**Final Penetration Testing Report**

**Bhargav Kotipalli**

**Harrisburg University of Science and Technology**

**Ethical Hacking Development Lab**

**Dr Christine Pierce**

**12/05/2023**

**Introduction**

This document outlines the comprehensive penetration testing endeavours performed on the client's systems and applications. The primary objective of this assessment was to assess the effectiveness of existing security measures and pinpoint potential vulnerabilities susceptible to exploitation by malicious entities.

**Project 1 – Preparing our Lab**

During this initiative, we established a dedicated laboratory environment to carry out penetration testing without any adverse effects on operational systems. Key tasks encompassed:

1. Setting up virtual machines equipped with susceptible operating systems and applications.
2. Deploying essential security utilities like Burp Suite, Nmap, and John the Ripper.
3. Verifying seamless network connectivity among the various systems within the laboratory.

**Project 2 - Implementing Tenable Nessus Vulnerability Scanner**

For this endeavour, we employed the renowned Nessus vulnerability scanner to evaluate networks, operating systems, and applications. Essential tasks undertaken included:

1. Set up and configured both the Nessus server and its corresponding agents.
2. Conducted host discovery to create an inventory of assets within the defined scope.
3. Executed comprehensive vulnerability scans to pinpoint security misconfigurations and identify absent patches.
4. Analysed the results of the scans and prioritized issues categorized as critical and high severity.

**Project 3 - Perform Web Services Vulnerability Scan**

In this phase, we subjected web applications to a comprehensive assessment targeting prevalent vulnerabilities such as SQL injection, cross-site scripting, and insecure authentication. Leveraging Burp Suite, our activities comprised:

1. Charting the functionality and attack surface of the applications.
2. Identifying parameters susceptible to manipulation.
3. Validating the exploitability of injection flaws.

**Project 4 - Web Services Penetration Test**

Continuing from the vulnerabilities identified in the scanning phase, we conducted penetration tests to showcase concrete compromises:

1. Employed SQL injection techniques to retrieve data from the database.
2. Achieved administrative privileges by circumventing authentication.
3. Established enduring access through the implementation of backdoors and shells.
4. Successfully accessed confidential documents from secure, restricted areas.

**Project 5 - Password Cracking**

In this initiative, we evaluated the robustness of password controls by decrypting hashed files acquired from compromised systems:

1. Collected password hashes extracted from the SAM database.
2. Employed rainbow tables and wordlists to decipher commonly used or weak passwords.
3. Executed brute force attacks to unveil complex password combinations.
4. Provided recommendations for enhancing password policies and implementing multi-factor authentication.

**Summary of Penetration Testing:**

This report encapsulates the outcomes of a comprehensive penetration testing initiative focused on identifying and rectifying vulnerabilities within web services. The project unfolded across five distinct phases: Lab Preparation, Tenable Nessus Vulnerability Scanner Implementation, Web Services Vulnerability Scan, Web Services Penetration Test, and Password Cracking. Our primary goal was to furnish a detailed overview of significant findings in each project phase. The assessments brought to light various vulnerabilities that, if unaddressed, could be exploited by malicious entities. It's important to acknowledge certain limitations stemming from time constraints that influenced the extent of our testing methodologies.

In the Lab Preparation phase, Project 1, we created a simulated network infrastructure using VirtualBox software, segregating servers and clients into separate subnets. Kali Linux served as our chosen penetration testing tool for scanning purposes.

Moving to Project 2, the Tenable Nessus Vulnerability Scanner Implementation, we installed the Nessus scanner, enabling the detection of diverse security weaknesses, including outdated patching schemes and weak passwords associated with confidential accounts within operating systems.

The Web Services Vulnerability Scan, Project 3, involved deploying a dedicated virtual machine running Burp Suite against DVWA. This phase revealed vulnerabilities such as information disclosure through error messages and flawed authentication mechanisms due to improperly implemented default login credentials.

Project 4 focused on an exhaustive Web Services Penetration Test, targeting specific application protocols transmitted over HTTPS, allowing for the interception of encrypted traffic.

In Project 5, the Password Cracking Exercise, technical tools like John-the-Ripper were utilized to crack passwords hashed via the MD5 algorithm, a result of prior breaches. This verification process aimed to assess whether users had reused passwords across multiple platforms, potentially heightening security risks.

Conclusion:

In conclusion, this report underscores the escalating significance of fortifying web service security in the contemporary landscape and the associated risks of neglecting known vulnerabilities. Organizations must take proactive measures to fortify their information systems against cyber threats, ensuring the safeguarding of confidentiality, integrity, and availability.

**Methodology Overview:**

This report outlines the procedural framework employed in our enterprise penetration testing initiative. The primary objective was to systematically assess and pinpoint potential vulnerabilities within an enterprise network, utilizing established tools, methodologies, and techniques prevalent in the industry.

1. Preparation:

In the initial phase, we established our lab environment, incorporating essential tools such as virtual machines, diverse operating systems, and web servers. Additionally, we thoroughly reviewed the target organization's best practice policies to inform our approach.

2. Vulnerability Assessment:

The subsequent stage involved the deployment of a Tenable Nessus Vulnerability Scanner. This powerful tool was employed to scrutinize a broad spectrum of hosts within the networks, identifying vulnerabilities and configuration issues that could be exploited by cyber threats (Nixon, 2021).

3. Web Service Scanning:

Moving forward, we conducted a comprehensive examination of the web services utilized by enterprise clients. This step included Bugtraq-Loaded website scans and cross-referencing against widely held exploit code repositories, providing valuable insights into potential vulnerabilities.

4. Penetration Test:

Phase four focused on attempting exploitations on all ports associated with identified services, particularly HTTPServices. A subjective vulnerability assessment provided clarity on the exploitability of each identified weakness, assessing the resilience of segmentation among sections against sophisticated intrusion attempts.

5. Password Cracking:

The final phase involved an in-depth review, revealing recurring instances of password non-compliance. Recommendations were made for innovative approaches and the imperative need for enhanced personnel training to bolster overall security posture.

In conclusion, our enterprise penetration testing involved meticulous preparation, advanced tools like Tenable Nessus, comprehensive examination of web services, and a focused password review. This approach enabled the identification of potential vulnerabilities, and recommendations for improvements were made, emphasizing innovative strategies and enhanced personnel training to strengthen overall security posture.

**Risk Assessment Overview:**

Prior to initiating penetration testing activities, a crucial step involves conducting a thorough risk assessment of the target system. This entails the identification of potential vulnerabilities and threats that could be exploited by hackers for unauthorized access or data theft. The primary aim of this assessment is to provide a comprehensive insight into the security posture of the target system, enabling the implementation of appropriate measures to enhance its defenses. In our project, a detailed risk assessment was conducted before commencing penetration testing activities, following methodologies outlined by Nixon (2021).

Utilizing a combination of tools and techniques, including vulnerability scanning through the Tenable Nessus Vulnerability Scanner and web service vulnerability scans supplemented by manual testing for deeper analysis, we uncovered significant weaknesses in the security posture. These weaknesses encompassed outdated software versions on servers lacking evidence of regular patching, exposed weak passwords detected through password cracking tools, and identified loopholes in web services allowing the circumvention of authentication controls, among others.

The implications of these identified risks are substantial. Successful exploitation by an attacker could result in full administrative control over compromised systems, posing a significant threat to data integrity and potentially leading to actions that could harm an organization's reputation. These findings underscore the critical importance of addressing identified vulnerabilities to fortify the overall security resilience of the target system.

**Remediation Recommendations:**

Following the outcomes of our penetration testing, we've identified vulnerabilities within the tested systems and web services. To enhance overall security, we propose the following remediation measures:

**Project 2: Tenable Nessus Vulnerability Scanner Implementation:**

1. Regularly update scanning schedules and include all new hosts in the scanning process.
2. Conduct routine vulnerability scans and prioritize patching based on risk ratings.

**Project 3: Web Services Vulnerability Scan:**

1. Ensure developers adhere to secure coding practices.
2. Implement periodic code reviews to identify potential vulnerabilities or weaknesses.

**Project 4: Web Services Penetration Test:**

1. Adhere to industry-standard best practices by closing all unnecessary ports.
2. Install host-based firewalls on servers handling critical applications or data storage.

**Project 5: Password Cracking:**

1. Implement stronger passwords with a combination of upper- and lower-case letters, symbols, and numbers, with a minimum length requirement of at least eight characters.
2. Regularly review password policies.

In conclusion, organizations should conduct regular vulnerability assessments using automated tools like the Tenable Nessus Vulnerability Scanner and manual penetration testing to proactively identify risks before they escalate. Additionally, prompt clean-up measures, such as closing unnecessary ports and resolving vulnerabilities swiftly, are crucial steps in maintaining a robust security posture.

**Detailed Findings Overview:**

**Project 1: Lab Establishment:**

In the initial phase, our primary objective was the creation of a resilient lab environment for penetration testing. We prioritized ensuring the operating system's currency with the latest security patches, deactivating unnecessary services, and configuring firewalls to exclusively permit essential network traffic.

**Project 2: Integration of Tenable Nessus:**

Moving to the second phase, we implemented the Tenable Nessus vulnerability scanner. Tailoring its settings to project requirements, we conducted scans on target machines, uncovering potential vulnerabilities within our lab environment.

**Project 3: Assessment of Web Services:**

Transitioning to web services, a comprehensive web application scan was executed using tools like OWASP ZAP and Burp Suite. The focus was on identifying vulnerabilities such as SQL injection, cross-site scripting, command injection flaws, and other issues related to web applications.

**Project 4: Penetration Testing for Web Services:**

Building upon identified vulnerabilities from earlier phases, particularly those associated with cross-site scripting and injection threats, we conducted penetration tests. Utilizing tools like the Metasploit Framework and automated exploitation toolkits, we gained insights into potential unauthorized access and exposure of sensitive data.

**Project 5: Password Strength Evaluation:**

The concluding phase involved a comprehensive password strength assessment, utilizing brute force methods and simulating various password policies. This phase emphasized the vulnerability of commonly used passwords and underscored the necessity for robust confidentiality measures when handling sensitive data.

Over the course of these initiatives, our cybersecurity professionals acquired crucial insights into common cyber-attack techniques. Specifically, Project 4 illuminated potential vulnerabilities that determined adversaries might exploit without detection, underscoring the necessity for proactive defence strategies. It became evident that organizations must deploy advanced security measures to thwart the ever-changing tactics of cybercriminals. In summary, routine penetration testing, coupled with stringent password protocols and regular device updates, enhances an organization's ability to withstand targeted attacks on valuable data or financial assets.

**Conclusion**

In summary, the penetration testing process plays a pivotal role in uncovering vulnerabilities within computer systems and networks. Our engagement in various projects has provided invaluable hands-on experience, covering aspects such as setting up a lab environment, deploying vulnerability scanners like Tenable Nessus, conducting web services scans, penetration tests, and exploring password cracking techniques. These acquired skills are poised to be highly beneficial in any forthcoming cybersecurity roles we may assume. It is vital to acknowledge that while automated tools aid in identifying potential threats, they cannot replace human expertise in detecting more intricate attacks. Therefore, continuous learning and training are imperative to remain abreast of the latest security risks and effectively implement countermeasures.

**References**

Nixon, I. K. (2021). Standard penetration test State-of-the-art report. In *Penetration Testing, volume 1* (pp. 3-22). Routledge.

Steinmetz, K. F. (2023). Executing effective social engineering penetration tests: A qualitative analysis. *Journal of Applied Security Research*, *18*(2), 246-266.