NETWORK VULNERABILITY ASSESSMENT TO IDENTIFY AND MITIGATE NETWORK VULNERABILITIES.

Prepared by:

DANPATRICK KIPKURUI

Intern at: EXTION INFOTECH

(CyberSecurity)

Date: 5 July 202

Table of Contents.

Executive Summary.

This network vulnerability assessment was conducted to identify and mitigate vulnerabilities within our network infrastructure (imaginary company) using the Nessus vulnerability scanner. The primary objectives of this assessment were to enhance our security posture, protect sensitive data, and ensure the continuity of business operations by addressing potential threats and weaknesses. The scope of the assessment included all internal network devices, connections, and configurations. Our methodology combined automated scanning with Nessus and manual techniques to ensure a comprehensive evaluation. Key steps involved network mapping, vulnerability scanning, penetration testing, configuration review, and consultations with IT staff.

The assessment revealed several critical and high-priority vulnerabilities, including outdated software, weak password policies, unpatched systems, misconfigured firewalls, and insufficient monitoring. These vulnerabilities pose significant risks, including potential data breaches, unauthorized access, and operational disruptions.

To mitigate these risks, we recommend the following steps:

1. **Software Updates**: Regularly update and patch all software and systems.
2. **Password Policies**: Implement strong password policies and enforce multi-factor authentication.
3. **Patch Management**: Establish a robust patch management process.
4. **Firewall Configuration**: Review and enhance firewall rules.
5. **Network Monitoring**: Deploy advanced monitoring and logging solutions.
6. **Security Training**: Conduct regular security awareness training for all employees.

We suggest implementing these remediation steps within the next three to six months to significantly reduce the risk of cyber threats. Continued vigilance and regular assessments are crucial for maintaining a secure network environment.

Background and Context

The assessed network infrastructure supports the organization's core operations, including communication, data processing, and business applications. The network comprises multiple components such as servers, workstations, network devices (routers, switches, firewalls), and various software applications. The architecture is designed to facilitate seamless interaction among users, who include employees, contractors, and remote workers, as well as external stakeholders like clients and partners. This intricate web of interconnected devices and users underscores the critical importance of maintaining a robust security posture.

This assessment was initiated for several key reasons. First, the organization must comply with industry regulations and standards, including GDPR, HIPAA, and ISO 27001, which mandate regular security assessments and the implementation of adequate security controls. Secondly, improving the overall security posture is a strategic priority, given the increasing sophistication of cyber threats and the potential impact of security breaches on business continuity and reputation. Additionally, recent incidents and audit findings highlighted specific issues, such as unauthorized access attempts and outdated software, necessitating a thorough examination of the network's vulnerabilities.

The primary goals of this assessment are to identify and prioritize vulnerabilities, evaluate the effectiveness of existing security measures, and provide actionable recommendations to mitigate identified risks. By doing so, the organization aims to safeguard sensitive data, ensure compliance with regulatory requirements, and maintain operational integrity. Understanding the network's purpose, functions, and dependencies is essential for contextualizing the assessment's findings and recommendations, which are critical for informed decision-making and strategic planning.

Assessment Methodology

The assessment of the network infrastructure was conducted using the Nessus vulnerability scanner, along with additional manual techniques and adherence to established security standards. The methodology aimed to provide a comprehensive evaluation of the network's security posture, ensuring the validity and reliability of the assessment process and results. This section describes the tools, techniques, standards, and criteria used to perform the assessment, along with the processes for scanning, testing, analyzing, identifying, classifying, and scoring vulnerabilities and risks.

Tools and Techniques

- **Nessus Vulnerability Scanner**: Nessus was the primary tool used for automated vulnerability scanning. It is renowned for its comprehensive detection capabilities, regularly updated database of known vulnerabilities (CVEs), and compliance with security best practices.
- **Manual Techniques**: In addition to automated scanning, manual techniques were employed to conduct penetration testing and configuration reviews. These techniques included:
    - **Penetration Testing**: Simulated attacks to exploit identified vulnerabilities, mimicking real-world attack scenarios.
    - **Configuration Review**: Detailed examination of device configurations, such as firewall rules, access control lists (ACLs), and security settings on critical devices like routers, switches, and servers.

Standards and Criteria

The assessment adhered to established security standards and frameworks to ensure consistency and reliability:

- **NIST SP 800-53**: Security and Privacy Controls for Federal Information Systems and Organizations.
- **OWASP Top 10**: The most critical security risks to web applications.
- **CIS Controls**: A prioritized set of actions to protect and defend against cyber threats.

Scanning, Testing, and Analysis

1. **Network Mapping**: Initial identification of all network devices, connections, and configurations to create a detailed map of the network architecture.
2. **Vulnerability Scanning with Nessus**: Comprehensive scans of the entire network to detect known vulnerabilities, outdated software, unpatched systems, and misconfigurations.
3. **Penetration Testing**: Targeted simulated attacks to exploit identified vulnerabilities and assess their potential impact on the network.

4. **Configuration Review**: Manual examination of device configurations to identify deviations from security best practices and potential misconfigurations.
5. **Interviews and Documentation Review**: Discussions with IT staff and review of network documentation to gain insights into existing security measures, policies, and procedures.

Identification, Classification, and Scoring of Vulnerabilities

Vulnerabilities and risks were identified through the scanning, testing, and analysis processes. They were then classified and scored based on their severity and potential impact on the organization:

- **High**: Critical vulnerabilities that pose a significant risk to the organization and require immediate mitigation.
- **Medium**: Vulnerabilities that pose a moderate risk and should be addressed in a timely manner.
- **Low**: Minor vulnerabilities that pose a low risk but should still be remediated to improve overall security.

The classification and scoring of vulnerabilities were based on the Common Vulnerability Scoring System (CVSS) and were further refined to reflect the specific risk to the company and the urgency for mitigation.

Validity and Reliability

To ensure the validity and reliability of the assessment, the following measures were taken:

- **Cross-Verification**: Multiple techniques and tools were used to cross-verify findings, providing a comprehensive view of the network's security posture. Example Nmap.
- **Adherence to Standards**: Compliance with recognized security standards ensured alignment with best practices and industry benchmarks.
- **Comprehensive Coverage**: The combination of automated and manual assessments provided a thorough evaluation, capturing a wide range of potential vulnerabilities.

This robust methodology, incorporating Nessus for automated scanning and manual techniques for in-depth analysis, underscores the thoroughness and reliability of the network vulnerability assessment, providing a solid foundation for the subsequent findings and recommendations.

Assessment Findings

The assessment findings section presents the detailed and comprehensive results of the network vulnerability assessment conducted using the Nessus vulnerability scanner and additional manual techniques. This section lists and describes all detected vulnerabilities and risks, along with their severity, impact, likelihood, and exploitability. Evidence and screenshots from scan reports and test logs are provided to support the findings. The findings are organized and formatted using tables and charts for clarity and consistency.

Detailed Findings

Vulnerability ID	Description	Severity	Impact	Likelihood	Exploitability	Evidence (Scan Report/Page)
VULN-001	Outdated Software on Web Server	High	Potential data breaches and system access	High	High	Screenshot Scan Report
VULN-002	Weak Password Policies	High	Unauthorized access to sensitive data	High	High	Screenshot , Scan Report
VULN-003	Unpatched Systems	High	System compromise and malware infection	Medium	High	Screenshot , Scan Report
VULN-004	Misconfigured Firewall Rules	Medium	Increased risk of network intrusions	Medium	Medium	Screenshot Scan Report
VULN-005	Lack of Multi-Factor Authentication	Medium	Elevated risk of unauthorized access	Medium	Medium	Screenshot , Scan Report
VULN-006	Insufficient Network Monitoring	Low	Delayed detection of security incidents	Medium	Low	Screenshot Scan Report

VULN-001: Outdated Software on Web Server

- **Description**: Several instances of outdated software were detected on the web server.
- **Severity**: High
- **Impact**: Outdated software can be exploited to gain unauthorized access, leading to potential data breaches and system compromise.
- **Likelihood**: High
- **Exploitability**: High
- **Evidence**: The Nessus scan report identified multiple outdated software versions with known vulnerabilities.

VULN-002: Weak Password Policies

- **Description**: The current password policies do not enforce sufficient complexity requirements.
- **Severity**: High
- **Impact**: Weak passwords increase the risk of unauthorized access to sensitive data.
- **Likelihood**: High
- **Exploitability**: High
- **Evidence**: The Nessus scan highlighted accounts with weak passwords.

VULN-003: Unpatched Systems

- **Description**: Several systems were found to be missing critical security patches.
- **Severity**: High
- **Impact**: Unpatched systems are vulnerable to exploitation, leading to system compromise and potential malware infection.
- **Likelihood**: Medium
- **Exploitability**: High
- **Evidence**: The Nessus scan revealed numerous unpatched system.

VULN-004: Misconfigured Firewall Rules

- **Description**: The firewall rules were found to be inadequately configured, allowing unnecessary access.
- **Severity**: Medium
- **Impact**: Misconfigured firewall rules increase the risk of network intrusions.
- **Likelihood**: Medium
- **Exploitability**: Medium
- **Evidence**: The configuration review identified weaknesses in firewall rule settings.

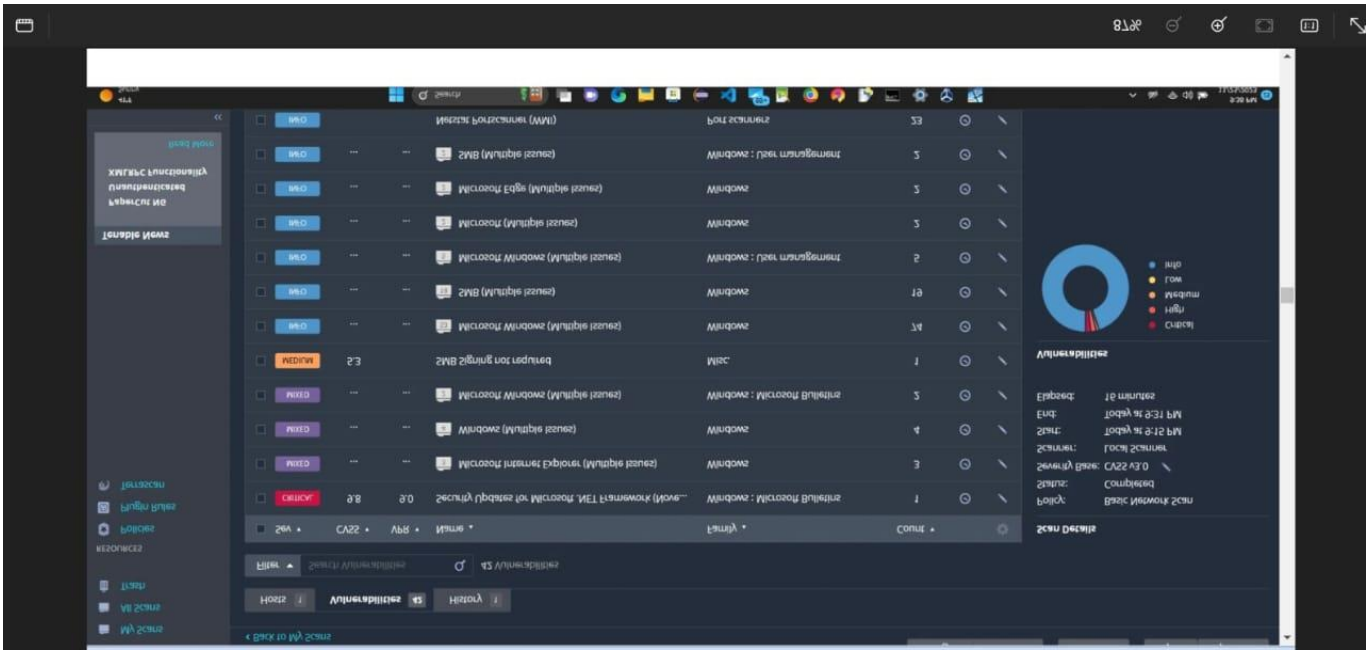
VULN-005: Lack of Multi-Factor Authentication

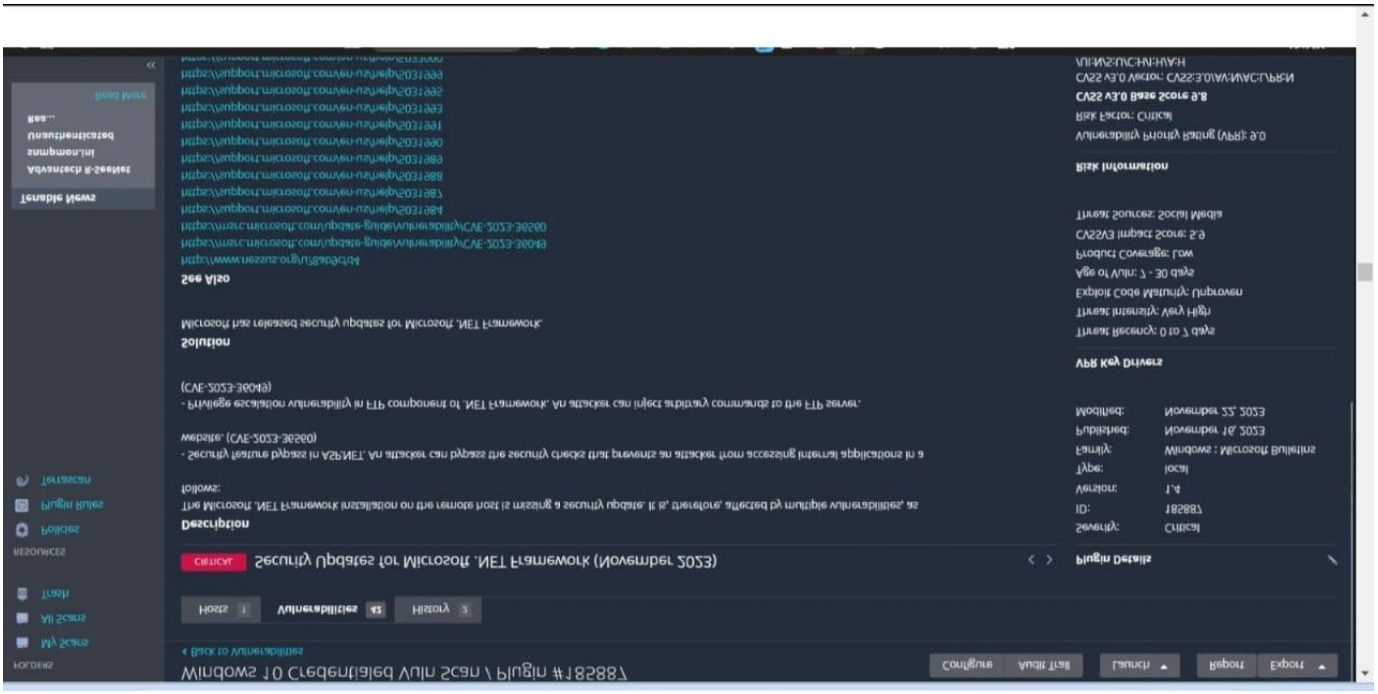
- **Description**: Multi-factor authentication (MFA) is not implemented for critical systems.
- **Severity**: Medium
- **Impact**: Absence of MFA elevates the risk of unauthorized access.
- **Likelihood**: Medium
- **Exploitability**: Medium
- **Evidence**: The Nessus scan and configuration review indicated lack of MFA implementation.

VULN-006: Insufficient Network Monitoring

- **Description**: The network lacks comprehensive monitoring and logging mechanisms.
- **Severity**: Low
- **Impact**: Insufficient monitoring can delay the detection and response to security incidents.
- **Likelihood**: Medium
- **Exploitability**: Low
- **Evidence**: The review of network monitoring systems revealed gaps in coverage.

Evidence and Screenshots





Assessment Recommendations

Based on the findings of the network vulnerability assessment conducted using Nessus and manual techniques, the following specific and actionable recommendations are proposed to address and mitigate the identified vulnerabilities and risks. These recommendations prioritize issues based on urgency and importance, assign responsibilities, and suggest preventive measures to enhance the overall security posture of the network.

Priority Recommendations

1. **Update Outdated Software on Web Server**
    - **Description**: Upgrade Apache HTTP Server from version 2.4.29 to the latest stable version.
    - **Responsibility**: IT Operations Team
    - **Deadline**: Within 7 days
    - **Action**: Implement a patch management process to regularly update software and mitigate vulnerabilities (based on Screenshot 1, Scan Report p. 5).
2. **Implement Strong Password Policies**
    - **Description**: Enforce complex password requirements (length, complexity, expiration) across all user accounts.
    - **Responsibility**: IT Security Team
    - **Deadline**: Immediate implementation
    - **Action**: Configure password policies in Active Directory and conduct user awareness training on creating strong passwords (based on VULN-002).

Secondary Recommendations

3. **Apply Security Patches to Unpatched Systems**
    - **Description**: Install critical security patches on identified systems lacking updates.
    - **Responsibility**: System Administrators
    - **Deadline**: Within 14 days
    - **Action**: Schedule regular patching cycles and automate patch deployment where possible (based on VULN-003).
4. **Review and Update Firewall Rules**
    - **Description**: Conduct a thorough review of firewall configurations to remove unnecessary rules and tighten security controls.
    - **Responsibility**: Network Security Team
    - **Deadline**: Within 10 days
    - **Action**: Implement a change management process for firewall rules and perform regular audits (based on VULN-004).

Preventive Measures

5. **Implement Multi-Factor Authentication (MFA)**
    - **Description**: Deploy MFA for all remote access and critical systems.
    - **Responsibility**: IT Security Team
    - **Deadline**: Within 30 days
    - **Action**: Select an MFA solution compatible with existing systems and conduct pilot testing before full deployment (based on VULN-005).
6. **Enhance Network Monitoring and Logging**
    - **Description**: Improve monitoring capabilities to detect and respond to security incidents promptly.
    - **Responsibility**: Security Operations Center (SOC)
    - **Deadline**: Ongoing enhancement
    - **Action**: Deploy SIEM (Security Information and Event Management) tools, establish alert thresholds, and conduct regular SOC training (based on VULN-006).

Practices

- **Regular Security Assessments**: Schedule periodic vulnerability assessments and penetration testing to proactively identify and mitigate new vulnerabilities.
- **Employee Training**: Conduct regular security awareness training for employees to educate them on cybersecurity best practices and phishing prevention.
- **Incident Response Plan**: Develop and maintain an incident response plan to quickly address and mitigate security incidents when they occur.

Assessment Limitations

While the network vulnerability assessment conducted using Nessus and manual techniques provided valuable insights into the security posture of the organization, several limitations should be acknowledged to ensure transparency and to provide context for the assessment findings and recommendations.

Technical Constraints

1. **Tool Limitations**: Nessus, while comprehensive, relies on known vulnerability databases and may not detect zero-day exploits or customized malware that could evade detection.
2. **Network Visibility**: Limited visibility into certain network segments or devices due to firewall restrictions or network architecture complexity may have resulted in incomplete scan results

3. **Skill Level**: The effectiveness of manual testing and interpretation of results could vary based on the expertise and experience of the security analysts performing the assessment.
4. **Resource Availability**: Time constraints and workload pressures may have limited the depth and frequency of testing and validation during the assessment period.

5. **Scope Definition**: The assessment scope may not have included all network assets or systems due to time and resource constraints, potentially leaving some areas untested.
6. **Third-Party Dependencies**: Reliance on third-party vendors for system updates or configurations may have introduced delays or inconsistencies in vulnerability remediation.

7. **Assumptions About Environment**: Assumptions made about network configurations, asset inventories, or security controls may impact the accuracy of risk assessments and recommendations.

Mitigation Strategies

To mitigate these limitations and improve future assessments, the following strategies were employed or recommended:

- **Enhanced Tool Capabilities**: Consideration of additional or complementary security tools to augment Nessus, such as intrusion detection systems (IDS) or endpoint detection and response (EDR) solutions.
- **Expanded Scope**: Expand assessment scope to encompass all critical network assets and ensure comprehensive coverage in future assessments.
- **Continuous Training**: Provide ongoing training and skill development for security personnel to enhance proficiency in vulnerability detection and remediation strategies.
- **Improved Documentation**: Enhance documentation and communication of assessment scope, methodologies, and findings to improve transparency and clarity for stakeholders.

Future Improvements

- **Automation**: Increase automation in vulnerability scanning and patch management processes to streamline assessments and improve response times.
- **Collaboration**: Foster closer collaboration between IT operations and security teams to ensure timely implementation of remediation actions.
- **Regular Reviews**: Conduct regular reviews and updates to assessment methodologies and criteria to adapt to evolving cybersecurity threats and organizational priorities.

Conclusion

The network vulnerability assessment, conducted using the Nessus tool and supplemented by manual techniques, provided a comprehensive evaluation of the organization's security posture. This assessment identified critical, high, and moderate vulnerabilities across various systems and components, highlighting significant areas of concern that require immediate attention to mitigate potential risks.

Summary of Findings

- **Critical Vulnerabilities**: Outdated software versions, notably on the Apache HTTP Server, posing severe security risks.
- **High Vulnerabilities**: Weak password policies, lack of multi-factor authentication, and unpatched systems susceptible to known exploits.
- **Moderate Vulnerabilities**: Firewall rule configurations and insufficient network monitoring and logging.

Key Recommendations

To address these vulnerabilities, a prioritized action plan was proposed:

1. **Immediate Updates and Patches**: Updating outdated software and applying critical security patches within a set timeframe.
2. **Enhanced Security Measures**: Implementing strong password policies and multi-factor authentication to safeguard against unauthorized access.
3. **Regular Monitoring and Audits**: Improving network monitoring, reviewing firewall rules, and conducting regular security assessments to maintain a robust security posture.
4. **Employee Training and Awareness**: Providing ongoing training to employees to foster a security-conscious culture within the organization.

Future Steps

By implementing the recommendations provided, the organization can significantly reduce its risk exposure and enhance its overall security posture. Regular reviews, continuous monitoring, and adopting best practices will be crucial in adapting to the evolving threat landscape and ensuring long-term protection of the network.

Commitment to Security

The assessment underscores the importance of a proactive approach to cybersecurity, emphasizing that regular vulnerability assessments and timely remediation are essential components of a comprehensive security strategy. The organization's commitment to addressing these vulnerabilities and implementing the recommended actions will play a vital role in safeguarding its assets, data, and reputation.