CIDM 6340

Network Management and Information Security

Research Report 4 – Vulnerability Scanning with Shields Up and Nessus

Vernice Tanquerido

**What did you do**

The goal of this activity is to prepare the organization for recovery in the event of a ransomware attack. In this case, our home network was used. The first step was to create an inventory of devices connected to our network. This was important to understand the scope of the network and identify the devices that need protection. To achieve this, Nmap was used to scan the home network and identify the devices and hosts associated with it. Nmap works by sending packets to network ports through various protocols or ping requests, allowing us to identify hosts and gather essential information about the devices connected to our infrastructure. Figure 1 shows the topology map generated by Nmap.

A network diagram with many dots and lines

Description automatically generated with medium confidence

Figure 1. Topology map of home network

Although Nmap provided valuable insights into the network, it had limitations in identifying certain devices. To address these gaps, the scan results were supplemented with knowledge of the devices actively in use within the household. By cross-referencing the Nmap data with personal understanding of the network, accurately labels and a complete the initial was created.

Once the inventory was completed, a priority list was created that ranked the devices according to the importance or sensitivity of the information that they hold and the potential impact if they are compromised. The following were considered during the ranking process:

1. Device importance and usage frequency - the device role in maintaining the functionality of the network
2. Sensitive files and data – ID’s, bank account transactions, tax documents, etc.
3. Photos and videos – Personal media that can be compromised
4. Software – essential software that contain important information
5. Emails and other communication systems – communication and other transaction that may contain sensitive information

Furthermore, the vulnerabilities of each of the devices were also considered when doing the ranking. The results from the Nessus vulnerability scan were used in this assessment. Figure 2 shows the dashboard generated by Nessus on the vulnerabilities of each device.

A graph with blue and white lines

Description automatically generated

Figure 2. Nessus dashboard

With the priority list in place and vulnerabilities identified, a list of essential backups was compiled so that in the event of a cyberattack, it would be possible to restore our data. Moreover, a list of apps and software that need to be updated was also created to maintain up-to-date security features.

Throughout this process, the guidelines provided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework was used as a reference. This framework is designed to help organizations assess risks and improve their cybersecurity management through a structured approach that encompasses five key functions: Identify, Protect, Detect, Respond, and Recover. Since this activity is focused on preparing the network to recover in the event of a ransomware attack, assessment was focused on the first two functions.

**What are the results**

The initial step was to create an initial inventory of the devices on the network. Then, using the factors identified, priorities were given to each of the devices. Table 1 shows the initial inventory produced through Nmap and the priority numbers assigned.

***Table 1****. Components identified by nmap and priorities*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Priority | Host | Number of open ports | Services | Device type | Operating System |
| 1 | 192.168.1.133 | 2 | tcpwrapped | Phone | Apple iOS 15.X |
| 2 | 192.168.1.115 | 2 | ccproxy-http, ms-wbt-server | General purpose (PC) | Windows 10|11 |
| 3 | 192.168.1.140 | 6 | msrpc, netbios-ssn, Microsoft-ds, enpp, mysql, http | General purpose (PC) | Microsoft windows 10 |
| 4 | 192.168.1.114 | 1 | enpp | General Purpose (PC) | Microsoft Windows 10|11 |
| 5 | 192.168.1.1 | 8 | Domain,http, netbios-ssn, upnp | General purpose (server) | Linux 2.6.12-2.6.36 |
| 6 | 192.168.1.124 | 1 | abyss | Specialized (router) | lwIP 1.4.1 - 2.0.3 |
| 7 | 192.168.1.123 | 5 | http, ssl/ajpl3, https-alt, cslistener, scp-config | Media device (Google home) | Google home device |
| 8 | 192.168.1.111 | 4 open, 1 filtered | tcpwrapped, printer jetdirect | Printer | Not detected |
| 9 | 192.168.1.145 | 0 |  | Camera | Not detected |
| 10 | 192.168.1.147 | 0 |  | Washing machine | Not detected |
| 11 | 192.168.1.148 | 1 | irc | Specialized | lwIP 1.4.1 - 2.0.3 |

Mobile devices were given high priority because they are the primary method of communication within the household and contain sensitive data. This includes banking information, transaction records, passwords, and personal media such as photos and videos. Due their usage frequency and to their central role in personal, financial, and other transactions especially in communication, their recovery takes precedence. The following backups need to be prepared and maintained:

1. Cloud backup – data is backed up to the cloud. In our case, the backup will be in iCloud for apple devices.
2. External storage backup – photos, videos, and other important files can be transferred to an external storage such as a hard drive.
3. App-specific backup – Individual apps such as facebook, whatsapp, and others offer backup options for users to save their data.

Computers were a close second for backup recovery because they store a significant amount of sensitive data. This includes financial records, tax documents, personal media like photos and videos, and other critical files. Given their role in managing and processing important information and their crucial role in day-to-day activities, ensuring that backups for computers are up-to-date and recoverable is crucial for maintaining functional continuity and personal security. For computers, the following backups will be prepared:

1. Full system backup – this is a complete package of the computer’s data that can be used to perform recovery in the event of an attack.
2. Local or external storage backup – transfer photos, videos, documents, and other important files to an external storage such as a hard drive.
3. Cloud backup – data such as documents, spreadsheets, photos, videos, and other important files can be backed up to an online storage such as google drive or onedrive.

Servers were also assigned high priority for data recovery because they manage and store extensive volumes of essential data. Effective recovery strategies for servers are vital to minimize operational disruptions and prevent widespread data loss or security breaches that could impact multiple users and systems.

In addition to performing backups, correcting the vulnerabilities in each of the hosts is crucial to ensure increased protection of the network. Table 2 lists the vulnerabilities and actions needed to be done:

|  |  |  |
| --- | --- | --- |
| Host | Vulnerability | Measure |
| 192.168.1.115 | SSL Cipher offer medium encryption | Configure server to where strong cipher suites are used instead |
| 192.168.1.140 | SSL Certificate cannot be trusted | Proper SSL certificate will be generated |
| 192.168.1.123 | SSL Certificate cannot be trusted | Proper SSL certificate will be generated |
| 192.168.1.140 | Self-signed SSL certificate | Proper SSL certificate will be generated |
| 192.168.1.123 | Self-signed SSL certificate | Proper SSL certificate will be generated |
| 192.168.1.140 | SMB signing not required | Proper authentication form host must be enabled |
| 192.168.1.115 | TLS versions are outdated | Update to TLS version 1.2 or higher |

Lastly, identifying accounts that require passwords and using a password manager to securely store and manage this login information is crucial for effective data recovery and security. Currently, there is no password management system in place and an inventory of accounts and passwords needs to be created. In the event of a recovery situation, having a well-organized system for managing and retrieving passwords can significantly streamline the process and reduce downtime. The following accounts are important to back up passwords for the home network and its associated devices:

1. System log-in accounts
2. Email accounts
3. Bank and other financial accounts
4. Social media accounts
5. Cloud storage accounts
6. Other software and applications such as Microsoft Office, Adobe, Slack, and others.

Applying these practices and preparing the network for a potential ransomware attacks can help maintain continued access to systems and devices and streamline recovery processes in the event of an attack.

**What did you learn**

Ransomware can happen to anyone regardless of the security of their systems. Through personal experiences, I’ve witnessed how even seemingly secure systems can be compromised. Over the years, I have observed friends and family members fall victim to social media hacks, where attackers gain control of their accounts and demand a ransom. In some cases, the attackers trick connections into sending money and exploiting the trust people have in the victims.

I have always been complacent that our devices and networks are secure. However, the reality is that no system is completely immune to ransomware. This activity helped me realize the importance of preparing your network just in case you find yourself in a ransomware attack situation. It made me recognize the criticality of regular data backups. Ransomware can hold our data hostage however a backup would ensure our data remains available and enable us to restore it without yielding to an attacker’s demands.

This also gave me a shift in perspective that it’s not only important to identify system vulnerabilities and attack surfaces but also critical to be prepared for recovery if an attack does happen.