**Shields Up/Have I Been Pwned**

***By***

**Mehnaz Afrose**

The fastest growing infrastructure of the internet is making our personal and confidential secured information vulnerable to cyberattacks and thus making online protection inevitable for us (Untawale, T. (2021). Some can be unaware of the security issues. It is very possible that a user can be Clueless that his/her cyber platform has already been exposed to some malicious attackers. This report is based on two websites, “ShieldsUP!” and “Have I Been Pwned”, which can help an internet user to identify hoe secure his internet platform and personal identity are.

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

At the very beginning, I looked for the general information of the page “SheildsUp!” to know better about the page, what is the page about, how they do the scanning, what is the main purpose of this web page, is this scanning is safe for my computer to use, how I am going to benefit by scanning my computer ports for security purpose and so on.

I found out that the online port scanning service ShieldsUP!, created by Steve Gibson from Gibson Research Company, is used by the users to identify which ports can be open to any cyber risk (Rogers & Herold, 2010) (Wikipedia). SheildsUp! perform the scanning by probing the network ports of the computer to identify which ports of this computer are open, closed, or stealth through their firewalls or through their NAT routers ( [ShieldsUP! Homepage](https://www.grc.com/shieldsup#:~:text=ShieldsUP!!,your%20computer%20and%20the%20Internet.)) (Ho, 2010). I also reviewed the comments posted on [Microsoft community](https://answers.microsoft.com/en-us/windows/forum/all/is-grc-shieldsup-safe/d133f373-643b-4aeb-bb7f-878dcae133bb) to understand the safety parameter of SheildsUp! Before using it.

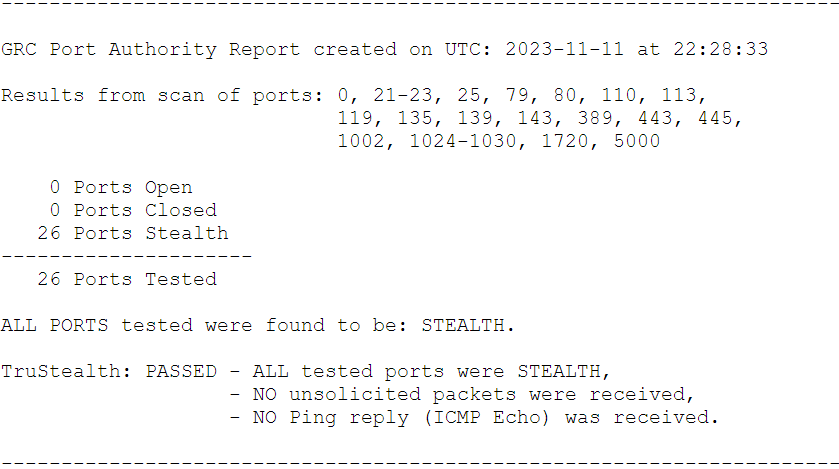
When I got to know all these aspects of this web page, I became interested in safety checking of my computer and network infrastructure. I scanned the common and troublesome ports of my network system. ShieldsUP! Scanned 26 post usable ports for the “TruStealth Analysis”. When it was running its analysis scan, I thought it would take a long time to scan all the ports. Surprisingly, it took only 6 seconds. After scanning the common ports, I scanned all the ports of my computer network system. It scanned 1056 ports of the system. It took a little bit more time, about 45 seconds, than the previous scanning, as the number of ports is a lot higher than the previous one. To check how accurate the results are, I have redone the scanning, first the common ports, and then for all the ports.

As a second step of the security check, I used “Have I Been Pwned” website.” This website was created by Tory Hunt on December 2013. It is used to identify whether any user’s personal identification data, such email addresses, passwords, have been compromised in any data breach incident ([Wikipedia](https://en.wikipedia.org/wiki/Have_I_Been_Pwned%3F)). This webpage gives two results. Whether the personal data is pwned or not. In the analysis, I entered three personal email addresses of mine, including my WT email. Then I entered two passwords, one is quite simple and easy to guess, and another is overly complex, to check which one is pwned and which one is not.

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

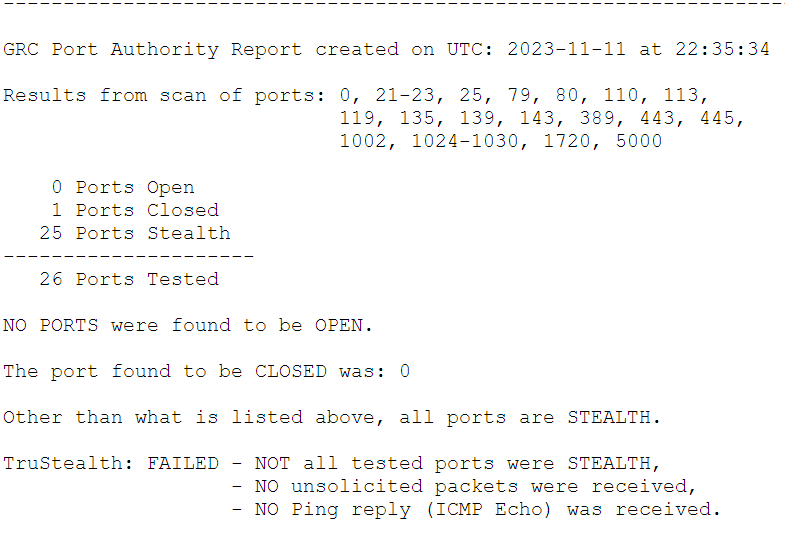
There are three categorical statuses about the scanned ports: closed, open, and stealth ports. [Closed](https://www.grc.com/su/portstatusinfo.htm#:~:text=Internet%20Port%20Status%20Definitions&text=A%20%22Stealth%22%20port%20is%20one,or%20%22Closed%22%20for%20business.) ports do not receive connections. If there are any attempts of incoming connection, the closed port rejects the attempt with a rejection message. An [open](https://www.grc.com/su/portstatusinfo.htm#:~:text=Internet%20Port%20Status%20Definitions&text=A%20%22Stealth%22%20port%20is%20one,or%20%22Closed%22%20for%20business.) port is a port which is actively running and waiting for connection. Users can open a port for necessary functions, but it can cause serious vulnerability risk if it is not carefully managed and secure. A [stealth](https://www.grc.com/su/portstatusinfo.htm#:~:text=Internet%20Port%20Status%20Definitions&text=A%20%22Stealth%22%20port%20is%20one,or%20%22Closed%22%20for%20business.) port is the port which neither acknowledges nor rejects any incoming attempts of connections without giving any indication of whether the port is open or closed.

To pass the “TruStealth Analysis” all the ports need to be in stealth mode. If a single port shows the status of being in the closed/open mode, the system test result will fail. In my first attempt to scan the most common and troublesome 26 ports, my network system passed. That means, all 26 ports were in stealth mode.



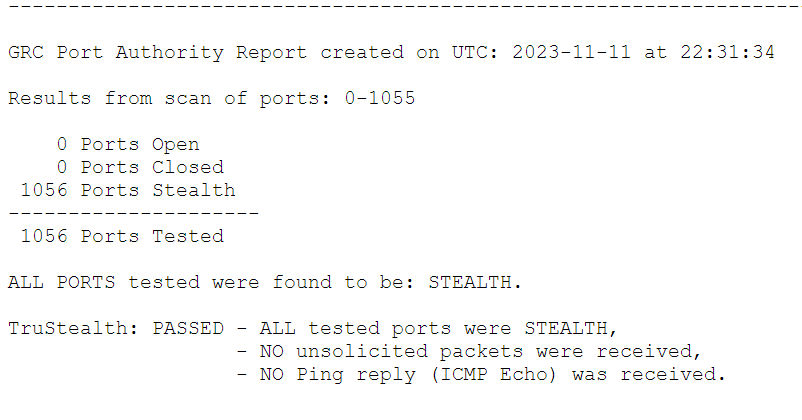
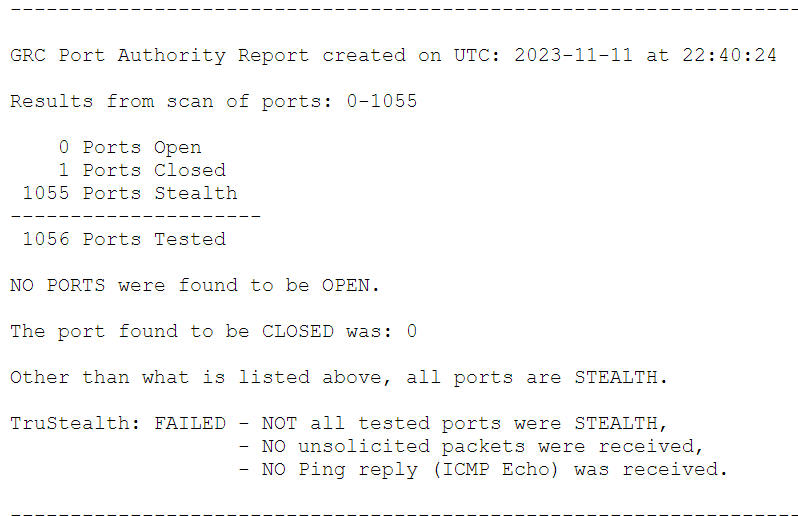
*Figure 1: Result of Common 26 ports on first attempt*

This result was satisfactory. But my skeptical mind could not accept the results this easily. So, I scanned for the second time to see if my system is this secure and does not need further protection to secure my network. On the second attempt, my system failed to pass. One port showed closed mode and it was “Port Zero.” The solicited TCP packets were received by this port. The purpose indicated that it was not a valid port number. As “Port Zero” does not officially exist, it can consider minimal risk of vulnerability of the computer network system.

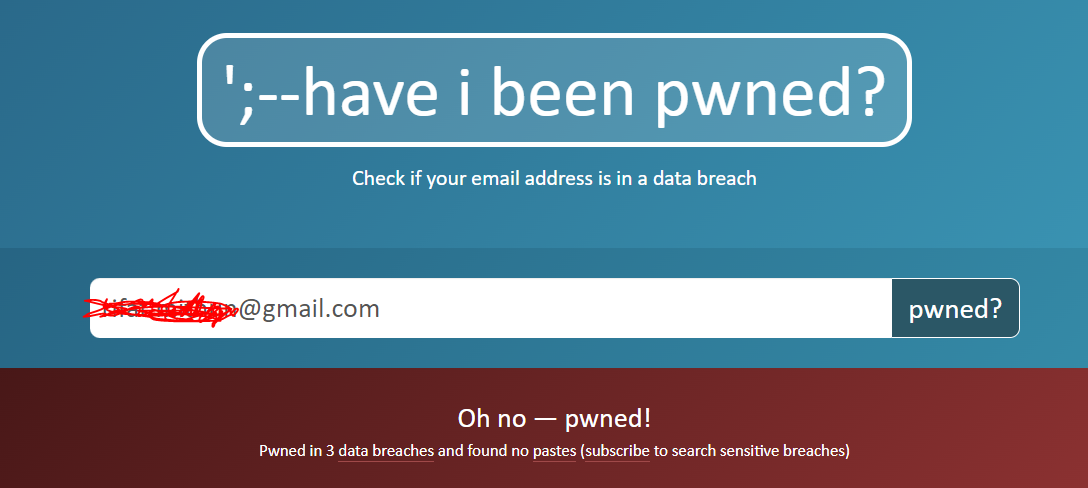


*Figure 2: Result of Common 26 ports on second attempt*

As like as the scanning process for the 26 common ports, the scanning of the first 1056 ports also passed the “TruStealth Analysis” test. All the ports were showing stealth mode. In the second trial, the “Port Zero” received the solicited TCP packets and it was in closed mode.

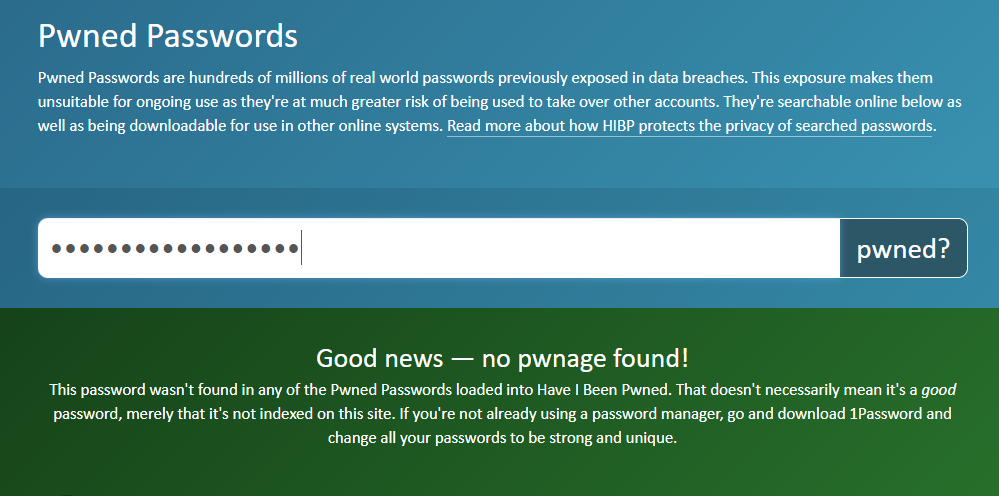
 *Figure 3: Result of the first 1056 ports on first attempt Figure 4: Result of the first 1056 ports on second attempt*

For the second part of the security check, which is using the website “Have I Been Pwned,” I entered two of my personal email addresses and my official WT email address. WT email address and one of my personal email addresses, which I have been using since 2010, has not been pwned. But another email address which I have been using since 2007, has been pawned, it’s been pwned in three data breaches. By going through the details, I found that for those data breach incidents, my personal information, such as name, password, username, social media profiles, bios, Google and Facebook IDs, and device information have been compromised.



*Figure 5: email address been pwned*

In case of checking how secure my passwords are, at first, I entered a quite simple common password, which I usually use for less important log information. This password does not have any upper case, or lower case, or any other special characters in it. Turned out to be pwned. On the other hand, I entered another password, which is overly complex, has special characters in it, has upper case and lower-case letter combination, and has a combination of numbers with letters. Turned out not to be pwned.



*Figure 6: Complex password has not pwned*

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

Before using this website “ShieldsUP!,” I did not know much about the open, closed, and stealth mode of the network system I use on a regular basis. Although the results indicate that the network system is secure enough, it can be vulnerable if I forget to change the mode of any stealth port which I intentionally open for any legitimate purpose.

In using “Have I Been Pwned” website, I realized securing only personal network and computer is not enough from cyber threats. Even external platforms can be a cause for personal data leakage by logging in external pages. It was very shocking for me when I found out that there have been severe data breach incidents happened in three renowned websites, and for those incidents my personal sensitive information has been compromised.

We can secure our personal information and cyber networks by taking various measures. But, these two websites, “ShieldsUP!” and “Have I Been Pwned” can provide the specific areas which are more prone to cyber-attacks.

Cyber security threats are evolving daily, and our online platforms are getting vulnerable (Jang-Jaccard & Nepal, 2014). What seems secure now, it is a matter of time, this secured platform can become accessible to cyber attackers who have advanced technology (Wang & Lu, 2013). So, to cope with time, we need to upgrade and check the security systems on a regular basis.

References:

1. Untawale, T. (2021). Importance of cyber security in digital era. International Journal for Research in Applied Science and Engineering Technology, 9(8), 963-966.
2. Rogers, M. K., & Herold, R. (Eds.). (2010). Encyclopedia of Information Assurance - 4 Volume Set (Print). (2010). United Kingdom: CRC Press.
3. [Wikipedia page](https://en.wikipedia.org/wiki/ShieldsUP)
4. [ShieldsUP! Homepage](https://www.grc.com/shieldsup#:~:text=ShieldsUP!!,your%20computer%20and%20the%20Internet.)
5. [Internet Port Status Definitions.](https://www.grc.com/su/portstatusinfo.htm#:~:text=Internet%20Port%20Status%20Definitions&text=A%20%22Stealth%22%20port%20is%20one,or%20%22Closed%22%20for%20business.)
6. Ho, Erica. (2010, April 7). ShieldsUP Tests Your Firewall for Vulnerabilities. Lifehacker. Retrieved April 7, 2010, from <https://lifehacker.com/shieldsup-tests-your-firewall-for-vulnerabilities-5511734>
7. [Microsoft community](https://answers.microsoft.com/en-us/windows/forum/all/is-grc-shieldsup-safe/d133f373-643b-4aeb-bb7f-878dcae133bb)
8. [Wikipedia](https://en.wikipedia.org/wiki/Have_I_Been_Pwned%3F)
9. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993. <https://doi.org/10.1016/j.jcss.2014.02.005>
10. Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57(5), 1344-1371. https://doi.org/10.1016/j.comnet.2012.12.017 (<https://www.sciencedirect.com/science/article/pii/S1389128613000042>