ORLOX

internship assignment

Modern Active Directory Security Framework

CONTACT

Kristof Laerenbergh

Veldkant 7, 2550 Kontich
info@orlox.be
www.orlox.be

TABLE OF CONTENTS

Description

Active Directory (AD) is at the core of organizational IT infrastructures, serving as the primary identity and access management system for around 95% of global organizations. However, the increasing reliance on AD has made it a prime target for cyberattacks, with malicious actors attempting to gain unauthorized access, compromise identities, and disrupt business operations. Consequently, the need for secure privileged access to AD environments has become paramount.

This internship project focuses on setting up a modern Active Directory security framework that utilizes Microsoft 365 security to enable secure privileged access to an on-premises AD environment. This framework incorporates various security measures, including a 3-tiered access model.

To accomplish this project, you will create a PowerShell Module that will automate the setup of the 3-tiered access model. Following this, you will configure the remaining components of the Orlox-developed Modern AD Security Framework to ensure secure access to the on-premises environment.

Deliverables

1. Set up an Active Directory environment with at least one Windows Server 2022 Jump server and one application server.
2. Design and develop a PowerShell module, that will take a JSON configuration file and which generates; Groups, OUs, GPO's, ACL's… in order to deploy a complete 3-Tiered AD structure.
3. Setup the Orlox PAM Basic solution in Microsoft Entra according to the provided runbook.
4. Deploy a Linux server and docker containers to setup HTML5 browser based access according to the provided runbook.
5. Validate the entire solution.

Project Methodology

Secure Application Development using CIS, NIST, and Microsoft Cybersecurity Frameworks

1. Framework Integration:
   - Integrate the key principles from the CIS, NIST, and Microsoft Cybersecurity Frameworks to define the foundational guidelines for the project.
   - Prioritize framework recommendations based on the criticality of application functionalities and the risk associated with vulnerabilities.
2. Requirement Analysis and Threat Modeling:
   - Use the NIST Cybersecurity Framework to identify, assess, and prioritize cybersecurity requirements tailored to the application's functionality and usage.
   - Leverage Microsoft's threat modeling techniques to identify potential vulnerabilities in the design phase.
3. Secure Development Environment:

- Establish a secure development environment in alignment with CIS best practices, ensuring that all tools, systems, and platforms used in development are regularly updated and free from vulnerabilities.

4. Secure Coding Practices:
   - Adopt secure coding practices, leveraging guidelines from all three frameworks to prevent common vulnerabilities like SQL injection, cross-site scripting, etc.
   - Conduct regular code reviews focusing on security, using tools that adhere to the principles of the integrated framework.
5. Testing & Validation:
   - Utilize the NIST framework for a rigorous testing regimen to validate application security. Ensure that testing includes penetration testing, vulnerability assessments, and source code analysis.
6. Feedback & Iteration:
   - Actively seek feedback during development and testing phases, using insights to iterate and enhance security postures.
   - Ensure any changes to the code are re-tested and reviewed for security implications.
7. Deployment & Maintenance:
   - Ensure secure deployment practices, considering guidelines from the CIS framework for cloud or on-premises deployments.
   - Continuously monitor the application in the production environment. Use the Microsoft Cybersecurity Framework to establish alerting mechanisms for potential threats.
   - Periodically review and update the application based on the evolving recommendations from the CIS, NIST, and Microsoft Cybersecurity Frameworks.