Student:	Email:
Christian Barba	christianbarba527@gmail.com

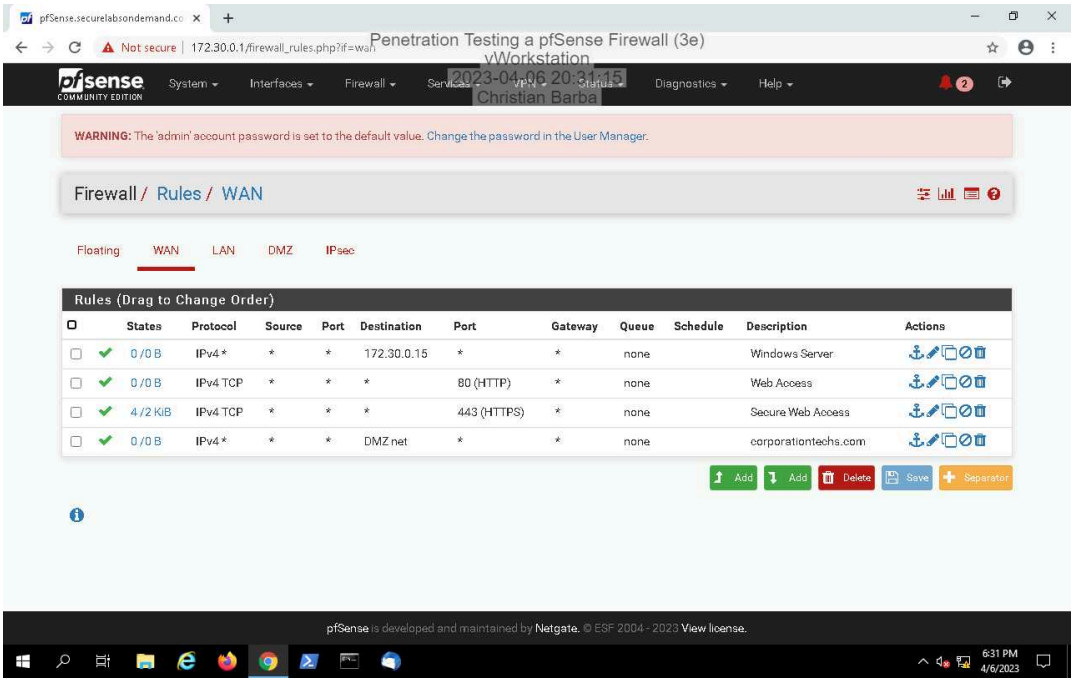
Time on Task:	Progress:
14 hours, 38 minutes	100%

Report Generated: Monday, April 10, 2023 at 5:33 PM

Section 1: Hands-On Demonstration

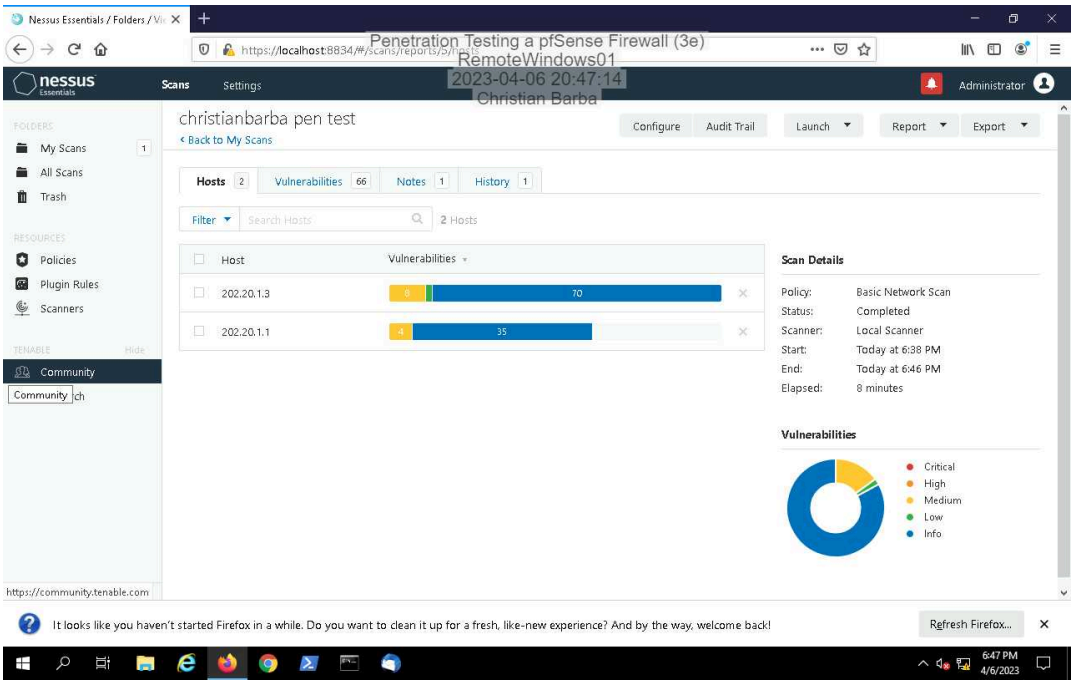
Part 1: Examine a pfSense Firewall Configuration

12. **Make a screen capture** showing the **WAN rules table**.

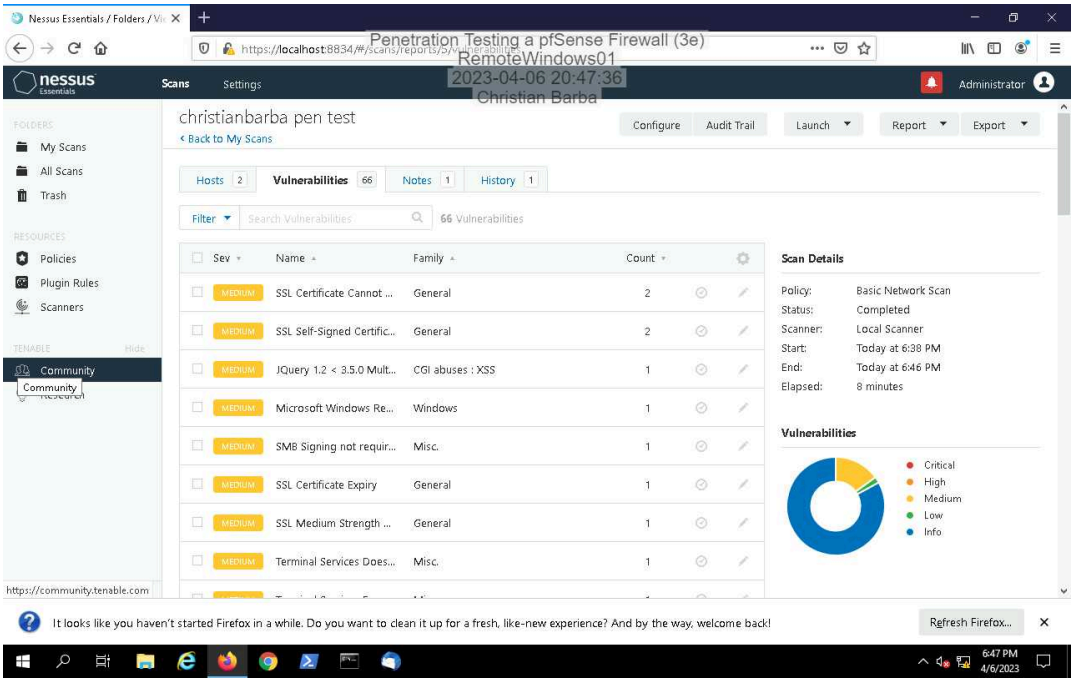


Part 2: Conduct a Penetration Test on the Network

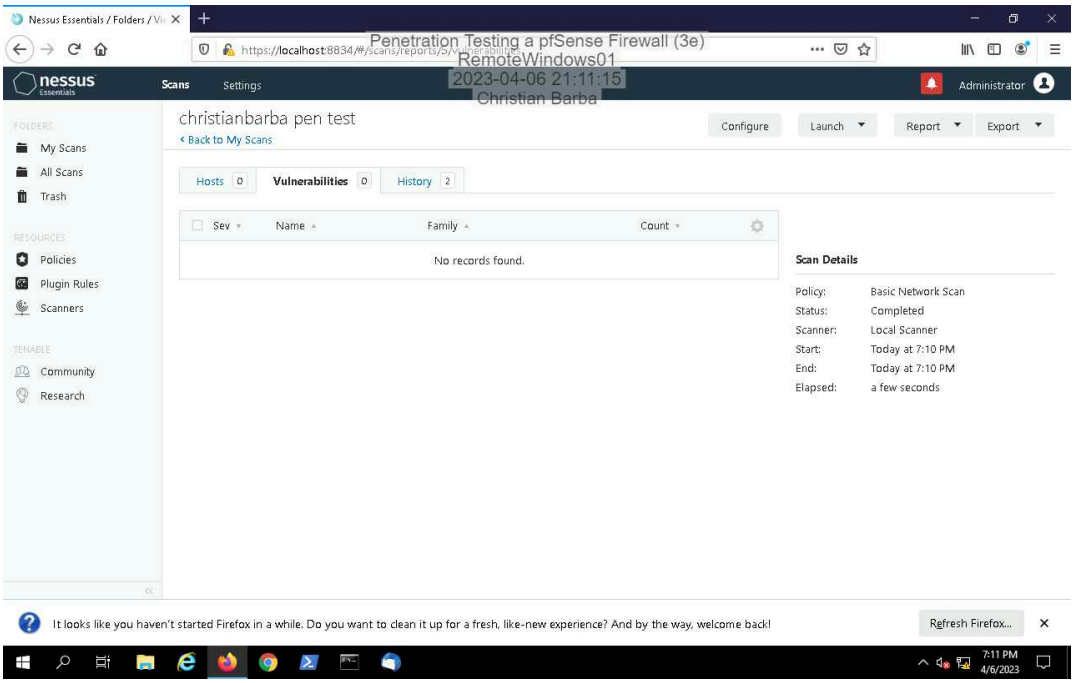
11. **Make a screen capture** showing the ***yourname*** **pen test scan results**.



13. **Make a screen capture** showing the **list of vulnerabilities**.



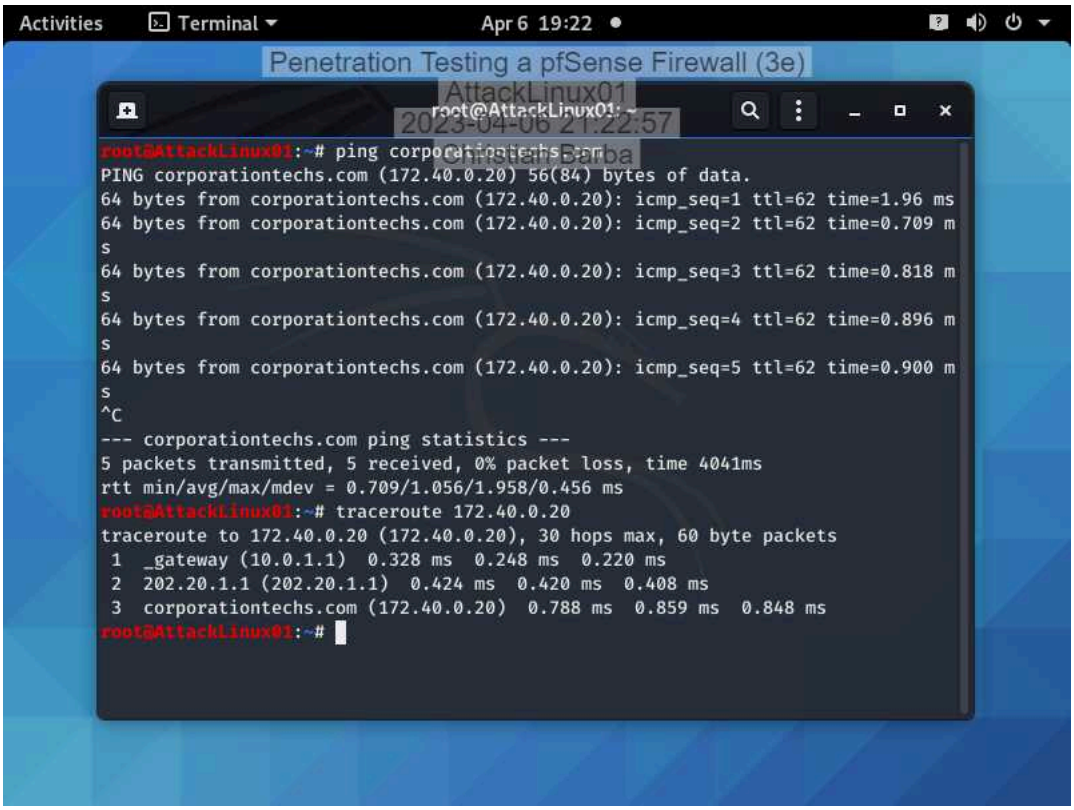
30. **Make a screen capture** showing the **updated vulnerability report summary**.



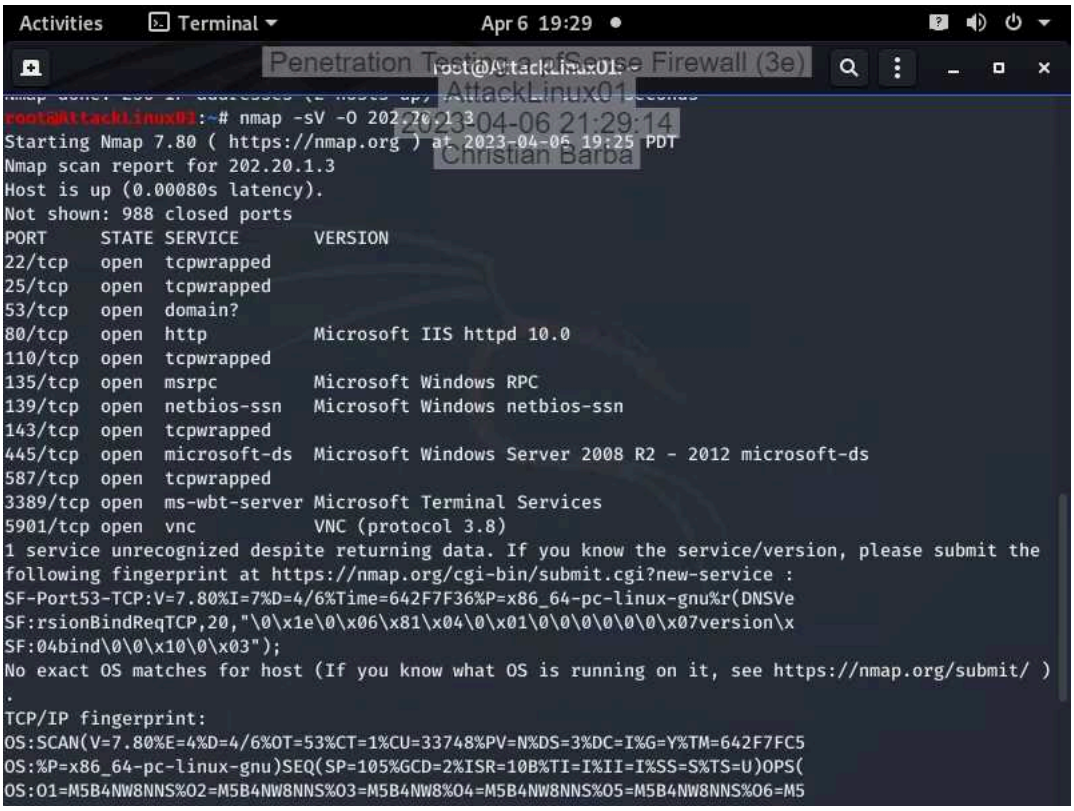
Section 2: Applied Learning

Part 1: Conduct a Port Scan on the Network

7. **Make a screen capture** showing the **results of the traceroute command**.

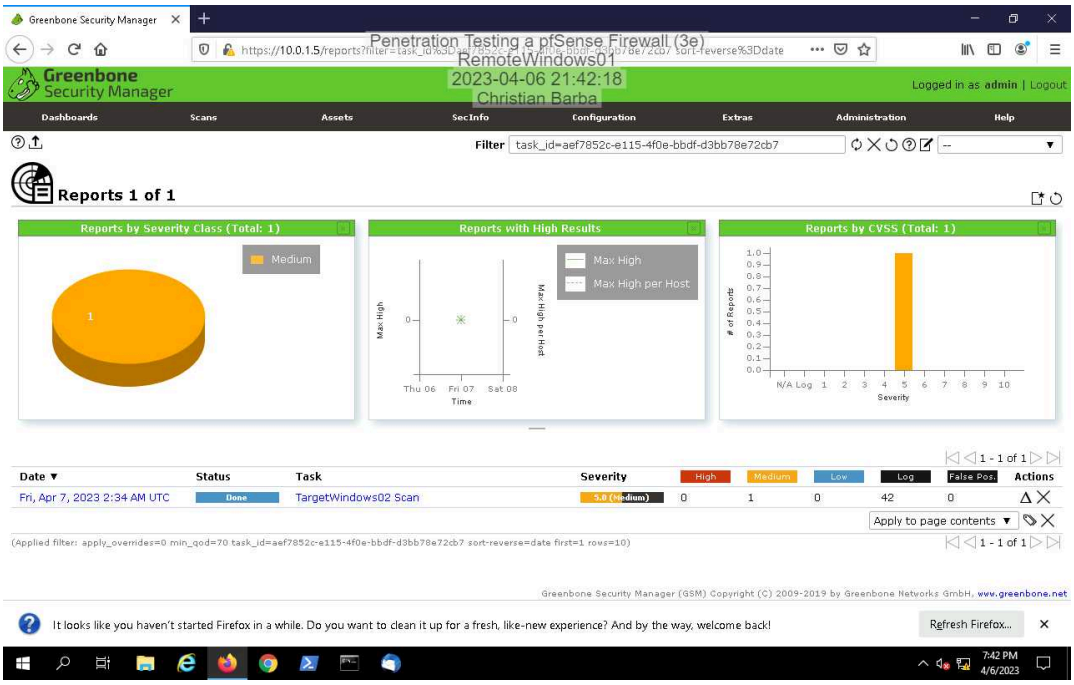


11. **Make a screen capture** showing the result of the **nmap scan with OS detection activated**.

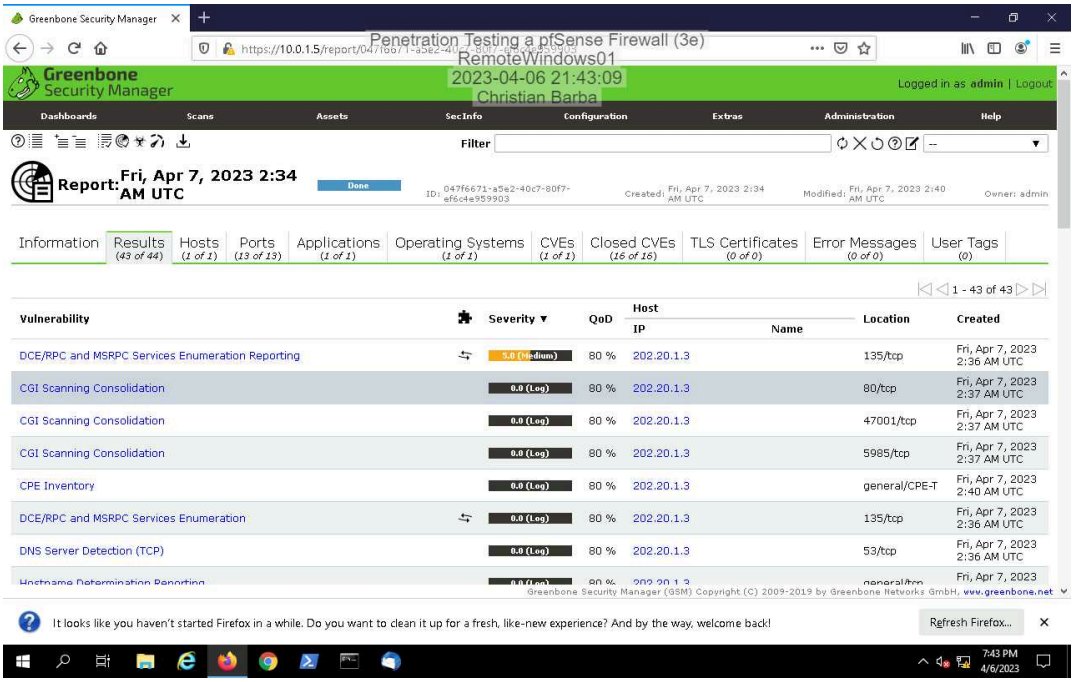


Part 2: Conduct a Vulnerability Scan on the Network

12. **Make a screen capture** showing the **OpenVAS scan report**.



14. **Make a screen capture** showing the **detailed OpenVAS scan results**.



Section 3: Challenge and Analysis

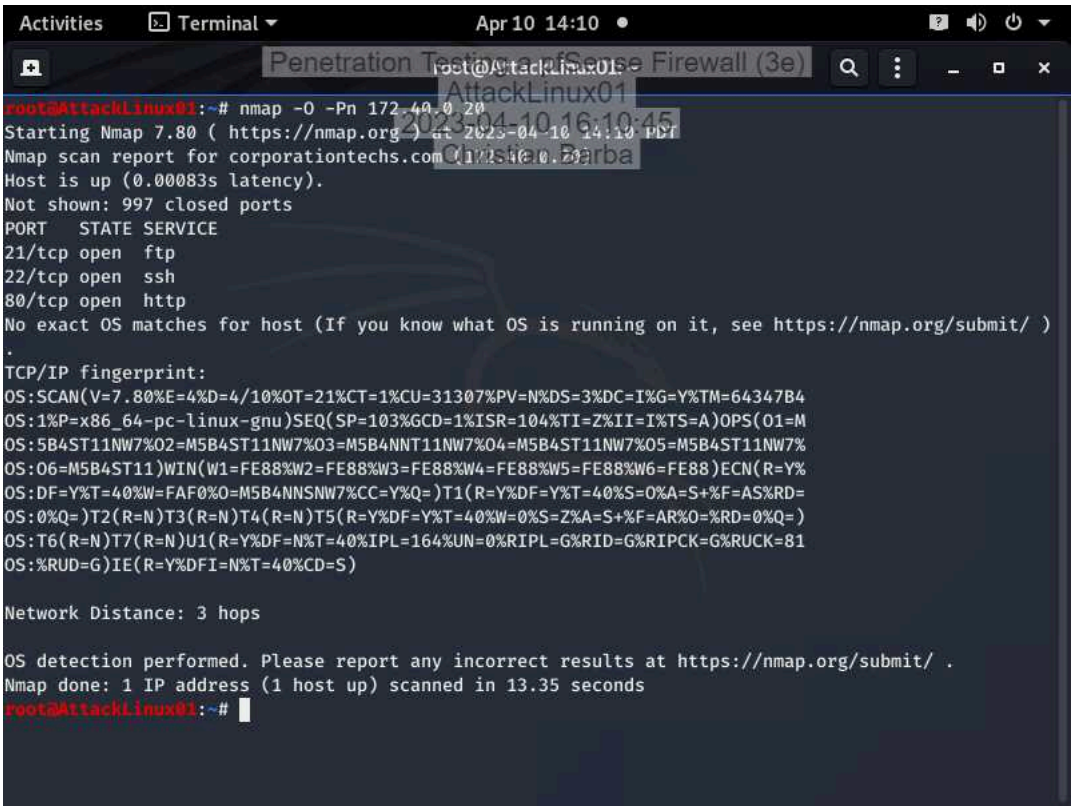
Part 1: Research DMZ Deployment Best Practices

Before beginning the technical portion of your penetration test, you decide to spend some time brushing up on best practices and common mistakes for DMZ deployments - both the network aspect and the servers located therein. Use the Internet to **research** DMZ deployments, then **identify** three best practices and one potential mistake or vulnerability.

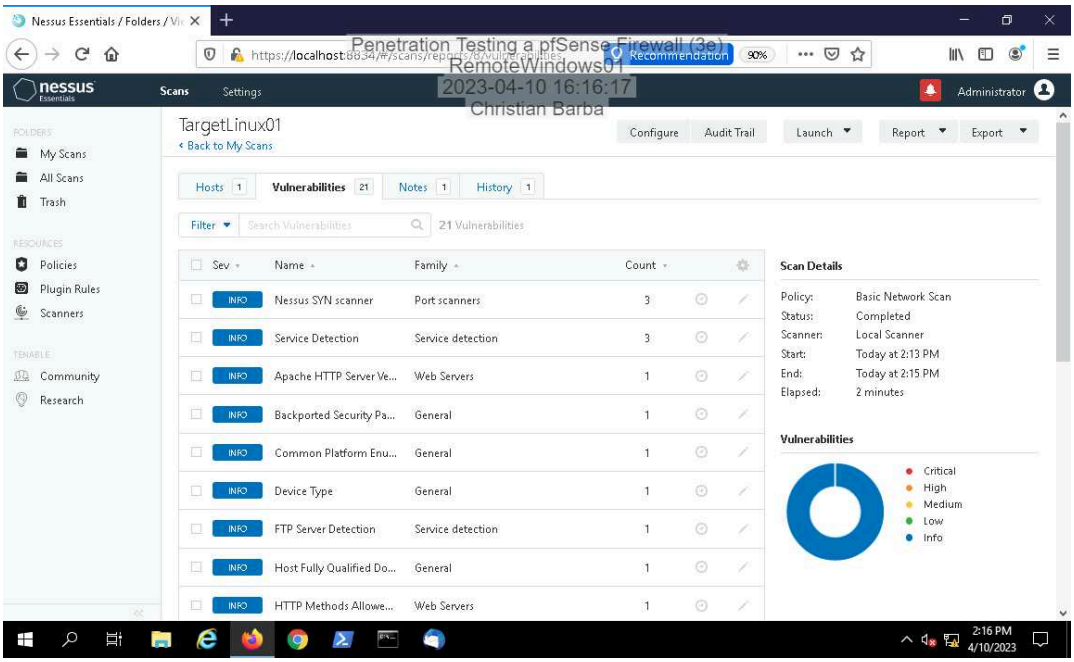
When using the internet to research more about the DMZ deployments, I came across multiple sources that explained some of the best practices to use. these practices include but are not limited to: enforce separation of duties and ensure that only the specific people that are trusted are the only ones able to monitor the system, make sure that the firewall is isolated, and regularly audit the firewall to ensure the functionality. Firstly, by letting only a few members of the organization monitor the firewall, there are less opportunities for someone to gain unnecessary access to the firewall. Limiting the amount of people with access will limit the accounts that could be hacked into, and there will be a small group of people to look at when things go wrong. Secondly, by isolating the firewall and ensuring there are no backdoors to the company's servers, there will be more complications for the malicious actor to go to in order to try to get on the protected servers. Since the firewall will not directly jump to the servers, there shouldn't be a way a for hackers to figure out the real IP address that the company uses. Lastly, checking the logs and making sure there are no threats will prove that the firewall is actually working. This could also be a potential mistake firewall managers run into because they put too much trust in the firewall to stop everything that gets thrown at it. There must be changes and updates to the firewall when they are needed and the only way to figure this out is to properly monitor it.

Part 2: Conduct a Penetration Test on the DMZ

Make a screen capture showing the **open ports on TargetLinux01 and the DMZ firewall interface**.



Make a screen capture showing the **vulnerability scan results**.



Part 3: Recommend Changes to the DMZ

Based on your research in Part 1 and your findings in Part 2, **prepare a brief summary** of recommended changes that Secure Labs on Demand should make to their DMZ deployment. Remember, your recommendations should apply to both the network configuration and the web server.

By using both nmap on the AttackLinux01 machine and Nessus on the RemoteWindows01 computer, I was able to witness a few vulnerabilities. These vulnerabilities were dealing with open ports and some outdated software. The open ports that were listed happened to be ports 21 (FTP), 22 (SSH), and port 80(HTTP). These ports are highly dangerous to have open because people would be able to attack file transfers and upload and/or steal information that others are sharing through this port. Port 22 is also dangerous because this has to deal with remote access for a machine, so if this port gets exploited, someone could gain full access to this vulnerable computer. Finally port 80 is a port that malicious actors could still use to access data that a host computer may hold. Also, Nessus shows that there are servers that are using these ports to function. My recommendations would be to patch up these ports as they are dangerous to have open, and they should check the firewall logs to see who has been interacting on these ports as well. The administrators should also close these servers only to those that should be allowed to have access to them. Leaving them open is irresponsible and dangerous because hackers could come and tinker with whatever they can find through these open ports. As far as the outdated and misconfigured software goes, the admin of the servers should ensure that the passwords are mandatory and up to date with patches that could be available to ensure security.