OpenVAS

Open Vulnerability Assessment Scanner

PROJECT PROPOSAL

NETWORK VULNERABILITY SCANNING

DANIYAL ALI | 27670 | 13/MARCH/2025

Project Proposal:

Network Vulnerability Scanning using OpenVAS/Nessus

1. **Project Title:**

   Network Vulnerability Scanning and Security Assessment using OpenVAS and Nessus

2. **Introduction:**

   With the increasing number of cyber threats, organizations must ensure their networks are secure. This project aims to conduct a vulnerability assessment using OpenVAS and Nessus to identify and mitigate security weaknesses in a network. The findings will help improve network security by providing actionable insights and remediation steps.

3. Objectives:

- To analyze a network for vulnerabilities using OpenVAS and Nessus.
- To classify security threats based on risk levels (Critical, High, Medium, Low).
- To generate a detailed vulnerability report with mitigation strategies.
- To implement security measures and re-evaluate the network's security posture.

4. Tools and Technologies:

- **OpenVAS (Greenbone Vulnerability Manager)** – Open-source vulnerability scanner.
- **Nessus** – Commercial vulnerability scanner with advanced threat detection.
- **Kali Linux** – Security testing platform.
- **Virtual Machines/Physical Network** – Target environment for testing.
- **Wireshark** – Packet analysis tool (optional for deeper inspection).

5. Methodology:

1. **Setup OpenVAS and Nessus** on a test network.
2. **Configure scans** by selecting target IP addresses and setting scanning parameters.
3. **Execute vulnerability scans** to detect misconfigurations, outdated software, and security risks.
4. **Analyze scan results** to identify vulnerabilities and assess their impact.

5. **Generate reports** and document recommended security improvements.
6. **Implement fixes** (patch updates, firewall adjustments, and access control changes).
7. **Re-scan the network** to validate security enhancements.

6. Expected Outcomes:

- A **detailed security assessment report** highlighting vulnerabilities.
- **Recommendations** for mitigating security risks.
- **Improved network security** through the application of fixes.
- **Hands-on experience** with industry-standard security tools.

8. Conclusion:

This project will provide valuable insights into network security vulnerabilities and mitigation strategies. By leveraging OpenVAS and Nessus, we can help organizations strengthen their security posture and prevent cyber threats.