Vulnerability Management System for small and Large Businesses

(Absa Cyberthon)

NAME : DALITSO NGULUBE

DATE: 11th November 9, 2024

Table of Content

1. Problem Statement 3
2. Solution 4
3. Limitations and Risks of Implementing the Vulnerability management System in Zambia 5
4. Design Diagrams 6
    Flowchart 6
    System Blueprint 8
    Data Flow 9
5. Analysis of Real World Scenario Related to Vulnerability Management 12

1. Problem Statement

As companies and businesses are adopting more of IT solutions to manage business processes, these solutions / systems become targets to cyberattacks. These attacks usually exploit vulnerabilities in their systems, networks, and applications.

However, many institutions lack the resources to perform regular vulnerability assessments and system checks, often due to a shortage of qualified cybersecurity personnel. Without professional oversight, these organizations face heightened risk, as vulnerabilities may remain undetected and unmitigated, leaving them susceptible to increasingly sophisticated cyber threats.

2. Solution

To address this gap, the solution being proposed is a comprehensive Vulnerability Management and Mitigation System. This system will monitor all network devices, detecting and reporting potential threats in real-time. It will automate patching/updating across devices and provide users with a clear, step-by-step guide for resolving any issues.

3. Limitations and Risks of Implementing the Vulnerability management System in Zambia

While such a system would be beneficial, there are a number of challenges that may limit the system to function at its full capacity. These limitations and risks are:

1. Limited IT infrastructure

Most infrastructure in Zambia, may not support the demands of the vulnerability management system, and this is mostly an issue in rural areas. Limited internet connectivity, low bandwidth and power outages can disrupt real-time monitoring and lower the effectiveness of the vulnerability management system.

2. Resistance to Change

Many organizations hesitate to adopt new technologies due to concerns over high initial costs, potential operational disruptions, and uncertainty about the product's long-term value. This reluctance can lead to slow adoption of critical systems.

3. Lack of awareness

Many businesses do not fully grasp, or even know the Cybersecurity best practices. Without widespread training and awareness initiatives, organizations may not fully grasp the importance of consistent vulnerability management or may inadvertently bypass critical security steps, leaving gaps in the system.

4. Design Diagrams

The following are design diagrams that depict the set-up of the system, and now the system interacts with other systems in the network

Flowchart

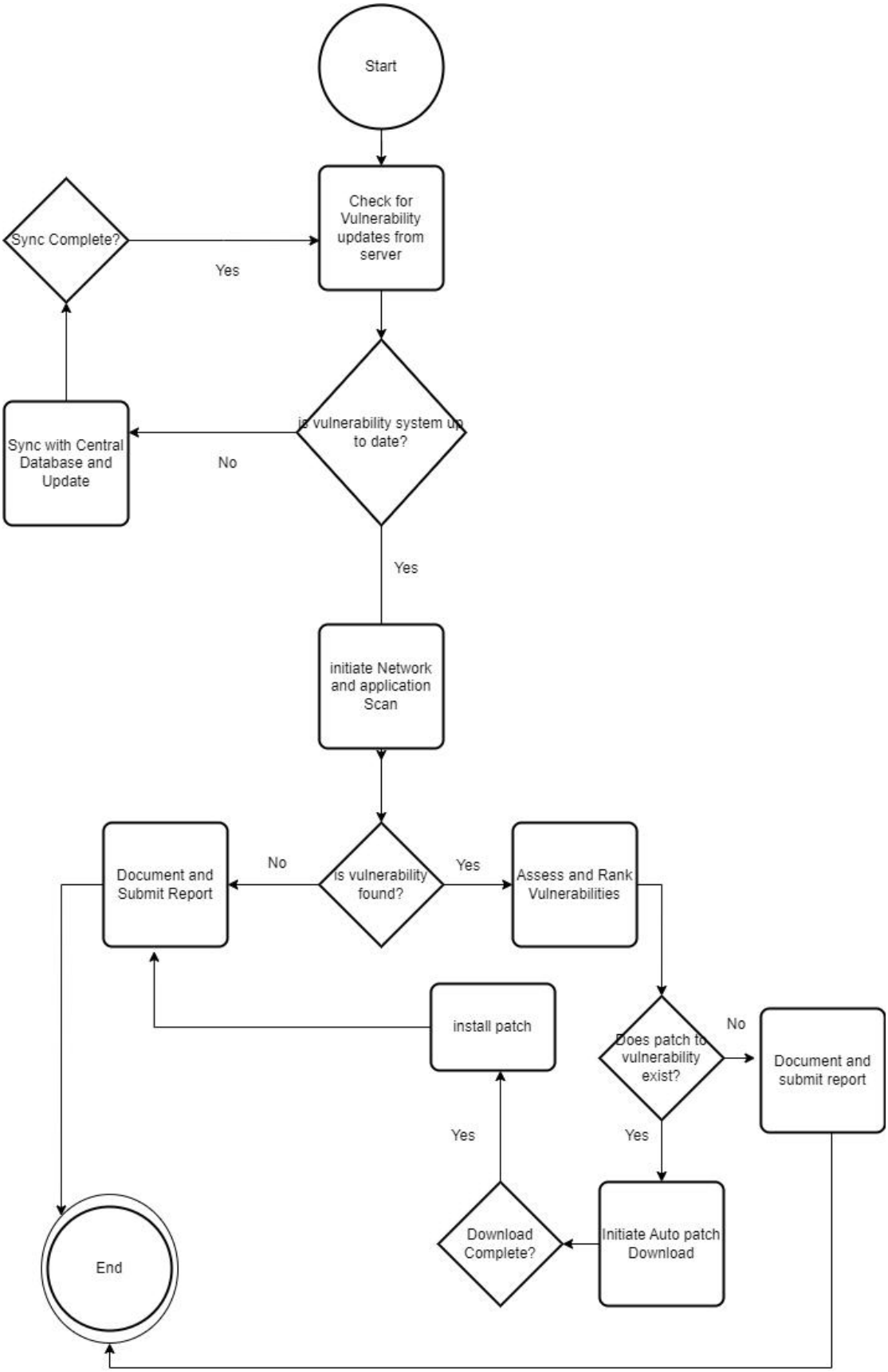
The flowchart below shows how the vulnerability management system operates. The major functions in the process are :

1) **Vulnerability scan** - Regular scans of the network, applications, and connected devices to detect outdated software, open or insecure ports, and misconfigurations that may pose a security risk.

2) **Vulnerability assessment** - the system assesses each detected vulnerability by evaluating its severity, potential impact, and exploitability.

3) **Prioritize and Remediate** - High-priority vulnerabilities are addressed first, with automatic or manual re-mediation actions applied.

4) **Report and Submit Record**s - All operations are submitted to the Central Vulnerability database


Start
Check for Vulnerability updates from server
Sync Complete?
Yes
is vulnerability system up to date?
Sync with Central Database and Update
No
Yes
initiate Network and application Scan
Is vulnerability found?
No
Document and Submit Report
Yes
Assess and Rank Vulnerabilities
install patch
Does patch to vulnerability exist?
No
Document and submit report
Yes
Initiate Auto patch Download
Download Complete?
Yes
End

System Blueprint

The Vulnerability management system continuously scans all network-connected devices for vulnerabilities, logging and assessing any detected issues. Upon identifying vulnerabilities, the system automatically applies relevant patches or updates, helping to maintain security across the organization's infrastructure. This proactive approach ensures that all departments benefit from up-to-date, protected systems, minimizing exposure to potential threats.

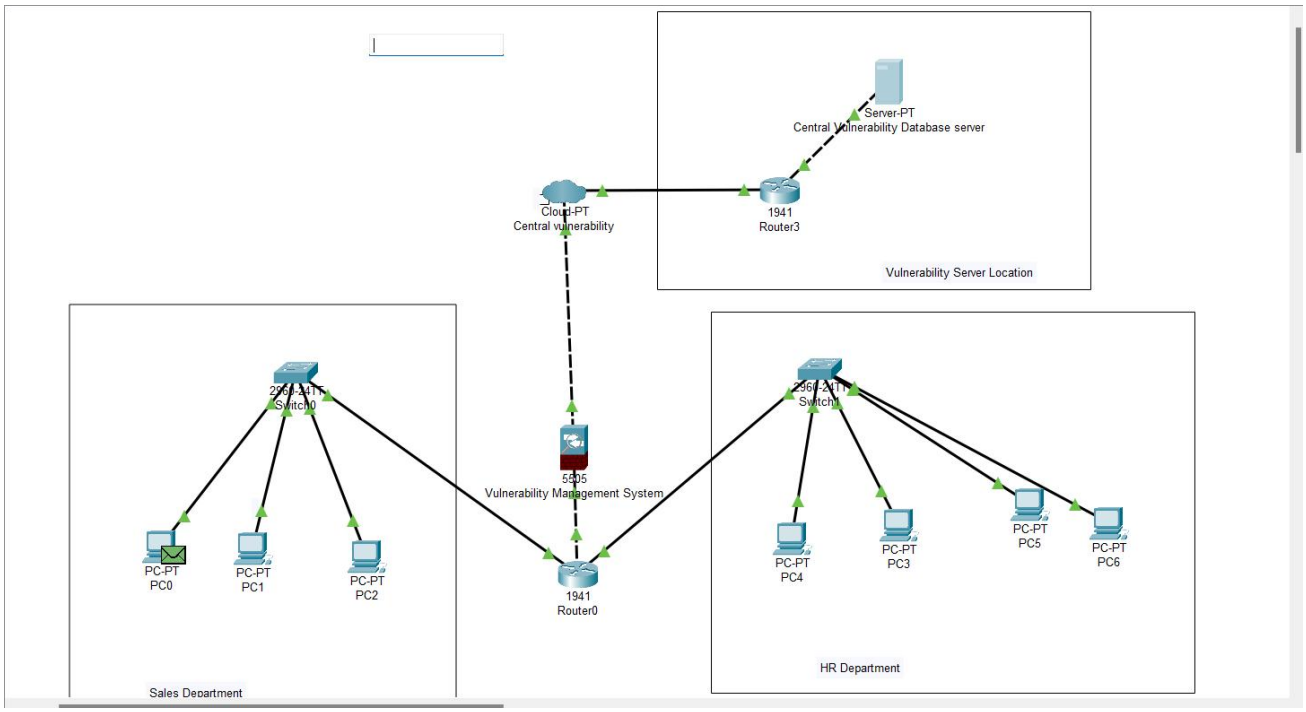


Figure 1

Data Flow

The diagrams show how data is handled by each component in the syetem, and the necessary databases to which data is sent and retrieved from:

Level 0 Context Diagram

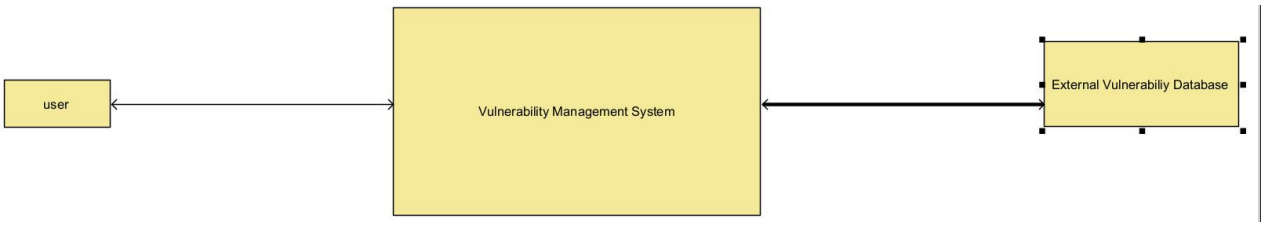


Figure 2

Level 1 DFD(Exploded Main Process)

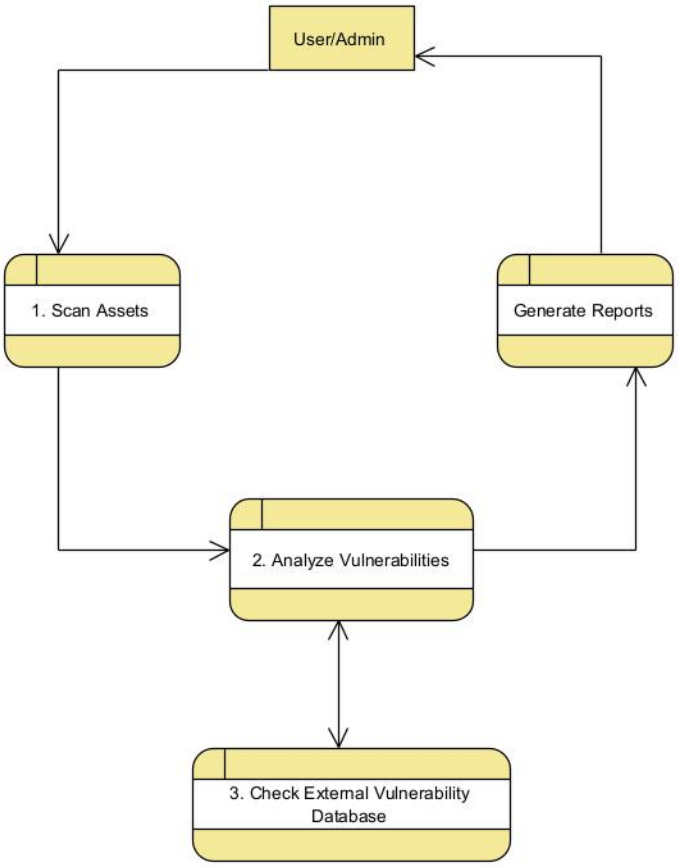


Figure 3

Level 2 DFD(Detailed View)

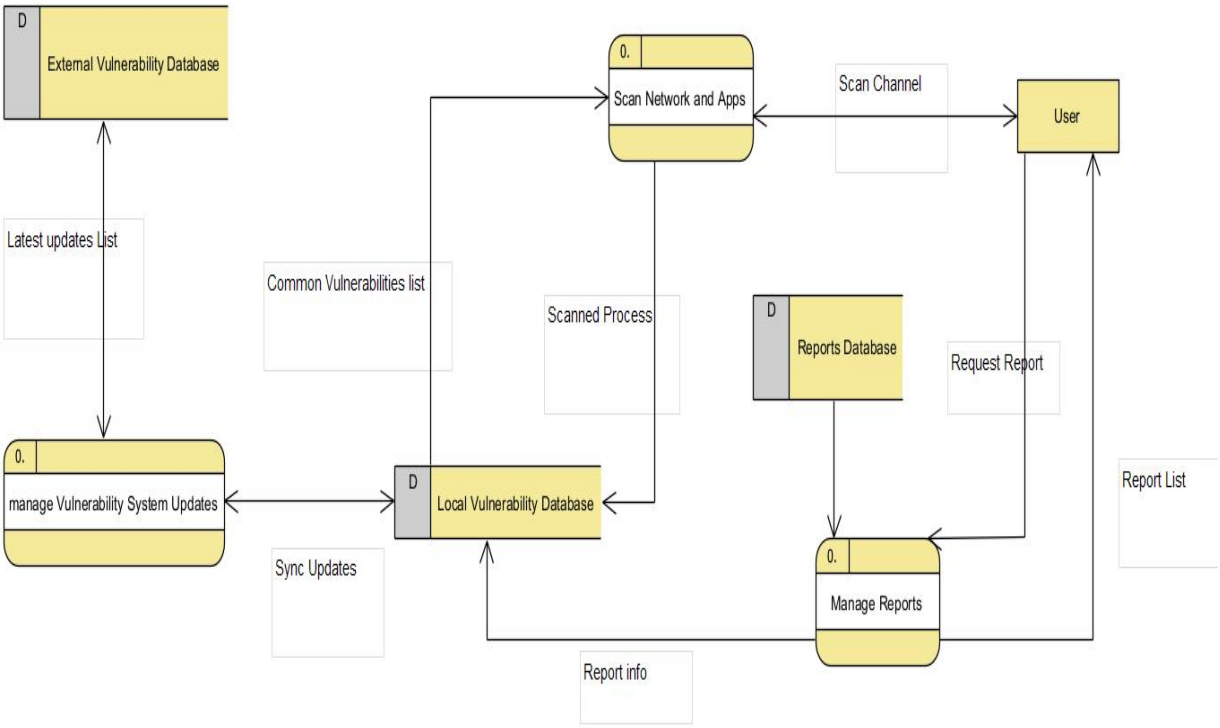


Figure 4

5. Analysis of Real World Scenario Related to Vulnerability Management

Equifax, a U.S.-based company, suffered a massive data breach that exposed the sensitive information of approximately 147 million people. Investigations revealed the exploit was due to an unpatched vulnerability in the Apache Struts framework. Although a security patch for this vulnerability had been released months earlier, a lack of consistent vulnerability management by the IT team left it unaddressed, leading to one of the largest identity theft incidents on record. Consequently, Equifax was forced to pay around $500 million in compensation to affected users. Had a robust vulnerability management system been in place, this breach—and the financial fallout—could have been prevented.