Report 4 Ransomware Recovery

By: Farzaneh Noroozi
Professor: Dr. Murray Jennex

Introduction

Ransomware attacks have become a significant threat to organizations, causing data breaches, financial losses, and operational disruptions. In this research report, we will explore the best practices for preparing an organization to recover from a ransomware attack. We will utilize the outputs from Nmap, Shields UP!!, and Nessus reports to analyze the organization's network assets, identify critical components for recovery, prioritize backups, assess password protection, and determine components needing updates. By implementing these findings, organizations can strengthen their defense against ransomware attacks and enhance their overall cybersecurity posture.

What Did You Do?

how you did to generate the outputs

For this research report, I conducted a comprehensive analysis using outputs from four different security tools: Nmap, Wireshark, Shields UP!!, and Nessus. The goal was to assess the organization's network assets, identify critical components for recovery, prioritize backups, assess password protection, and determine components needing updates. The process involved various data gathering and analysis steps to prepare the organization to recover effectively from a potential ransomware attack.

Firstly, I utilized Nmap to perform a thorough network scan, which involved identifying live hosts, open ports, and active services on the network. This scan provided valuable insights into the network's infrastructure, allowing me to create a detailed inventory of network devices. The inventory helped prioritize components for recovery based on their criticality.

Next, I employed Shields UP!! from Gibson Research Corporation to conduct port scanning and security testing. Analyzing the results allowed me to identify potential vulnerabilities in the organization's network and assess its overall security posture. This step was crucial in understanding the organization's current vulnerabilities and potential points of exploitation.

Subsequently, I conducted a vulnerability scan on the target system using Nessus. The Nessus report highlighted critical vulnerabilities, misconfigurations, and areas requiring updates. This information was vital for determining components that needed immediate attention to enhance security and protect against potential cyber threats.

Additionally, I used Wireshark, an open-source network protocol analyzer, to capture and inspect real-time network traffic. Wireshark proved instrumental in troubleshooting network issues, analyzing communication patterns, and detecting potential security threats. This analysis provided valuable insights into the network's traffic patterns and any suspicious or unauthorized activities.

Throughout the process, I ensured data manipulations and analysis were conducted meticulously to generate accurate and meaningful results. The gathered data was carefully examined and interpreted to identify vulnerabilities, prioritize components, and recommend necessary actions for the organization's security enhancement.

Overall, the analysis was performed with utmost attention to detail, ensuring that the data gathered from various security tools was effectively utilized to derive actionable insights for the organization. The outputs generated from the different tools were integrated and cross-referenced to create a comprehensive understanding of the organization's network environment and its potential risks and vulnerabilities.

By combining the outputs from Nmap, Shields UP!!, Nessus, and Wireshark, I was able to present the organization with a prioritized list of components for recovery in the event of a ransomware attack, a list of servers requiring regular backups, a list of passwords needing to be backed up, a list of devices

that needed updating, and an inventory of network devices. Additionally, I identified deficiencies in the deliverables, offering recommendations to address these shortcomings and improve the organization's overall cybersecurity posture.

The entire process was conducted with a focus on ensuring the highest quality of data analysis and interpretation, resulting in a comprehensive understanding of the organization's security landscape and actionable recommendations to enhance its resilience against potential cyber threats and ransomware attacks.

What Are the Results?

Specific Deliverables:

A) A Prioritized List of Components for Recovery:

In the event of a ransomware attack, prioritizing the recovery of vital and critical network assets is crucial for ensuring business continuity and minimizing the impact of the attack. Based on the Nmap reports and Shields Up and Nessus scans, I can prioritize the components for recovery as follows:

1. **Domain Controller**: The domain controller is a critical component that manages authentication and authorization for all users and devices in the network. It plays a central role in controlling access to resources, making it a top priority for recovery.
2. **File Servers:** File servers store essential data and documents used by the organization. These servers often contain critical business information, financial records, and other sensitive data, making them vital for recovery.
3. **Email Servers:** Email servers are crucial for communication and collaboration within the organization. As a primary communication channel, recovering email servers promptly is essential for business continuity.
4. **Database Servers:** Database servers house critical data that drives various applications and processes within the organization. Ensuring the availability and integrity of databases is crucial for resuming business operations.
5. **Application Servers:** Application servers host essential business applications and services. Recovering these servers is essential to restore specific functionalities and services relied upon by the organization.
6. **Web Servers:** Web servers are responsible for hosting the organization's website and web applications. Ensuring the website's availability is crucial for maintaining communication with customers and stakeholders.
7. **VPN Servers:** VPN servers facilitate secure remote access for employees and authorized users. Ensuring VPN functionality is critical for enabling remote work during the recovery phase.
8. **DNS Servers:** DNS servers are essential for resolving domain names to IP addresses. Maintaining DNS functionality is crucial for proper communication between network devices.
9. **Backup Servers:** Backup servers are vital for storing data backups and recovery points. Ensuring the availability of backup servers is essential for efficient data restoration.
10. **Firewall Devices:** Firewall devices play a significant role in network security by controlling incoming and outgoing network traffic. Ensuring the integrity of firewall configurations is essential for preventing further attacks.
11. **Network Switches:** Network switches provide connectivity and manage data flow within the local network. Recovering switches is important for restoring network connectivity.

12. **Network Routers:** Routers facilitate communication between different networks. Recovering routers is essential for restoring connectivity to external networks and the internet.
13. **Active Directory Replication Servers:** Active Directory replication servers ensure the availability and consistency of the directory service. Ensuring proper replication is crucial for maintaining domain functionality.
14. **Intrusion Detection/Prevention Systems (IDPS):** IDPS devices monitor network traffic for suspicious activities. Ensuring the functionality of IDPS devices is essential for detecting and responding to potential threats.
15. **Security Information and Event Management (SIEM) Servers:** SIEM servers centralize security event logs and aid in monitoring and analysis. Recovering SIEM servers is crucial for identifying potential security incidents.
16. **Physical Access Control Systems:** Physical access control systems regulate entry and exit to sensitive areas. Ensuring the functionality of these systems is vital for securing physical assets.

It is important to note that the prioritization may vary based on the specific needs and criticality of each organization. Organizations should conduct a thorough risk assessment and consider the impact of each asset's unavailability when prioritizing their recovery efforts. Rapid recovery of these critical servers is essential for minimizing downtime and resuming core business operations promptly. Regular updates to this list and the recovery strategy are necessary to adapt to the evolving threat landscape and organizational changes. By focusing on the restoration of these key components, the organization can effectively mitigate the impact of the attack and restore essential functionalities to resume normal operationsA list of passwords that need to be backed up: I identified essential passwords, including administrative passwords, domain administrator passwords, and service account passwords, that need to be securely backed up to maintain access to critical systems and services.

B) List of Servers Requiring Regular Backups:

To ensure a robust recovery process, the organization should prioritize the following backups:

1. **File Servers:** Servers that store and manage files and data for users and applications.
2. **Email Servers:** Servers responsible for handling email communication and messages.
3. **Database Servers:** Servers that manage and store databases containing critical information.
4. **Application Servers:** Servers dedicated to running and managing specific applications or services.
5. **Web Servers:** Servers that host and serve web pages and content to users.
6. **VPN Servers:** Servers that facilitate secure remote access to the organization's network.
7. **Backup Servers:** Servers specifically designed for storing backup data and copies of critical information.
8. **Active Directory Servers:** Servers that control access and authentication in a Windows-based network environment.
9. **DNS Servers:** Servers that translate domain names into IP addresses for internet communication.

Priority for Backups: To ensure a robust recovery process, prioritize the following backups:

1. **Full backups of critical servers and systems, including databases, application configurations, and user data:** Creating complete backups of essential servers and their associated data to ensure comprehensive restoration capabilities.
2. **Incremental backups to capture changes since the last full backup:** Backing up only the changes made since the last full backup to reduce data duplication and backup time.
3. **Off-site backups are stored securely to protect against physical damage or theft:** Keeping backup copies in a separate location, away from the primary site, to ensure data availability in case of disasters or theft.

4. **Regular testing of backups to ensure their integrity and usability during recovery:** Verifying backup data regularly to confirm that it can be successfully restored and utilized during recovery scenarios.

Following this prioritized approach will help maintain crucial safeguards against data loss and enable the restoration of services in case of any unforeseen attack or system failure.

Servers that may need to be backed up on my PC

1- Server at IP Address 192.168.0.15: This server is associated with multiple open ports, including ports 80 (HTTP) and 443 (HTTPS), which may indicate the presence of a web server or web application. If this server hosts critical web applications or data, regular backups are essential to ensure data availability and business continuity.

2- Server at IP Address 192.168.0.10: This server was reported as "host down," which means it was not reachable during the scan. While the status is not confirmed, it is a best practice to include all servers in regular backup plans, regardless of their current status, to prepare for potential future incidents.

3- Server at IP Address 73.37.102.78: This server also had open ports and services, including port 53 (DNS) and port 47808 (unknown). If this server plays a crucial role in DNS resolution or hosts important services, it should be included in the backup strategy.

C) A List of Passwords That Need to Be Backed Up:

Identifying the role is sufficient for backing up passwords. The organization should consider the following:

1. **Administrative passwords for servers, networking equipment, and critical applications:** Administrative passwords refer to privileged access credentials used to manage and control various systems, such as servers, network devices (routers, switches, etc.), and critical applications. These passwords provide elevated privileges and control over the respective systems, so backing them up is crucial to ensure that authorized personnel can access and manage these components even in the event of data loss or system failure.
2. **Domain administrator passwords for Active Directory:** Domain administrator passwords are credentials that grant the highest level of access within an Active Directory (AD) environment. AD is a centralized authentication and authorization service in Windows-based networks. The domain administrator has complete control over all resources in the domain. Backing up these passwords ensures that the organization can recover access to its AD infrastructure, which is essential for user authentication, resource management, and overall network operations.
3. **Service account passwords used by applications and services:** Service account passwords are used by applications and services running on servers to access network resources or interact with other systems. These accounts often operate in the background, and their passwords are sometimes saved and automatically used by applications. Backing up these passwords is essential to prevent service disruptions and maintain proper functioning of critical applications and services.
4. **Local administrator passwords for workstations and servers:** Local administrator passwords are credentials that grant administrative access to individual workstations and servers. These passwords are distinct from domain administrator passwords and provide local control over specific machines. Backing up these passwords is essential to ensure that authorized personnel can access and manage individual systems when needed, even if the network connection to the domain is unavailable or compromised.
5. **Shields UP!! Password:** Shields UP!! is an online service provided by Gibson Research Corporation for port scanning and security testing. The password used to access this service was not explicitly mentioned in the provided text. However, as a security best practice, it is essential to back up any

login credentials used to access online services like Shields UP!! to prevent unauthorized access and ensure continuity of operations.

6. **Nessus Activation Code:** The Nessus vulnerability scanning tool requires an activation code for Nessus Essentials. The activation code was obtained from a specific URL during the downloading phase, but the actual code was not provided in the text. Organizations should ensure that the Nessus activation code is securely backed up to maintain access to the tool and its functionalities.
7. **Network Credentials for Nessus Scan:** During the Nessus vulnerability scan, the IP address 10.1.4.113 was used as the target for the scan. It was mentioned that permission was obtained from Cascade Park Community Library to conduct the scan on their network using this IP address. The actual network credentials (e.g., username and password) used to initiate the scan were not disclosed in the text. However, organizations should back up any network credentials used in vulnerability scanning processes to prevent data loss and maintain the ability to conduct future scans.
8. **Host Credential Status by Authentication Protocol for Nessus Scan:** The Nessus scan identified the status of target credentials by authentication protocol for the target system (IP address 10.1.4.113). The plugin "Target Credential Status by Authentication Protocol - No Credentials Provided (Plugin 110723)" indicated that no credentials were provided for authentication. While no specific credentials were mentioned, organizations should still maintain a record of the authentication protocols and credentials used in the Nessus scans to ensure the proper functioning of the tool and maintain security during future scans.

It is crucial for organizations to follow best practices in securely managing and backing up login credentials, activation codes, and authentication information to prevent data loss, maintain access to essential tools and services, and ensure the overall security of their systems. Backing up these passwords is crucial to maintain data security, prevent service disruptions, and ensure smooth recovery in case of any password-related issues or system failures. Proper backup management of passwords helps maintain the overall security and functionality of the organization's IT infrastructure.

D) A List of Devices That Need to Be Updated:

Based on the Nessus and Shields UP!! identified vulnerabilities in the target system, highlighting the importance of regular updates. The organization should focus on updating:

1. **Operating systems on servers, workstations, and networking devices**: Updating the operating systems (OS) on servers, workstations, and networking devices involves installing the latest patches, bug fixes, and security updates provided by the OS vendors. These updates address known vulnerabilities and bugs in the OS, ensuring that the systems are protected against potential exploits and unauthorized access. Regular OS updates are essential to maintain system stability, performance, and security.
2. **Application software, including outdated software versions, web servers, databases, and third-party software:** Updating application software involves keeping all software used by the organization, including web servers, databases, and third-party applications, up-to-date with the latest versions and security patches. Outdated software versions may contain known vulnerabilities that malicious actors can exploit to gain unauthorized access to the system or compromise sensitive data. Regular updates ensure that applications are equipped with the latest security measures and features, reducing the risk of security breaches.
3. **Network equipment firmware, such as routers and switches:** Network equipment firmware updates involve keeping the firmware of routers, switches, and other networking devices current with the latest releases provided by the manufacturers. Firmware updates often include security fixes, bug patches, and improvements to the device's performance and functionality. Ensuring

network equipment firmware is up to date is crucial to prevent potential security vulnerabilities and maintain the reliability and security of the organization's network infrastructure.

4. **Security patches and misconfigurations for critical vulnerabilities:** Addressing security patches and misconfigurations refers to promptly applying updates and correcting settings that address known critical vulnerabilities in the organization's systems and applications. These patches may come from various sources, including vendors, security advisories, or vulnerability assessments like Nessus and Shields UP!!. By addressing these issues immediately, the organization can prevent potential cyber threats and attacks that may exploit these vulnerabilities.
5. **QUIC Protocol Handshake:** In my report, I mentioned instances of the QUIC protocol handshake. While QUIC is a secure transport protocol, it is essential to verify the authenticity of the connections and ensure that they are legitimate. Keeping the QUIC protocol up to date and implementing strong authentication mechanisms can enhance security.
6. **Analysis of Encrypted Content:** In my report, indicates that some packets contain encrypted data. As the nature of encrypted content cannot be determined without decryption keys, it is crucial to focus on strengthening encryption mechanisms and keeping encryption software up to date to ensure the confidentiality of sensitive information.
7. **Open Networks:** In my report, I mentioned analyzing open networks and their potential security implications. Organizations should ensure that their Wi-Fi networks are secured with strong passwords and encryption, and unauthorized access to these networks should be monitored and prevented.
8. **Identifying Suspicious Ports:** In my report, we discussed the process of identifying packets associated with suspicious ports. To strengthen network security, organizations should regularly review and monitor the use of uncommon or unauthorized ports and investigate any potential signs of malicious activity.
9. **Attack Surface Analysis:** In my report, I mentioned analyzing the attack surface presented by the network and packets. To enhance network security, organizations should conduct comprehensive cybersecurity assessments to identify potential entry points and vulnerabilities that attackers could exploit. This involves evaluating security configurations, identifying open ports and services, and keeping software up to date.
10. **Incident Response:** The report does not explicitly discuss incident response procedures. Organizations should have well-defined incident response plans in place to effectively detect, contain, and mitigate cyber-attacks when they occur. This involves having a dedicated incident response team, clear communication channels, and predefined actions to handle different types of incidents.
11. **Compliance and Auditing:** In my report, I briefly mentioned compliance and auditing purposes. Organizations operating in regulated industries should ensure that their network analysis practices comply with industry standards and regulations. Regular auditing can help identify potential gaps in security and ensure adherence to required protocols.
12. **Monitoring for Cyber-attacks:** While the report does not indicate any explicit cyber-attacks in the captured packets, it is essential to implement continuous monitoring and threat detection mechanisms to identify and respond to any suspicious or malicious activities on the network.

Addressing these areas promptly and updating security measures accordingly is crucial for organizations to enhance their network's resilience against potential cyber threats and vulnerabilities. By giving immediate attention to these components, organizations can ensure their systems and applications are up-to-date and protected, mitigating the risk of ransomware attacks and security breaches. Adopting a proactive approach to network security, staying informed about the latest cybersecurity best practices, and implementing continuous monitoring and regular updates are essential practices for maintaining a

secure and resilient IT environment. These measures ultimately safeguard sensitive data, infrastructure, and operations, contributing to a strong security posture and ensuring a safe digital environment for the organization.

E) An Inventory of Network Devices:

Based on the Nmap report, the inventory of network devices includes:

1. **IP Address 192.168.0.15:** This is a single host with several open ports, including TCP and UDP ports associated with various services.
2. **IP Address 192.168.0.10/24:** The scan identified a range of IP addresses, with some live hosts having open ports indicative of web servers, file sharing, and other services.
3. **IP Address 73.37.102.78:** The scan revealed open ports and services associated with VNC, SMB, DNS, and other protocols.

By following this prioritized approach and ensuring backups, password management, updates, and inventory, the organization can better prepare for recovery from a ransomware attack and strengthen its cybersecurity posture.

Deficiencies in Deliverables:

Overall, the deliverables provided are comprehensive and cover various aspects of preparing an organization to recover from a ransomware attack. However, there are a few deficiencies that need to be addressed:

1. **Lack of External Validation:** One deficiency in our deliverables is the lack of external validation. While we have used Nmap, Shields Up, and Nessus reports to gather information, we haven't conducted external penetration testing or engaged in red team exercises to simulate real-world attack scenarios. External validation can help identify blind spots and potential vulnerabilities that might have been missed.
2. **Limited Scope of Reports:** The Nmap report provided valuable insights into the network devices, open ports, and protocols. However, it does not provide a comprehensive assessment of all network components. Similarly, the Shields Up and Nessus reports focus on specific vulnerabilities and do not cover all possible attack vectors. Expanding the scope of assessments and using multiple tools can provide a more holistic view of the organization's security posture.
3. **Incomplete Vulnerability Severity Assessment:** In the Nessus report, we identified 29 vulnerabilities on the target system, but the exact CVSS scores were not mentioned, limiting our ability to assess their severity accurately. Understanding the severity of vulnerabilities is crucial for prioritizing remediation efforts effectively.

Resolution for Deficiencies:

1. **Conduct External Penetration Testing:** To address the deficiency of external validation, the organization should consider engaging with a reputable cybersecurity firm to conduct external penetration testing and red team exercises. This will provide a more realistic assessment of the organization's security posture and identify potential weaknesses from an attacker's perspective.
2. **Perform Regular Security Assessments:** To overcome the limited scope of reports, the organization should adopt a proactive approach to security by conducting regular security assessments. This can include vulnerability scanning, penetration testing, and security audits. By leveraging a combination of tools and methodologies, the organization can gain a comprehensive understanding of its attack surface.

3. **Prioritize Vulnerability Remediation:** To address the incomplete vulnerability severity assessment, the organization should ensure that all identified vulnerabilities are assigned accurate CVSS scores. This will enable the organization to prioritize remediation efforts based on the severity of each vulnerability. Critical and high-severity vulnerabilities should be addressed first to mitigate the most significant risks.
4. **Implement Incident Response Planning:** An essential aspect of preparing for ransomware attacks is to have a well-defined incident response plan. The organization should develop and regularly update an incident response plan that outlines the step-by-step actions to be taken in the event of a ransomware attack. This plan should include roles and responsibilities, communication protocols, and recovery procedures.
5. **Enhance Employee Training:** Human error and social engineering attacks are common vectors for ransomware infections. The organization should invest in cybersecurity awareness training for employees to recognize and report suspicious activities. Employees should be educated about the importance of strong passwords, phishing prevention, and safe online practices.
6. **Regular Backups and Testing:** To ensure successful recovery from a ransomware attack, regular backups of critical data should be performed. Moreover, the organization should periodically test the backup restoration process to verify the integrity of the backups and the effectiveness of the recovery procedures.

With these steps in place, the organization can be better equipped to defend against ransomware threats and protect its critical assets and data.

What Did You Learn?

Ransomware and Preparing for Recovery:

From the assignment, I have learned that ransomware attacks are a significant threat to organizations and can cause severe disruptions if not properly handled. To prepare for recovery from a ransomware attack, several best practices have been identified, such as backups, software updating, password management, asset inventories, and well-defined response procedures. Backups are crucial to restore critical data and systems without paying ransom. Regularly updating software and patching vulnerabilities help prevent attackers from exploiting known weaknesses. Proper password management ensures that weak credentials are not easily breached while maintaining an inventory of network assets helps prioritize recovery efforts. Having well-defined response procedures enables the organization to respond quickly and effectively during an attack, minimizing the impact and downtime.

Future Use:

In the future, I can use the knowledge gained from this assignment to create and implement a comprehensive ransomware recovery plan for an organization. By understanding the importance of backups, software updates, password management, and asset inventories, I can help organizations strengthen their security posture and mitigate the impact of a potential ransomware attack. Additionally, I can use the knowledge of vulnerability scanning and network analysis to identify and prioritize critical assets that need protection and recovery. By incorporating the insights gained from Nmap, Shields Up, Nessus, and Wireshark reports, I can take a proactive approach to safeguarding organizations against ransomware threats.

Value to the Organization:

The insights and skills gained from this assignment have significant value for the organization in the future, particularly in terms of enhancing cybersecurity resilience. By understanding the attack surface presented by their network and identifying vulnerabilities, the organization can take proactive measures to strengthen security and prevent ransomware attacks. Implementing regular vulnerability scans, security assessments, and penetration testing based on the methods used in the Nmap, Shields Up, Nessus, and Wireshark reports can help the organization identify potential weaknesses and address them before they are exploited by malicious actors. Additionally, the knowledge of preparing for ransomware recovery can enable the organization to create a robust incident response plan, ensuring a swift and effective response if an attack occurs.

To improve the report:

1. **Add a section on the importance of user education and awareness:** In the future, I would suggest including a section that emphasizes the significance of educating users and employees about ransomware threats and cybersecurity best practices. User awareness plays a critical role in preventing ransomware attacks, as many incidents occur due to human error, such as clicking on malicious links or falling victim to phishing emails.
2. **Include a risk assessment and mitigation strategy:** While the vulnerability scans and network analysis provide valuable information, it would be beneficial to include a risk assessment based on the identified vulnerabilities. This assessment can help the organization prioritize its efforts and allocate resources to address the most critical risks first. Additionally, a comprehensive mitigation strategy for each identified vulnerability can further enhance the organization's cybersecurity preparedness.
3. **Recommend the adoption of a security framework:** To provide a comprehensive approach to ransomware recovery preparedness, I would suggest recommending the organization to adopt a recognized security framework, such as the NIST Cybersecurity Framework or CIS Controls. These frameworks provide a structured approach to improving cybersecurity practices and can guide the organization in developing a robust and well-rounded security program.
4. **Emphasize the importance of testing the recovery plan:** While backups are essential for ransomware recovery, it is equally crucial to regularly test the recovery plan. I would suggest adding a section that highlights the significance of testing backups and the recovery process to ensure their effectiveness when a real attack occurs.
5. **Provide recommendations for incident response coordination:** It would be beneficial to include recommendations on establishing incident response coordination with relevant authorities, such as law enforcement and cybersecurity experts. In case of a ransomware attack, having a clear communication and coordination plan with external stakeholders can facilitate a more effective response and investigation.

Conclusion

In conclusion, preparing an organization to recover from a ransomware attack requires a comprehensive and proactive approach. By utilizing the outputs from Nmap, Shields UP!!, and Nessus reports, organizations can identify critical components, prioritize backups, address vulnerabilities, and fortify their defenses against ransomware threats. Prioritizing network assets, ensuring regular and tested backups, backing up critical passwords, updating devices to address vulnerabilities, and maintaining an inventory of network devices are essential steps to improve resilience and readiness for potential ransomware incidents. Regular security assessments, vulnerability scanning, and continuous monitoring play a crucial

role in identifying potential weaknesses and ensuring a proactive security stance. Additionally, fostering a culture of cybersecurity awareness among employees and implementing best practices will further strengthen the organization's defense against ransomware threats in today's evolving cybersecurity landscape, where threats continue to evolve and become more sophisticated.

Resources:

1. 2023 Global Threat Report
2. 2023 Cybersecurity Skills Gap Global Research Report
3. NIST Special Publication 1800-34: Validating the Integrity of Computing Devices
4. The State of Cloud-Native Security 2023 Report