Nmap Scan Result

a. Summary - No. of Vulnerable Ports Open

Total Count : : **7**

b. Detailed Report

i. Port Number: 22

ii. Protocol: tcp

iii. Service: ssh

iv. Recommended Action or Best Practices: Ensure strong SSH configurations, including key-based authentication and disabling root login.

i. Port Number: 25

ii. Protocol: tcp

iii. Service: smtp

iv. Recommended Action or Best Practices: Implement proper email filtering and authentication mechanisms.

i. Port Number: 80

ii. Protocol: tcp

iii. Service: http

iv. Recommended Action or Best Practices: Apply security headers, keep software updated, and implement secure coding practices.

i. Port Number: 110

ii. Protocol: tcp

iii. Service: pop3

iv. Recommended Action or Best Practices: Consider using POP3 over SSL/TLS (POP3S) for secure email retrieval.

i. Port Number: 443

ii. Protocol: tcp

iii. Service: https

iv. Recommended Action or Best Practices: Apply security best practices for HTTPS services.

i. Port Number: 587

ii. Protocol: tcp

iii. Service: submission

iv. Recommended Action or Best Practices: Secure email submission by using submission over SSL/TLS.

i. Port Number: 993

ii. Protocol: tcp

iii. Service: imaps

iv. Recommended Action or Best Practices: Implement IMAPS (IMAP over SSL/TLS) for secure email access.

ZAP Scan Result

a. Summary

i. No. of Total Vulnerabilities Identified: : 0

ii. No. of Total Vulnerabilities Identified grouped on Risk Rating: : {}

b. Detailed Report