Network Security Tools Report

Introduction

This report documents the usage and analysis of three essential network security tools: Wireshark for packet analysis, a vulnerability scanner (Nessus Essentials), and a penetration testing tool. The report provides a detailed analysis of the data captured, identifies vulnerabilities, and offers actionable recommendations for improving network security.

Wireshark Capture Analysis

Summary

Wireshark was used to capture network traffic for a 10-minute window during peak usage hours. The capture focused on monitoring HTTP, HTTPS, and DNS protocols across the network.

Observations

1. **Unencrypted HTTP Traffic**:
    - Several HTTP packets revealed sensitive data transmitted in plaintext, including potential login credentials and session cookies.
2. **DNS Queries**:
    - Numerous DNS queries to external servers were observed, with some domains flagged as suspicious based on reputation analysis.
3. **High Volume Traffic from a Single IP**:
    - Anomalous activity detected from IP `192.168.1.105`, which generated a high volume of outbound traffic, possibly indicating a compromised host or misconfiguration.

Recommendations

1. **Enforce HTTPS**:
    - Mandate the use of HTTPS for all web traffic and ensure SSL/TLS certificates are properly configured.
2. **DNS Security**:
    - Implement DNS filtering and monitor outbound queries to prevent data exfiltration.
3. **Monitor and Mitigate Anomalies**:

- Investigate the high outbound traffic from IP `192.168.1.105` and isolate the host if necessary.

Network Vulnerability Scanner Report Analysis

Summary

A vulnerability scan was conducted using Nessus Essentials. The scan identified critical, high, and medium vulnerabilities across the network, providing insights into potential risks.

Findings and Observations

1. **Critical Vulnerabilities**:
   - Unpatched operating systems.
   - Insecure software versions.
   - Exposed critical services with default configurations.
2. **High Risk Vulnerabilities**:
   - Firewall misconfigurations.
   - Lack of encryption for sensitive transmissions.
   - Deprecated protocols (e.g., TLS 1.0).
3. **Medium to Low Risk Vulnerabilities**:
   - Information leaks through exposed banners or headers.
   - Systems with improper access controls.
   - Default credentials in use.
4. **Other Issues**:
   - Unnecessary services running on critical nodes.
   - Weak backup and logging configurations.

Recommendations

1. **Patch Management**:
   - Apply updates to all unpatched systems and software.
   - Schedule regular vulnerability scans to identify new risks.
2. **Configuration Hardening**:
   - Disable unnecessary services and close unused ports.
   - Strengthen firewall rules and disable deprecated protocols.
3. **Encryption and Authentication**:
   - Enforce TLS 1.2+ for all data exchanges.
   - Replace default credentials and implement strong passwords.
   - Enable multi-factor authentication (MFA).
4. **Monitoring and Response**:
   - Enhance logging for critical nodes.

    - Monitor for unauthorized access attempts and anomalies.
5. **Access Control**:
    - Enforce least privilege access for all users and services.
    - Regularly audit access control lists (ACLs).

Next Steps

Once the penetration testing tool output is provided, it will be analyzed and integrated into this report to offer a comprehensive security posture assessment. Further actions will then be recommended based on identified risks and vulnerabilities.

Conclusion

This report highlights the importance of leveraging network security tools for identifying vulnerabilities and monitoring traffic. By addressing the recommendations provided, the network's security posture can be significantly enhanced.