Name: Amarachi Anthony

Course: Network Management & Info Security

Research Report 4

Assignment: Ransomware Recovery

What did I do?

Through the utilization of Nmap scan results, I was able to gain a deep understanding of the structure of my home network and identify all connected devices. By analyzing open ports and identifying vulnerable points, I gained insight into the overall topology of the network and identified potential risks that needed to be addressed.

To achieve this comprehensive analysis, I utilized a variety of network scanning utilities, such as Nessus and Shields Up, in addition to carefully examining network packet records. This allowed me to take the following actions:

- A Nessus vulnerability scan was conducted to identify any open ports, security threats, and vulnerabilities within the networked devices.

- An exhaustive inventory of all network devices was taken, then prioritized based on my familiarity with each device's configuration.

- Crucial assets were assessed and prioritized, ensuring backup and recovery measures were in place for all server components.

- Wireshark-generated insights were used to identify components that required updates to enhance the overall system.

- Essential passwords were identified and securely backed up to protect all crucial information.

What is the results?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Inventory of Network Devices | Critical Assets For Recovery | Devices/Servers That needs Backups | Devices/Servers That needs Updates | Password backups |
| [Laptop-210CDM39.attlocal.net](http://laptop-210cdm39.attlocal.net/) (192.168.171) | 192.168.171 | 192.168.171) | Routers, firmware | Admin Password for this IP 192.168.171) |
| [unknown4447ccbab5d8.attlocal.net](http://unknown4447ccbab5d8.attlocal.net/) (192.168.1.77) |  |  | Software’s | [unknown4447ccbab5d8.attlocal.net](http://unknown4447ccbab5d8.attlocal.net/) (192.168.1.77) |
| [unknown5803fb626cae.attlocal.net](http://unknown5803fb626cae.attlocal.net/) (192.168.1.79) |  |  | Security Configurations | [unknown5803fb626cae.attlocal.net](http://unknown5803fb626cae.attlocal.net/) (192.168.1.79) |
| [unknown6452998c124d.attlocal.net](http://unknown6452998c124d.attlocal.net/) (192.168.1.80) |  |  | SSDP/UPnp | [unknown6452998c124d.attlocal.net](http://unknown6452998c124d.attlocal.net/) (192.168.1.80) |
| [unknown5803fb62cc9.attlocal.net](http://unknown5803fb62cc9.attlocal.net/) (192.168.1.81) |  |  |  | [unknown5803fb62cc9.attlocal.net](http://unknown5803fb62cc9.attlocal.net/) (192.168.1.81) |
| [unknown5803fb62cba.attlocal.net](http://unknown5803fb62cba.attlocal.net/) (192.168.1.83) |  |  |  | [unknown5803fb62cba.attlocal.net](http://unknown5803fb62cba.attlocal.net/) (192.168.1.83) |
| [unknown40aa5668cef7.attlocal.net](http://unknown40aa5668cef7.attlocal.net/) (192.168.1.84) |  |  |  | [unknown40aa5668cef7.attlocal.net](http://unknown40aa5668cef7.attlocal.net/) (192.168.1.84) |
| [ubnt.attlocal.net](http://ubnt.attlocal.net/) (192.168.1.87) |  |  |  | [ubnt.attlocal.net](http://ubnt.attlocal.net/) (192.168.1.87) |
| [ATT\_Motorola\_AP\_2D4612.attlocal.net](http://att_motorola_ap_2d4612.attlocal.net/) (192.168.110) |  |  |  | [ATT\_Motorola\_AP\_2D4612.attlocal.net](http://att_motorola_ap_2d4612.attlocal.net/) (192.168.110) |
| [unknown40aa56682ae7.attlocal.net](http://unknown40aa56682ae7.attlocal.net/) (192.168.1.111) |  |  |  | [unknown40aa56682ae7.attlocal.net](http://unknown40aa56682ae7.attlocal.net/) (192.168.1.111) |
| [unknowna067203693b6.attlocal.net](http://unknowna067203693b6.attlocal.net/) (192.168.1.127) |  |  |  | [unknowna067203693b6.attlocal.net](http://unknowna067203693b6.attlocal.net/) (192.168.1.127) |
| [unknown0c1932c4a0.attlocal.net](http://unknown0c1932c4a0.attlocal.net/) (192.168.1.184) |  |  |  | [unknown0c1932c4a0.attlocal.net](http://unknown0c1932c4a0.attlocal.net/) (192.168.1.184) |
| [Canonc63d2c.attlocal.net](http://canonc63d2c.attlocal.net/) (192.168.1.186) |  |  |  | [Canonc63d2c.attlocal.net](http://canonc63d2c.attlocal.net/) (192.168.1.186) |
| [My-ecobee-2.attlocal.net](http://my-ecobee-2.attlocal.net/) (192.168.1.187) |  |  |  | [My-ecobee-2.attlocal.net](http://my-ecobee-2.attlocal.net/) (192.168.1.187) |
| [My-ecobee.attlocal.net](http://my-ecobee.attlocal.net/) (192.168.1.189) |  |  |  | [My-ecobee.attlocal.net](http://my-ecobee.attlocal.net/) (192.168.1.189) |
| [Samsung.attlocal.net](http://samsung.attlocal.net/) (192.168.1.192) |  |  |  | [Samsung.attlocal.net](http://samsung.attlocal.net/) (192.168.1.192) |
| [Samsung.attlocal.net](http://samsung.attlocal.net/) (192.168.1.195) |  |  |  | [Samsung.attlocal.net](http://samsung.attlocal.net/) (192.168.1.195) |
| [dsldevice.attlocal.net](http://dsldevice.attlocal.net/) (192.168.1.254) |  |  |  | [dsldevice.attlocal.net](http://dsldevice.attlocal.net/) (192.168.1.254) |
| 192.168.1.247 |  |  |  | 192.168.1.247 |

This report contains valuable information about our network devices. It focuses on critical assets for recovery, devices and servers that need backups, devices and servers that require updates, and password backups. Here is a breakdown of each section:  
  
Inventory of Network Devices: This section lists all network devices and their associated hostnames and IP addresses. Each entry is for a unique device on the network.  
  
Critical Assets for Recovery: In this section, we highlight devices that are essential for recovery. These devices are critical components that play a vital role in the network's operation. Identifying and addressing these assets quickly during recovery efforts is crucial.  
  
Devices/Servers That Need Backups: This section lists devices or servers that need to have backups created. Backups are crucial for data protection and recovery. It also specifies the type of data that needs to be backed up, such as software or security configurations.  
  
Devices/Servers That Need Updates: This section specifies devices or servers that require updates. Keeping devices up to date is essential for maintaining security and optimal performance. The mention of "Routers, firmware" suggests that updating router firmware is necessary.  
  
Password Backups: This section emphasizes the importance of backing up passwords associated with specific devices. Passwords are sensitive credentials that need safeguarding to prevent unauthorized access.  
  
This report provides a thorough overview of our network devices, their roles, and the necessary actions to ensure the network's security, stability, and recoverability. It emphasizes critical components, data backups, updates, and password protection to enhance network posture

What did I learn?

Upon delving deeper into the subject matter of ransomware and cybersecurity risks, I have come to the realization that taking proactive measures is of utmost importance to safeguard my digital assets. These measures involve a variety of tasks, including but not limited to

Regularly updating my software, configuring my security settings to appropriate levels, and creating backups of my important data. In the unfortunate event of a ransomware attack, it is essential to prioritize crucial components, maintain up-to-date backup protocols, and strengthen administrative passwords to mitigate the damage.

As I move forward, I plan to apply my newfound knowledge to strengthen the security of my household network. This will involve regularly updating and patching my network apparatus, firmware, and software to counter any vulnerabilities. I will also implement robust security configurations and access management to minimize any potential weak points. Additionally, maintaining comprehensive backups of essential elements will expedite recovery in case of an intrusion.

To stay ahead of potential threats, I will continuously monitor network operations for any unusual activity and take proactive measures to counteract any potential risks. I will also enlist the help of cybersecurity experts for intermittent evaluations to ensure that my security stance remains strong. It is essential to note that cyber threats are continually evolving, and my security measures must evolve with them.

Overall, this exercise has helped me gain a better understanding of how to protect my digital possessions and minimize potential adversities. I am confident that by implementing these measures, I can safeguard my digital assets and prevent cyber-attacks from causing severe damage. It is crucial to remain vigilant and proactive to ensure that my cybersecurity measures remain up-to-date and relevant in the face of any evolving cyber threats.

Through these carefully executed actions, I was able to achieve a comprehensive analysis of my home network that culminated in a prioritized list of components requiring restoration, an inclusive enumeration of backups that required establishment and maintenance, a list of crucial passwords that require backup, a register of devices that required updates, and an exhaustive inventory of all network devices. Overall, this allowed me to ensure the safety and security of my home network and provide me with valuable insights into its overall structure and potential risks.