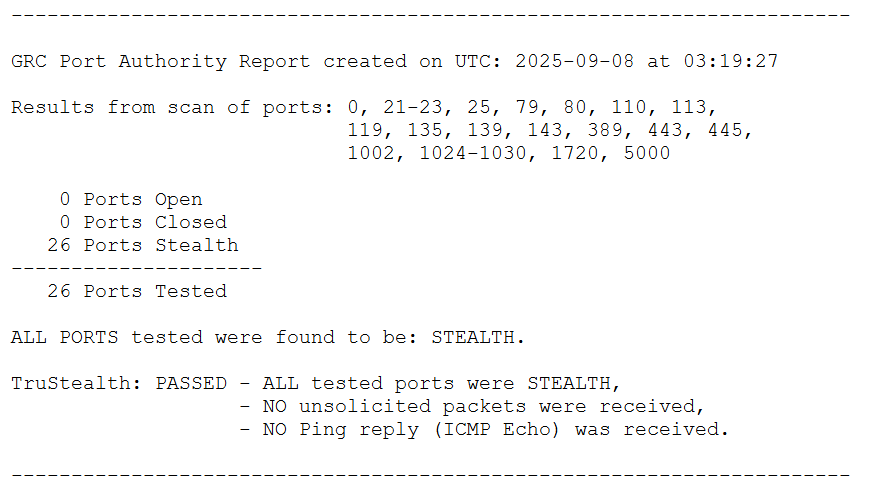
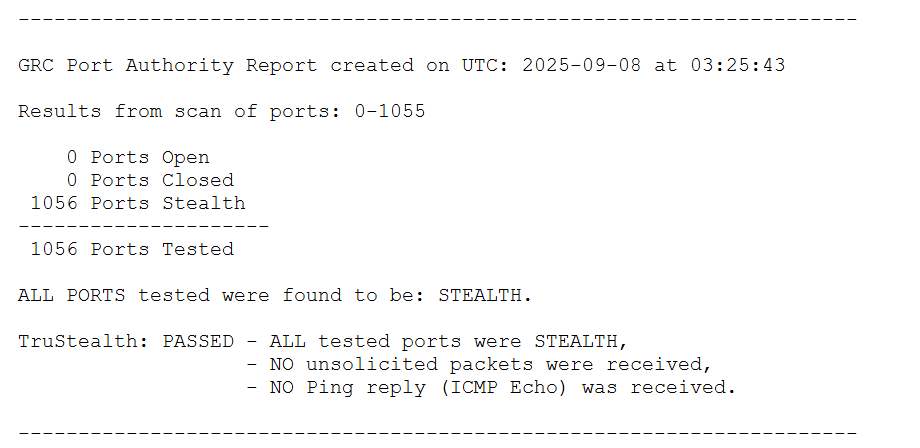
ShieldsUp/HaveIBeenPwned Assignment

Jim Kinter

CIDM6340

1. What did you do – I started with the requested vulnerability investigation/assessment of my PC by running the Common Ports scan using ShieldsUp. In the spring of 2024 I took CIDM 6310 and we did a similar exercise to this using ShieldsUp. At the time the software found a litany of security vulnerabilities. Following that exercise, I really took the matter seriously and undertook a process of remediating the vulnerabilities and patching all of the devices on the network, including this PC. That exercise seems to have resulted in a better security posture for myself and my family. The experience of running the scans was straight forward and resulted in a clean bill of health. Next I used my personal email in the HaveIBeenPwned website. The result was that my email address was found in 29 breaches. I then retried the scan using my WT Email address and the result there was zero breaches found. I also tried using my password for my personal email address and found zero records with that password.
2. What are the results – As you can see below, both of the ShieldsUp scans yielded a healthy report with no public exposures. The HaveIBeenPwned scan found 29 breaches for my personal email address and zero records when I searched using the password associated with that email address.





A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

1. What did you learn – My biggest learning from this exercise is that the time and effort spent last year to minimize the attack surface of the network and implement practices to ensure that all devices on the network are running patched OS and the most up to date firmware has been time well spent. Taking a defense in depth approach, regularly assessing network devices, monitoring changes in network behaviors or hosts, using tools like NMAP, ShieldsUp, Wireshark, and Nessus , and reviewing event logs are great steps to protect my family; however, I also can’t use this finding to get complacent or convince myself that the things that you’ve taught me are enough. Risk mitigation is a never-ending process of inspection, adaptation, and investment. As part of that remediation plan in 2024 I subscribed to Norton’s LifeLock Service for myself and my family and, as a result of that I get alerts when my email address (or those of my family) are found in a breach. This has been a relatively common occurrence. As my traditional response to these notifications I routinely investigate the breach, the scope of the exposure, and make a risk assessment and plan of action for how to respond. This usually entails cycling my passwords, implementing multi-factor authentication when possible, or most recently, implementing passkeys for sites and services that are affected. I have also purchased a family subscription to a password manager and taught everyone to use it to manage their passwords, rotate passwords frequently, and never reuse passwords.