Vulnerability Assessment & Remediation

Nessus Concepts • Patch Validation • Security Operations

Vulnerability Scanning	Nessus Concepts	Linux Updates	Patch Management

Overview

This public sample summarizes vulnerability management work including scan review, prioritization, patching, and validation. It is designed to show capability without releasing raw vulnerability reports.

Business Challenge

Organizations often have outdated packages, exposed services, and untracked remediation work. Without a process, high and critical vulnerabilities can remain open longer than necessary.

Example Solution

A remediation workflow was followed: identify critical and high-risk items, apply updates, validate fixes through follow-up scanning, and document closure evidence.

Technologies / Methods Demonstrated

- Vulnerability Scanning
- Nessus Concepts
- Linux Updates
- Patch Management
- Remediation Tracking
- Validation Scans

Business Outcomes

- Reduced critical/high vulnerability exposure.
- Documented the remediation process.
- Created evidence that fixes were validated after patching.

What This Shows a Client

- Shows security operations workflow knowledge.
- Shows patching and validation discipline.
- Shows ability to communicate vulnerability risk.

Details intentionally not published

- Raw scan exports.
- Plugin lists tied to exact hosts.
- Hostnames, IP addresses, and system fingerprints.

- Step-by-step exploit or remediation details.

This document is designed to give website visitors confidence in EPIC TECH LLC capability without publishing full implementation playbooks or reusable client deliverables.