Student:	Email:
Saliman Zadran	sz2740@email.vccs.edu

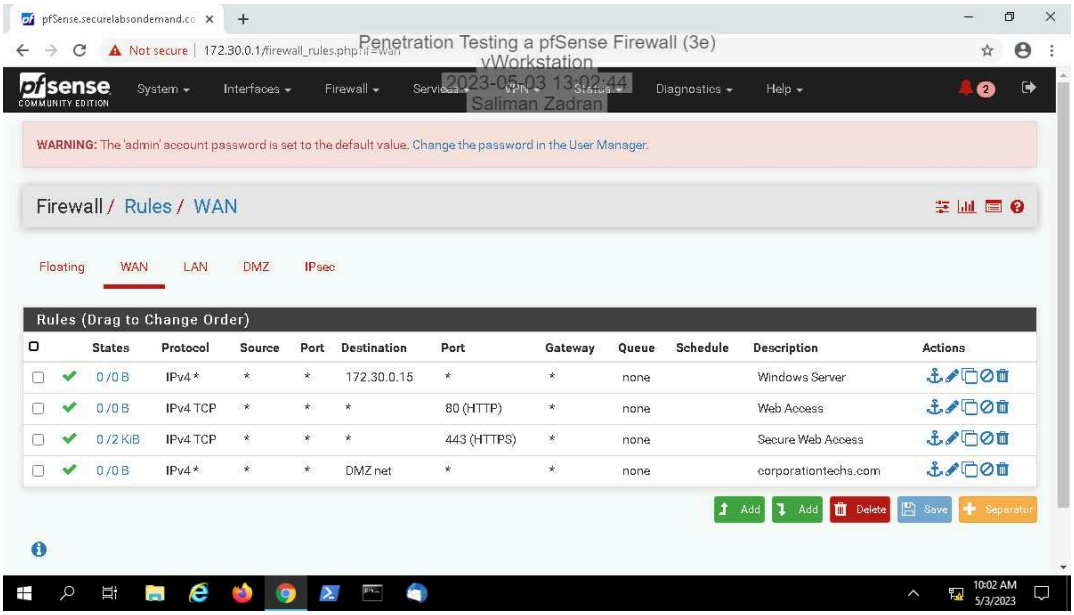
Time on Task:	Progress:
4 hours, 12 minutes	100%

Report Generated: Wednesday, May 3, 2023 at 2:56 PM

Section 1: Hands-On Demonstration

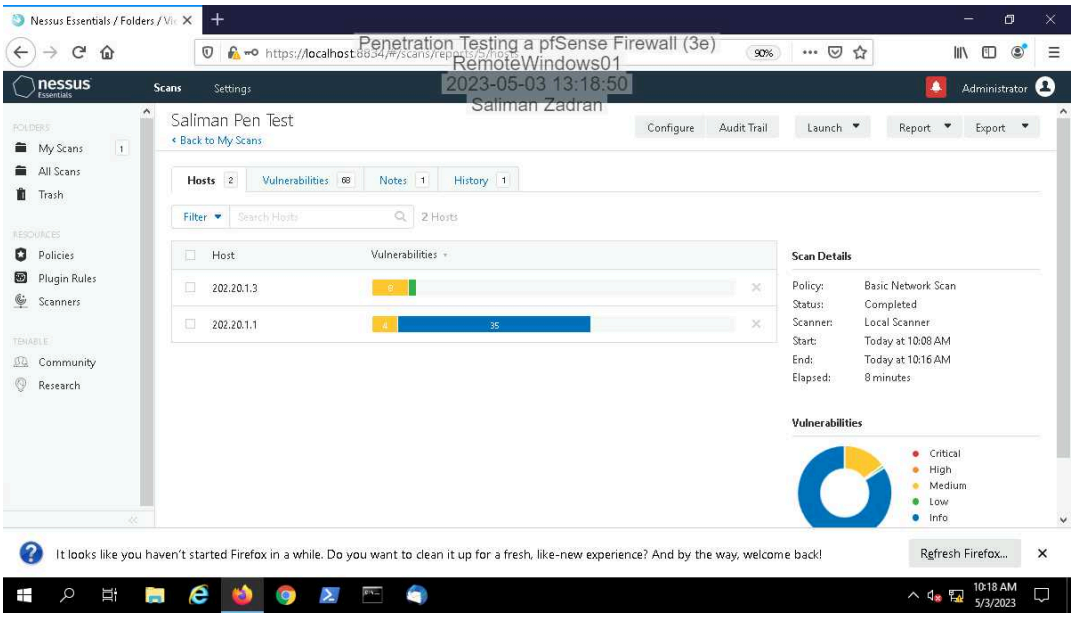
Part 1: Examine a pfSense Firewall Configuration

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

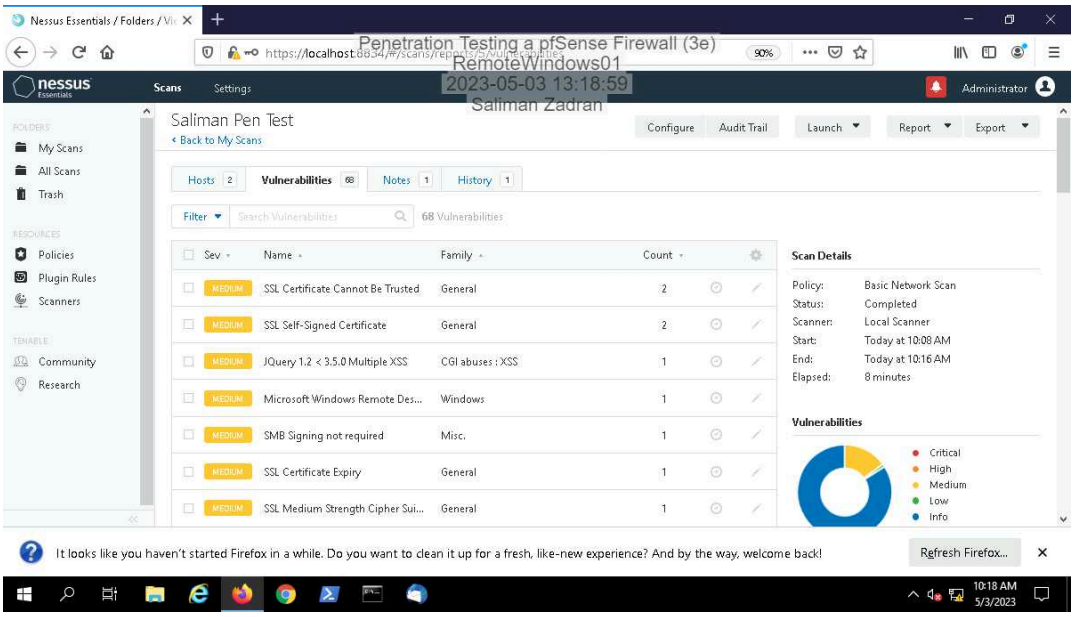


Part 2: Conduct a Penetration Test on the Network

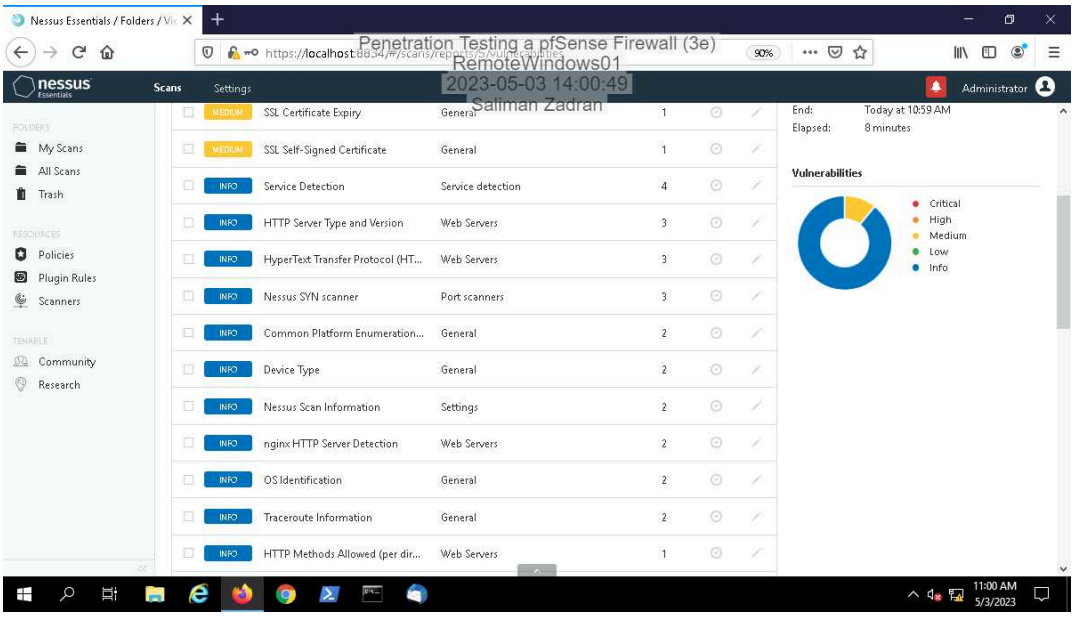
11. **Make a screen capture** showing the ***yourname*** **pen test scan results**.



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



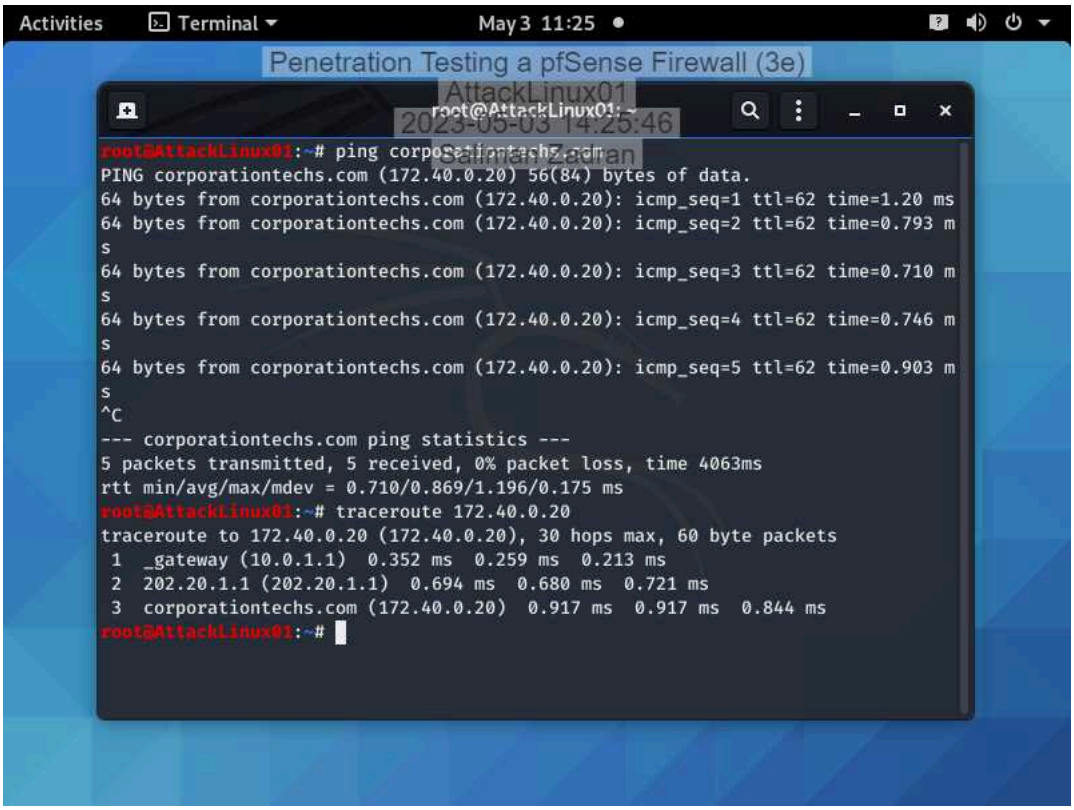
30. **Make a screen capture** showing the **updated vulnerability report summary**.



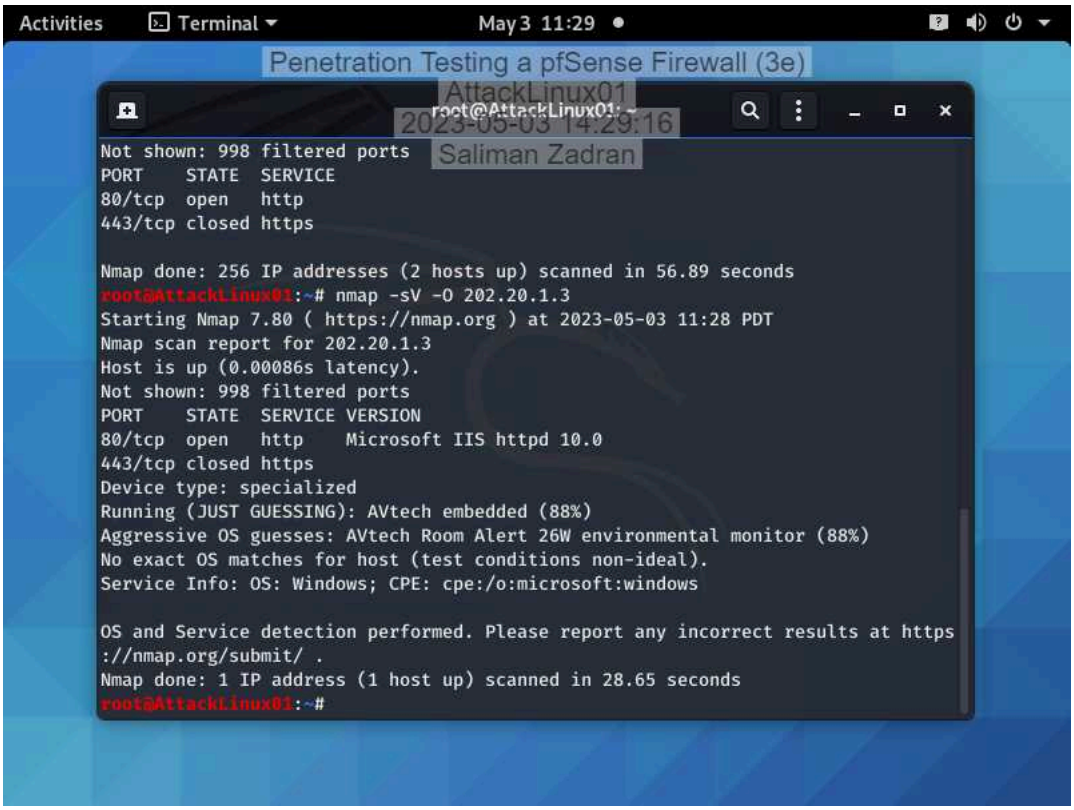
Section 2: Applied Learning

Part 1: Conduct a Port Scan on the Network

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

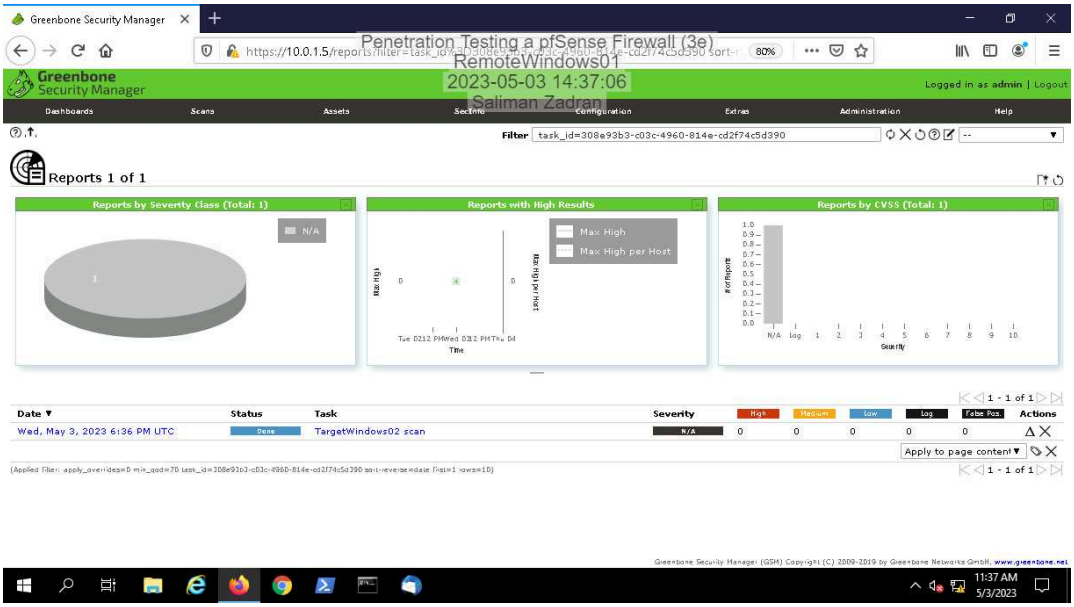


11. **Make a screen capture** showing the result of the **nmap scan with OS detection activated**.

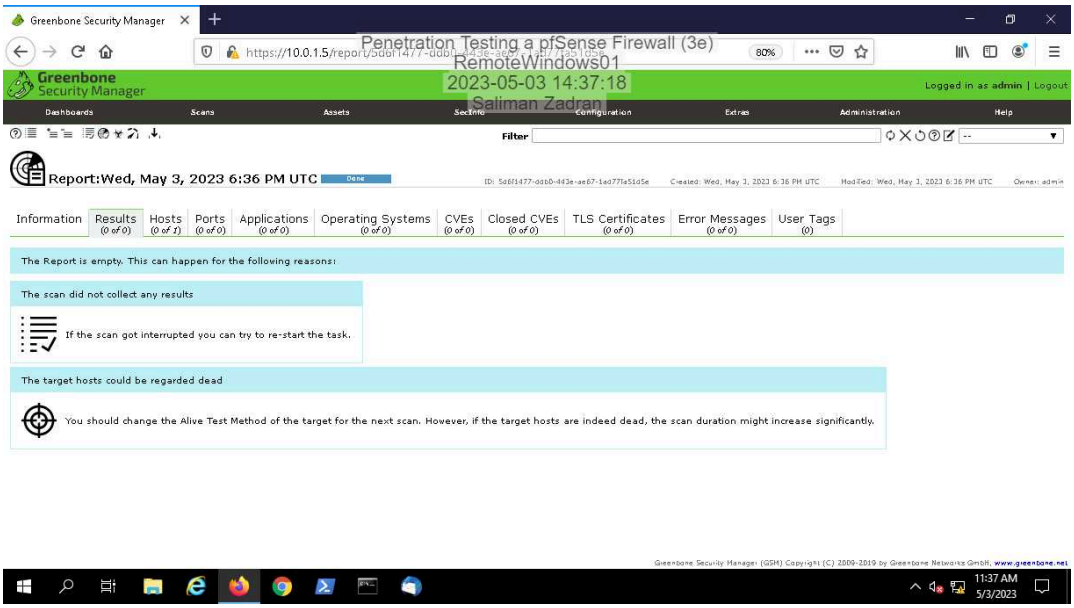


Part 2: Conduct a Vulnerability Scan on the Network

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

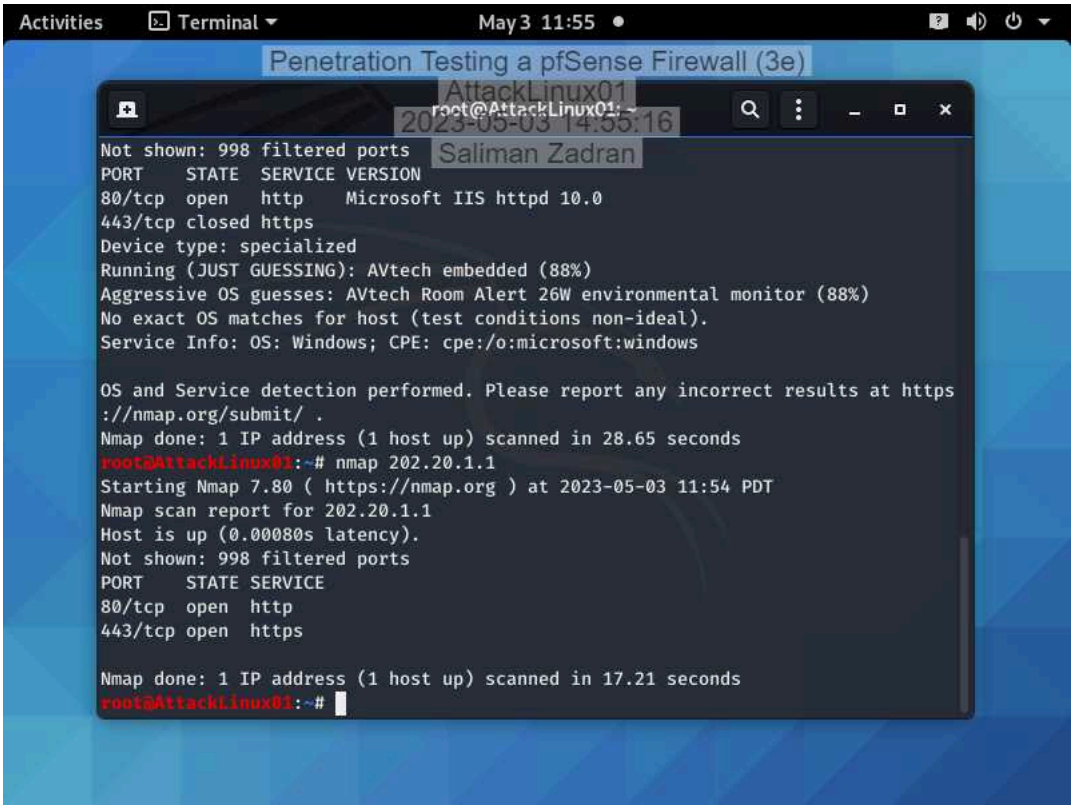
Part 1: Research DMZ Deployment Best Practices

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.

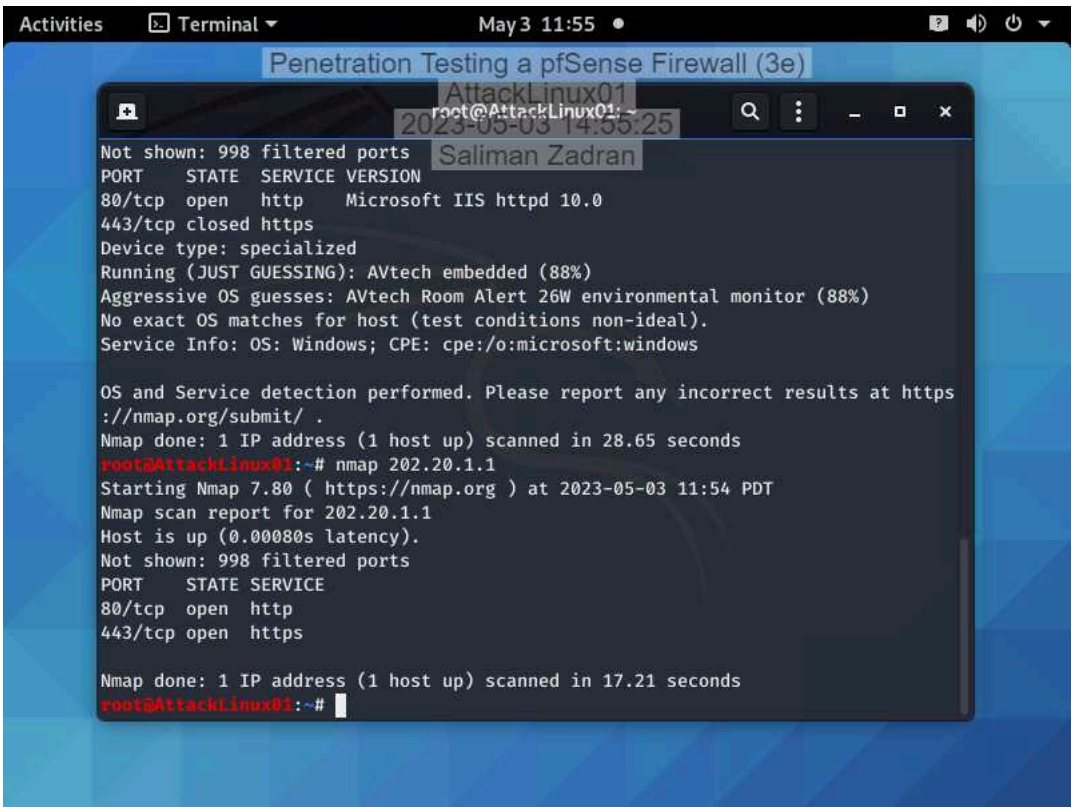
Three best practices include: Hardening and isolating service console, clearly labeling each zone within the DMZ, and regular auditing of the configuration. A mistake would be not auditing the configuration regularly.

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.

Unnecessary ports should be closed, ICMP ping requests need to be locked as well. Discoverability of hosts is too easy.