Student:	Email:
Stephen Asamoah	stephen.asamoah@howardcc.edu

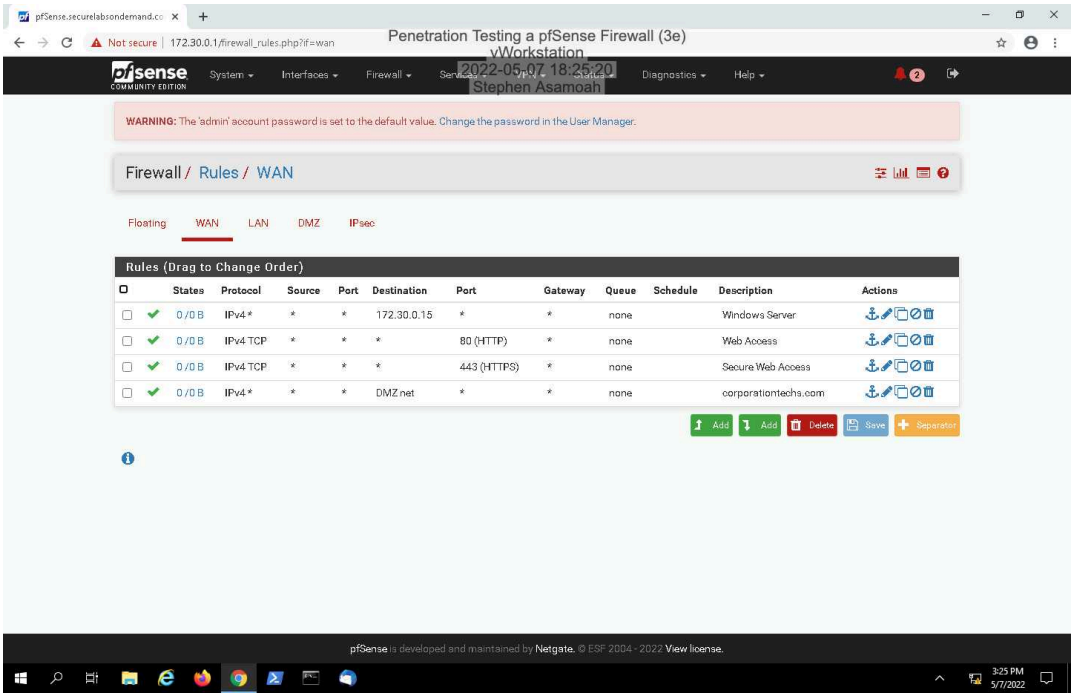
Time on Task:	Progress:
2 hours, 50 minutes	100%

Report Generated: Saturday, May 7, 2022 at 8:58 PM

Section 1: Hands-On Demonstration

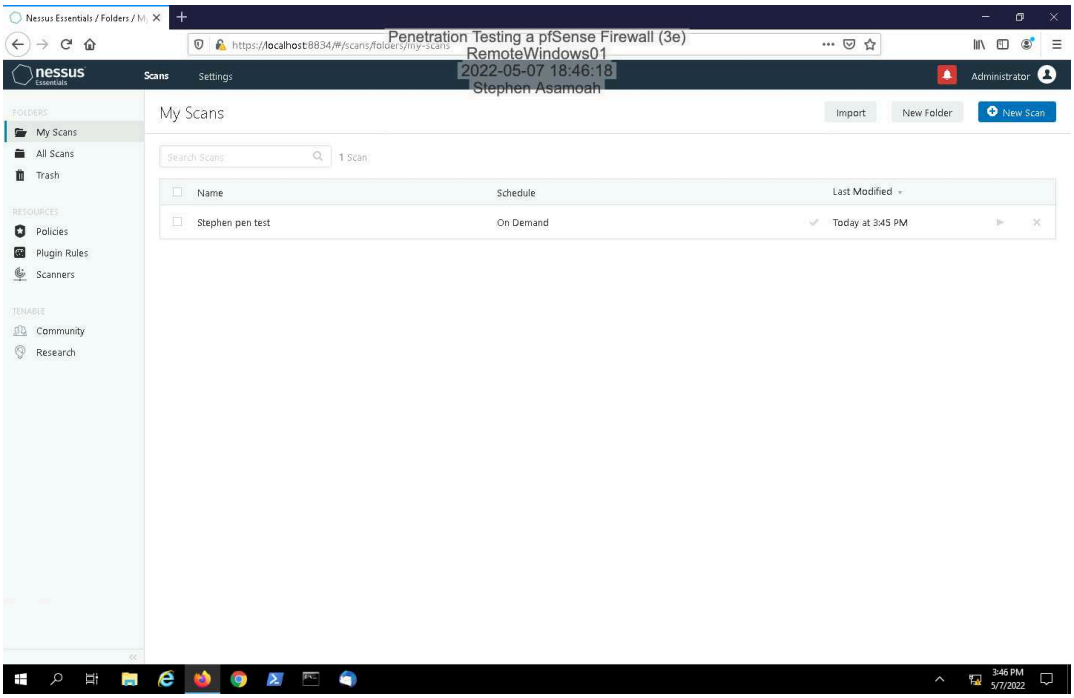
Part 1: Examine a pfSense Firewall Configuration

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

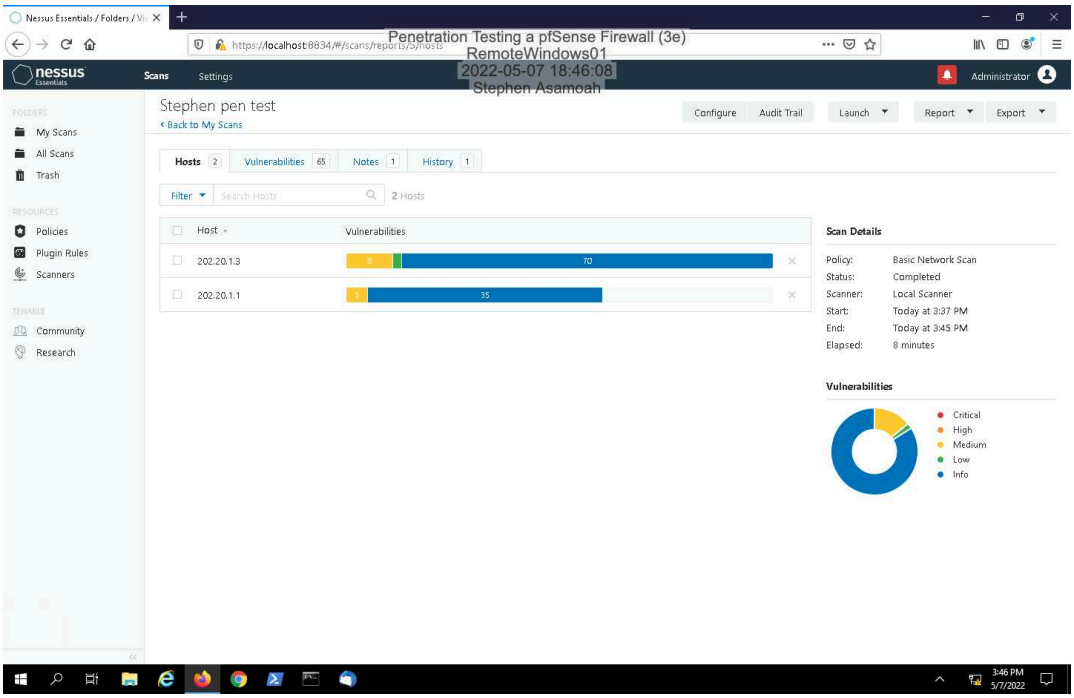


Part 2: Conduct a Penetration Test on the Network

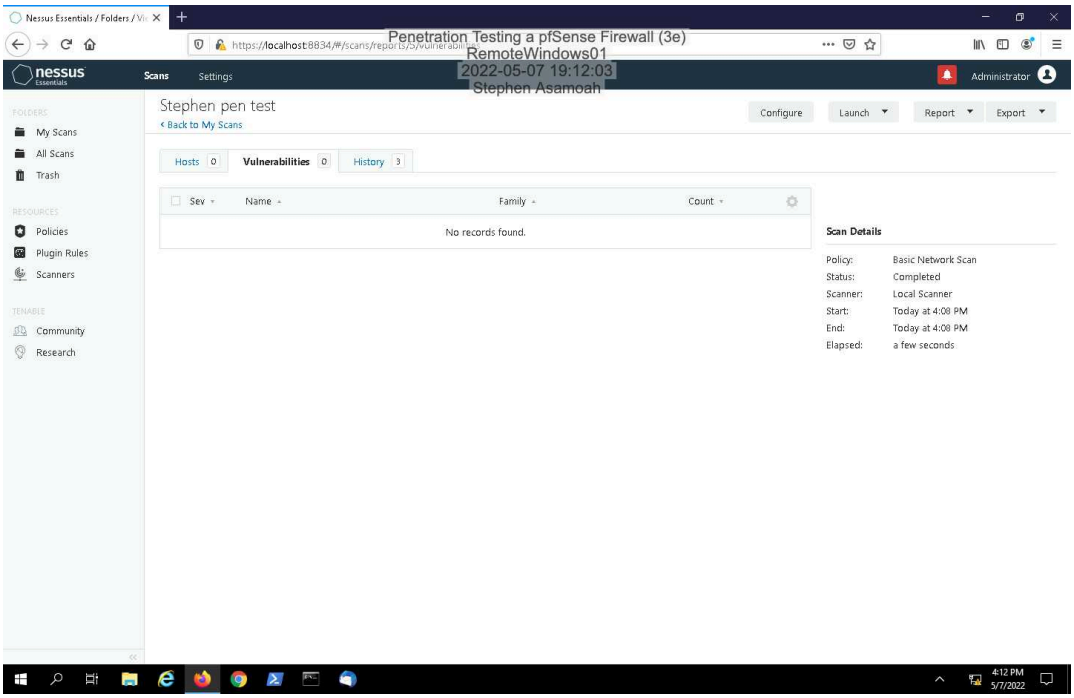
11. **Make a screen capture** showing the ***yourname*** **pen test scan results**.



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



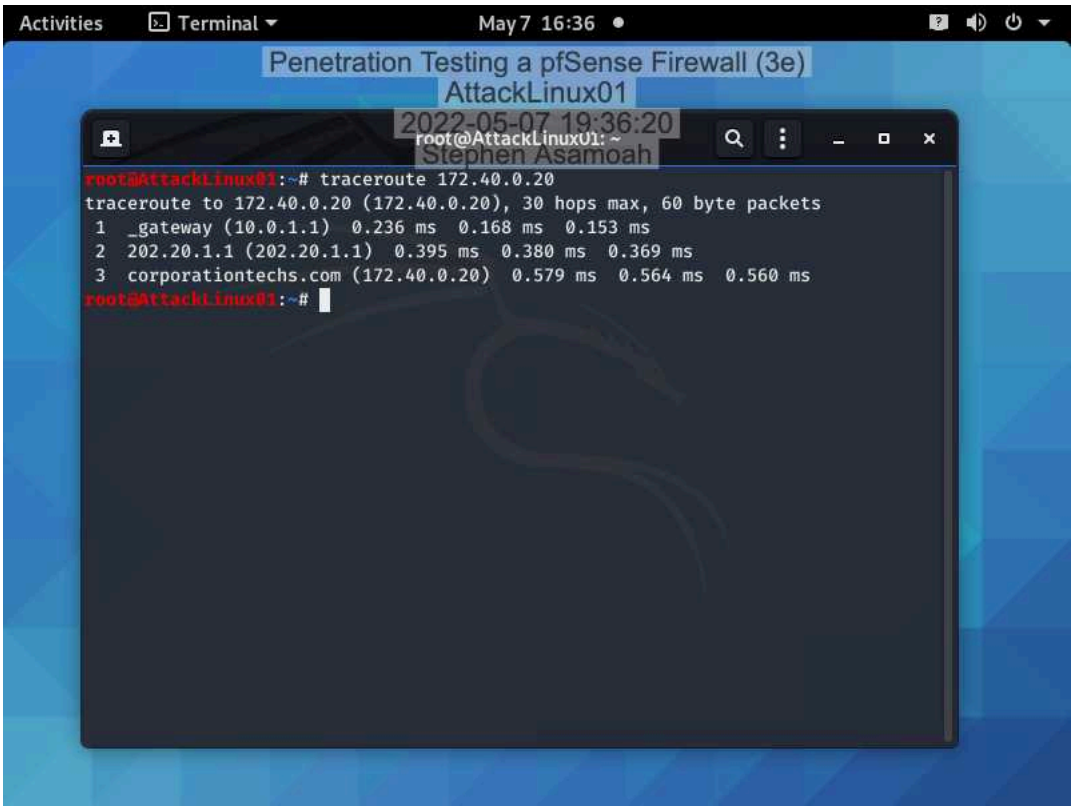
29. **Make a screen capture** showing the **updated vulnerability report summary**.



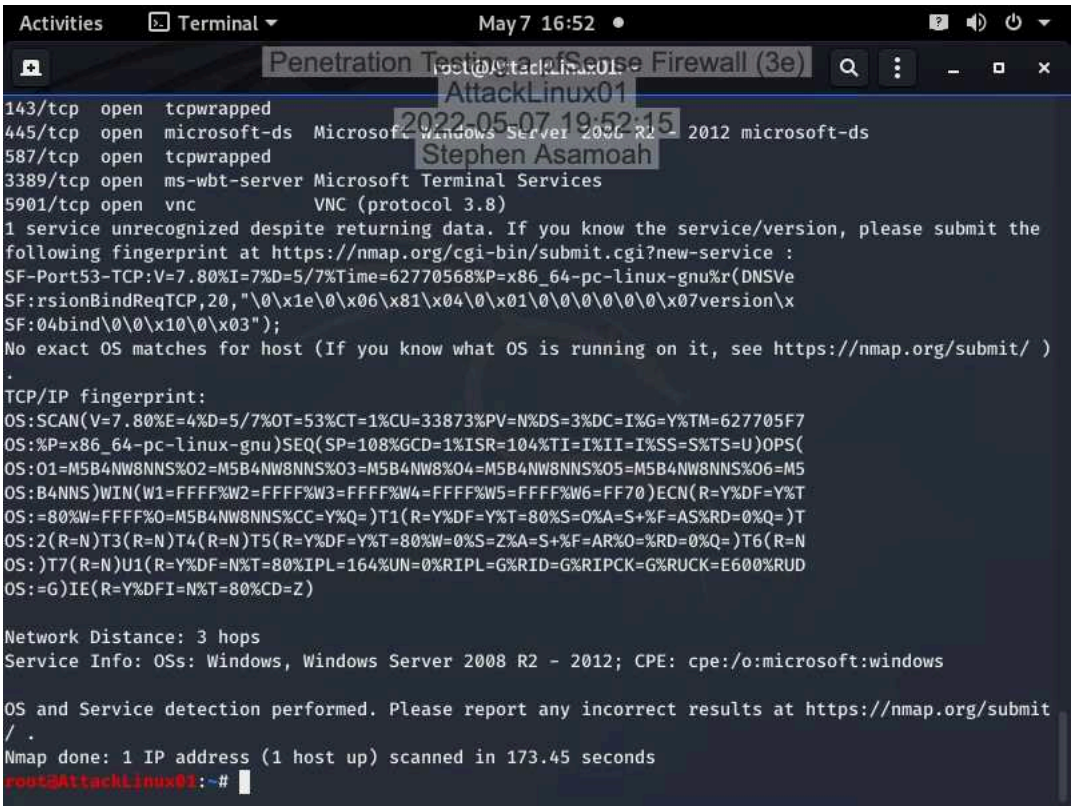
Section 2: Applied Learning

Part 1: Conduct a Port Scan on the Network

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

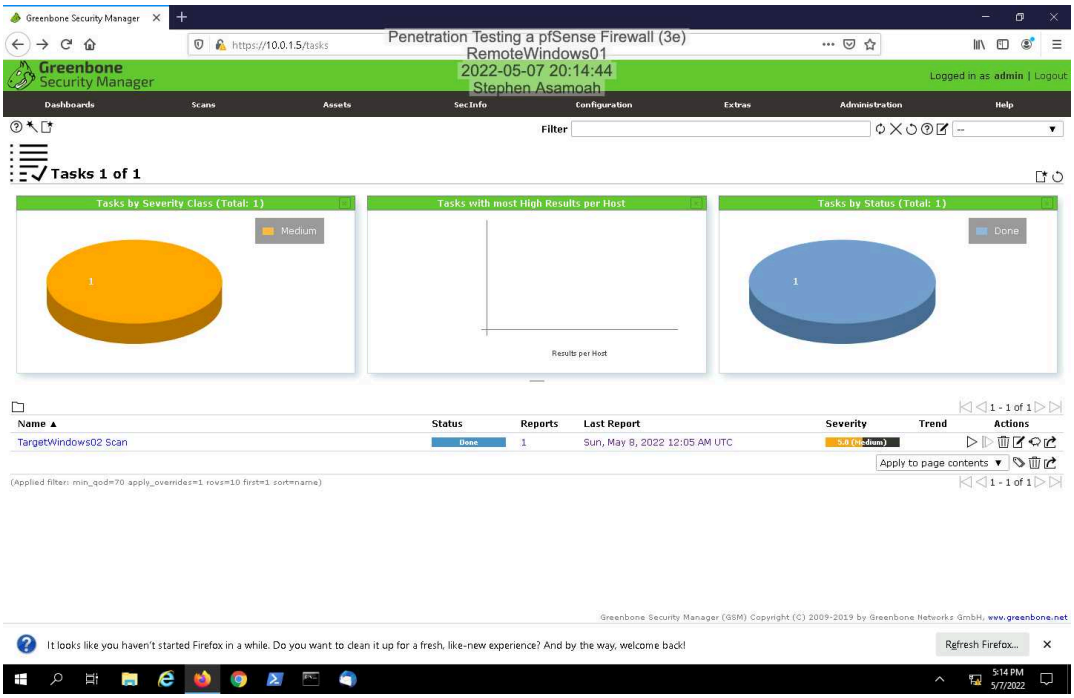


11. **Make a screen capture** showing the result of the **nmap scan with OS detection activated**.

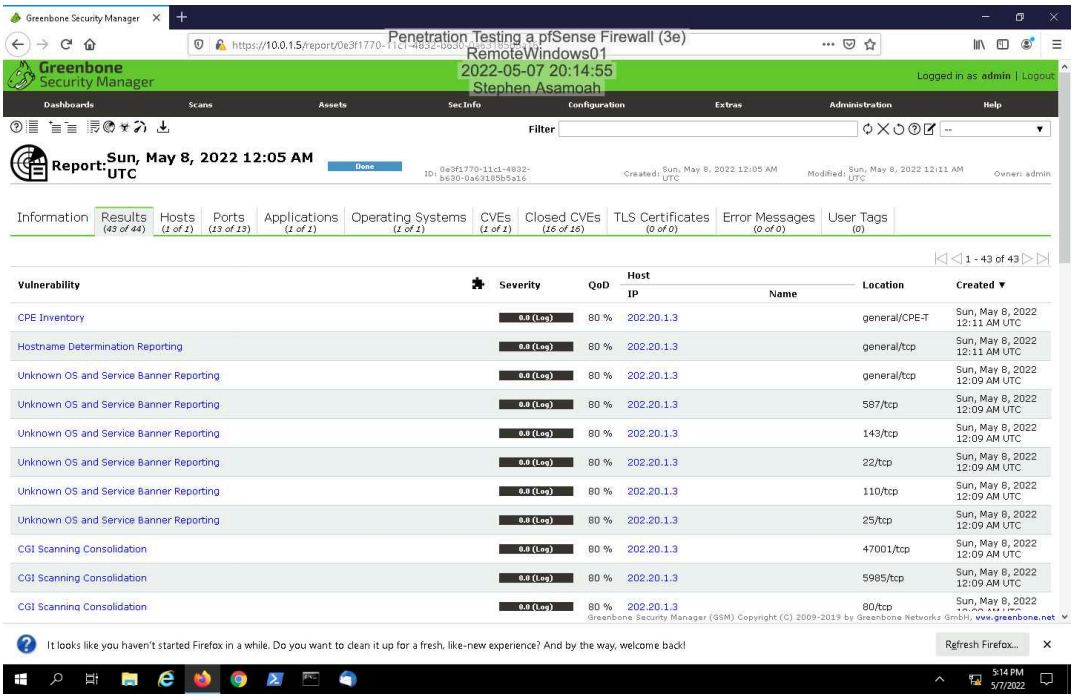


Part 2: Conduct a Vulnerability Scan on the Network

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

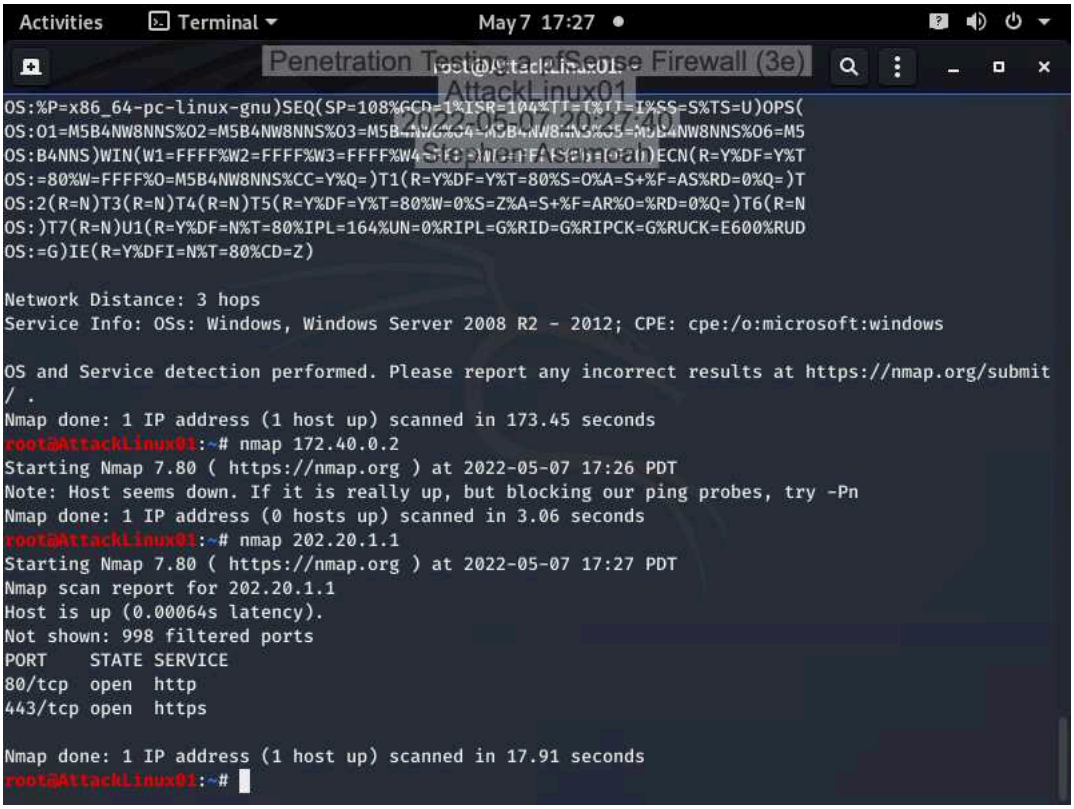
Part 1: Research DMZ Deployment Best Practices

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.

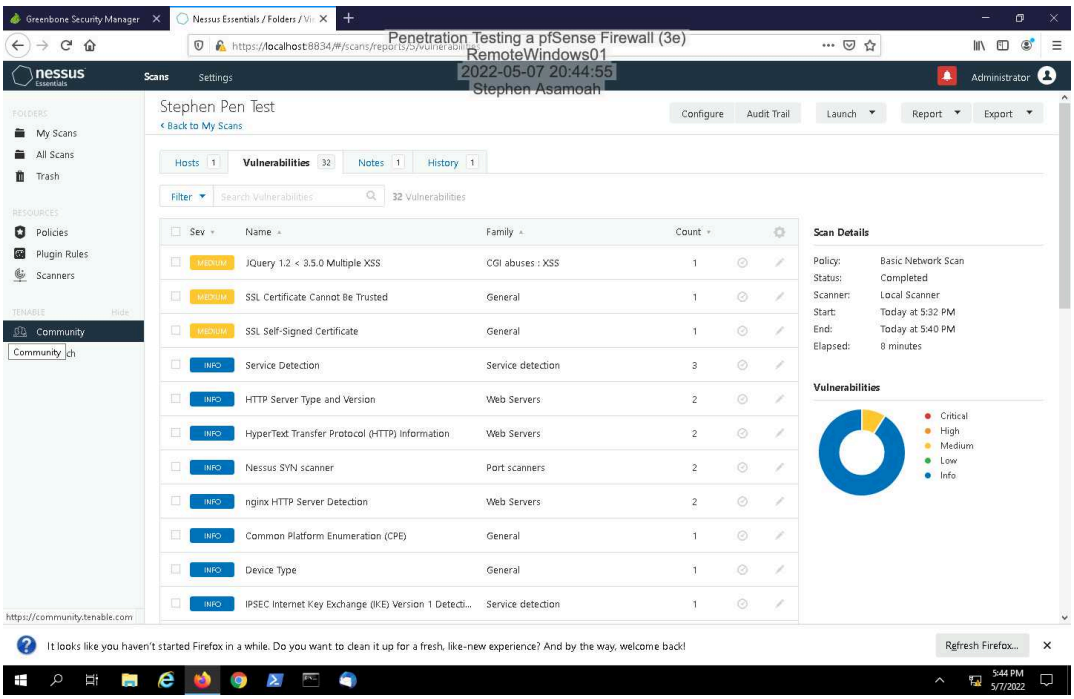
These are some of the 3 best DMZ deployment practices 1.Preserve isolation as much as possible 2.Practice good vulnerability management 3.Use application layer defenses for exposed services One potential mistake is Monitoring. The DMZ should be one of the major focus of an organization's network. IDS, systems logs and other tools must be used to remain vigilant for signs of attacks

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.

There should be regular software update on the server. For example, we saw in the vulnerability results that, the Jquery hosted on the remote server needs an update. Failure to perform system updates and patches is a major vulnerability to network security. Secure Lab on demand should also ensure they are using better SSL certificate