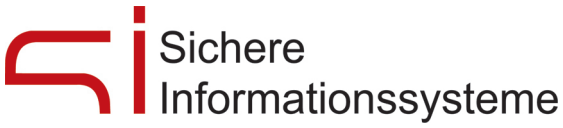

Projekt (PRO3)

Projektideen

Jakob Mayr, Lukas Kaiser, Jonas Pfeiffer

WS 2023/2024

Projektideen

1. **Security Audit of a Small Business or University System**: Conduct a thorough security audit of a small business's or your university's IT infrastructure. This could involve vulnerability scanning, assessing the effectiveness of existing security measures, and providing recommendations for improvements.

2. **Cybersecurity Training Game or Application**: Develop an interactive game or application that teaches basic cybersecurity concepts to users, such as password security, safe browsing habits, and understanding of common cyber threats.

3. **Incident Response Drill**: Plan and execute a simulated cybersecurity incident for your university's IT infrastructure, followed by a thorough incident response that includes identifying the breach, containing it, and recovering from it.

4. **Homelab-Security-Infrastructure**:

Goal

To build a scalable and secure home-lab environment that can onboard client systems (both Linux and Windows) and provide critical cybersecurity services like WAF and SIEM.

Project Phases

(a) **Planning and Design:**
Define Objectives: Clearly outline what you want to achieve with each service (WAF, SIEM, etc.). Infrastructure Design: Plan the network architecture, including the placement of services, segmentation, and how clients will be onboarded. Tool Selection: Choose the appropriate tools and software (e.g., Splunk for SIEM, and a suitable WAF solution).

(b) **Setting Up the Infrastructure:**
Hardware and Software Setup: Acquire necessary hardware and install required software. This may include virtualization solutions for creating different client environments. Network Configuration: Set up the network, ensuring proper segmentation and security measures are in place.

(c) **Service Implementation:**
WAF Setup: Install and configure the WAF to protect web applications from common threats and attacks. SIEM Implementation: Deploy a SIEM solution like Splunk, configure it to collect logs from various sources, and set up dashboards for monitoring.

(d) **Onboarding Clients:**
Client Preparation: Prepare Linux and Windows systems with necessary configurations for onboarding. Integration: Integrate these client systems into the home-lab, ensuring they are properly communicating with the WAF and SIEM services.

(e) **Testing and Optimization:**
Functionality Testing: Test the services for basic functionality and performance. Security Testing: Conduct vulnerability assessments and penetration testing to identify and rectify security gaps. Optimization: Fine-tune the services based on the test results for optimal performance and security.

(f) **Documentation and Reporting:**
System Documentation: Create comprehensive documentation of the setup, configurations, and procedures. Findings and Recommendations: Document the findings from testing and provide recommendations for improvements.

(g) **Presentation:**
Final Presentation: Prepare a presentation detailing the project's objectives, implementation, challenges, findings, and learning outcomes.

(h) **Considerations:**
Scalability: Ensure the design allows for easy scaling and addition of more clients or services. Security: Maintain a strong focus on security best practices throughout the project. Budget and Resources: Be mindful of the budget and resources available for the project.

(i) **Learning Outcomes:**
Hands-on experience with WAF and SIEM tools. Understanding of network configuration and client onboarding. Insight into the challenges and considerations of managing cybersecurity services in a network environment.
This project would not only enhance your technical skills but also give you valuable insights into the operational aspects of cybersecurity services. It's a comprehensive way to apply theoretical knowledge in a practical setting.