Jane Aldakkour

Shields Up and Nessus

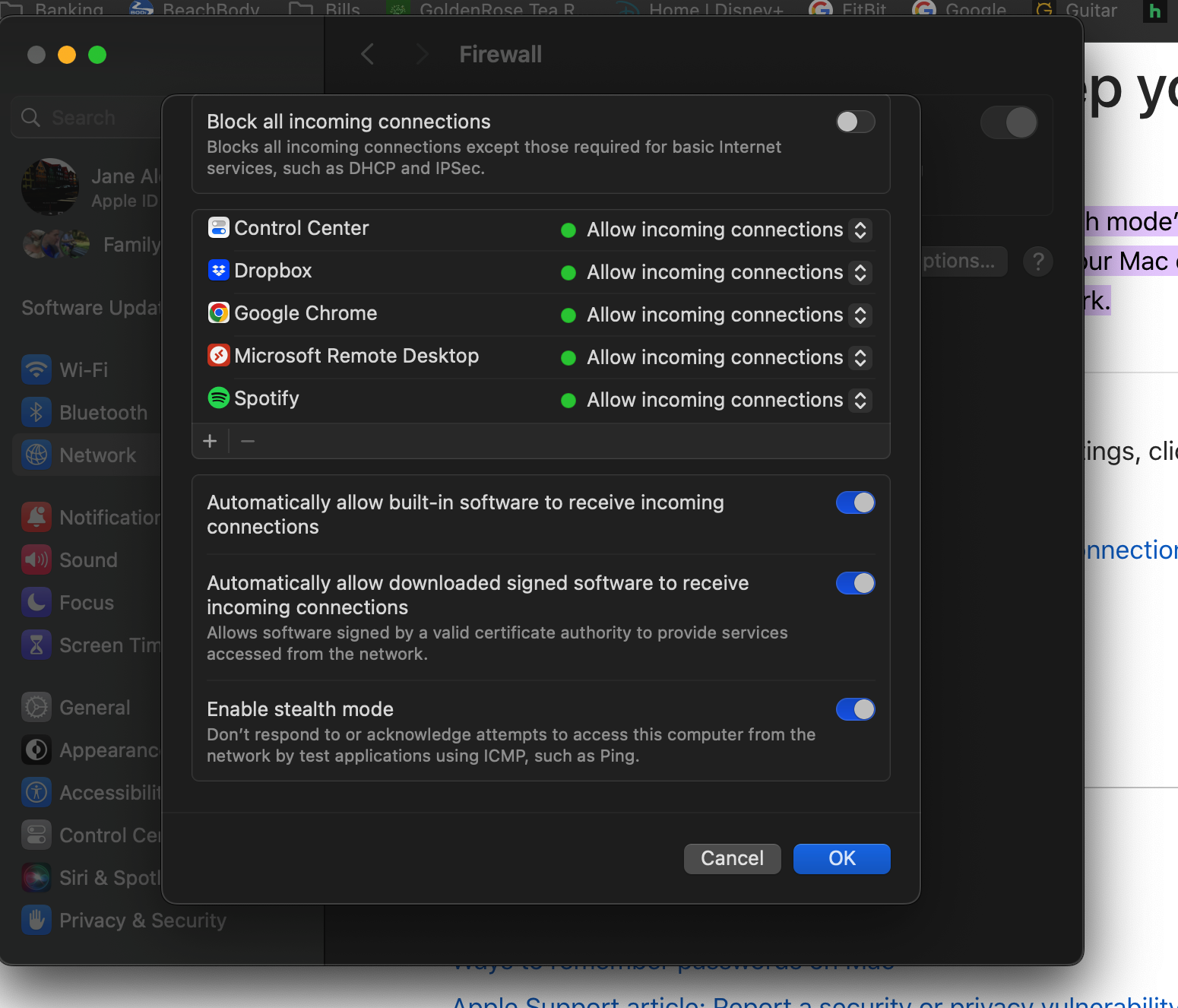
Network Management and Information Security

CDIM 6340

To do the write-up use the three-question format:

1. What did you do – in this section tell me how you did your vulnerability scans, how the softwares work, and how you analyzed the output. This section is all about how you are doing things, do not put results or outcomes here, just how you did it.

To start this assignment, I followed the instructions above, and went to Shields Up website. Once there, I clicked on “proceed” then selected common ports. This ran the test on the commonly used ports only. There were 26 scanned ports in total. Shields Up works by probing the target computer from their server. Once it was complete, I took a snapshot of the results. I then went to the “all service port” scan and scanned the network for these results and took a snapshot of the results. I had to do some research about the program and how it operates, as well as what the results mean, and learned in doing so that results are similar to NMAP results. I wondered what the difference was, so I tried to do some research on the matter, but it was not very successful. From what I could gather, the main difference between Shields Up and NMAP is that NMAP is scanning the DNS server for open ports, whereas Shields Up is reporting open ports on the router and machine [3]. I then began to analyze the results. After my analysis of the results, I did some more research to determine how I could activate “stealth” mode. I went to my network settings, opened the firewall and closed all the connections I thought were unnecessarily shown as being open (so everything except the “Enable stealth mode” was changed to stop allowing connections). I then ran the Shields Up test again; however, the results were still yielding “closed” ports instead of all in stealth mode.

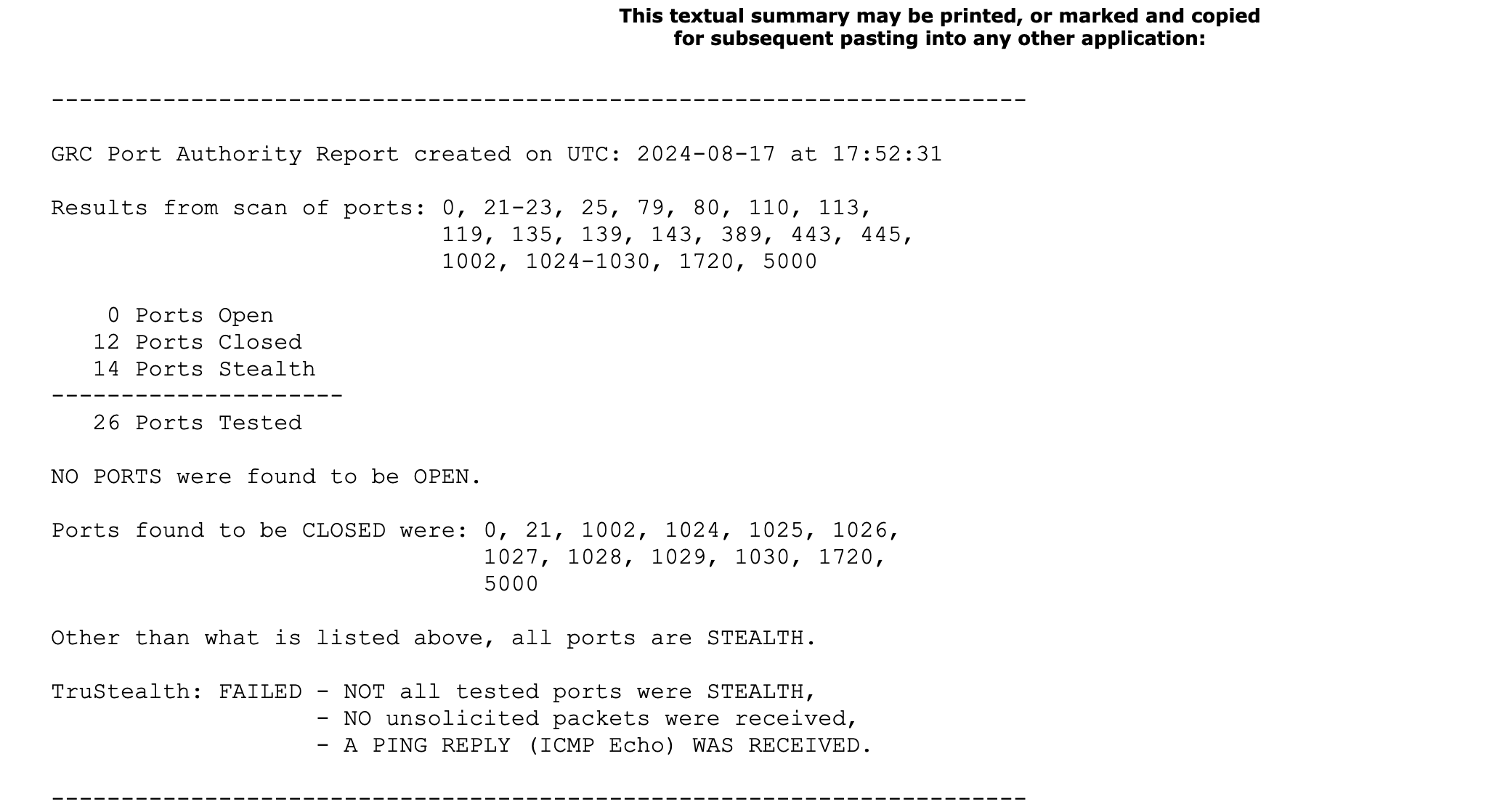


I did some more research, learned that there are settings on my router that need to be changed to enable complete stealth mode. I learned that there are settings on my router that need to be changed to enable complete stealth mode and proceeded to change attempt to change these settings. I was struggling to do find where I should be doing this, so I enlisted Austin’s help to try and get things figured out. We attempted looking through the app that we have for maintaining the routers settings but could not find in the settings where this was an option. Austin determined that it might possibly be a security setting that we would have to pay extra for. I stopped looking down that road and focused on moving on to the next task.

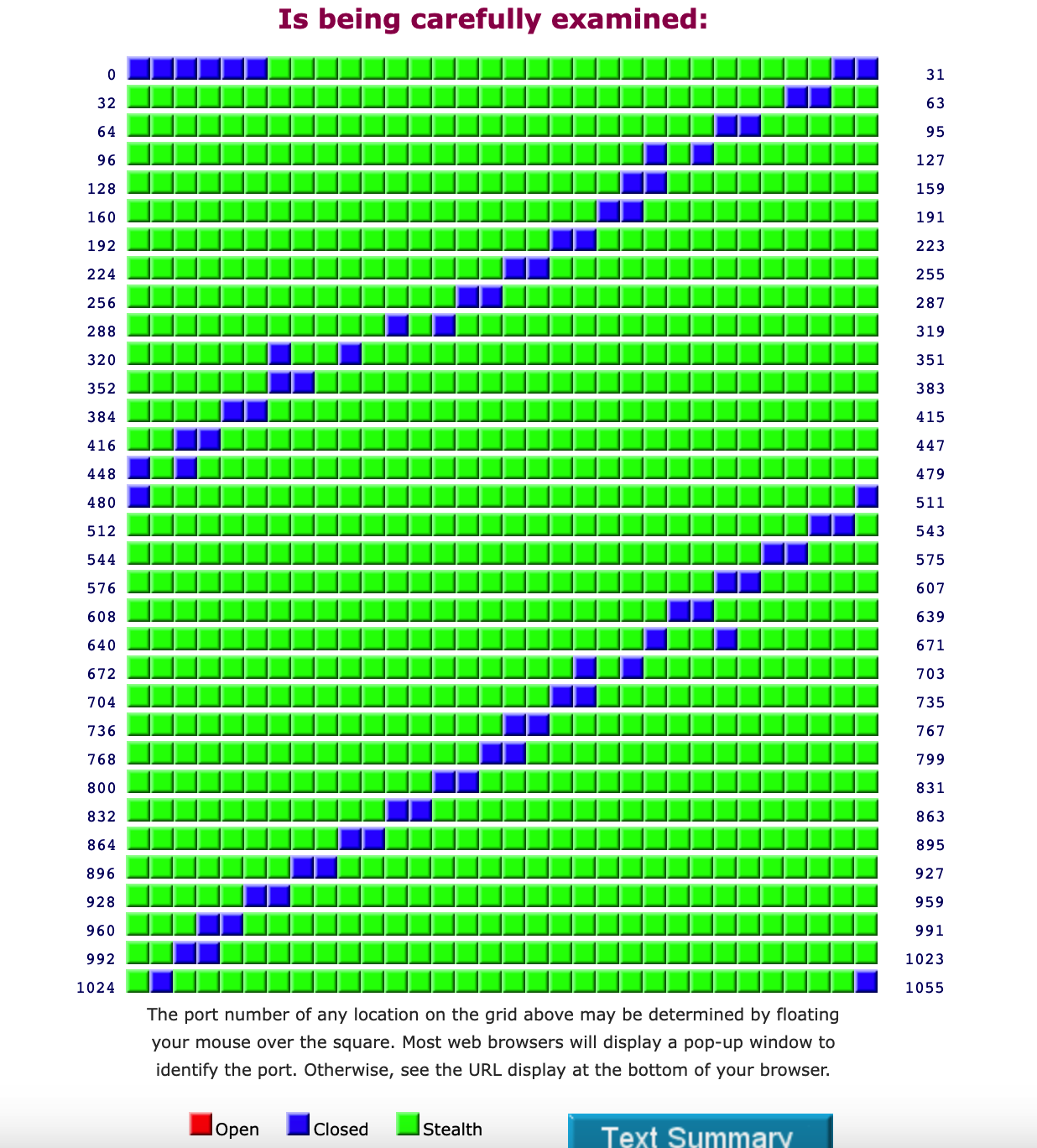
Once I completed the shields up part of this project, I moved on to the Nessus portion of the assignment. Nessus is another vulnerability scanner that works by testing each port on a device to determine the service that it is running. Once this has been determined, it then tests the service to find vulnerabilities that could be used by hackers. To complete the Nessus scan, I followed the instructions on the assignment to download Nessus. I ran into some issues in doing so, so I found a video that walked through the process of downloading and starting Nessus [7]. After Nessus was fully downloaded and operational, I watched a video on how to run the network scans before running them myself [8]. I then ran the scans on the network, chose which reports I wanted to pull from this scan, and analyzed the results.

1. What are the results – in this section tell me about what vulnerabilities were found, how severe they are, and what the organization should do to mitigate them.

The results of the Shields Up scan came back as a “failed” test. This means that my computer failed at having good security in place, as it reacted to the pings that the Shields Up sent. Although most of the ports responded with “stealth” which is what is wanted, there were a few ports that responded “closed.” The “stealth” status meant that that the port did not respond at all to the ping that was sent, neither accepting nor declining the ping and therefore appearing nonexistent. The “closed” status meant that the port responded to the ping, but did not allow a connection to go through. By responding to the ping, the user attempting to establish a connection is notified that a device exists and is there. This is a vulnerability, although not as bad as it could be. Since all the ports pinged were closed, it means that they denied a connection to the device that was pinged. Ideally, however, all ports would report back to be in “stealth” mode.

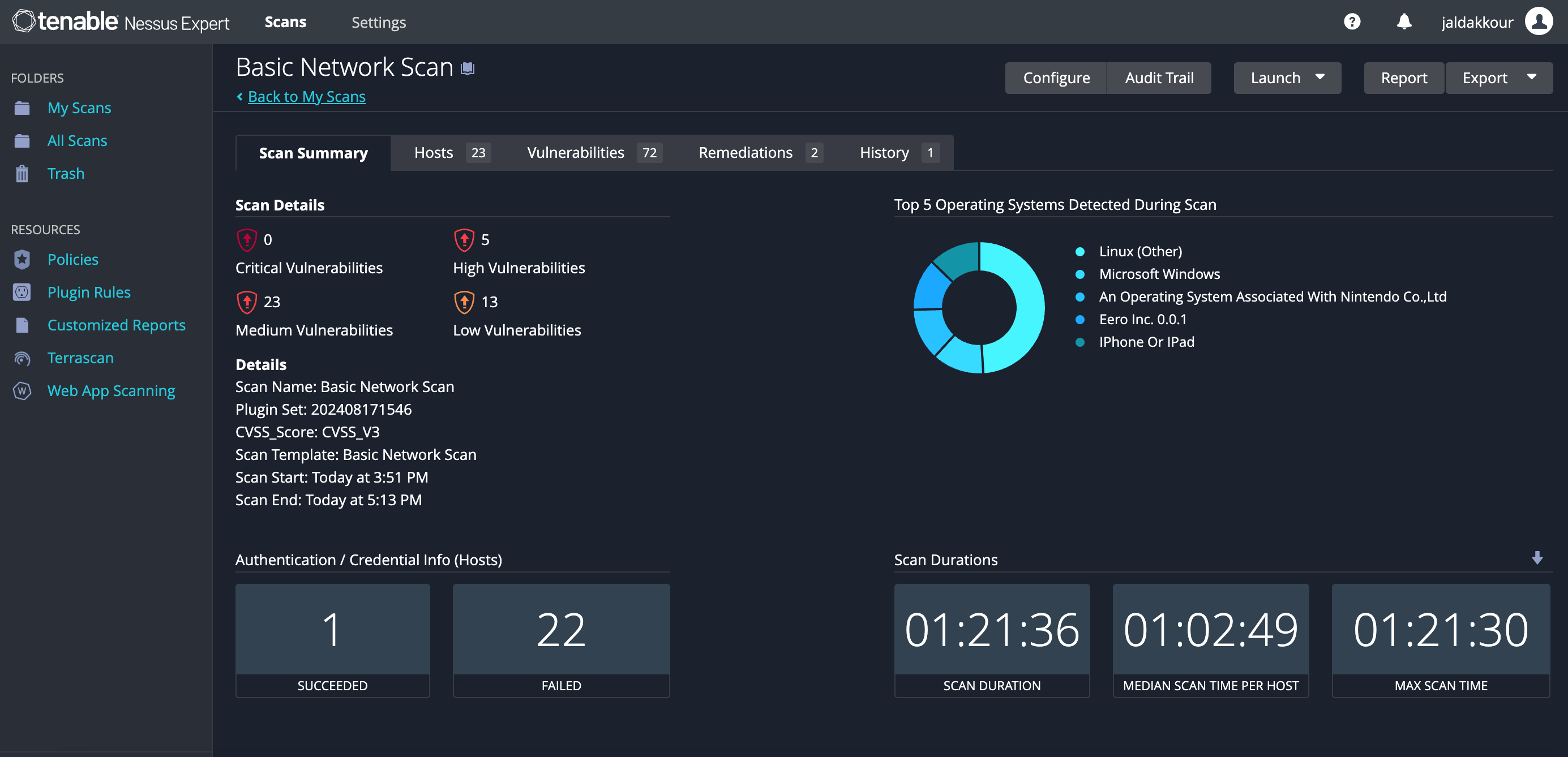


I also ran the Shields Up test on the first 1056 ports, the results of which are shown below. The results were like the first test run, in that all ports were either operating stealth or closed.



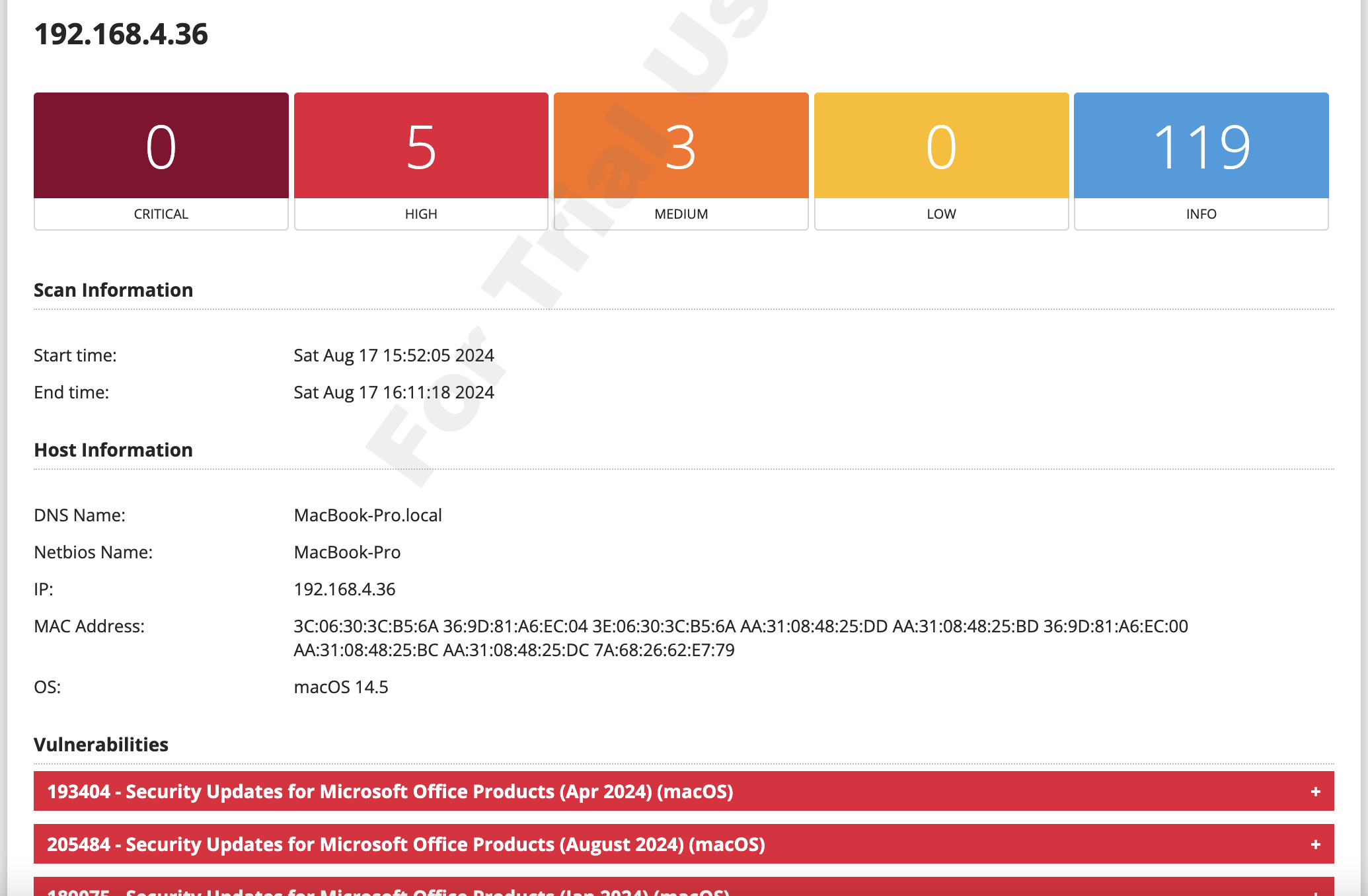
To try to resolve this problem of “closed” ports, I did some research. I found that one way to do this would be to go into the firewall settings and stop these connections from happening manually [4]. I closed all the connections I thought were unnecessarily shown as being open (so everything except the “Enable stealth mode” was changed to stop allowing connections). I then ran the Shields Up test again; however, the results were still yielding “closed” ports instead of all in stealth mode. I did some more research to try to determine why this was still happening. I learned that there are settings on my router that need to be changed to enable complete stealth mode and proceeded to change attempt to change these settings. I was struggling to do find where I should be doing this, so I enlisted Austin’s help to try and get things figured out. We attempted looking through the app that we have for maintaining the routers settings but could not find in the settings where this was an option. Austin determined that it might possibly be a security setting that we would have to pay extra for. Since the ports were at least closed, we stopped looking and determined that, should we want to increase our network security, this would be something we could look further into.

For the Nessus scans, there were a couple of different reports that I pulled from the scan that I ran, which was the basic network scan. This scan ran on the entire network to detect all the vulnerabilities the network has and lasted for about 1 hour and 20 minutes. There was a lot of information that came back with this report, but the home page looked like this:

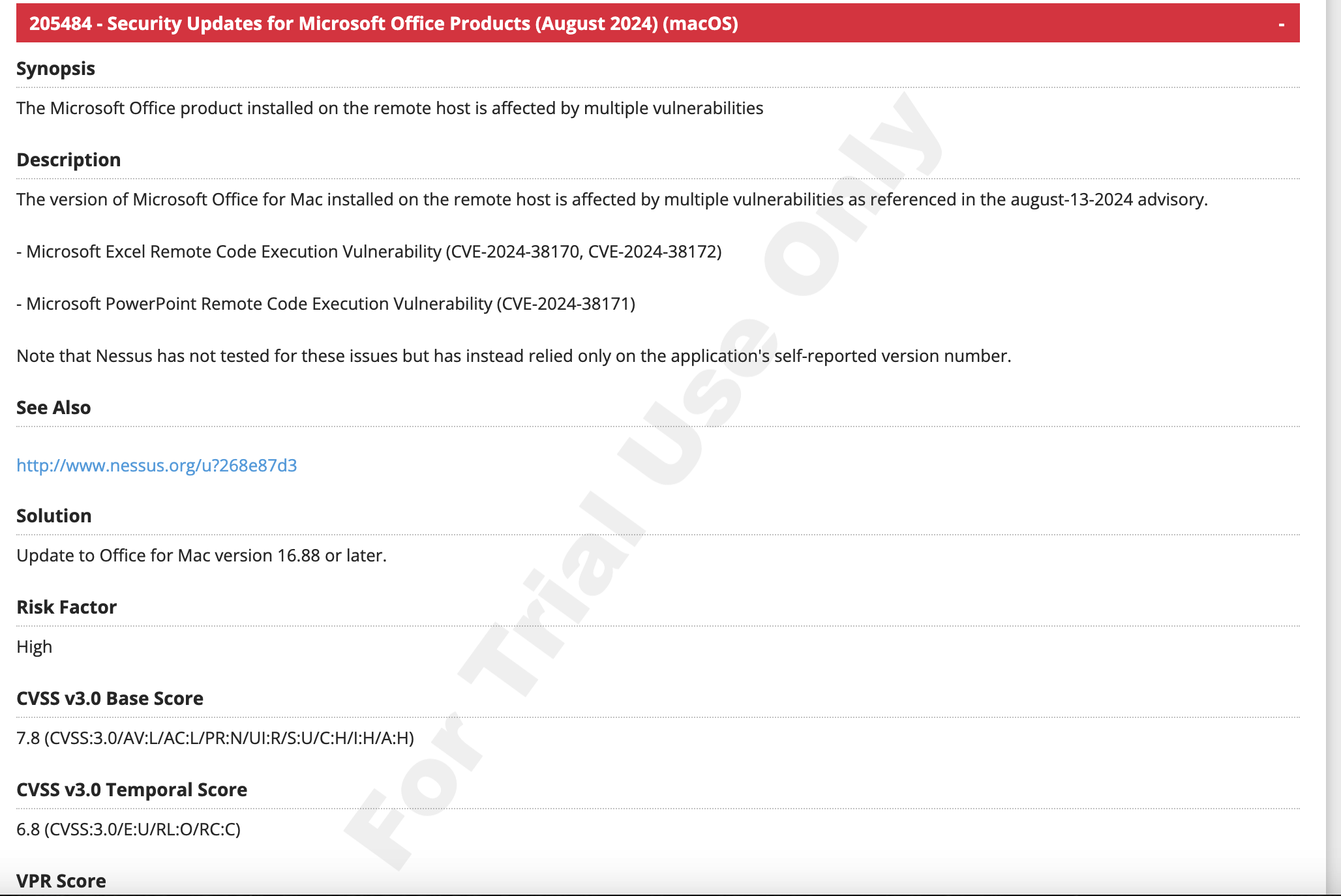


As can be seen, there are many vulnerabilities that were detected on the network – 5 high, 23 medium, and 13 low. Luckily, there were no critical vulnerabilities, however there are quite a few high and medium vulnerabilities. Nessus provides the option to print many kinds of reports that provide details on the scan's findings. I printed the complete list of vulnerabilities scan, as well as a detailed list of vulnerabilities, and an exploitable vulnerabilities scan. For this assignment, I will focus on the vulnerabilities found on my Macbook, which also happened to have the most vulnerabilities.

Some of the results of the detailed scan are shown below. There are many vulnerabilities located here, and therefore I cannot show them all. I will review the most critical security hazards.



As shown above, there are five high risk vulnarbilities, 3 medium risk vulnerabilities, and 119 informational vulnerabilities. The high-risk vulnerabilities are almost all exclusively missing updates. Four of the five are missing updates for Microsoft office products, and the last one is for the Mac’s operating system itself. Although these appear as high vulnerabilities, this is an easy fix, fortunately. The reason that this is rated as high is because there are likely security updates in these updates that would fix vulnerabilities in the software’s security. Fortunately, this one is an easy fix. All I have to do is go into settings for the Mac and upload the latest update. I included images of the latest update missed (for August 2024).





The next vulnerability was that the SSL certificate cannot be trusted, which appeared as a medium vulnerability. This is another problem that does not take much to fix. Nessus provides responses to these security threats in the detailed report. There is a statement at the bottom of this vulnerability, which says:

“The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  
  
|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=MacBook-Pro.local  
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority”

When I activated Nessus, I was given a warning that the website was not secure and that there was risk for me continuing. I accepted the risk of running the scan, and so I believe that this is where this specific vulnerability is coming from. The fix would be to have the certificate signed by a valid authority. The next vulnerability is also a medium level. This one is about TeamViewer, an app I downloaded to be able to remote into my old job’s network. It states that the app is operating on an outdated system and needs to be updated. This is an easy fix, which would be to update this program. This addresses all the major critical issues that are generated by my MacBook. The other 119 are informational vulnerabilities, which are still dangerous as it provides hackers with a lot of information that can be used to find ways to get into the system. The most shocking ones that I found were that it showed some of the applications that I had downloaded on my device, such as Dropbox, Google Chrome, and MySQL to name a few.

Another vulnerability issue I saw across multiple hosts (but was not one on my MacBook) was the “ICMP timestamp request remote date disclosure,” which was marked as a low vulnerability. The ICMP timestamp is described as the date set on the targeted machine, which can be used to assist in time-based authentications. The security vulnerability lies in the fact that the remote clock is the same as the local clock, which should not be the case. Based on the research that I did; this is likely happening because the firewall that enables this protection has been taken down. This can be fixed by restoring the firewall.

1. What did you learn – discuss your takeaways from the assignment, tell me what you learned about vulnerability scanning and how you can use it in the future, also discuss how they could be of value to the organization in the future.

There was a lot to learn about vulnerability scanning. I learned about shields up and Nessus, and how these programs work and can be used to detect network vulnerabilities. The Shields Up results were very similar to NMAP results from assignment one, so I tried to learn the difference between running these programs. I was surprised to find that there was not much information on this topic, however what I was able to find stated that NMAP runs it scans from your network on your network, whereas Shields Up uses DNS scanning to run its scans from their servers to your network. Shields Up can be useful as it shows what people outside the network see when trying to connect to devices within. Knowing which ports are returning these pings helps network administrators know which ports need to be watched more closely to ensure that they are not targeted and attacked.

Nessus had a lot to show about my network as well. I learned that a lot of my security issues were caused by not updating my devices. This is dangerous, because oftentimes updates contain patches to fix security issues in the previous version’s software. When this update is released, it also signals to all potential hackers what those security issues are exactly, which makes it very easy for them to exploit. Using Nessus also showed in general how much information there is to gather about an individual’s network and how easy it is to get this information. This one scan that I performed on my network through Nessus showed several different devices, what they are, IP addresses, vulnerabilities on each of these devices, the level of vulnerability, the reason for that vulnerability, solutions to resolving these vulnerabilities, as well as many other things. Nessus is extremely valuable to the organization, as it can be used to detect vulnerabilities and help address them as they arise in the future. After seeing all the updates that I need to make to my MacBook (some of which I was unaware of), I will be doing so.

Resources:

[1] Steve Gibson, GIBSON RESEARCH CORPORATION. “GRC : Shieldsup! - Internet Vulnerability Profiling .” *GRC | ShieldsUP! - Internet Vulnerability Profiling* , [www.grc.com/shieldsup#:~:text=ShieldsUP!!,your%20computer%20and%20the%20Internet](#:~:text=ShieldsUP!!,your%20computer%20and%20the%20Internet). Accessed 18 Aug. 2024.

[2] Steve Gibson, GIBSON RESEARCH CORPORATION. *Shields up!! — System Error*, www.grc.com/x/ne.dll?rh1dkyd2. Accessed 18 Aug. 2024.

[3] “Board Index.” *Nmap and Shield’s up{Solved}*, forums.linuxmint.com/viewtopic.php?t=328583. Accessed 18 Aug. 2024.

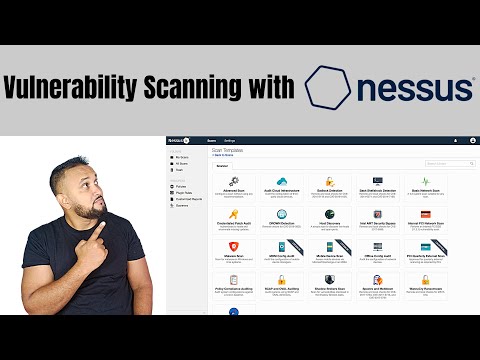
[4] “Use Stealth Mode to Keep Your Mac More Secure.” *Apple Support*, support.apple.com/en-gb/guide/mac-help/mh17133/mac#:~:text=If%20you’re%20concerned%20about,closed%20TCP%20or%20UDP%20network. Accessed 18 Aug. 2024.

[5] Enterprise, James T Kirk USS. “How Do You Get into ‘Stealth’ Mode?” *Tom’s Hardware Forum*, Tom’s Hardware Forum, 25 Feb. 2014, forums.tomshardware.com/threads/how-do-you-get-into-stealth-mode.1717981/#post-12159252.

[6] “Welcome to Tenable Nessus 10.8.X.” *Welcome to Tenable Nessus 10.8.x (Tenable Nessus 10.8)*, docs.tenable.com/nessus/Content/GettingStarted.htm?\_gl=1%2Aaek052%2A\_gcl\_au%2AMTQyNjk5NTc3Ny4xNzIyODY1MDY1LjEwNDg0NDI5NjYuMTcyMzkyNDcwNy4xNzIzOTI0NzA3%2A\_ga%2ANzQ5NjUyOTI0LjE3MjI4NjUwNjY.%2A\_ga\_HSJ1XWV6ND%2AMTcyMzkyNDYzNC40LjEuMTcyMzkyNDcxNi41Ni4wLjEwOTQ0MTc2NjE. Accessed 18 Aug. 2024.

[7] *YouTube*, YouTube, www.youtube.com/watch?v=CKZfTqDBq4A. Accessed 18 Aug. 2024.

[8] *YouTube*, YouTube, www.youtube.com/watch?v=tzp0YC0MkVE. Accessed 18 Aug. 2024.

[](https://www.youtube.com/watch?v=tzp0YC0MkVE)