**Name:** Amarachi Anthony

**Buff Id:** 1130441

**Course:** CIDM 6341(Cybersecurity)

**Assignment:** Shields Up/Have I Been Pwned

**Shields Up**

**What did I do?**

I researched SheildsUp and found that it's an online service for Internet security testing. It helps users evaluate the security of their systems by identifying open ports and vulnerabilities. The platform offers tests to identify weaknesses in firewall protection, UPnP devices, and open ports that could be exploited by hackers. It also assesses the effectiveness of firewalls and other security measures.  
I then ran a vulnerability scan on my computer using the Shield Up website to check if it had been compromised. The scan covered both common ports and all service ports. It involved sending pings to the ports on the computer, and the router responded to the scans.

**What were the results?**

In the scan results, it successfully passed the stealth test with 0 open ports, 0 closed ports, and 26 stealth ports for the common ports. This indicates that all the scanned ports were in stealth mode, meaning that they were not responding to probes. Additionally, there were no unsolicited packets received, and no ping replies were detected.

And for the All-ports scan, all ports tested were also found to be stealth with 0 ports open, 0 ports closed and 1056 stealth.

**Below is the screen shot of the results**

**Common Port**

**A screenshot of a computer

Description automatically generated**

Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,

119, 135, 139, 143, 389, 443, 445,

1002, 1024-1030, 1720, 5000

0 Ports Open

0 Ports Closed

26 Ports Stealth

---------------------

26 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: PASSED - ALL tested ports were STEALTH,

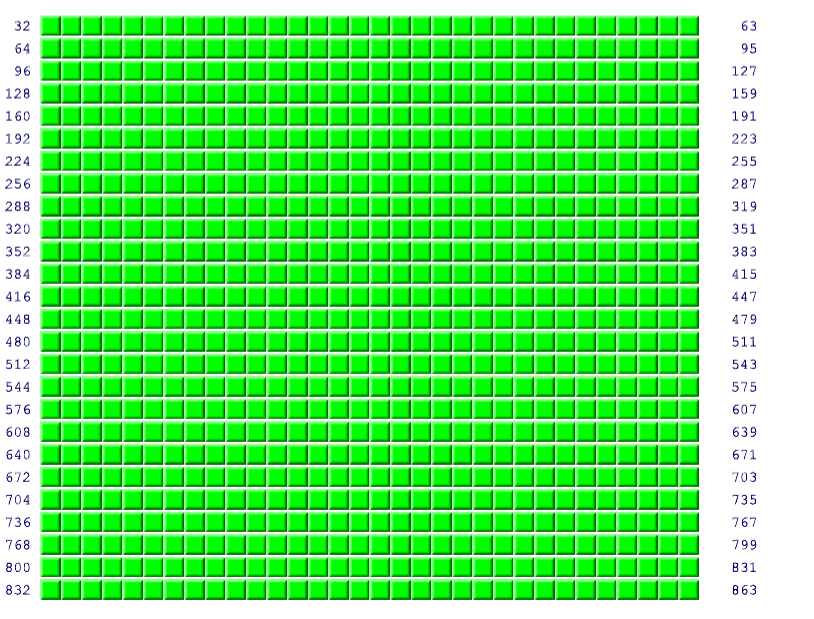
- NO unsolicited packets were received,

- NO Ping reply (ICMP Echo) was received.

**All Ports**

**A green squares with purple text

Description automatically generated**

****

**A screenshot of a computer

Description automatically generated**

Results from scan of ports: 0-1055

0 Ports Open

0 Ports Closed

1056 Ports Stealth

---------------------

1056 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: PASSED - ALL tested ports were STEALTH,

- NO unsolicited packets were received,

- NO Ping reply (ICMP Echo) was received.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**What did I learn?**

I learned that my computer has been found to be highly secure against external probing attempts. All tested ports are in stealth mode, meaning my system is entirely invisible to potential hackers or malicious entities scanning the internet for vulnerabilities. This stealth status effectively makes the system "non-existent" to potential attackers, significantly reducing the risk of unauthorized access. Additionally, the system does not respond to unsolicited packets or pings, confirming its strong security posture.

I also learned that the Internet Common Ports Probe tests standard TCP connections by trying to connect with well-known, vulnerable, and problematic ports. It displays which ports are open and visible to passing Internet port scanners. A port can be open, closed, or stealth, indicating whether it's actively listening for incoming connections or traffic.

An "open" port is ready to receive incoming connections, a "closed" port is not accepting incoming traffic, and a "stealth" port does not respond to incoming requests and does not disclose any information about the device's state or associated application.

**Have I been Pwned?**

**What did you do?**

I researched the website “Have I Been Pwned” to learn more about its purpose and functionality. This site is designed to verify whether a user's personal details, like email addresses and passwords, have been compromised in data breaches.

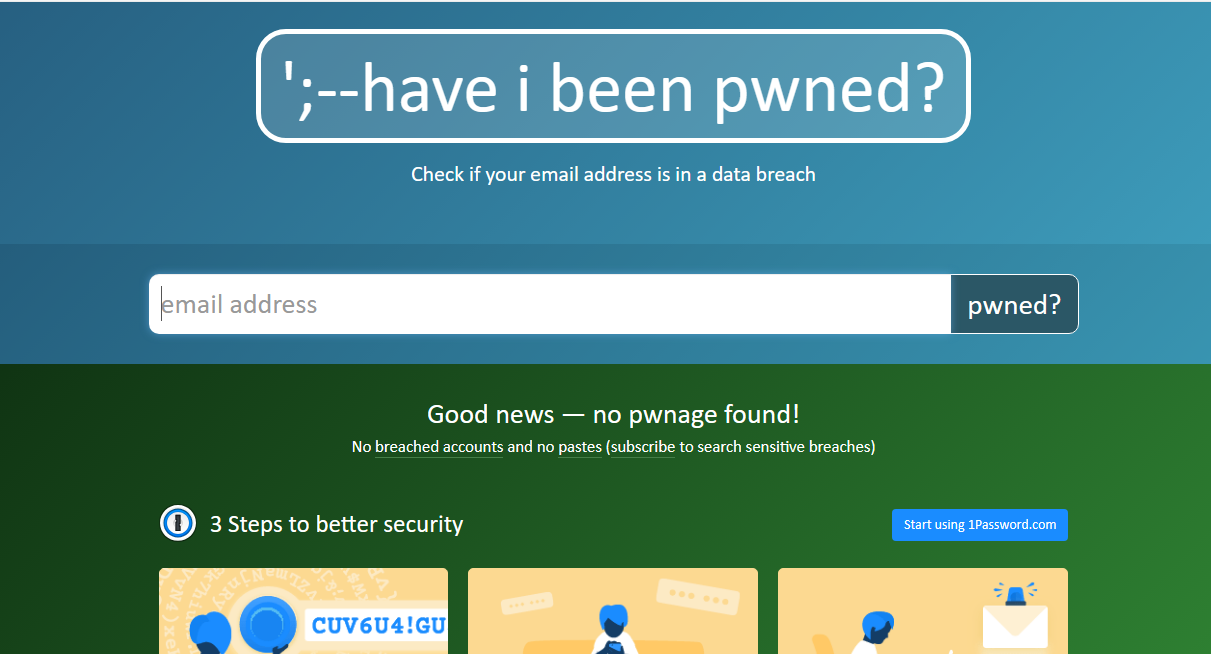
I then used the website to conduct security checks to determine if my email address, phone number and password had been compromised. I entered my email address, phone number and password differently in the search bar to check if any has been compromised or if they appear in any data breaches.

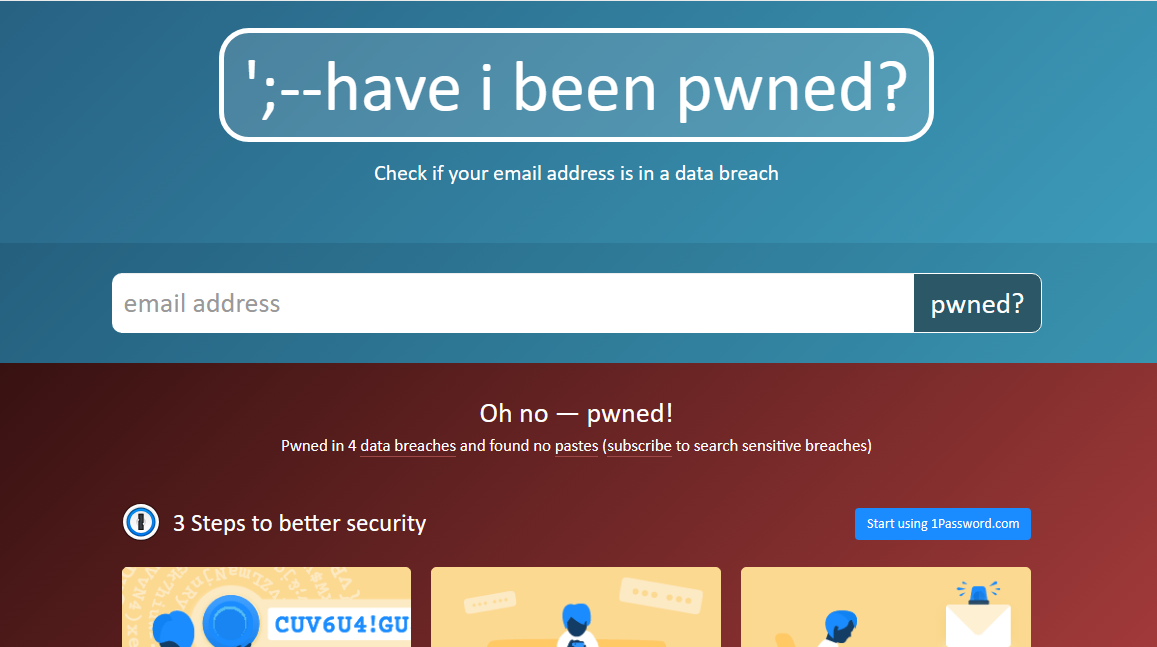
**What were the results?**

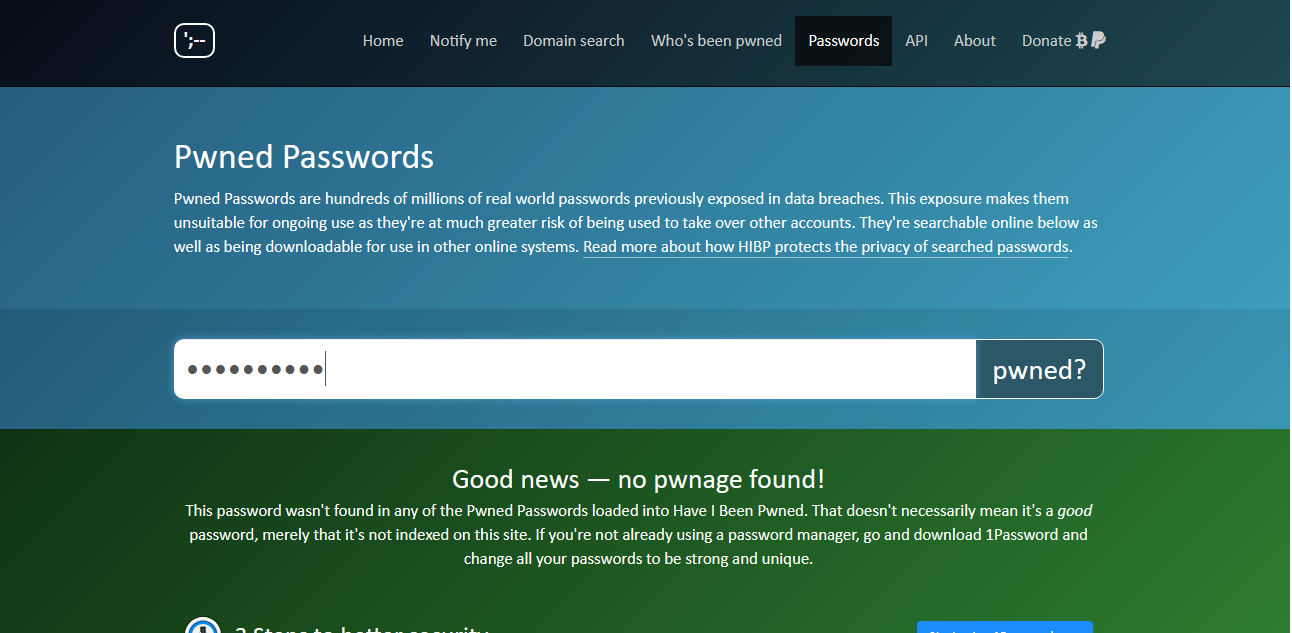
The search indicated that the email address had not been compromised. The website returned a message stating, "Good news — no pwnage found!" indicating that this email address was not involved in any known data breaches.

For the Second Email Address: The search showed that the email address had been compromised. The website displayed a message stating "Oh no — pwned!" and indicated that the email was involved in four data breaches.

And for the password I tested, there were no breaches found.







**What did I learn?**

This exercise has shown me how important it is to regularly check email addresses for data breaches as part of good cybersecurity practices. By doing so, I can proactively manage my online security. The tool "Have I Been Pwned?" is effective in identifying whether email accounts have been involved in data breaches. It allows users to take immediate action, such as changing passwords or enhancing security measures, to protect their personal information. I also realized that, even if some email addresses are not currently compromised, it's crucial to remain vigilant and use strong, unique passwords across different platforms to reduce potential risks.