**What Did You Do?**

Beginning by analyzing the Nmap report from Assignment 1, it is understood we have a “list” (an informal inventory) of network devices, open ports, and IP addresses. This map needs to be compiled into a refined directory that aims at how many devices, which devices are critical, and what type of devices (routers, servers, etc.). To assess this and appropriately denote each piece of technology, we consider what roles each device has within an operation and how sensitive it could be to a security breach. Another great lesson taught by the reading Dzimiela and Jennex (2023) is to identify the servers needing updates and/or backups.

Based on my outputs from Assignment 1, I made a detailed inventory of the organizations network sectioned into categories of importance and which should be prioritized for backups. To focus on relevance and clarity, I omitted the non-critical devices and focused on the pieces that would alter how a plan would be made to recover from an attack. These unknown devices for this company are likely inactive or non-responsive to port scanning as they all have closed ports. However, for the sake of this research, I have added them in a separate table within the next section.

How I organized the priorities of each device was derived from its dependency within the company. For example, the network printers (critical priority) can be accessed by multiple users and these specific devices would have a major impact on productivity if there was an attack due to the nature of this business. Likewise, the database server is also categorized as critical, because it is a fundamental element to everyday operations. If a cyberattack were to occur and impact this server, the consequences would be severe as there is confidential customer data. The network switch is critical as well, because it is the backbone to network communication and managing data traffic. Lastly, the network router and file server were classified as important due to the fact it is heavily implied there are other systems/redundancies available to handle these components given that one fails.

To classify the need for a backup or not, I followed criteria that circled around whether the device handled critical data and how data could be restored. For the network and switch, backups are not often needed as they rely on configurations that can be restored/stored elsewhere. The two servers do handle sensitive information and should be updated and backed up as to prevent data loss in the event of a ransomware attack. Finally, the two printers are less critical in terms of actual data and typically cannot hold the type of data that would require a backup. However, it is always a good business practice to back up everything you can as to lessen the intensity of an attack. To quote Dzimiela and Jennex (2023), “it is knowledge and expertise that is most needed in responding and recovering from a ransomware attack”.

Moving onto the outputs from Assignment 2 (Nessus and Shields Up) and which components need to be updated, the main vulnerabilities surround around Ruby, a system update (version 14.5 to 14.6), and untrusted SSL certificates. I have compiled a list for this portion as well to highlight which updates need to be performed and why. To complete analyzing and prioritization, a compiled list of passwords is needed to identify which are crucial to the backup process. I have amended the device inventory table with a column for passwords to include based on all three outputs. Each password is associated with the appropriate device along with an explanation as to why it is critical.

**What Are the Results?**

Most Relevant Devices:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device ID** | **IP Address** | **Device Type** | **Role** | **Critical Priority** | **Backup?** | **Password/Role** |
| 1 | 192.168.1.1 | Router | Primary Network Router | Important | No | Router Admin Password- needed for network management |
| 2 | 192.168.1.5 | Switch | Network Switch | Critical | No | Switch Admin Password- network management and recovery |
| 3 | 192.168.1.20 | Server | Database Server | Critical | Yes | Database Admin Password- critical for database access |
| 4 | 192.168.1.26 | Server | File Server | Important | Yes | Server Admin Password- needed for file access and recovery |
| 5 | 192.168.1.32 | Printer | Network Printer | Critical | No | Printer Admin Password- important for management and recovery |
| 6 | 192.168.1.230 | Printer | Network Printer | Critical | No | See Above |

Unknown Devices:

\*\*\*Although we have unknown devices, it does not fully excuse them from the process of maintaining security health; monitoring still needs to be continued to ensure their status does not change.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device ID** | **IP Address** | **Device Type** | **Role** | **Critical Priority** | **Backup?** |
| 7 | 192.168.1.8 | Unknown | Unknown/Inactive | Non-Critical | No |
| 8 | 192.168.1.44 | Unknown | Potential Network Device | Non-Critical | No |
| 9 | 192.168.1.254 | Unknown | Unknown/Inactive | Non-Critical | No |

Vulnerability Table/ Updates Required and Why:

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability** | **Critical Level** | **Update Required** | **Reason** |
| macOS 14.5 to 14.6 | High | Upgrade to macOS Sonoma 14.6 | Fix multiple security vulnerabilities, protect private information access |
| Ruby | Medium | Upgrade to Ruby 3.0.7, 3.1.5, 3.2.4, 3.3.1 or later | Fix code execution vulnerability, RDoc configuration |
| SSL Certificate Cannot be Trusted | Medium | Ensure proper SSL certificates | Ensure trustworthiness, prevent man-in-the-middle attacks |

As the above information provides, the specific deliverables include a device inventory (along with prioritization), password management, and a vulnerability assessment. There are still a few deficiencies that lie within this documentation; for starters, there are inconsistencies with reporting which passwords need to be backed up. There are most likely several more passwords that need to be included, some that may even be fundamental to ensuring a proper recovery. There are almost certainly additional administrative accounts that need to be considered. However, this can be resolved by the business; a complete list of any additional accounts/ credentials should be produced to further remedy this issue. The unknown devices also pose a significant deficiency as the status could become active and if continuous monitoring is not performed, this action could be missed. There are several policies that could be put in place (NAC or IDS) to establish a strong and effective solution. Often the most overlooked stage of a recovery deals with the policies themselves. Considering this point ahead of time could save a lot of distress, and again, continuous monitoring would reduce risks.

**What Did You Learn?**

First and foremost, I have learned the importance of having a comprehensive inventory. When starting a new business/venture, I think we often get so caught up in the operations that we forget to document anything. At the time it can seem far more important to “get off the ground” and start producing, but in reality, the business becomes nothing if it falls victim to an attack and there is no recovery plan. This assignment highlighted the importance of having a detailed and accurate inventory along with lists of what is generally going on within a company (i.e. what updates are needed, important passwords). I used to believe software updates were primarily for user navigation, feature/ performance functionality, or bug fixes; however, this class has taught me the true vulnerabilities you expose yourself to if you do not manage them correctly.

Regarding a ransomware attack, the above statements capitalize on why it is important to take these measures and how they integrate into recovery and preparation. I see myself using quite a few techniques we have learned over this course, for example, frequently performing backups, keeping a confidential book of passwords, and performing periodic network scans to monitor the health of my devices. This information can also add value to the company as it not only outlines an approach to strategically managing potential incidents, but also how to prevent them. It lessens the impact of security breaches and financial losses, which furthers the company’s stability and success.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated