Fougnigue Sefon

Cybersecurity CIDM

Fall 2023

ShieldsUp/HaveIBeenPwnd Report

As Sun Tzu famously advocated, understanding your adversary is only part of the equation; you should also know your own strengths and weaknesses to maximize your chances of success. This principle also holds true in the field of cybersecurity, where the principles of Confidentiality, Integrity, and Availability (CIA) play an important role in protecting data and systems from cyber threats.

In the context of this report, I seek to identify and understand my own weaknesses and security vulnerabilities, a critical step in the pursuit of mitigating cybersecurity risks.

The objective is to use two services, namely "ShieldsUp" and "HaveIBeenPwned," to conduct a vulnerability assessment on my computer system and personal data. By doing so, I intend to enhance the confidentiality, integrity, and availability of my digital assets, thereby strengthening my overall cybersecurity posture.

**1/ What did you do?**

To start this investigation, my initial task was to utilize ShieldsUp, a service provided by the Gibson Research Corporation on their website (Grc.com). ShieldsUp offers users the ability to conduct a vulnerability scan on their computer and network infrastructure. This process involved ShieldsUp profiling my IP address and subsequently sending pings to my laptop. By sending pings, it sends connection requests to various ports of my computer to determine their operational status. These statuses could be categorized into three distinct states: Open, Closed, and Stealth. An open port meant that the port was actively accepting requests, potentially leaving it susceptible to exploitation by malicious third parties. A closed port signified that the port was not accepting requests but was still responsive, making it possible for a third party to detect my presence on the network. The stealth status, considered the most secure, indicated that the port did not respond to requests, making it challenging for hackers to identify my computer's presence. With an understanding of these different status categories, I proceeded to execute two types of scans. The initial scan focused solely on the 26 most common and high-risk internet ports to determine their status. Remarkably, ShieldsUp completed this scan in only five seconds. In contrast, the second scan tested my system's first 1056 ports and was done in 60 seconds. The longer duration of the latter scan was easily attributable to the higher number of ports being assessed.

My second task involved using the HaveIBeenPwned website to assess whether my personally identifiable information had appeared in data breaches. This website maintains a comprehensive database containing records of various data breaches that have happened over the years. When entering personal data, the website is able to search its database to determine if the provided information has been compromised. Two possible outcomes can be obtained from this search. If no instances of data compromise are detected, the user receives the reassuring message, "Good news — no pwnage found!”. Conversely, if the user's data is discovered within the HaveIBeenPwned database, a less comforting message appears, "Oh no — pwned!". That message also includes the number of times the compromised data has surfaced in breaches. In such circumstances, immediate action can be necessary to strengthen one's account security. In my personal evaluation, I focused on verifying the security of my emails and passwords, as some of my emails contain highly sensitive and personal information. To this end, I examined four of my email addresses and cross-referenced them with four of my most frequently used passwords.

**2/ What were the results?**

When conducting a ShieldsUp scan, it is essential to note that the scan follows a strict TrueStealth analysis, where success depends on all ports being in stealth mode, offering no discernible response to external requests. In the initial scan targeting the 26 most common and troublesome internet ports, 24 ports were confirmed to be in stealth mode, indicating good security. However, there was concern after finding 2 open ports. Open ports can serve as potential entry points for unauthorized access and control. The two open ports identified were 80 and 443. Port 80 is associated with the Hypertext Transfer Protocol (HTTP), potentially implying a web server running on my laptop. Port 443, the Hypertext Transfer Protocol Secure (HTTPS) port, was also open. Compared to HTTP, it adds an additional layer of secure communication. ShieldsUp highlighted that this setup is typically employed for transmitting sensitive data like credit card information, which is pertinent in my case given that my credit cards information is stored on my computer. Io never really envisioned the danger of storing that data on my machine since anyone would need my fingerprints to physically access my computer. While the physical security of my credit card information is reassuring, potential network-level vulnerabilities remain concerning. It may be prudent to avoid storing sensitive credit card data on my computer to mitigate potential security risks. The second scan, consisting of the first 1056 ports, confirmed the previous findings. Among these ports, 1053 were in stealth mode, while 3 remained open. As expected, the three open ports were the same as those identified in the initial scan—Ports 80, 443, and an additional discovery, Port 53, associated with the Domain Name System (DNS). The presence of an open DNS port poses risks, as it could potentially grant hackers unauthorized access, leading to potentially severe consequences. A good practice would be to configure both the firewall and router to close these open ports, allowing access only to authorized requests.

In contrast, the evaluation using HaveIBeenPwned brought reassuring news. After checking both my email addresses and passwords, none of them were found in the HaveIBeenPwned database of data breaches. Each query yielded the reassuring message, "Good news — no pwnage found!". This outcome is particularly satisfying, given that my emails contain valuable information. The absence of compromised data reduces concerns, as there would have been a need to consider changing personal information if any data breaches had been detected. It is worth noting that the separation of email addresses and passwords in data breaches provides a layer of security, as linking them would have posed more significant risks.

**3/** **What did you learn?**

Through this investigation, I have gained several key lessons and insights.

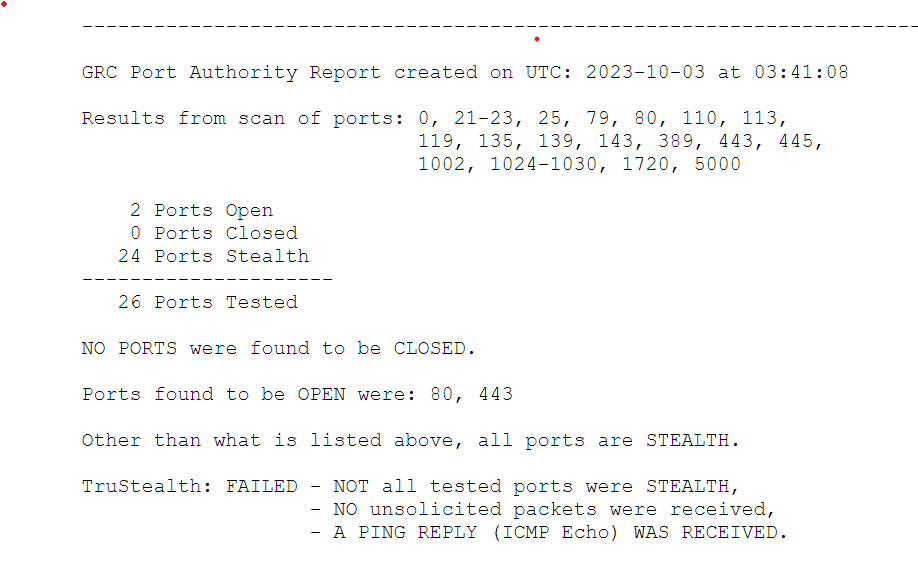
I learned that open ports on my computer can pose a significant security risk. Even though my credit card information is physically secure on my machine, the presence of open ports like 80, 443, and 53 can potentially allow unauthorized access to my system. To enhance network security, it's essential to configure both the firewall and router to close these open ports, allowing access only to authorized requests. This experience highlighted the importance of not only physical data security but also network-level security. The identification of an open DNS port (Port 53) was an eye-opener. A compromised DNS can have severe consequences, as it can be exploited for various malicious purposes, including domain hijacking and traffic redirection.

Using HaveIBeenPwned to check the security of my email addresses and passwords provided peace of mind. None of my personal data was found in data breaches, which is reassuring. However, this experience emphasized the importance of regularly checking for data breaches and practicing good password protocol to maintain personal security.

This exercise underscored the need for constant vigilance and awareness of cybersecurity threats. Hackers are continually evolving their tactics, and maintaining due care and due diligence in safeguarding personal and digital assets is crucial. While achieving absolute security is challenging, striving for an appropriate level of security is essential. This includes regularly assessing vulnerabilities, closing unnecessary open ports, and monitoring for potential threats. It is vital to recognize that cybersecurity is an ongoing process that requires continuous effort and adaptation.

**Appendix A: Scan Results**

**Figure A1. ShieldsUp Initial Scan Results**



*Screen capture showing the results of the initial ShieldsUp scan targeting the 26 most common internet ports.*

**Figure A2. ShieldsUp Extended Scan Results**

**A computer error message

Description automatically generated**

*Screen capture displaying the results of the extended ShieldsUp scan covering the first 1056 ports, including open ports 80, 443, and 53.*