacob_Wilkin