SECURITY STRATEGY FRAMEWORK

Alabi Kehinde Oluwasemilore

Information Systems Engineering and Management, Harrisburg University

CISSC 661: Principles of Cybersecurity & Cyberwarfare

Dr. Bruce Young

06/16/2023

Objective

The objective is to protect against various types of attacks and ensure the security of systems and data. The framework presented here encompasses tools and techniques commonly used in the field, selected for their effectiveness in defending against different attack vulnerabilities. While this cybersecurity strategy provides a general framework, it is adaptable to specific project tasks and organizational requirements. By utilizing the information and knowledge gained from previous projects and coursework, I have developed a strategy that strikes a balance between theoretical foundations and practical implementation.

Virtual Box Lab Setup

This virtual lab served as a controlled and isolated environment where security assessments and simulate real-world attacks could be performed. The tools used include Kali Linux, Metasploitable, Nmap, Legion, and Armitage.

Kali

Kali Linux is a specialized operating system designed for penetration testing and ethical hacking. It comes with a wide range of pre-installed tools for various stages of testing, allowing testers to perform reconnaissance, scanning, exploitation, and post-exploitation activities effectively.

Metasploitable

Metasploitable is a deliberately vulnerable virtual machine used for practicing penetration testing. It features intentionally weak configurations and vulnerable services, enabling testers to simulate real-world security flaws and practice exploiting vulnerabilities in a controlled environment.

Nmap

Nmap is a versatile network scanning tool. It helps identify hosts, open ports, and services on a network. By using Nmap, testers can gather critical information about target systems, enabling them to plan and execute penetration testing activities more effectively.

Legion

Legion is an open-source security auditing and penetration testing framework. It offers a comprehensive set of tools that simplify vulnerability scanning, exploitation, and post-exploitation tasks. Legion integrates various tools and techniques into a unified platform, making it easier for testers to conduct security assessments.

Armitage

Armitage is a user-friendly graphical interface for the Metasploit Framework. It simplifies the process of exploiting vulnerabilities by providing an intuitive interface for visualizing target networks, selecting exploits, and launching attacks. Armitage also includes features like automated scanning, session management, and collaboration capabilities.

Penetration testing

To test the security of our systems, it is important to follow key steps. We start by defining the testing scope, focusing on specific areas to check for vulnerabilities. Leveraging tools like Nmap, Metasploit, and Armitage, we scan networks, identify weaknesses, and visualize the testing process. Executing the outlined steps includes testing connections, conducting scans, and using commands to search for known vulnerabilities. Documenting findings is critical, describing vulnerabilities, assessing severity, and recommending remediation actions. Prioritizing vulnerabilities helps create an action plan for effective mitigation. Follow-up

testing verifies the effectiveness of fixes. Continuous improvement involves learning from testing, enhancing security practices, maintaining confidentiality, and complying with legal requirements (Shinde & Ardhapurkar, 2016).

Strengthening Attack Detection and Monitoring

Configuration of an Intrusion Detection System (IDS) enables the detection, monitoring, and alerting of potential cybersecurity attacks in an organization. By setting up rules, monitoring critical areas, and generating real-time alerts, the IDS can identify suspicious activities and enable timely response. Regular analysis of logs and alerts informs ongoing enhancements to the IDS configuration, enhancing overall cybersecurity defenses.

Snort

Snort Host IPS is a powerful tool used to configure an Intrusion Prevention System (IPS) for detecting, monitoring, and alerting potential cybersecurity attacks. By customizing the IPS rules and settings, Snort Host IPS can actively analyze network traffic, identify suspicious patterns, and generate real-time alerts to mitigate security threats. This tool enhances the overall cybersecurity defense by providing proactive protection against various types of attacks and enabling swift incident response. Leveraging Snort Host IPS, organizations can enhance their security defenses and respond promptly to potential threats.

Secure Networking with Traffic control and Policy enforcement

Implementing a firewall by creating a separate virtual machine, and configuring network interfaces, organizations can establish a secure testing environment. This approach isolates potential security risks, prevents unauthorized access, and enables efficient analysis. With optimized network settings on various systems and a well-defined firewall policy, network security is enhanced, protecting against data breaches. Regular testing and refinement of security

measures contribute to better detection and prevention of cyber-attacks, safeguarding critical data, preserving reputation, and ensuring uninterrupted business operations.

Summary

Integrating Security & Risk Management, Asset Security, Security Engineering, Identity & Access Management, and Security Assessment & Testing is crucial to protect against various types of attacks. Alongside these domains, establishing a Virtual Box Lab Setup provides a controlled environment for penetration testing, using tools like Kali Linux, Metasploitable, Nmap, Legion, and Armitage. Configuring an Intrusion Detection System (IDS) with Snort Host IPS strengthens attack detection and monitoring capabilities. Additionally, secure networking with traffic control and policy enforcement, including the creation of a separate virtual machine and firewall policy, enhances network security. Integrating these elements, organizations can establish a proactive and layered cybersecurity strategy, effectively identifying and mitigating security risks, safeguarding assets, designing secure systems, managing identities and access, conducting assessments, and testing vulnerabilities. This comprehensive strategy approach helps protect against cyber threats and maintains a robust security posture. Additionally, it's important to regularly review and update your strategy to adapt to evolving threats and technologies.

References

Lyu, M. R., & Lau, L. (2000). *Firewall security: policies, testing and performance evaluation*. https://doi.org/10.1109/cmpsac.2000.884700

Shinde, P. V., & Ardhapurkar, S. B. (2016). *Cyber security analysis using vulnerability assessment and penetration testing*. https://doi.org/10.1109/startup.2016.7583912