General Information Gathering

Automated Steps

☐ Run Spiderfoot with the base domain name and an appropriate level based on your scope.

- ☐ Stick to passive scans pre-engagement.
- ☐ Known that web crawling may hit out-of-scope targets and take a long time.

Manual Steps

☐ Manually review social media sites for interesting info.

- ☐ Twitter, Facebook, YouTube, Instagram, LinkedIn, Glassdoor, Reddit, etc.

☐ Manually review corporate website.

☐ Manually search GitHub, Gitlab, StackOverflor, etc for company and product names.

- ☐ If company has their own repos, consider running gitrob.

DNS Enumeration

☐ Run amass with a config file including API keys and a brute-force strategy.
amass -d <domain name> -config <config file>

☐ Run theHarvester
./theHarvester.py -d <domain name> -b all

☐ Use cloud_enum to enumerate public resources on Amazon, Azure, and Google Cloud.

Username Enumeration

☐ Run linkedin2username.

☐ Search through your hoard of password dumps.

Breached Account Reporting

☐ Run usernames through pwned_report