Risk Assessment and Information Gathering

Prepared by: Leo D. Dorsey

Objective

To conduct a comprehensive risk assessment and information-gathering process in order to identify security vulnerabilities, assess business impact, and provide actionable recommendations to reduce organizational risk.

Tools & Methods

Tools Used: Qualys, OpenVAS, Wireshark, OSINT Framework

Information Sources: Network topology diagrams, asset inventories, employee interviews, historical incident reports

Assessment Standards: NIST SP 800-30, ISO/IEC 27005

Approach:

- Asset identification and classification
- Threat modeling
- Vulnerability and impact analysis
- Likelihood estimation and risk scoring

Implementation Steps

1. Scope Definition: Worked with stakeholders to define organizational boundaries and critical assets.

2. Data Collection: Collected data from internal systems, logs, and personnel to map vulnerabilities and information flows.

3. Threat Identification: Identified internal and external threats relevant to each system or data type.

4. Risk Analysis: Evaluated the likelihood and impact of each threat using a quantitative risk matrix.

5. Recommendations: Developed mitigation strategies, including risk avoidance, transference, reduction, or acceptance.

Results / Findings

- Mapped all IT assets and their relative business importance

- Identified several high-impact risks tied to outdated internal processes and legacy hardware

- Presented findings to management with clear business-aligned recommendations

- Helped initiate a broader organizational risk management framework

Conclusion

This project improved organizational risk visibility and laid the groundwork for a formalized risk management strategy. It provided decision-makers with the insight necessary to prioritize resources and plan for future risk-reduction efforts.

Screenshot Section