**Question 1: what did you do?**

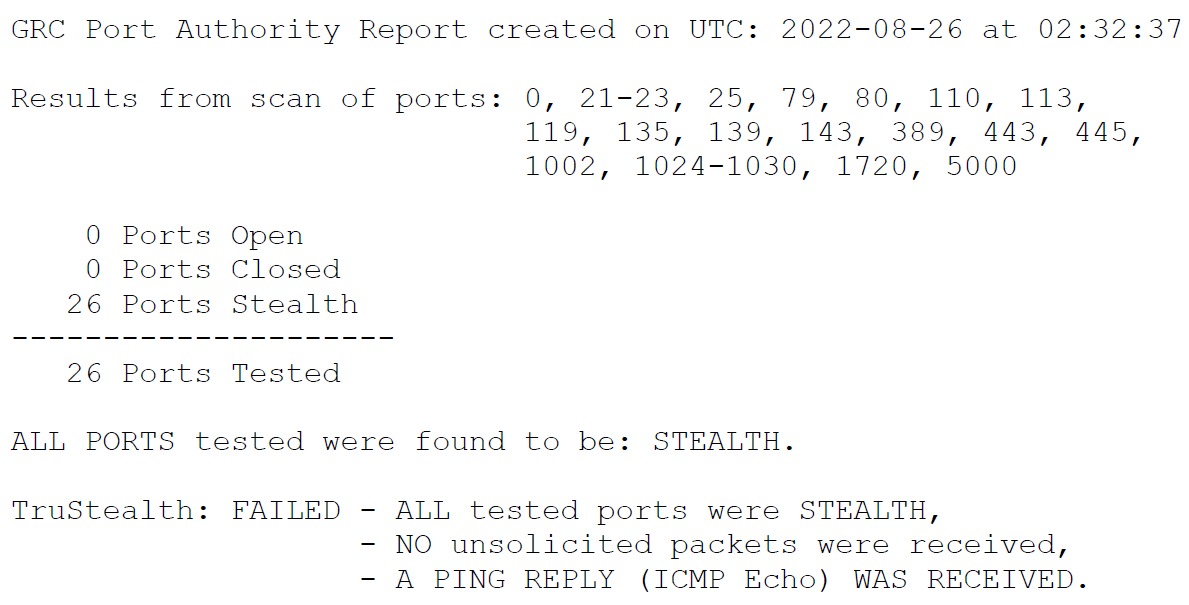
For this assignment, I scanned my personal system for vulnerabilities in a variety of ways along with what parts of my contact information have been exposed in data breaches. The first part using Shields Up is to see how well my system is protected with its existing firewall. The second part of the assignment is to see if things I use on a daily basis such as my email, phone number or password have been compromised.

The number of methods hackers can use to gain entry into your own personal system are much greater than I ever expected. Working from home has been a wonderful blessing since the start of the pandemic but I can see how a company would have high concerns of how they could best protect their IP or system data. Now more than ever, cybersecurity is of front and center importance for both personal and business-related assets.

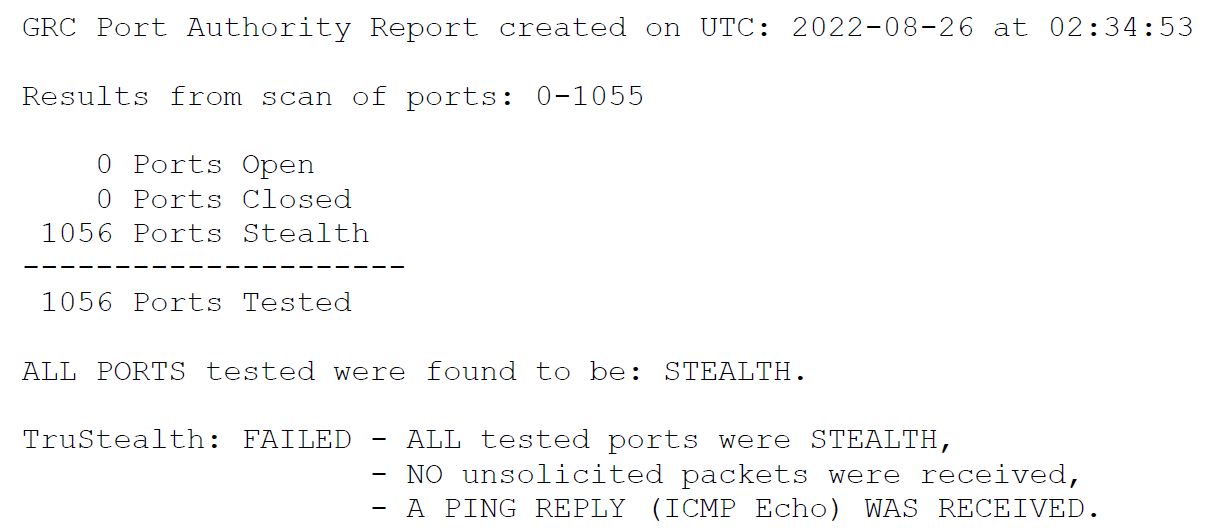
**Question 2: what were the results?**

First of the results were the two GRC Shields Up vulnerability scans done on my personal laptop. These are seen below with Common Ports followed by All Service Ports. In good news, no ports were found open or closed on either scan. All received the Stealth label. This was good to see as a stealth port is one that basically ignores and drop any incoming packets of information without responding to the sender the actual open or closed status of the port. Seeing as all my system ports are stealth, my system should be invisible to the random scans I might encounter over the internet. My system did however fail the TruStealth portion on each scan. This is due to the system replying via a ping which would make it visible. It would be best if I could update my system firewall so it was configured to block, drop or ignore the ping requests so it could better hide from being hacked.

Common Ports

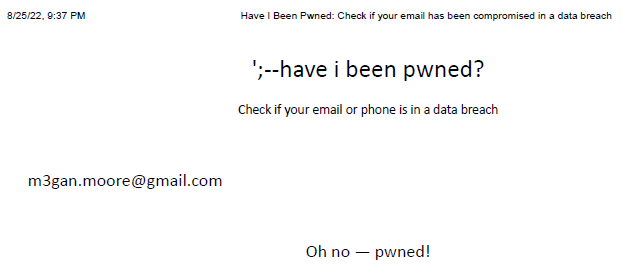


All Service Ports

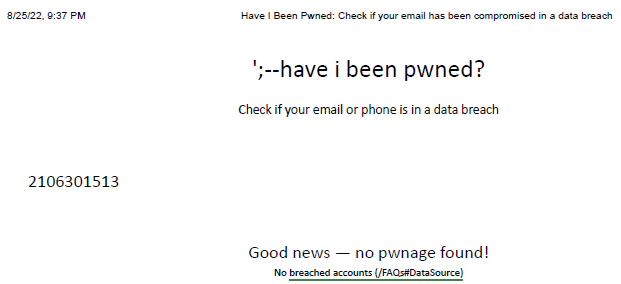


The second portion of the assignment was to go to HaveIBeenPwned to check if certain things such as my email address, my phone number or my typical choice password have been disclosed as part of any pasta data breach. What I found is slightly surprising and somewhat not. I assumed my email would have been disclosed and I wasn’t wrong. I use this email for many things so the higher use would mean higher exposure and chances for being part of a data breach. What did surprise me was my cell phone number has not been part of a breach. I have owned this number for a very long time so I felt this would definitely fail just due to the period of time and how I freely distribute my number for all kinds of things. Last was my password and thankfully it has not been part of a data breach. While I don’t use a password generator, I do tend to try to select complex passwords and then change them after a period of time has passed.

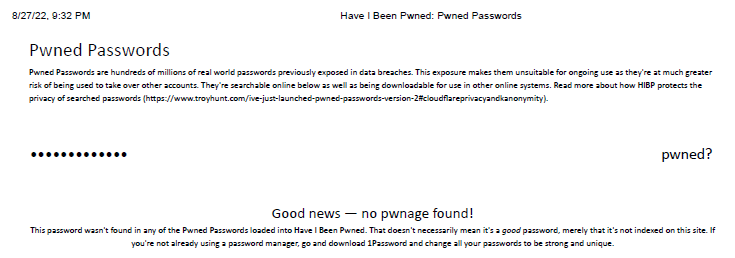
Email Address



Cell Phone Number



Password



**Question 3: what did you learn?**

I personally did not realize these types of websites existed to check my exposure. Now that I know what this does, I will probably routinely cheek in on that far more frequently. I discovered my system successfully has no open ports, thus been better protected than I assumed the scan would show. I would be curious if installing some kind of antivirus software would aid in further protecting my system going forward. I have only ever used what came with my system (Windows firewall) and never any additional program. Regardless of my results from the vulnerability scans, the free version of the scans are not reflective of a full system scan but only a subset. In the future, it could be worthwhile to expand into using the paid version.

As I have become more aware of how much of my own information is distributed online, I have been more cautious in what I do when connected to the internet. In the past, I did not value my information as an asset any hacker would like to steal. I assumed such things were reserved for corporations or public figures. Now these days, I realize the protection of my information is key just from dealing with a credit card being stolen from a Target data breach. Hackers don’t care how big a fish is sometimes. They just want a fish they can use. Full identity theft or information extortion is not something I wish to ever experience.

Second thing I learned is while it may not be necessary to change passwords as often as I do, chances are passwords become exposed over time in data breaches. The best way to improve my chances of remaining protected is a complex password perhaps generated by a password manager. The stronger and more unique a password is, the less likely it will be guessed. I may need to revisit all of my logins and update those to be more complex. I don’t believe I can ever reduce my risk in using my email address as it is needed in so many places. I expect it to always have some level of exposure. Overall, I know my own personal risk can be reduced through education. As I learn more techniques I can adapt or apply for my system, the higher I raise my security against threats. Social engineering use is becoming more widespread and trickier along with phishing attacks sent in email. I know my work email is constantly tested by our IT admins along with various test phishing campaigns. While the goal is to pass these tests when work rolls them out, the real point is to make us familiar to the types of risk being connected to the internet poses and how to best protect yourself.