Vision Statement

Project: NovaSight/NovaCoast

Team: Human Error is a Myth

- Graham Foster - (gmfoster@ucsb.edu)
- Diego Segundo (diegosegundo@ucsb.edu)
- Blake Johnson (brjohnson61@gmail.com)
- Quintin Hill (quintinhill1316@gmail.com)
- Fernando Mendoza - (Fmendozarincon@ucsb.edu)
- Omer Cohen (Omerc65@gmail.com)

Team lead: Graham Foster

Problem

Companies across the world have incentive to protect and to ensure the integrity of their data. Breaches in a company's data infrastructure can have serious ramifications. People will not feel comfortable doing business with such a company and they can face legal trouble as well. A company with users that provide their personal information is responsible for protecting this information. Not only that, they must continuously work to update their infrastructure to ensure they are keeping up with security standards. Take the Equifax situation for example, in May of 2017, the credit reporting agency was breached by hackers leaving their client's social security information and other financial data exposed. The company took a whole month to release a patch and then another month to release this information to the public. Leaving the social security information of upwards of 140 million people exposed for over two months. This created real problems for their clients potentially leaving millions vulnerable to identity fraud. Computer security is a critical field in today's society and is an area that is constantly changing with the advancement of technology.

Existing Solutions

The domain of our project is computer security. More specifically, we want to design a platform that can search for an individual's or company's leaked information (i.e. passwords, user data, bank info, social security info...etc.) and notify them without the risk of exposing it. This is one of the greatest challenges in our opinion. Currently there are many sources that you can use to determine if your information has been used without your consent, but they all focus on individual pieces of leaked data, and do not do a good job at securing it. No security system or data infrastructure is 100% secure. Furthermore, finding vulnerabilities and determining if a breach has occured is extremely difficult and can require significant resources. Despite this, there are steps that can be taken to discover a vulnerability before it becomes a major problem or help mitigate the risks of a vulnerability. White hat testing teams can illuminate aspects of a system or service that are not secure by breaking it in a confidential and ethical manner before it is deployed.

Project Outcome

Our vision is to create an aggregation of all current pwnge identification sources, (i.e, have i been pwned) for email, bank account, social media. Furthermore, we plan to implement a system to ensure the integrity of a dataset, where if an unauthorized modification occurred, the administrators would be notified. This platform will help companies and individuals understand their digital footprints and potentially remediate unwanted information leaks. Our platform will perform 4 key security functions: Aggregate, analyze, monitor, and report on data. We envision our MVP as a web application, which could eventually ported over to a mobile application.

Project Milestones & How we Plan to Articulate and Design a Solution

While some group members are currently enrolled in a Computer Security class, as a whole we are fairly novice in our expertise. In order to assure completion of our project, we will develop a calendar for exactly which processes will be focused on and who will take on the first 6 tasks at the top of that stack. We will design our project to first be a basic functioning program, and then build up more and more features and specifications. We plan on designing and articulating our solution by first brainstorming the Minimum Viable Product with our group and mentors on Tuesday, October 16th. MVP will have clear functionalities, and we will use these functionalities and the main purpose of our project to design a clean and interactive UI to help users. In addition to the basic function, we will identify reach goals and more challenging features to pursue once our basic functionality is established.

Technologies

We plan on using multiple different platforms to help us plan and develop our product. While this is not a complete list of everything we will need, there are a couple obvious technologies and platforms we will start with and expand these to others as they arise, and as the need for each new platform becomes apparent. We will start with ClearNet: Pastebin, Google, DuckDuckGo, WhitePages, Namechkr, Shodan, Censys, Pipl, Lexis Nexis, ViewDNS, Facebook, Instagram, Public Records and other databases. However, our search will not be limited to everyday platforms like Facebook and Instagram. We will also search the dark web platforms like Darknet: The Hub, Empire Market, Dream Market Forums, SilkRoad, and Dread. Some tools we plan to use to help us in evaluating these platforms include Maltego, theHarvester, and Recon-NG. We will use github and trello for code hosting and workflow.

Milestones:

- Sprint 1: Vision Statement, MVP modules selected
- Sprint 2: **Skeleton Backend**: Docker Container with Flask up and running, define /search/ endpoint in flask, Deploy backend to AWS. **Define Rest API.**
- Sprint 3: Completed backend, Module 1: HaveIBeenPwned/Pastebin
- Sprint 4: Module 2: HaveIBeenPwned/Pastebin

- Sprint 5: Module 3: Darkweb