Assignment 1

[10 pts] What subdomain is out of scope regarding open redirects?

There are no out-of-scope targets.

[15 pts] Using passive methods only, what subdomains can you find for indeed.com?

Must have at least 25 subdomains

1. https://au.indeed.com/
2. https://be.indeed.com/
3. https://de.indeed.com/
4. https://uk.indeed.com/
5. https://fr.indeed.com/
6. https://ie.indeed.com/
7. https://de.indeed.com/
8. https://ca.indeed.com/
9. https://nl.indeed.com/
10. wiki.indeed.com
11. bugs.indeed.com
12. api.indeed.com
13. js.indeed.com
14. t.indeed.com
15. https://central.indeed.com/
16. https://docs.indeed.com/
17. https://resumes.indeed.com/
18. https://support.indeed.com/hc/en-us
19. https://sso.indeed.com/
20. https://socialmediaimages.indeed.com/
21. https://profile-api.indeed.com/
22. https://prod.statics.indeed.com/
23. https://optimizely.indeed.com/
24. https://partnerships.indeed.com/
25. https://secure.indeed.com/auth?hl=en&continue=%2Fsettings%2Faccount

[15 pts] From those subdomains, what unique IPs can you find?

Must have at least 25 IP addresses

1. 162.159.130.67
2. 162.159.129.67
3. 104.16.51.111
4. 104.16.53.111
5. 104.17.74.206
6. 104.17.72.206
7. 104.17.71.206
8. 104.17.73.206

9. 104.17.70.206
10. 104.18.41.248
11. 104.18.41.71
12. 104.18.42.87
13. 104.18.32.23
14. 104.18.36.17
15. 104.18.36.88
16. 104.18.37.138
17. 104.18.38.92
18. 172.64.146.185
19. 172.64.145.169
20. 172.64.151.239
21. 172.64.151.168
22. 172.64.155.233
23. 172.64.150.118
24. 172.64.146.8
25. 172.64.149.164

[15 pts] What netblocks are granted to or associated with the company, and who owns them? Must have at least 4 netblocks

1. 207.226.200.0/28 - The organization Indeed owns this netblock
2. 66.90.225.72/29 - The organization Indeed owns this netblock
3. 63.233.135.144/29 - The organization Indeed owns this netblock
4. 207.191.44.144/28 - The organization Indeed owns this netblock

[20 pts] What employee email addresses can you find? Must have at least 6 email addresses

1. joe@indeed.com
2. kbyrne@indeed.com
3. rshannon@indeed.com
4. srubes@indeed.com
5. vgambo@indeed.com
6. wbalistrieri@indeed.com

[25 pts] Using a non-aggressive method we covered in class, such as Google dorking, polite recon-ng modules, or Eyewitness, find at least one endpoint, service, or exposure which could be used for future research or testing. For example, an API that doesn't require a key/token, an interesting file, error page, service, etc. It does not have to be a proven vulnerability, just something that should be researched more as we enumerate the attack surface. Provide the method and the findings.

I found this interesting file that could be researched more: https://www.indeed.com/robots.txt. These are the steps I followed to obtain this finding:

1. Open recon-ng
2. Enter input: “workspaces create lab”
3. Enter input: “modules load discovery/info_disclosure/interesting_files”

4. Enter input: “options set SOURCE indeed.com”
5. Enter input: “run”