**What Did You Do?**

I ran a Shields Up scan on the common ports and all service ports of my system. I did this quite easily as it was only a few buttons to click- you go to the website, click on “proceed”, and then simply choose which scan you want to run. Shields Up runs this scan by examining your ports to look for potential vulnerabilities that hackers can manipulate. It also tests any firewalls for effectiveness and tests your system on how well it handles connection attempts. For the Nessus vulnerability scan, I chose to utilize my husband’s company, Legacy Land Co., as it is a smaller business that operates on the devices within our home, I thought it would be beneficial to see if there are any concerns towards its security. I downloaded the software, entered in the activation code it emailed to me, and then needed to wait for the Nessus Plugins to download. Once that was complete, I created a folder for this project, and selected “Create a New Scan”. From here, I did a Basic Network Scan and entered the IP address to the target when prompted. This produced results from the scan, and I was able to read about any risks and information the network had. Nessus uses plugins to analyze the network for vulnerabilities; you can choose to scan all ports or a selected range of ports. The basic network scan I performed worked by identifying a live host, running the plugins, and identifying any services running on the ports. It then gives a very detailed report with information and risks associated to your network, along with solutions to fix any concerns. Analyzing the output from Shields Up was straight forward, it gives a screen that lists each port and its status. It also provides a summary of how the system handled packets and ping responses (signals from one computer to another, often used to test availability). For Nessus, analyzing the output was a little more complicated as there was so much information to take in. It gave a prioritized list of all the risks and their levels of severity along with a group of informational findings that give detailed context about the network/system. From here, you can read through each one and understand what information is being passed on.

**What Are the Results?**

After running the scan to check my common ports, my system reported a perfect “TruStealth” rating. Not one packet was received and the system ignored Pings. The analysis states, “from the standpoint of the passing probes of any hacker, this machine does not exist on the Internet”. It also stated my system remained silent in every way. This details that I have a strong level of protection, and this is beneficial as it lowers my chances of attacks. I have gathered that this means my system is ‘inactive’ on the network and that is it also avoiding issues of counter-probing. With all 26 ports being classified as “Stealth”, it applies pressure to attacks and makes it more difficult to determine what and if there are programs/services running. Overall, this service gave the results that my system is nicely protected and has a low chance of being involved in a targeted hack.

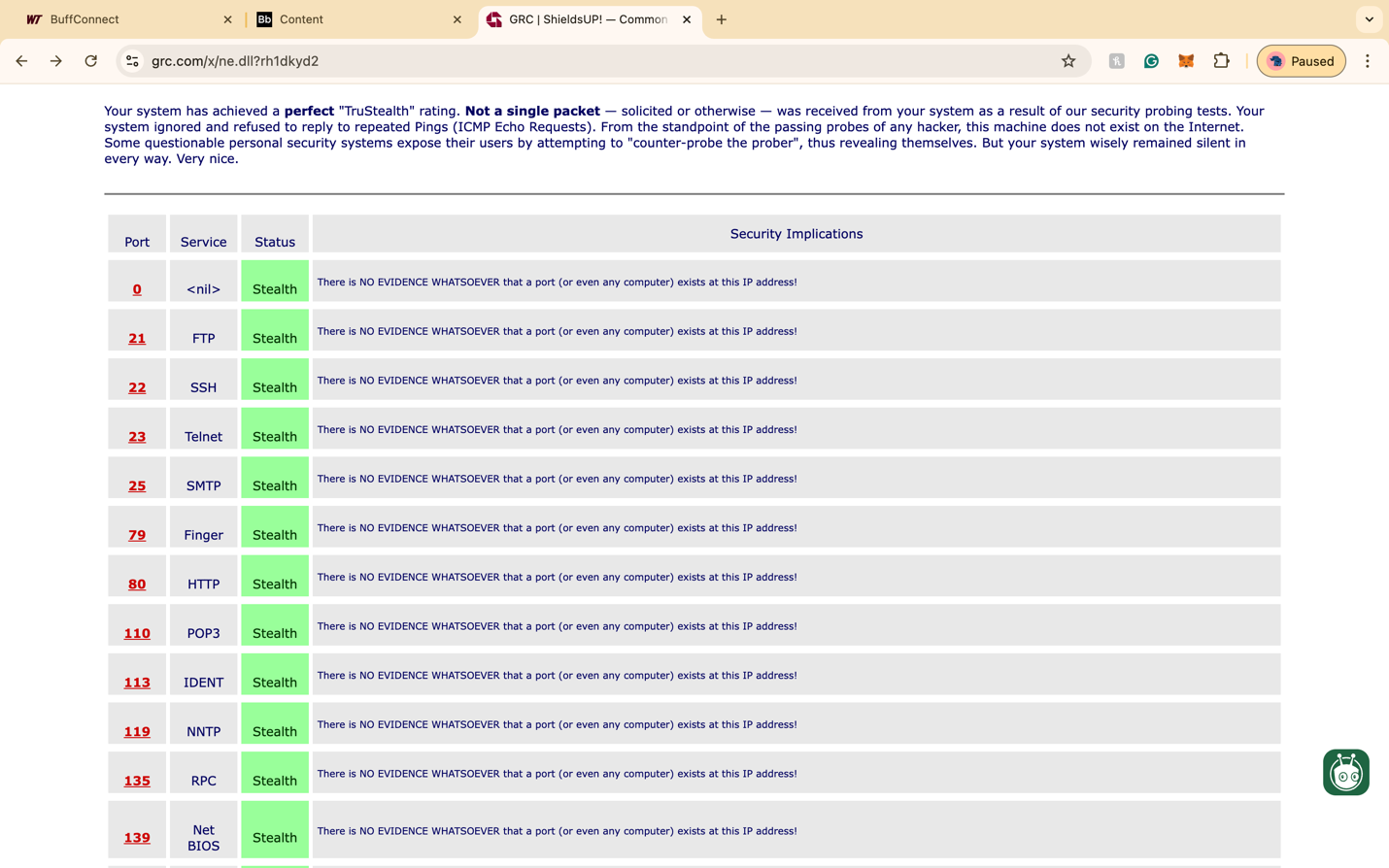
For the results I gathered on Nessus, 95% of the report was information, 3% posed a medium risk, and 2% high risk. The high risk was alerting to the fact that the system was not updated to the latest version (14.5 rather than 14.6). The medium risks were: 1, Ruby was running on an outdated version, and 2, untrusted SSL certificates. All these risks are quite severe, which surprised me. I never thought failing to update to the newest version right away was that big of a deal, however it exposes you to an unlimited number of risks. Looking at what this new version provides, it actually consists largely of security updates. For example, AppleMobileFileIntegrity has available updates due to an app that may be able to bypass Privacy settings. Likewise- Accounts, AppleVA, CoreGraphics, CoreMedia... (the list is tremendous) all state the previous version paves a way for attackers to bypass settings/ privileges or place malicious applications on your device. This reinforces how important it is to mitigate this concern by performing an update. Next up, we had Ruby running on an outdated version as well; this poses a threat as Ruby is a language the system uses and without updating it, you run the same risks as that of the system update. You would want to install the new version of Ruby to mitigate not only the security risks, but also compatibility and support issues. Lastly, the risk with untrusted SSL certificates is highest in my opinion, due to its quicker access it gives attackers. Man-in-the-Middle attacks and phishing often use this method to intercept the user and exploit your system. A way to avoid this and fix this concern would be to pay more attention to your browser (what is popping up on the screen, etc.), use HTTPS rather than HTTP (as we learned from the Wireshark exercise), and effectively manage trusted certificates.

**What Did You Learn?**

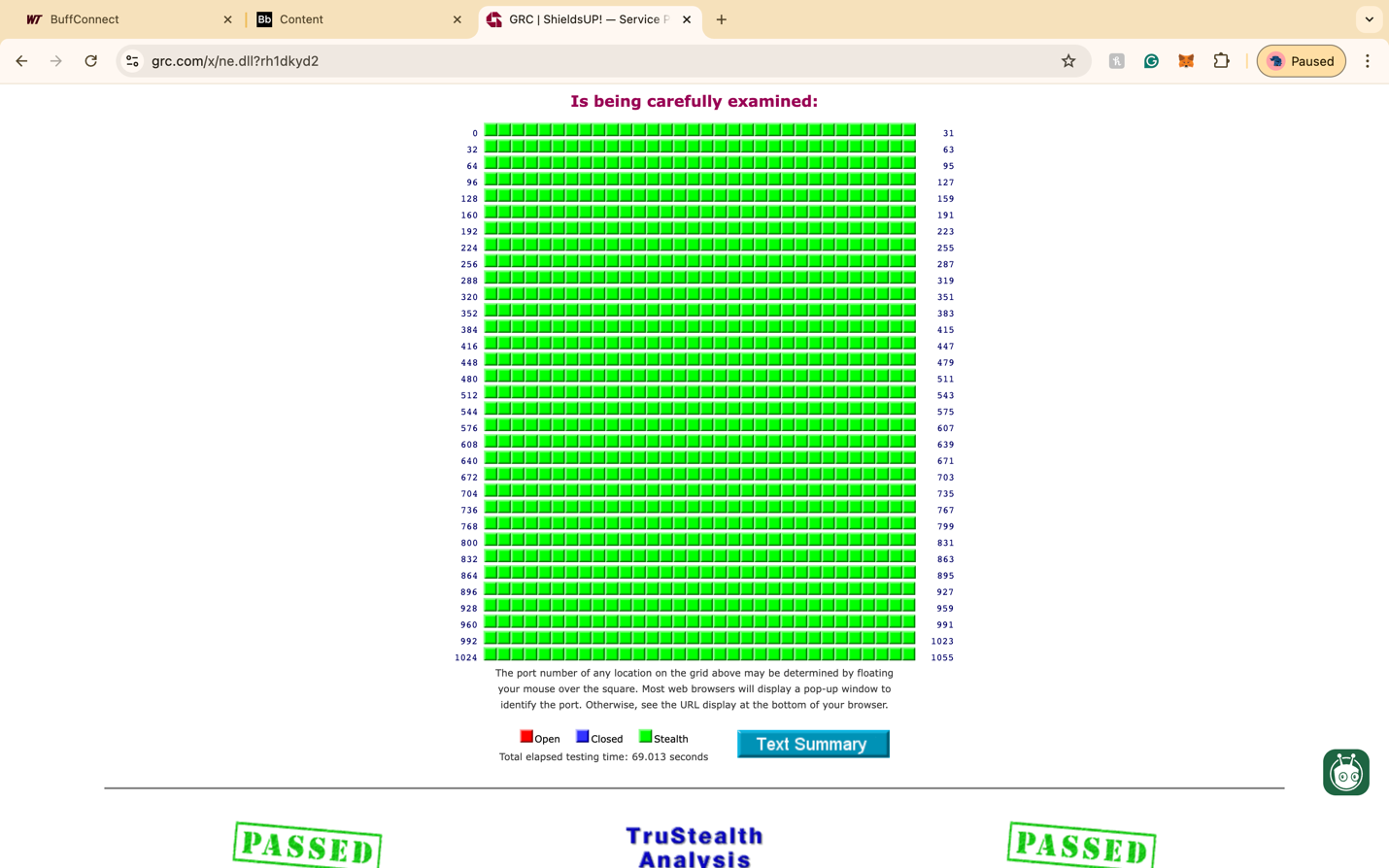
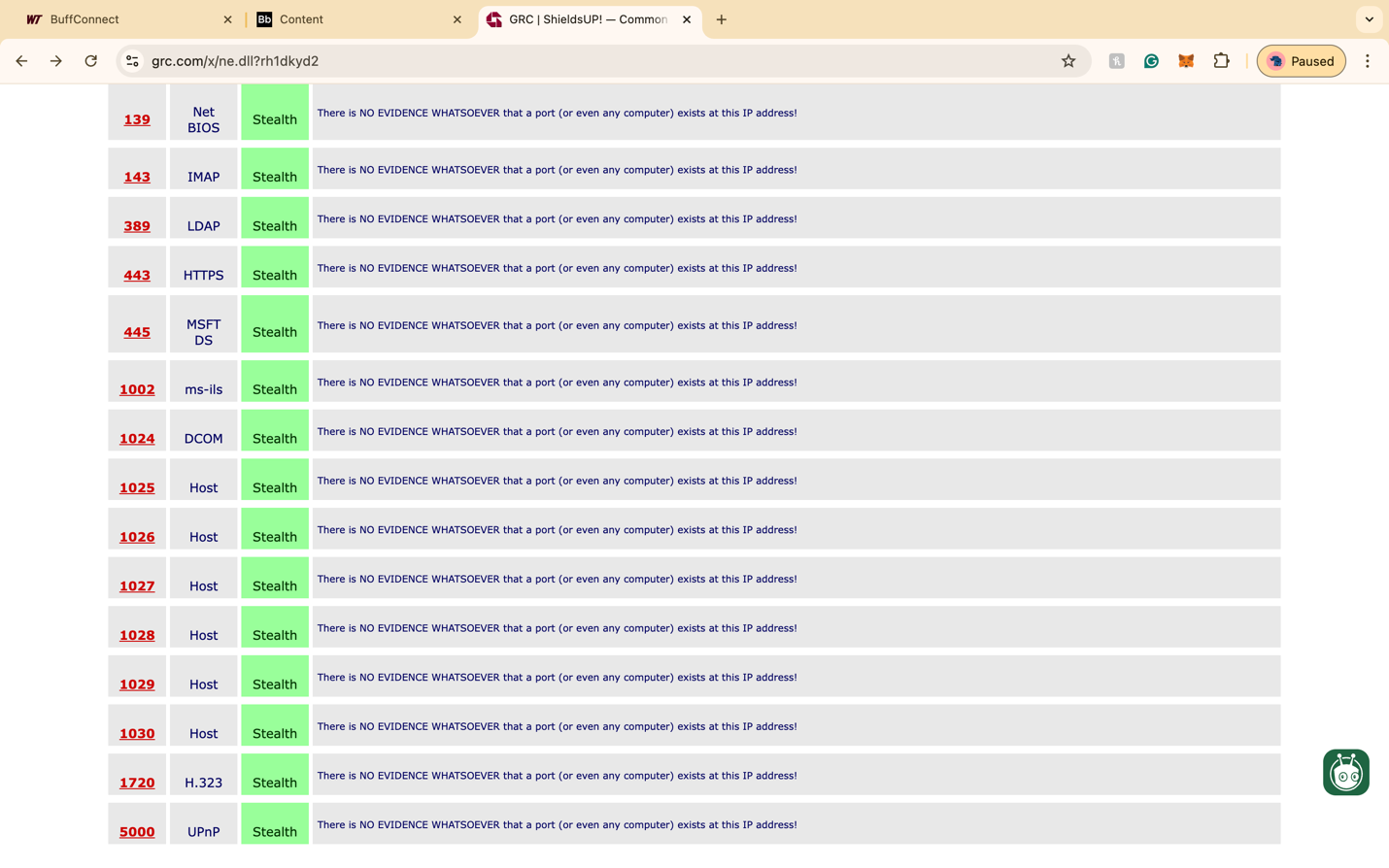
To begin this process, I researched the service Shields Up to get ahead of what to expect and how to interpret the results. I found several discussion forums that touched on how Shields Up denotes what ports are open and explains that the service is a simple, third-party way to run a quick network scan. I also found tons of information on the services web site itself; for example, the general research page has a warning that describes permissions are needed and that the service will probe a target computer. Upon probing (sending requests to) the equipment used between your computer and the Internet, it will produce entries that summarize your network’s port statuses. It allows the user to decipher if there are any potential threats to their system. After running the scan, I saw the status of my ports were all green and had a “Stealth” label, but I understand they can also say “Open” with a red color entry, or “Closed” with a blue color entry. The scan also gives you information on unsolicited packets and ping replies if you select the text summary option.

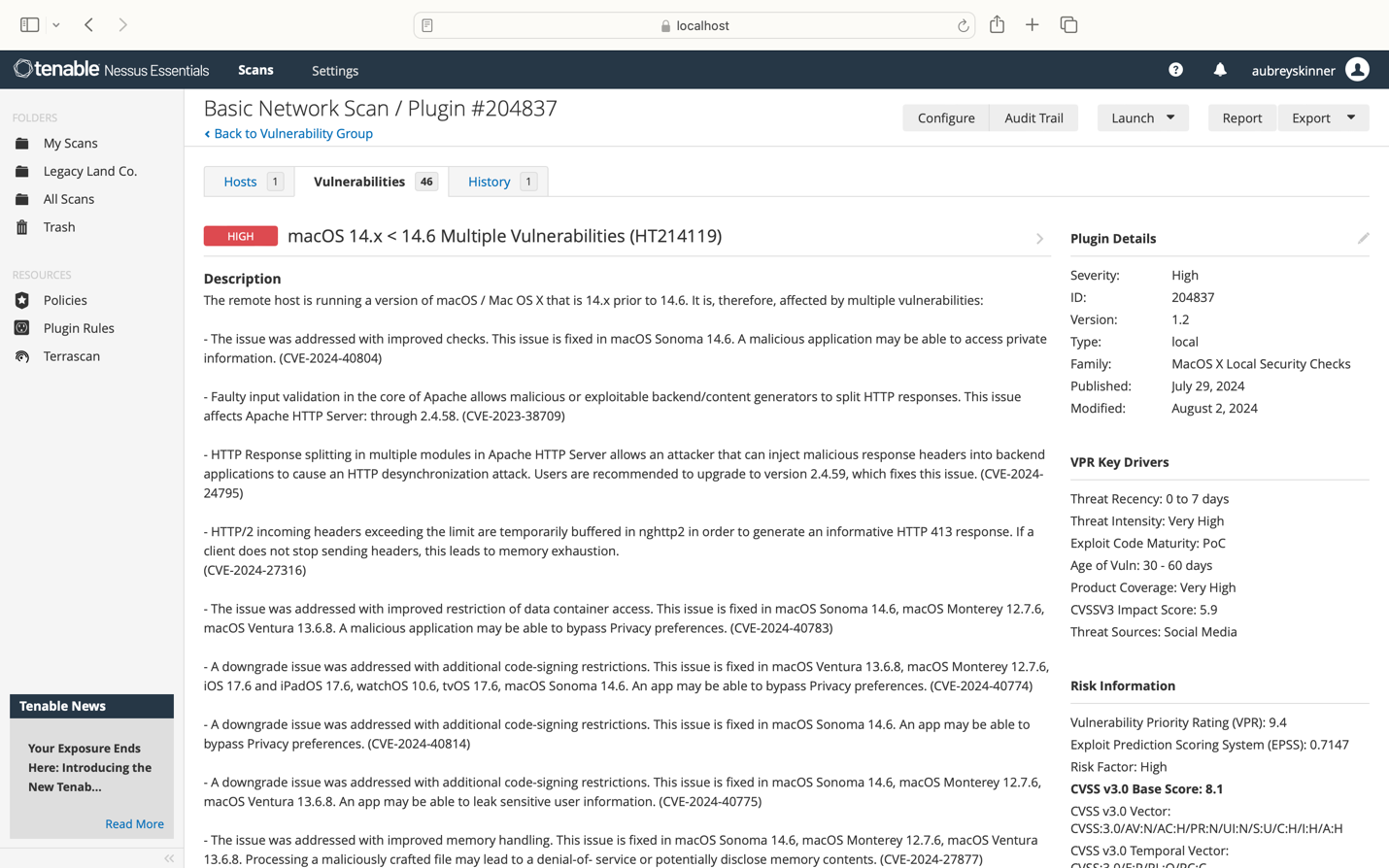
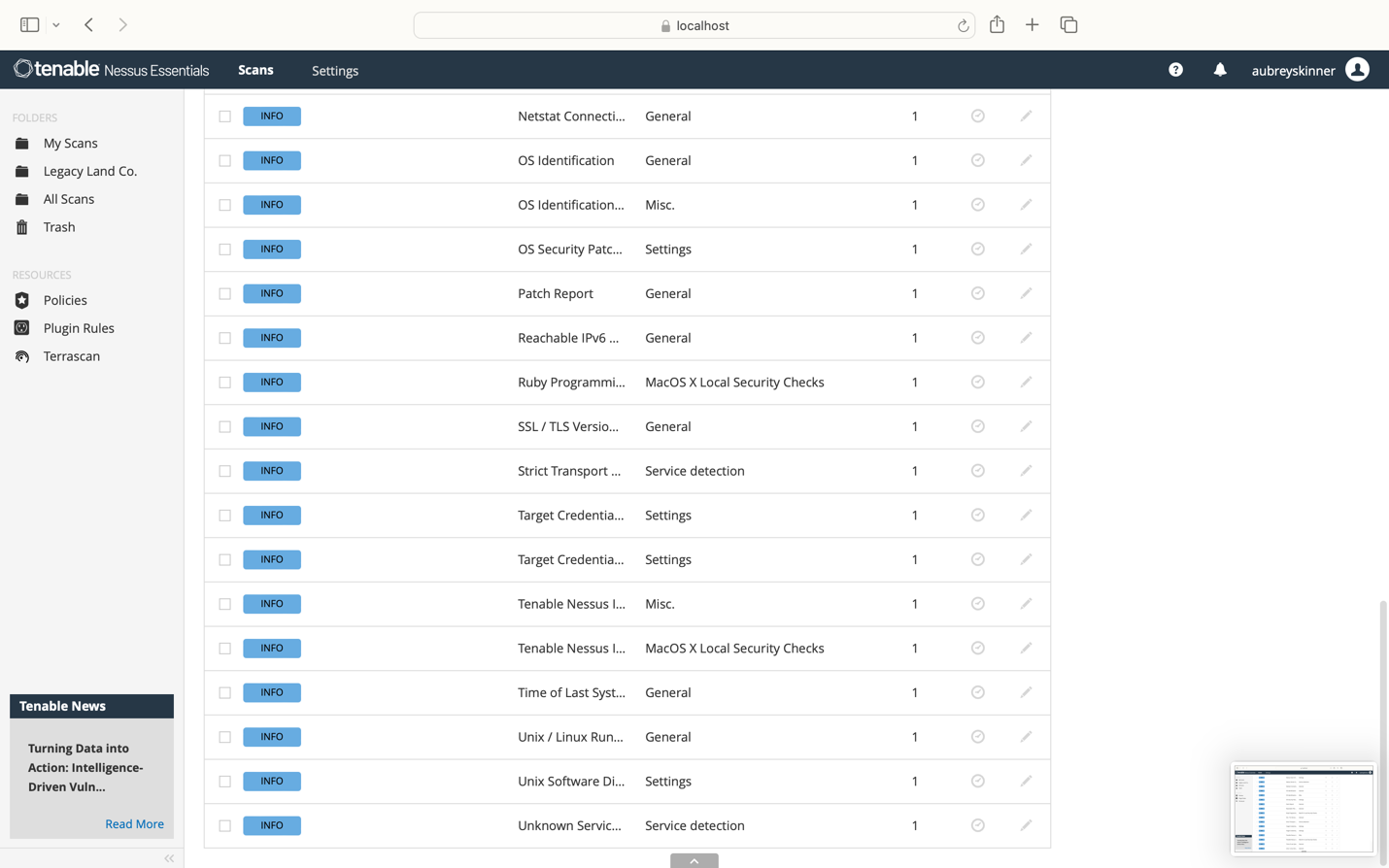
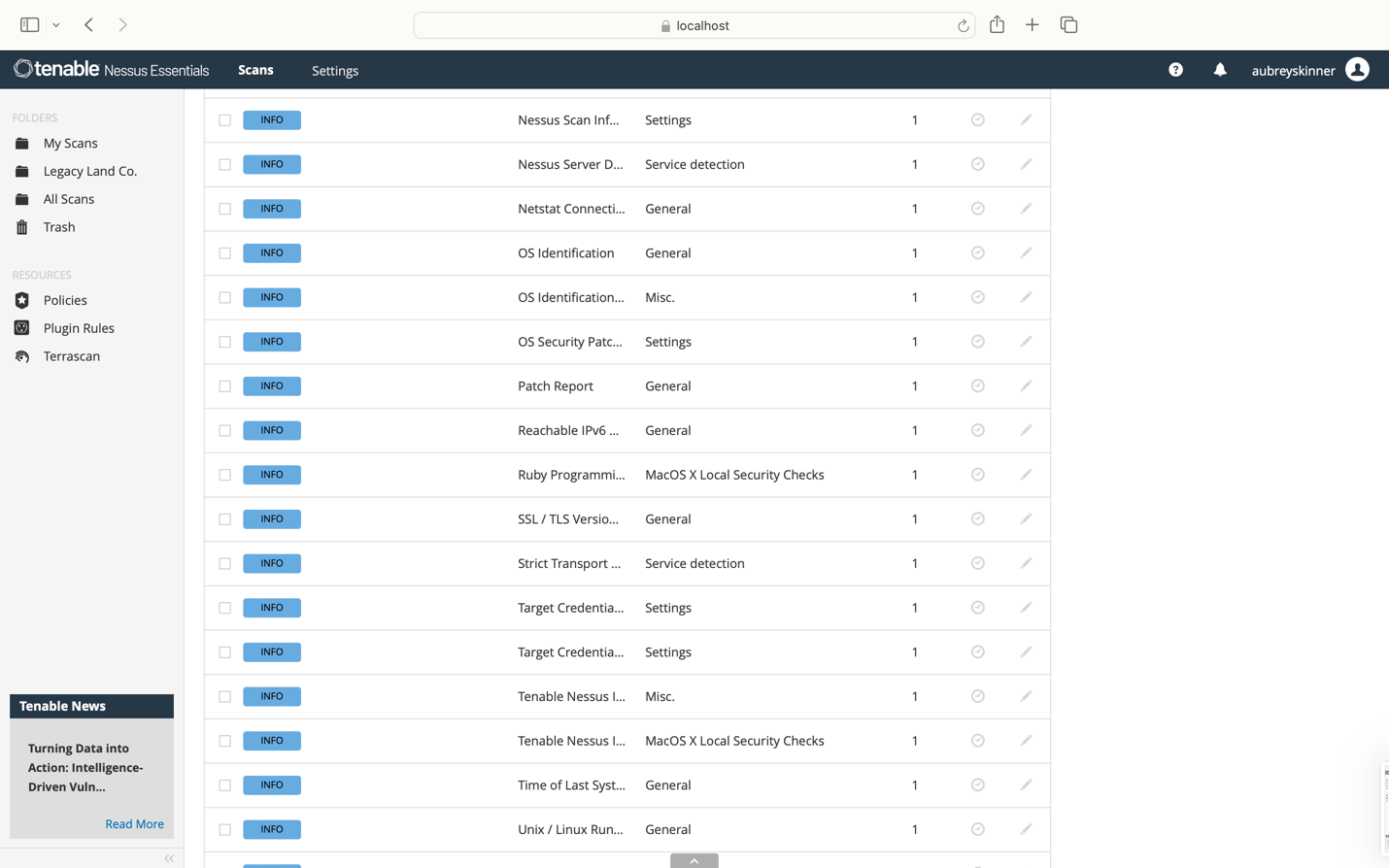
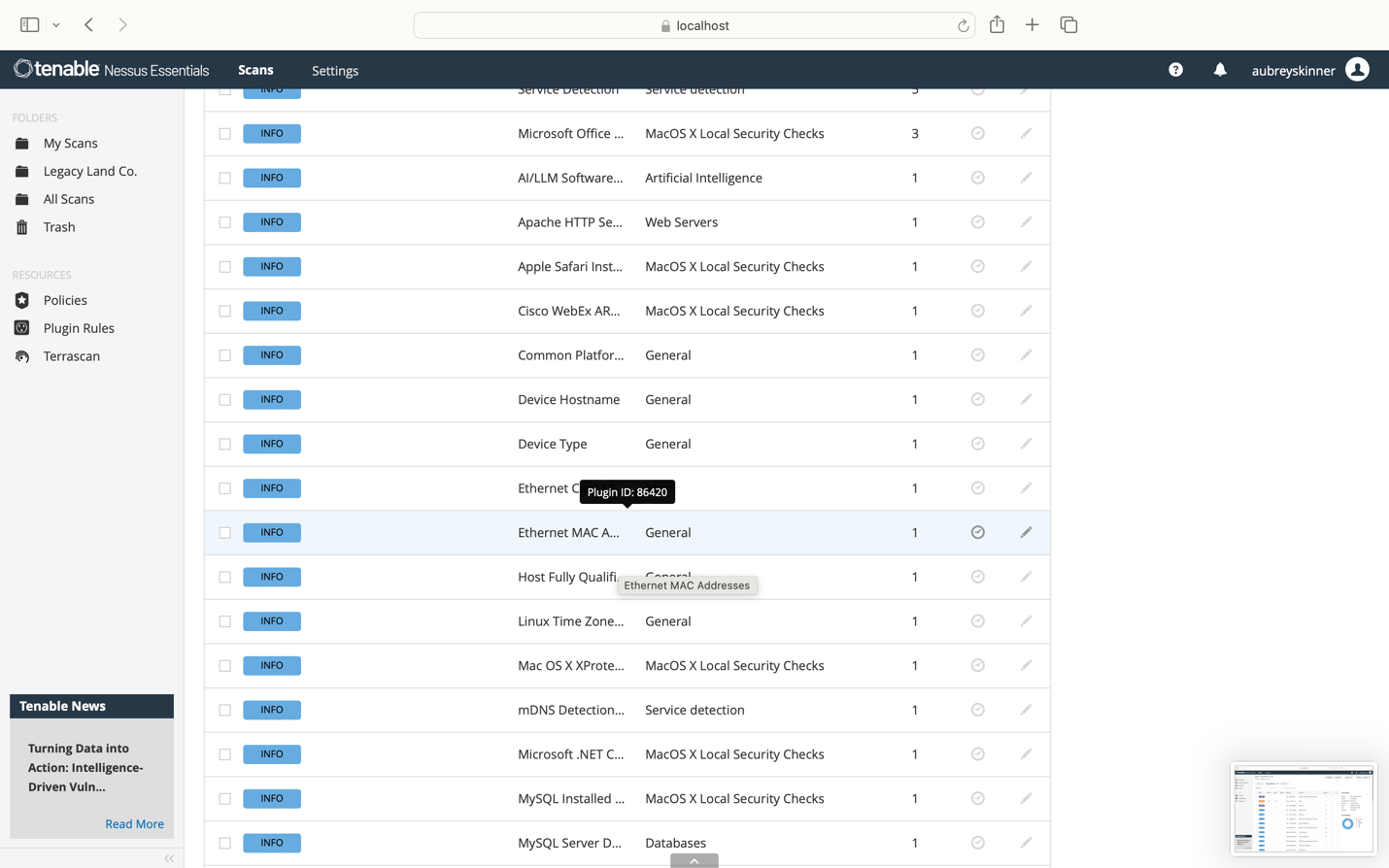
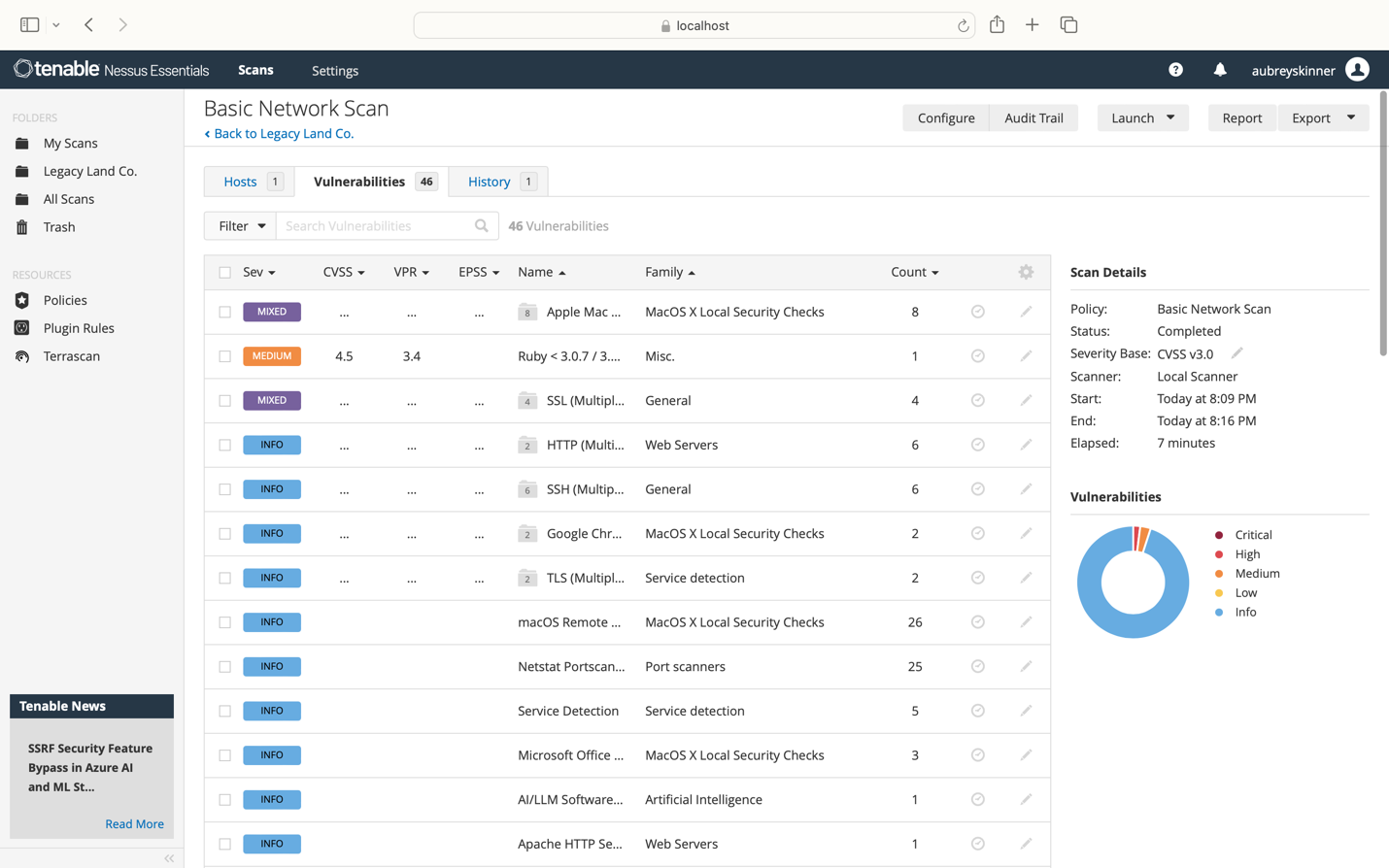
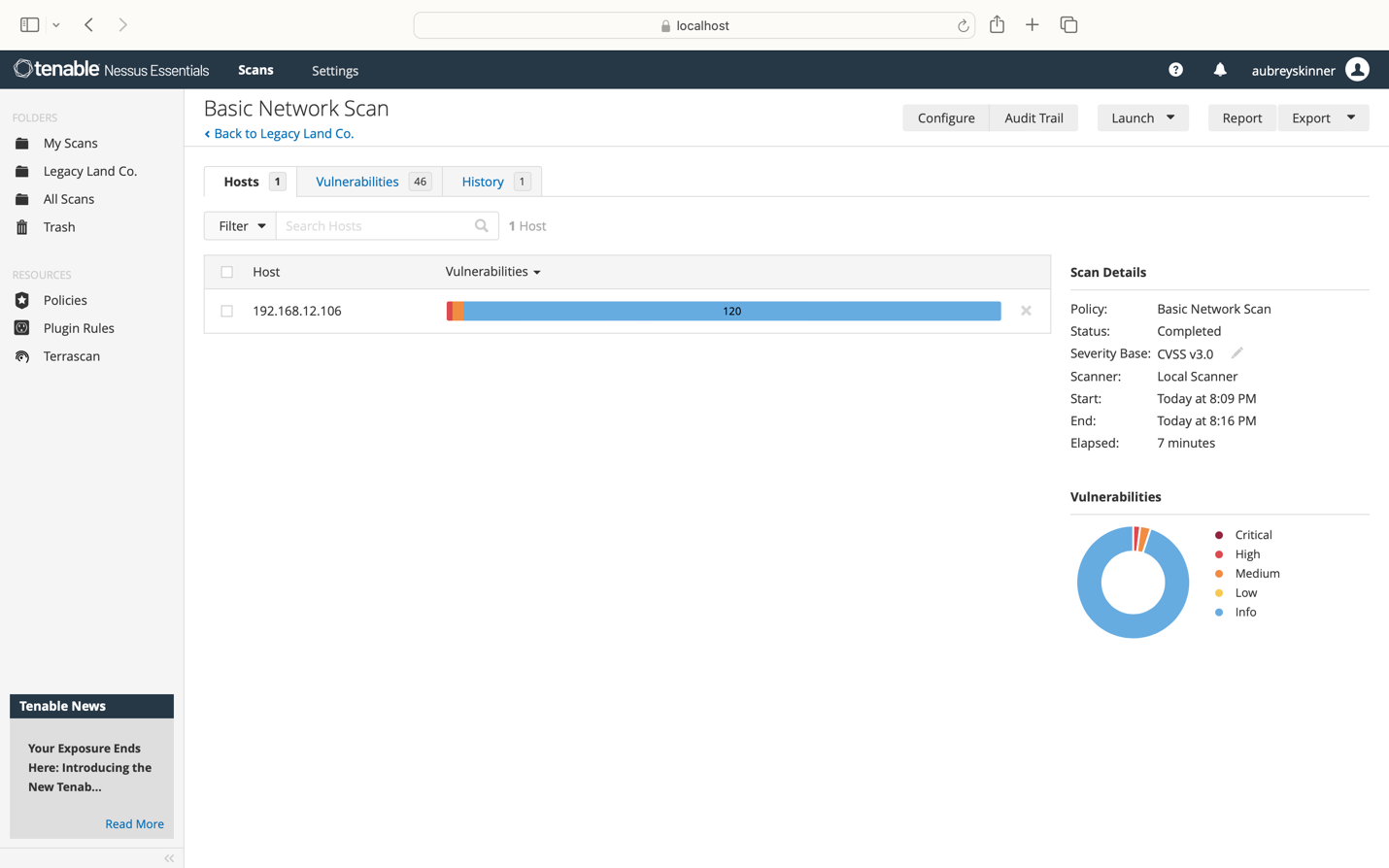
Moving onto Nessus, I performed some Google searches to get familiar with the software, but mainly followed the instructions to download and run the scan initially. Once I got a complete vulnerability scan for the network, I was able to comb through and decipher what was information and what was alerting me to a high, medium, low, or even mixed security risk. From this, I learned this network needed a version update, Ruby was vulnerable to attacks due to an outdated version, and there are some untrusted SSL certificates that could result in a compromised system.

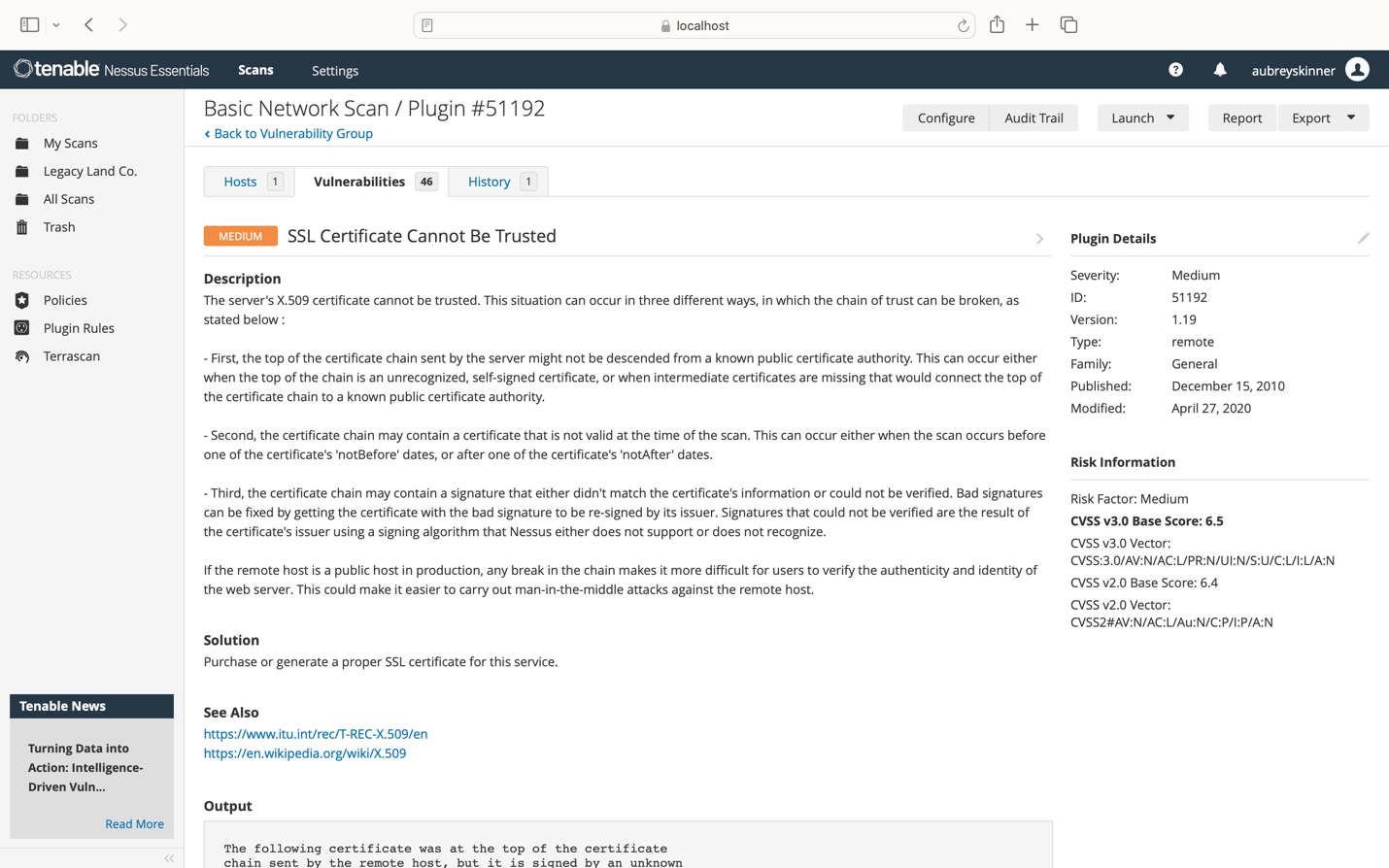
This is all very useful information I can use in the future because it rewards me the asset of maintaining my own cybersecurity. Routine scans can keep me updated on the health of my network and the systems that operate within it. If I were to have an incident where there is an attack, these tools would allow me to exploit that vulnerability whereas before, I wouldn’t have known this was available to me. The same can be said for this business, he will now be able to keep his operations safe, especially seen as there are money and clients involved in this organization. You can prevent data breaches and identify weaknesses before attackers take advantage of them. All of this is healthy for a business as it gains trust from the customers as well.

** A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**