Nessus Vulnerability Assessment

Presented By Team 3

Content Overview

1. Introduction
2. Objective
3. Credentials Scan
4. Web Application Vulnerability Scan
5. Recommendations

Executive Summary

At CyberTech Solutions, our cybersecurity team was tasked with strengthening the organization’s internal security posture through a comprehensive vulnerability assessment.
This initiative involved performing credentialed scans on Linux servers, conducting web application testing, configuring automated reporting via Nessus, and patching identified vulnerabilities.
The goal was to proactively detect potential weaknesses, enhance system resilience, and ensure a secure and compliant infrastructure across all critical assets.

Objective

Conduct Credentialed Scans

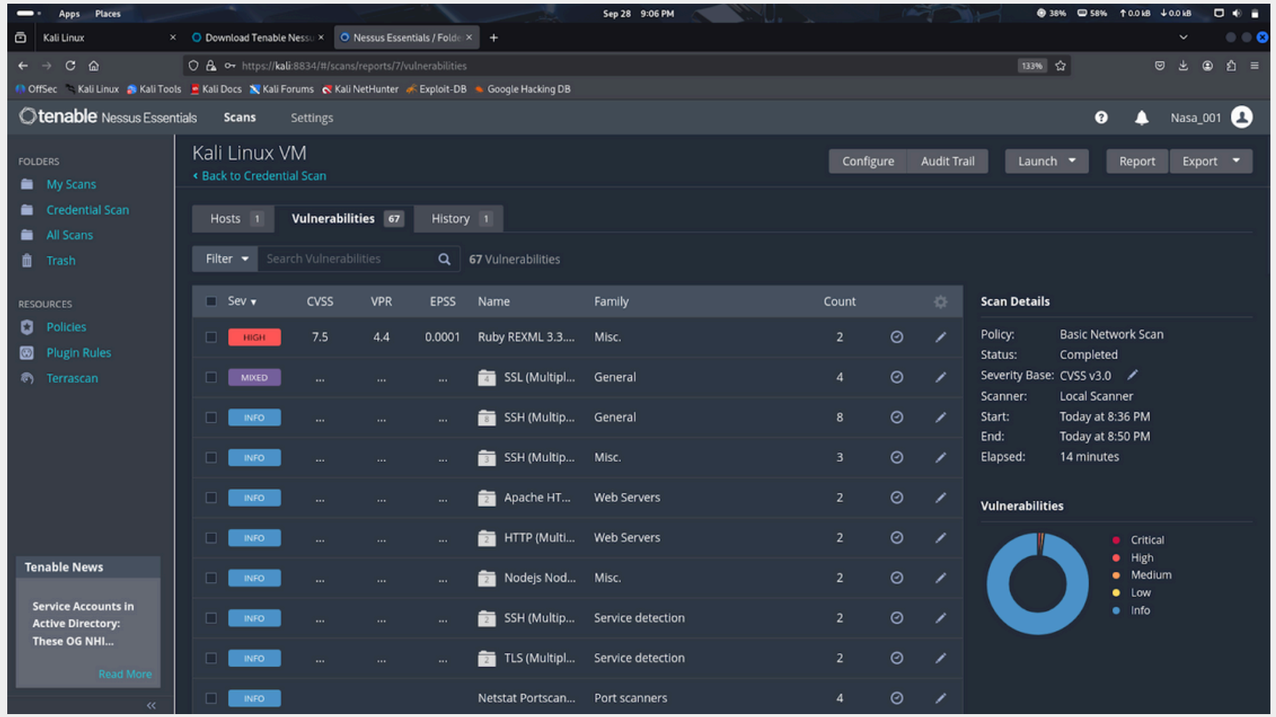
Execute Web Application Scan

Configure Automated Email Reporting

Implement Patch Management

Credentialed Vulnerability Scan

- Assess the internal Linux infrastructure for security weaknesses using Nessus with OpenSSH-based credential authentication.

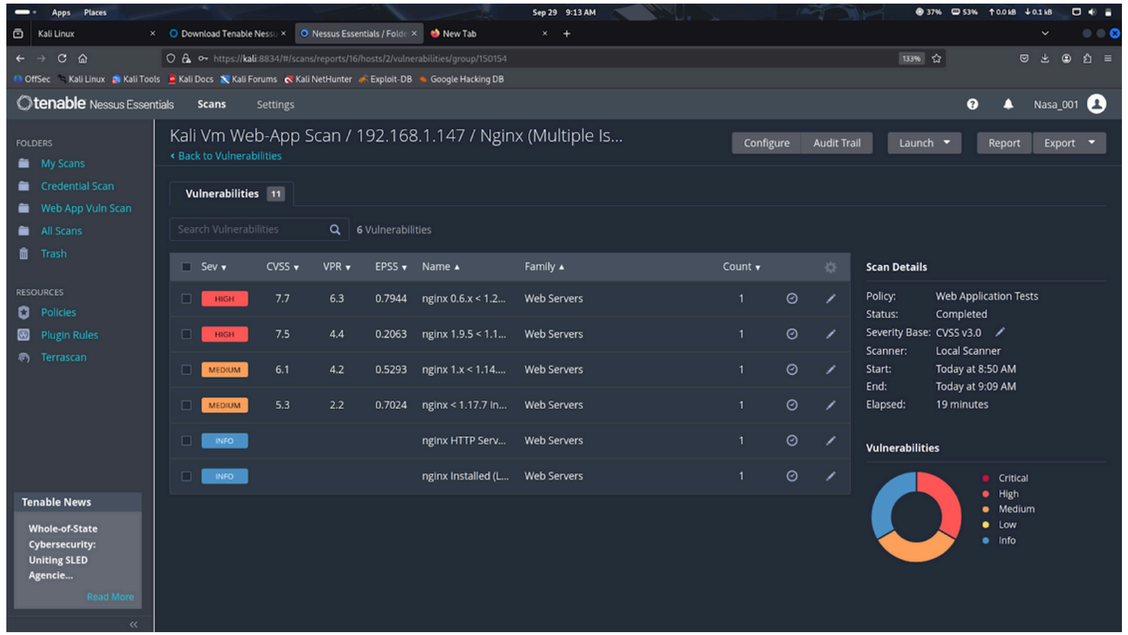


Result

67 VULNERABILITIES
2 HIGH
4 MEDIUM
REST INFO

WEB APPLICATION VULNERABILITY SCAN

- **Evaluate the web application hosted on the Linux environment to uncover exploitable weaknesses and misconfigurations, focusing on the Nginx web server.**



While no Critical issues were found, two High-severity RCE and DoS vulnerabilities were detected in the Nginx server, which could escalate to critical impact if left unpatched.

WEB APPLICATION VULNERABILITY SCAN (CONTD)

Risk Level	Number of vulnerabilities	Percentage
Critical	0	-
High	2	40%
Medium	2	40%
Low	0	-
Info	1	20%
Total	5	100%

Automated Email Configuration

- **Enable automated SMTP reporting for scan results to ensure continuous oversight.**

Actions Taken:

- **Configured Nessus SMTP with Gmail (TLS, Port 587).**
- **Generated secure Gmail App Password for authentication.**
- **Tested successful delivery of scan reports via email.**

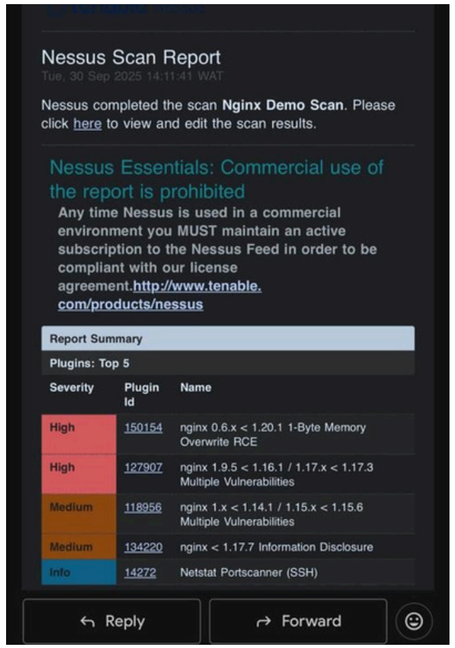
Outcome:

- **Automated email alerts now support real-time vulnerability tracking.**

Patch Management

Remediated high-severity vulnerabilities by applying the latest Nginx patch through Ansible automation. The patch was successfully deployed, validated, and the service upgraded to Nginx version 1.28.0

Screenshots from various assessment



Nessus Scan Report

Tue, 30 Sep 2025 14:11:41 WAT

Nessus completed the scan **Nginx Demo Scan**. Please click here to view and edit the scan results.

Nessus Essentials: Commercial use of the report is prohibited

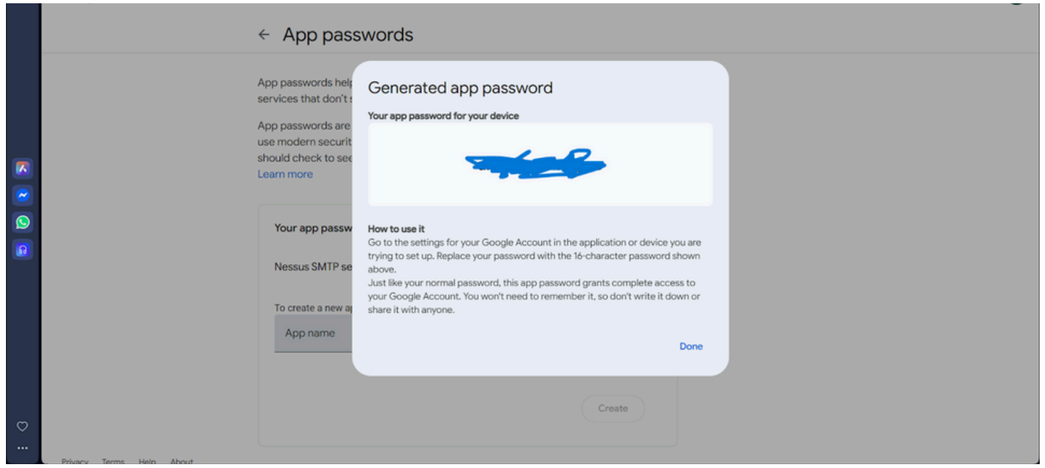
Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the Nessus Feed in order to be compliant with our license agreement.http://www.tenable.com/products/nessus

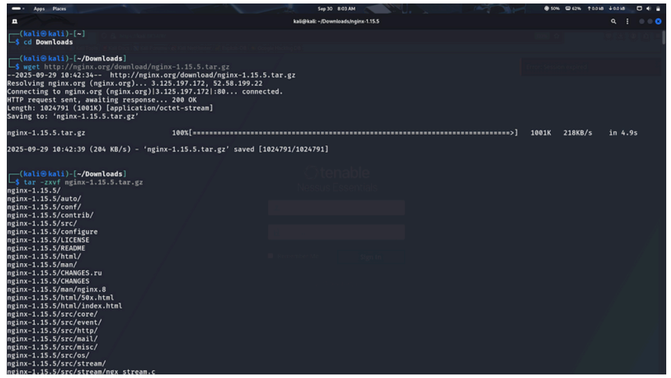
Report Summary

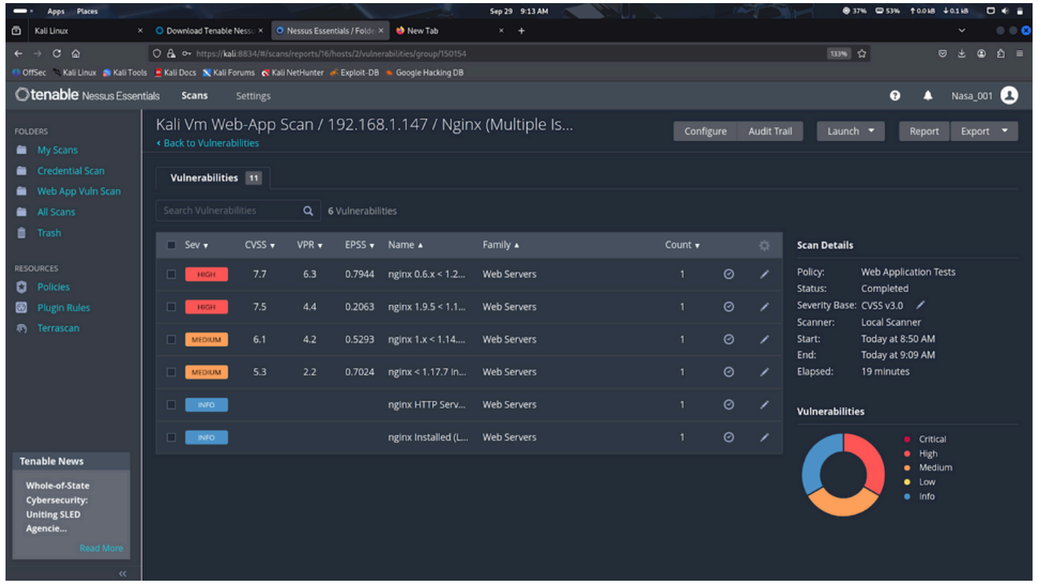
Plugins: Top 5

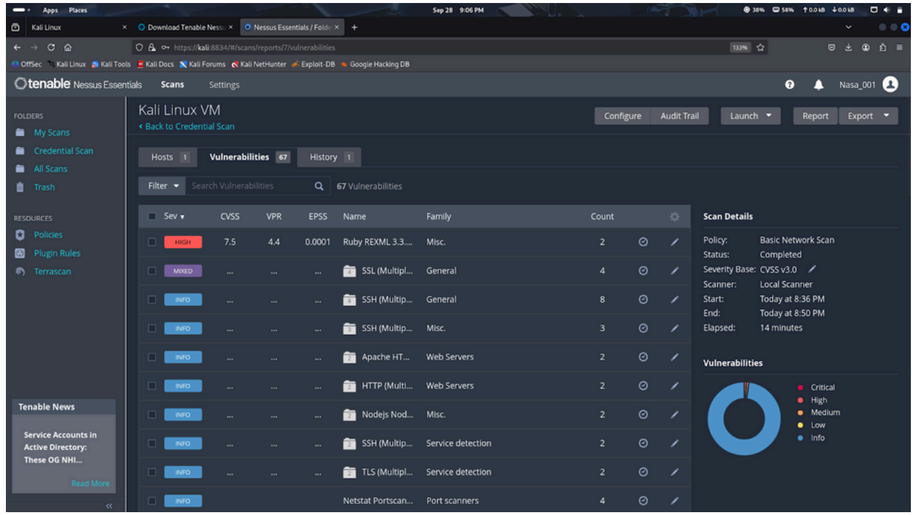
Severity	Plugin Id	Name
High	150154	nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE
High	127907	nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities
Medium	118956	nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilities
Medium	134220	nginx < 1.17.7 Information Disclosure
Info	14272	Netstat Portscanner (SSH)

Reply Forward









Recommendations

1. Maintain Continuous Scanning
2. Automate Patch Management
3. Enhance Monitoring
4. Harden Configurations
5. Implement a Risk Review Cycle

Conclusion

The security assessment successfully identified and mitigated critical risks across CyberTech Solutions' internal infrastructure. Through credentialed scanning, web application analysis, and automated patch deployment, the team strengthened the organization's overall security posture and demonstrated effective use of industry-standard tools like Nessus and Ansible.

THANK YOU