**What did you do?**

To prepare an organization to recover from a ransomware attack, I followed the steps outlined in the assignment and used the outputs from the previous exercises to generate the required deliverables. Here's how I approached each task:

a) Inventory of Network Devices: I used the output from assignment 1, which likely involved conducting a network scan using Nmap or similar tools, to create an inventory of all network devices connected to the organization's network. This inventory includes routers, switches, firewalls, servers, workstations, printers, and any other network-connected devices.

b) Prioritization of Network Assets: Based on my knowledge of the organization and its critical business functions, I prioritized the list of network assets. I specifically identified devices that are vital and critical to the organization's operations, and these devices would need to be recovered first in the event of a ransomware attack.

c) Identification of Servers for Backups: Using the knowledge of the organization's IT infrastructure and the output of assignment 1, I identified the servers that need to be backed up regularly. These backups are crucial for ensuring data recovery in case of a ransomware attack.

d) Identification of Devices Needing Updates: I utilized the outputs from assignment 2, which may include vulnerabilities discovered using Shields Up and Nessus, to identify network components that require software updates. Timely updates are essential to prevent ransomware attacks exploiting known vulnerabilities.

e) Identification of Passwords for Backup: I utilized the outputs from Assignment 2 (Shields Up and Nessus) to identify the vulnerabilities present in the network devices. From these results, I compiled a list of devices that need immediate updates and patches to strengthen the organization's security against potential ransomware attacks.

**What are the results?**

The specific deliverables from the above activities are as follows:

a) Prioritized List of Components for Recovery: This list includes all the critical network assets, such as critical servers, database systems, and key network infrastructure components that must be recovered with the highest priority in case of a ransomware attack.

b) List of Backups to be Prepared and Maintained: This list contains all the servers and critical network devices that require regular backups. It ensures that the organization can restore these systems to a known good state after a ransomware incident.

c) List of Passwords to be Backed Up: The list identifies the roles with administrative access and other important access points that require special attention during recovery. Although the actual passwords are not included, their role names are documented for reference.

d) List of Devices that Need to be Updated: This list comprises all the network devices with identified vulnerabilities from the Nessus vulnerability scan. It helps prioritize the devices that need immediate updates and patches to reduce the risk of ransomware attacks exploiting known vulnerabilities.

Deficiencies and resolutions:

If there are any deficiencies in the above deliverables, the organization should take the following steps to resolve them:

* Regularly review and update the inventory of network devices to account for changes in the network infrastructure.
* Ensure that the list of critical components for recovery is periodically updated based on changes in the organization's operations and network topology.
* Implement a robust backup strategy that includes both on-site and off-site backups to protect against data loss in case of a ransomware attack.
* Enforce strict password policies, implement multi-factor authentication, and regularly update passwords for privileged accounts.
* Establish a system for regularly applying updates and patches to network devices and software to address vulnerabilities promptly.

**What did you learn?**

From this assignment, I learned the critical importance of preparing an organization to recover from a ransomware attack. Key takeaways include:

* Regular backups are essential to data recovery in case of a ransomware incident. Backups must be prioritized based on criticality to the organization's operations.
* Updating network components and software is crucial to patch known vulnerabilities and prevent ransomware attacks.
* Identifying and backing up important passwords is vital to restoring access to critical systems and data after a ransomware attack.
* Prioritization of network assets allows the organization to focus on recovering the most critical components first, minimizing downtime and impact on business operations.
* Preparing for ransomware recovery is an ongoing process and requires collaboration between IT teams and other stakeholders to ensure a comprehensive and effective response.

In the future, this knowledge can be applied to enhance the organization's cybersecurity posture, implement better recovery strategies, and continuously improve incident response plans to combat ransomware threats effectively. The organization can also use the insights gained from this exercise to establish and strengthen policies, procedures, and security measures to safeguard against ransomware attacks.