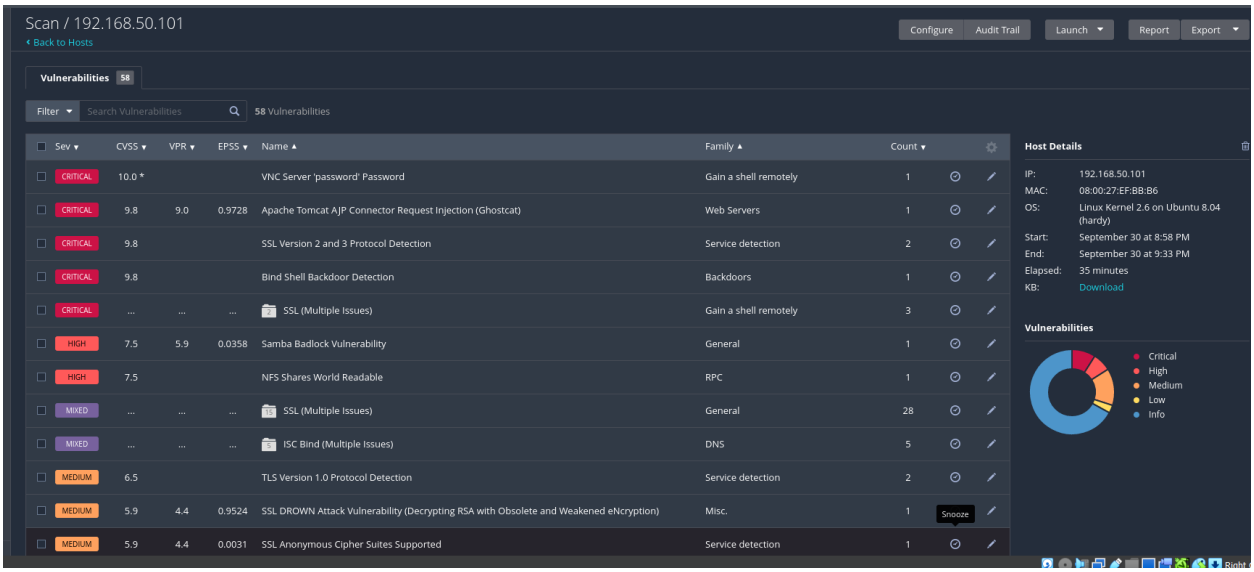
# Comparison Report: Initial Scan vs. Post-Remediation Scan

## Summary:

This report compares the results of the first vulnerability scan and the final scan conducted after remediation of critical vulnerabilities on the Metasploitable machine. The goal was to remediate high-risk vulnerabilities identified in the initial scan and improve the security posture of the system.

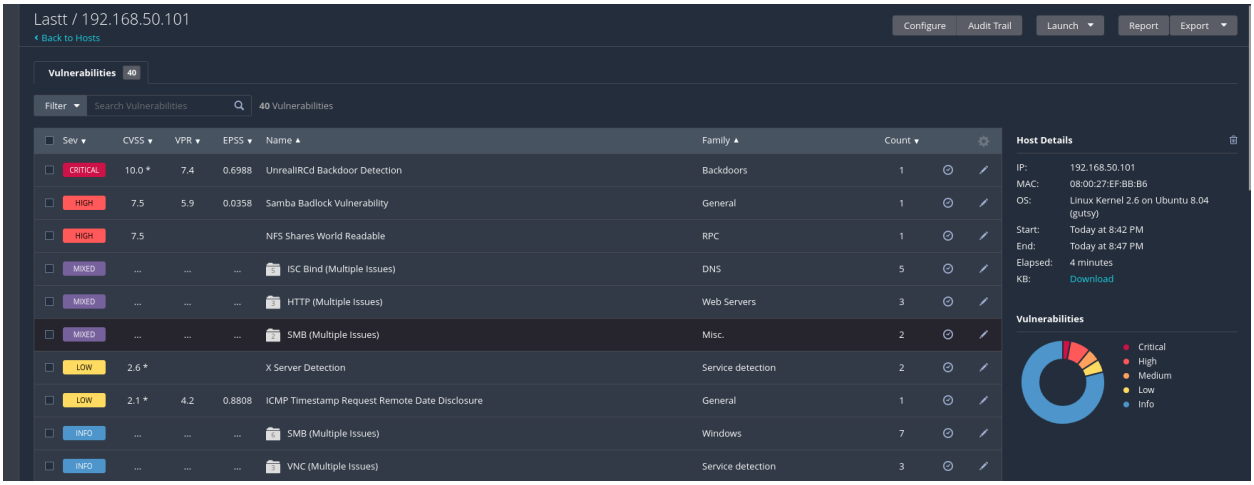
## Initial Scan Results (Before Remediation):

The initial scan identified 58 vulnerabilities in total, including critical, high, and medium severity issues. Below are the key vulnerabilities found:



## Final Scan Results (Post-Remediation):

After the remediation actions, a second scan was conducted to verify the success of the fixes. Below is a comparison of the vulnerabilities that were addressed:




## Post-Remediation Observations:

- Overall Reduction: The critical vulnerabilities were reduced or mitigated using a combination of password hardening and network-layer controls.
- Firewall as Temporary Mitigation: As the Metasploitable machine was too outdated to apply software patches, the firewall served as an effective mitigation for SSL-related vulnerabilities.
- **Recommendations for Future Scans:**
    - Continue to monitor the blocked ports to ensure that no new vulnerabilities arise.
    - Upgrade the system if feasible, or consider isolating the system in a secure network environment due to its outdated software.
    - Regularly update passwords and restrict user access to prevent future backdoor installations.

**Conclusion:**

While not all vulnerabilities could be remediated due to the limitations of the outdated Metasploitable system, significant progress was made by hardening passwords and using firewall rules to block vulnerable services. The second scan shows that critical vulnerabilities were either resolved or mitigated, providing a more secure environment.