Student:	Email:
Belizaire Bassette II	bebasset@syr.edu

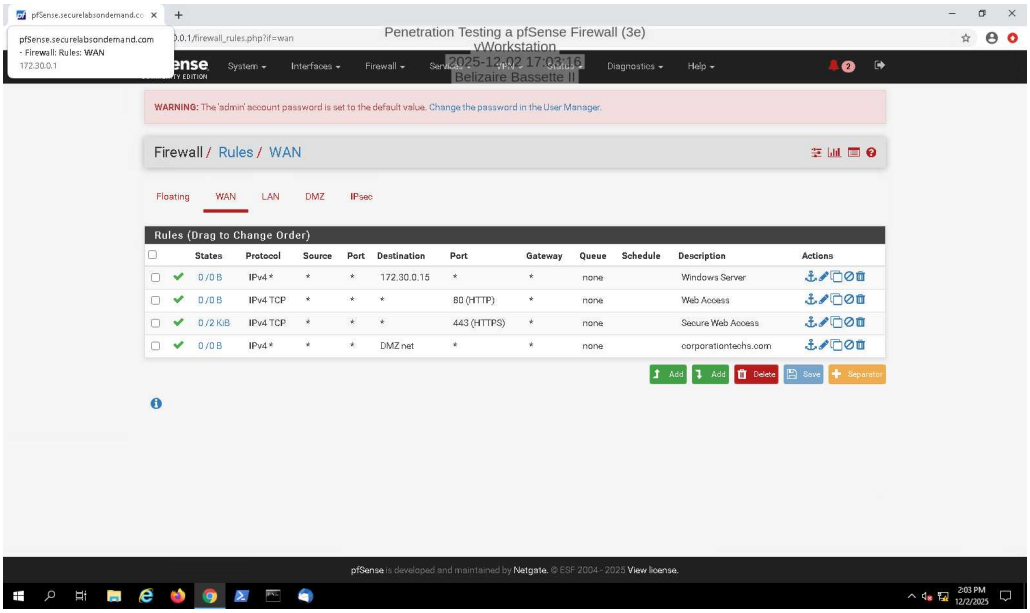
Time on Task:	Progress:
57 hours, 52 minutes	100%

Report Generated: Wednesday, December 3, 2025 at 6:48 PM

Section 1: Hands-On Demonstration

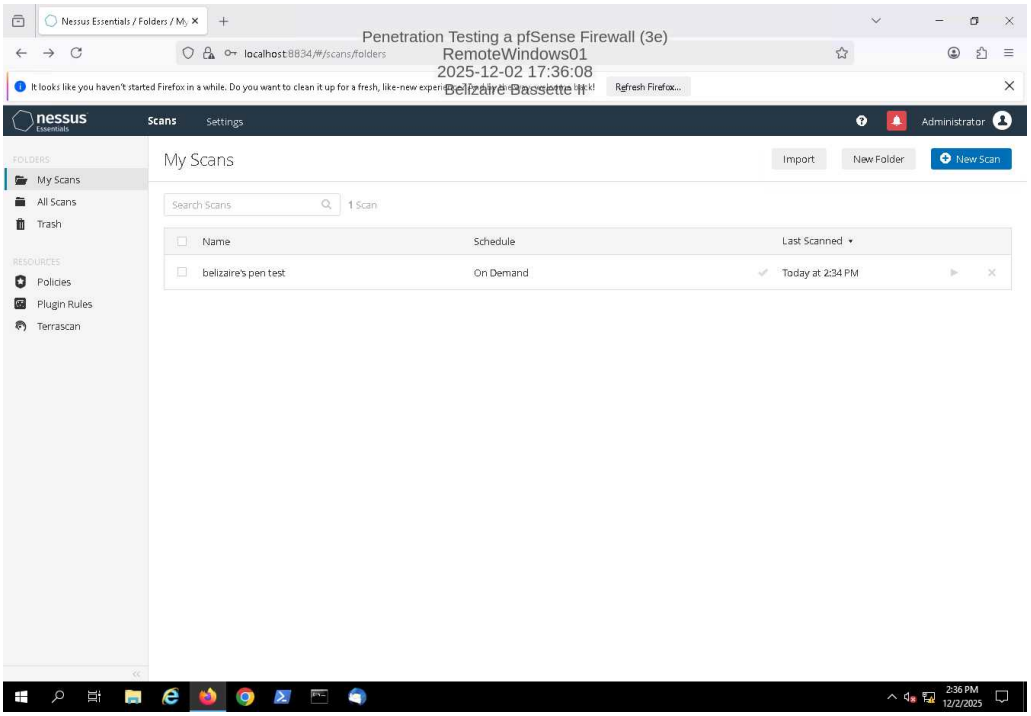
Part 1: Examine a pfSense Firewall Configuration

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

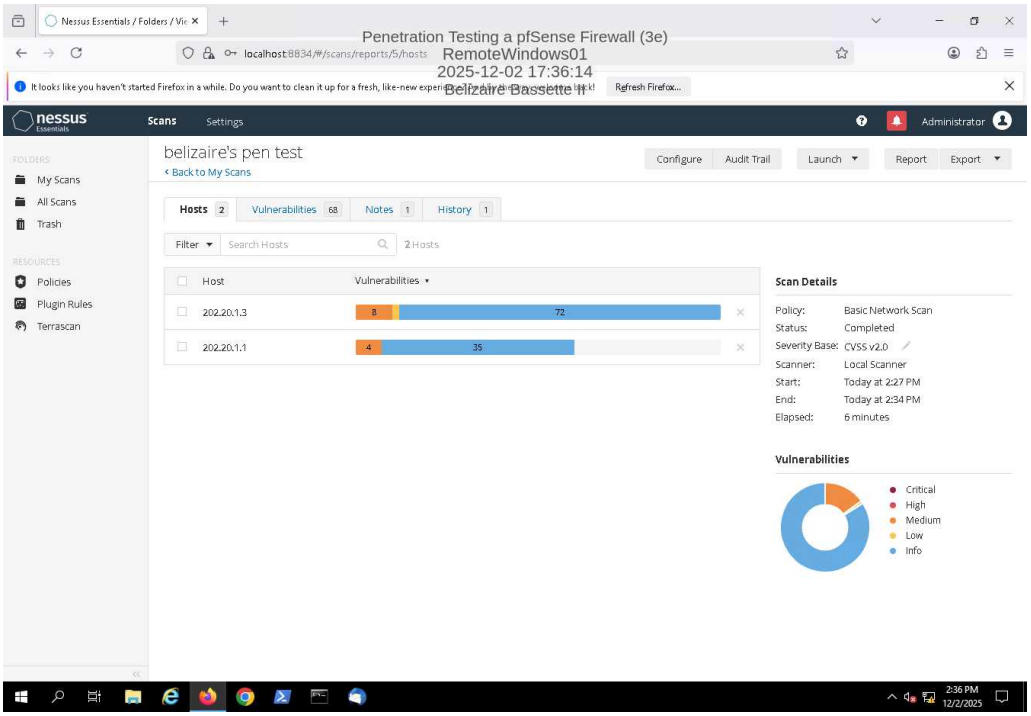


Part 2: Conduct a Penetration Test on the Network

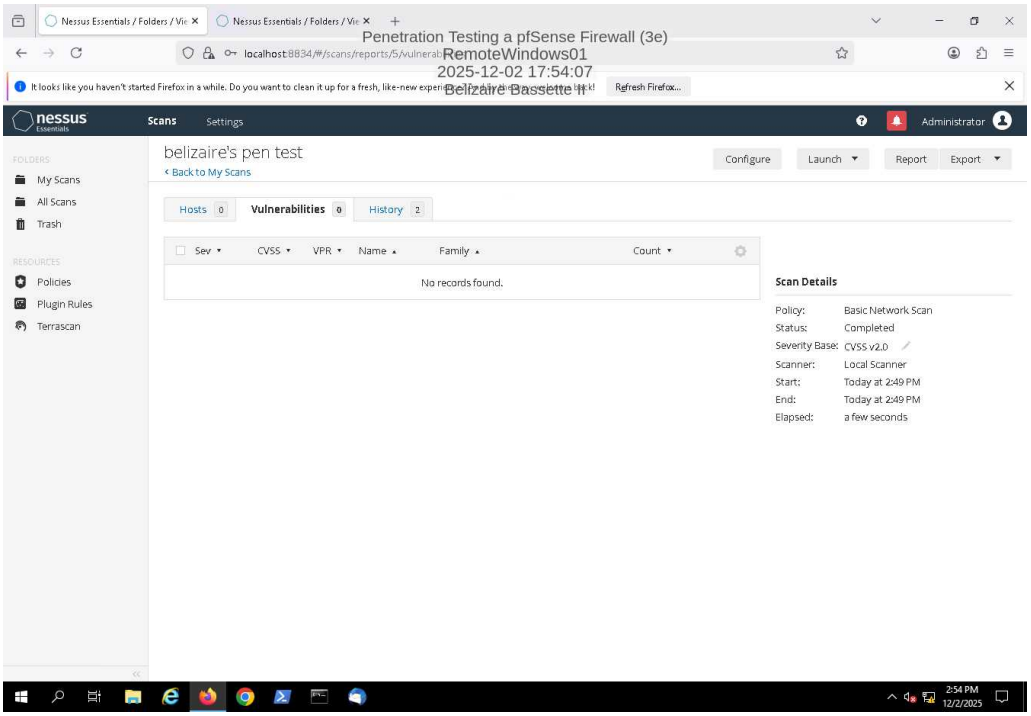
11. **Make a screen capture** showing the ***yourname*** **pen test scan results**.



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



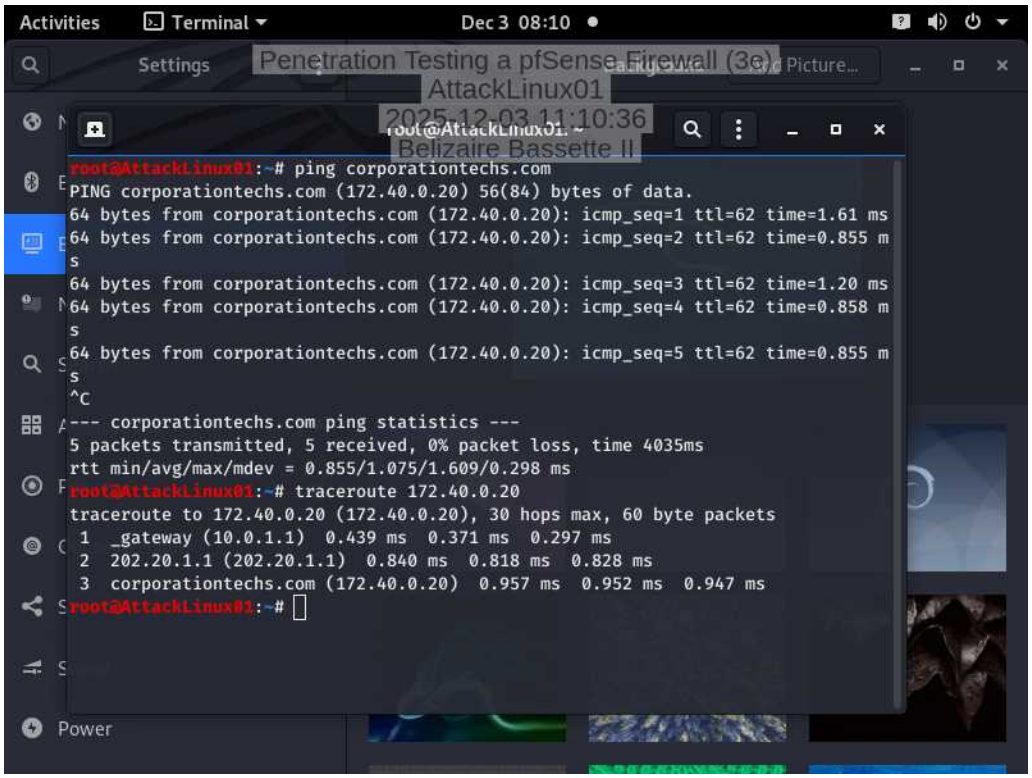
30. **Make a screen capture** showing the **updated vulnerability report summary**.



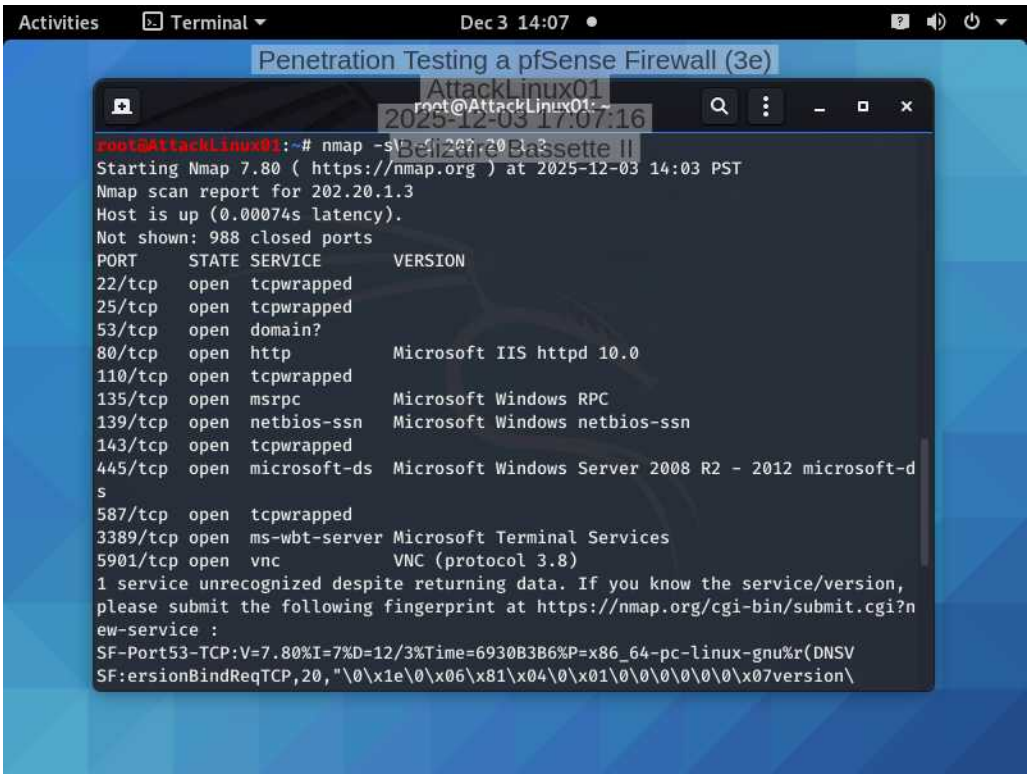
Section 2: Applied Learning

Part 1: Conduct a Port Scan on the Network

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

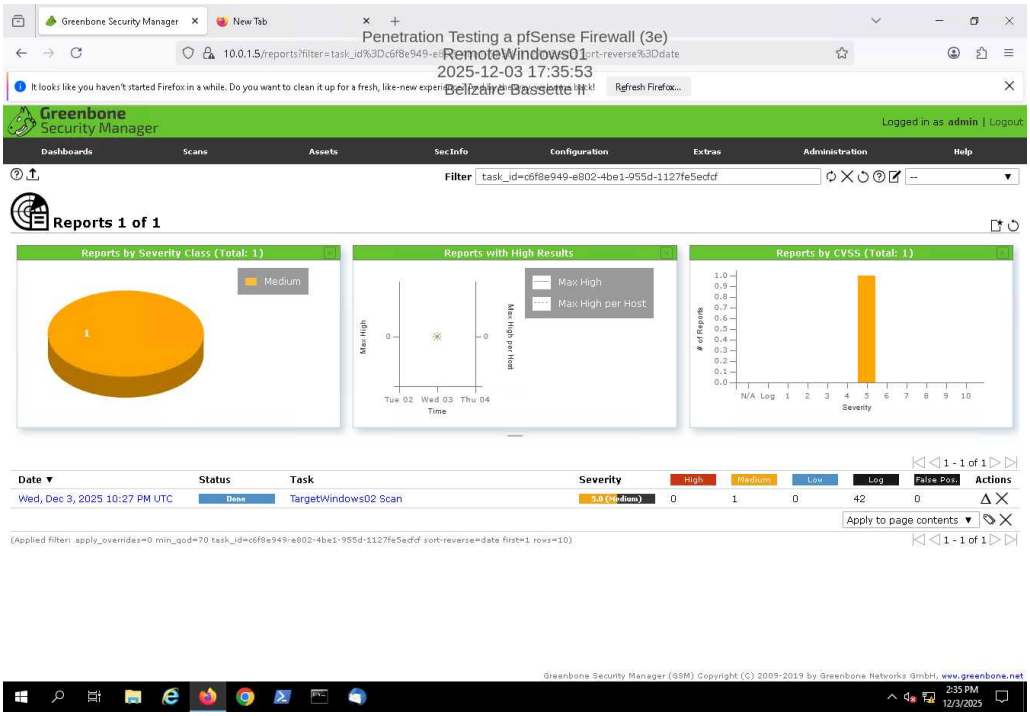


11. **Make a screen capture** showing the result of the **nmap scan with OS detection activated**.

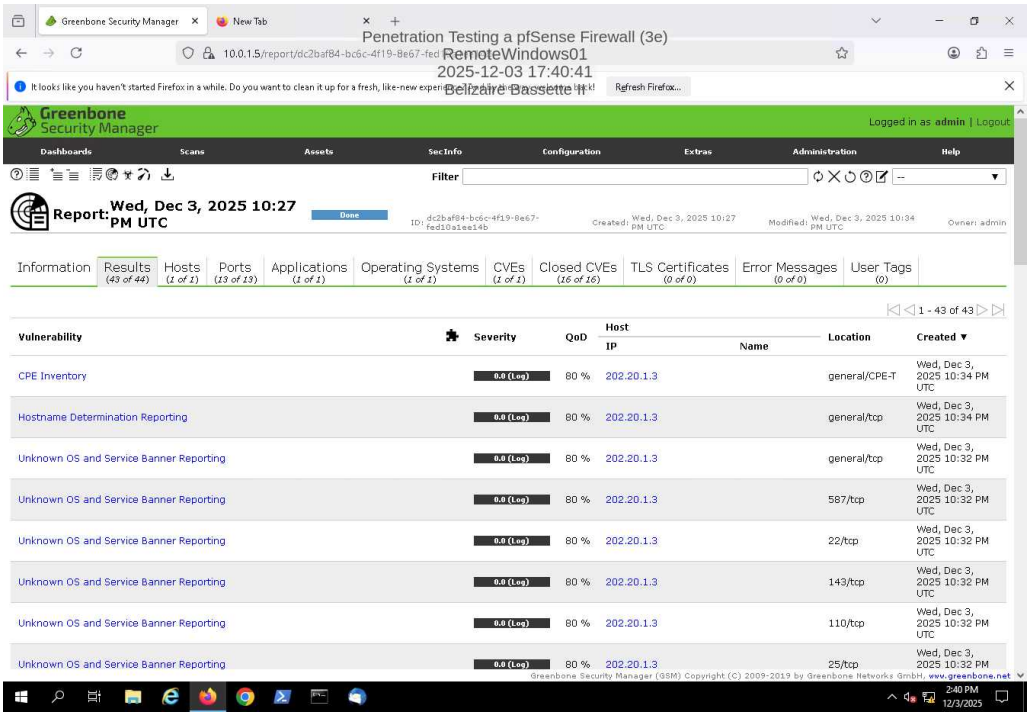


Part 2: Conduct a Vulnerability Scan on the Network

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

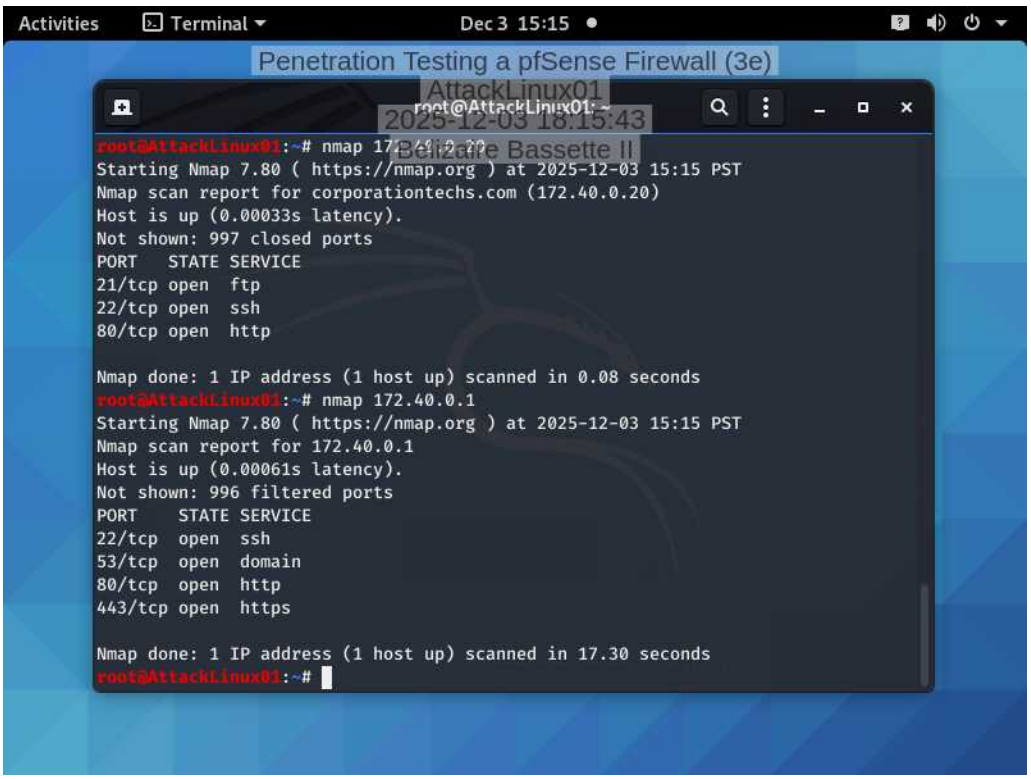
Part 1: Research DMZ Deployment Best Practices

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.

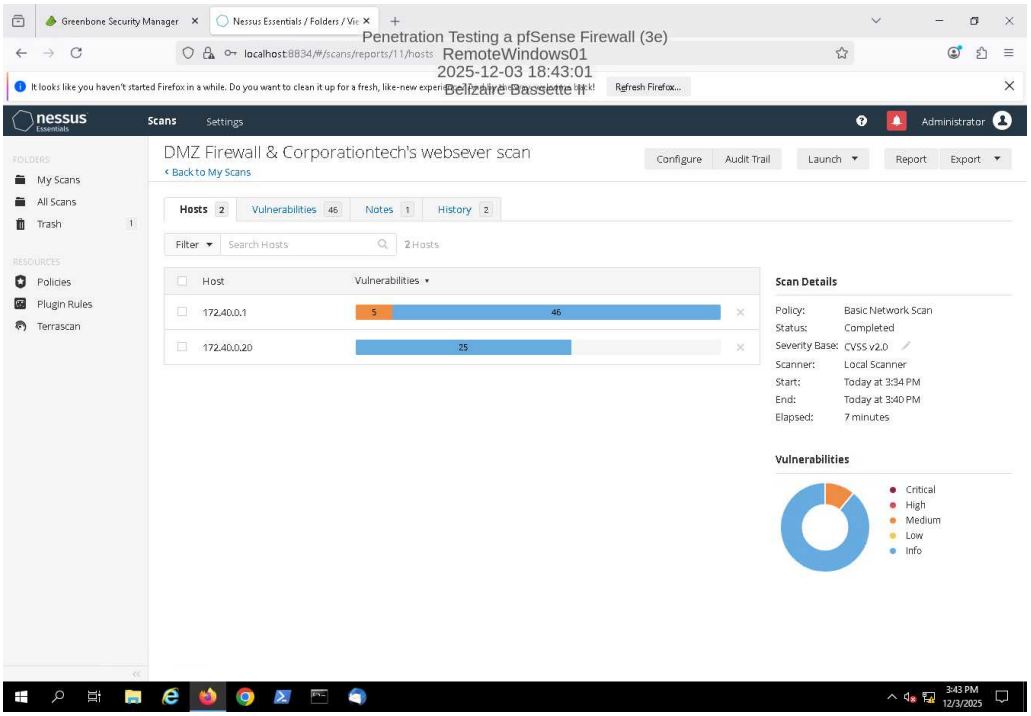
#1 Use multiple firewalls {layered security) - use two separate fiewalls: one between the Internet -> DMZ- One between the DMZ -> internal network
#2 Strict, Minimal Access Rules Inbound: Allow only required ports (ex: HTTP/HTTPS for a web server)
Outbound: Restrict DMZ servers so they cannot initiate arbitrary connections
East/West: Limit DMZ server-to-server communicationWhy: Reduces the attack surface and prevents lateral movement.
#3 Continuous Monitoring and Logging
DMZ systems are exposed to the internet and they must be heavily monitored.
Implement:
IDS/IPS
SIEM log forwarding
Real-time alerting
Vulnerability scans and patching
Benefit: You detect attacks early and reduce the chance of unnoticed breaches.
A Common Mistake/Vulnerability — Overtrusting the DMZ (Too Much Internal Access)
The biggest mistake: Allowing DMZ systems to directly access internal networks or sensitive databases.

Part 2: Conduct a Penetration Test on the DMZ

Make a screen capture showing the **open ports on the corporationtechs.com web server 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.

Strict, Minimal Access Rules

Only allow exactly what's needed — nothing more.
Rules should be:

Inbound: Allow only required ports (ex: HTTP/HTTPS for a web server)

Outbound: Restrict DMZ servers so they cannot initiate arbitrary connections

East/West: Limit DMZ server-to-server communication