Project Deliverable #4**: VPN Optimization, Penetration Testing, and Mid-Project Presentation Preparation**

**Description:**

In Week 6, the team focused on optimizing the VPN configuration, conducting penetration testing to identify vulnerabilities, and preparing for the mid-project presentation to stakeholders. This deliverable outlines the key tasks completed and the results achieved during the week.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Optimization of VPN Configuration (6-Oct-24 to 10-Oct-24)**

* **Task**: Enhance encryption protocols and bandwidth efficiency.
* **Details:**

Reviewed feedback from testing and advisor meetings, focusing on encryption protocols like AES-256 for improving security. Conducted performance testing after applying the optimizations, confirming improvements in data transmission speed and encryption handling. As a result, we tried and Enhanced encryption security with minimal impact on network performance. Bandwidth usage was reduced, increasing overall efficiency.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2.** **Penetration Testing (7-Oct-24 to 9-Oct-24)**

* **Task**: Conduct security assessments to identify vulnerabilities.
* **Details:**

Based on our project’s work schedule for this week we must design and make prototypes and ensure and work upon what type works the best. Performed vulnerability scans on the VPN infrastructure, identifying potential flaws in encryption protocols and access control mechanisms. Team members ensured and detected several medium-level vulnerabilities related to access control lists (ACLs) and user authentication processes. Created a prioritized list of vulnerabilities, with a timeline to address critical issues immediately. Proposed adjustments to access control settings and stronger authentication protocols.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.** **Business Risk Analysis (8-Oct-24)**

* **Task:** Enlightened by the project coordinator to run a business, more precisely project risk analysis.
* **Details:**

According to the analysis performed by the team, there could be new legislation or compliance standards related to data protection, encryption, or privacy, which might necessitate changes in the VPN setup. Failure to comply could result in legal penalties. Optimizing and securing the VPN may involve unforeseen expenses such as additional hardware or more robust encryption tools. If vulnerabilities are identified, addressing them could escalate costs. We also tried SWOT and PESTLE analysis through which we inferred Cyberattacks exploiting weak VPN points could result in data loss, regulatory fines, or damage to reputation. External factors like changes in technology (Technological), evolving cyber threats (Economic), or new data privacy laws (Legal) could impact the VPN configuration and require ongoing monitoring and adaptation

**4. Mid-Project Presentation Preparation (9-Oct-24 to 10-Oct-24)**

* **Task:** Develop presentation materials and practice for stakeholder meetings.
* **Details:**

Created presentation slides highlighting key milestones, including VPN optimization, encryption improvements, and penetration testing results. Included visual aids such as network diagrams, testing graphs, and vulnerability charts to illustrate progress. Practiced presentation with the team to ensure clarity, coherence, and readiness to answer stakeholder questions. Received feedback from the project advisor, who suggested focusing more on the roadmap for addressing identified vulnerabilities.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5. Progress Report #4 + Activity Log (10-Oct-24):**

* **Task**: Compiled the Week 6 progress report and activity log.
* **Details**: Week 6 saw significant progress in both the configuration and testing of VPN security protocols, ensuring the network's robustness against potential threats. The team is on track to present these updates during the upcoming mid-project review. ​

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6.**Issues Encountered:**

* **Packet Tracer Bugs**: During testing, a minor bug was encountered in Cisco Packet Tracer that caused intermittent connection drops in the VPN tunnel. The issue was resolved after troubleshooting network parameters, but the team will monitor the system for any recurring problems.

​

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Deliverables:**

1. **Optimized VPN Configuration:**

Documented the improvements in encryption protocols and bandwidth efficiency, including the specific configurations applied to the VPN tunnels.

1. **Penetration Testing Report:**

A detailed report outlining the vulnerabilities identified during penetration testing, with a risk assessment and mitigation plan.

1. **Mid-Project Presentation Slides:**

A well-structured set of slides showcasing project progress, results from testing and optimization efforts, and a roadmap for the remaining project phases.

**Next Week’s Agenda (Week 7)**

1. **Finalizing VPN Vulnerability Mitigation**

Implement the proposed adjustments to **Access Control Lists (ACLs)** and enhance user authentication protocols. Re-Test the VPN infrastructure after changes to ensure all medium and critical vulnerabilities have been resolved.

1. **Advanced Security Protocol Implementation**

Research and integrate **two-factor authentication (2FA)** for remote access VPN users to improve login security. Investigate the use of **IPSec** or **OpenVPN** improvements to strengthen VPN encryption.

1. **Preparation for Final Presentation**

Start drafting a final report detailing all phases of the VPN project, including configurations, testing, security measures, and performance results. Create initial slides for the final presentation, summarizing the project's achievements, challenges, and next steps. Schedule practice sessions to refine the final presentation.