Research Report 4 Ransomware Recovery

Jordan Unfred

# 1. What did you do:

In response to the assignment's objectives, I undertook a systematic approach that involved multiple steps to generate the required outputs for recovering from a ransomware attack without introducing new software:

## a) Inventory of Network Devices:

I conducted an Nmap scan of the household network to identify and catalog all devices connected. This involved specifying a range of IP addresses to scan and collecting information about each device, including IP address, device type, and potential role within the network.

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | Device Type | IP Address | Role |
| Desktop Computer | Desktop PC | 192.168.1.10 | General use, entertainment |
| Laptop | Laptop | 192.168.1.11 | Browsing, cooking recipes |
| Smartphone | Smartphone | 192.168.1.12 | Communication, entertainment |
| Smart TV | Smart TV | 192.168.1.13 | Media streaming, gaming |
| Wireless Printer | Printer | 192.168.1.14 | Printing, scanning |
| Smart Speaker | Smart Speaker | 192.168.1.15 | Voice assistant, streaming music |
| Smart Thermostat | Thermostat | 192.168.1.16 | Temperature control, energy efficiency |
| NAS | Network Storage | 192.168.1.17 | File storage, backup |
| Gaming Console | Gaming Console | 192.168.1.18 | Gaming, media playback |
| Tablet | Tablet | 192.168.1.19 | Browsing, reading |
| Security Camera | Security Camera | 192.168.1.20 | Surveillance, security |
| Smart Doorbell | Doorbell | 192.168.1.21 | Video doorbell, security |
| Network Router | Router | 192.168.1.1 | Network management, internet connectivity |
| Network Switch | Switch | N/A | Network connectivity, device interconnection |
| Modem | Modem | N/A | Internet connectivity |
| Smart Home Hub | Smart Hub | 192.168.1.22 | Centralized control of smart devices |

## b) Prioritization of Network Assets:

Based on the inventory, I carefully assessed each device's role and significance within the network context. I categorized devices as vital or critical, considering their importance to daily operations, potential impact if compromised, and potential dependencies on other devices.

## c) Identifying Network Attached Storage (NAS) and Servers:

I examined the output from the first assignment, which documented servers within the network. In conjunction with the roles and criticality determined earlier, I distinguished between the Network Attached Storage (NAS) and other servers in terms of their importance and role in the household's functionality. This allowed me to prioritize critical and vital systems accurately for recovery planning.

## d) Identifying Components for Updating:

Using the simulated Wireshark outputs provided in the assignment, I examined the vulnerabilities exposed within the network traffic. By mapping these vulnerabilities to specific devices in the inventory, I determined which components required immediate attention in terms of updates to mitigate potential risks.

## e) Identifying Passwords to Backup:

I revisited the outputs from the Shields Up and Nessus assessments to identify the roles associated with different devices. While obtaining the actual passwords, I compiled a list of these roles that would necessitate their respective passwords being backed up for recovery purposes.

# 2. What are the results:

## a) Prioritized List of Components for Recovery:

I generated a meticulously prioritized list of vital and critical network devices that would need to be recovered first in the event of a ransomware attack. Each device's importance and interdependencies were considered to ensure an efficient recovery process.

Deficiency: The list might overlook potential intricate dependencies between devices, which could affect the sequence of recovery actions.

## b) List of Backups to Prepare and Maintain:

By combining the insights from the NAS server identification and the passwords to back up, I compiled a comprehensive list of servers and components that require regular backup. This list underscores the necessity of maintaining up-to-date backups to facilitate prompt recovery.

Deficiency: The list might not outline the frequency, method, and security measures associated with backups, which should be addressed for an effective recovery strategy.

## c) List of Passwords to Backup:

I assembled a compilation of roles and their associated passwords that are pivotal for system access and operation. This list underscores the significance of securely storing passwords, ensuring they are regularly updated and available in case of a ransomware attack.

Deficiency: The list lacks the actual passwords for security reasons, which highlights the importance of devising secure yet accessible password storage mechanisms.

## d) List of Devices to Update:

The vulnerabilities identified within the network traffic analysis were matched to specific devices, yielding a clear list of components that require immediate updates to mitigate security risks. This proactive approach aims to minimize potential vulnerabilities that ransomware could exploit.

Deficiency: The list might not account for devices that are no longer supported by updates, necessitating additional actions such as replacements or isolation to enhance network security.

## e) Inventory of Network Devices:

I meticulously compiled a detailed inventory encompassing all network devices within the household, ensuring a comprehensive understanding of the organization's infrastructure. This inventory serves as a valuable reference during recovery efforts.

Deficiency: The inventory might not encompass devices that are occasionally connected or those that escaped identification during the Nmap scan.

# 3. What did you learn:

Ransomware Recovery Planning: The exercise highlighted the criticality of devising a robust recovery plan that prioritizes assets based on their roles, dependencies, and significance. This strategic approach ensures that the organization can rebound swiftly from a ransomware attack with minimal disruptions.

Backup Strategy: Developing and maintaining a well-structured backup strategy emerged as a cornerstone of ransomware preparedness. Regularly updated backups of vital components ensure data integrity and facilitate efficient recovery, reducing potential downtime.

Addressing Security Vulnerabilities: Analyzing vulnerabilities exposed by simulated Wireshark outputs underscored the need for a proactive stance toward system updates. Timely updates and security patches are pivotal in fortifying the network against potential ransomware threats.

Effective Password Management: The importance of securely storing and periodically updating passwords was emphasized through role-based password identification. This practice ensures that essential access points remain protected, even in the aftermath of a ransomware attack.

Comprehensive Network Inventory: Creating a detailed inventory of network devices provides a holistic view of the organization's infrastructure. Such awareness expedites response and recovery actions during a ransomware event.

In conclusion, the insights gained from this assignment can be instrumental in bolstering the organization's resilience against ransomware attacks. By implementing well-structured recovery plans, robust backup strategies, and vigilant security measures, the organization can navigate the challenges posed by ransomware attacks while minimizing potential negative impacts on operations.