

Penetration Test

Report Analysis

Evaluation of a PenTest Engagement plan

Damian Yates | D484 | Aug 1, 2024

# **Penetration Test Engagement Plan Analysis**

## Overview

Western View Hospital, a 100-bed facility, has been serving the residents of a rural community for over 80 years. The administration recently completed a comprehensive modernization of the medical and patient records system to provide better care for the community.

Before the new system can be launched, the hospital administration has authorized Pruhart Tech to conduct a thorough test for potential vulnerabilities and ensure the IT infrastructure secures sensitive patient medical and financial data in compliance with HIPAA requirements (HIPAA for Professionals, 2024). A senior manager at Pruhart Tech has tasked our team with developing a penetration testing engagement plan for Western View Hospital that aligns with their goals and adheres to industry best practices. This document is an evaluation of the proposed testing engagement plan to evaluate its appropriateness, provide recommendations for improvements, and propose solutions to any identified problems.

# Alignment Evaluation

## Hospital’s Goals, Objectives, functions, processes and practices

### Goals

##### Ensure the Security and Privacy of Patient Medical and Financial Data:

* **Security:** Implementation of robust security measures to protect against unauthorized access, cyberattacks, and data breaches. This includes using firewalls, encryption, intrusion detection systems, and regular security audits.
* **Privacy:** Ensure that patient data is only accessible to authorized personnel and used per privacy laws and regulations. This involves establishing clear policies for data handling and ensuring all staff are trained in these policies.

##### Achieve HIPAA Compliance:

* **Regulatory Compliance:** Adherence to the Health Insurance Portability and Accountability Act (HIPAA) regulations, which set standards for the protection of sensitive patient information (HIPAA for Professionals, 2024). This includes conducting regular risk assessments, implementing necessary safeguards, and maintaining documentation of compliance efforts.
* **Patient Rights:** Ensuring patients are informed of their rights under HIPAA, including their right to access their health information, request corrections, and understand how their data is used.

##### Provide Better Care for the Community by Leveraging Modernized Medical and Patient Records Systems:

* **Efficiency:** Using advanced electronic health record (EHR) systems to streamline the collection, storage, and retrieval of patient information, which can reduce errors and improve the efficiency of healthcare delivery.
* **Quality of Care:** Enhancing the quality of patient care by ensuring that healthcare providers have access to comprehensive and up-to-date patient information, enabling more informed and timely decision-making.

### Objectives

##### Identify and Mitigate Potential Vulnerabilities in the New IT Infrastructure:

* **Vulnerability Assessment:** Conduct thorough assessments to identify weaknesses in the hospital’s IT infrastructure, including software, hardware, and network components.
* **Mitigation Strategies:** Implementing measures to address identified vulnerabilities, such as patching software, updating security protocols, and improving system configurations.

##### Prevent Data Breaches and Unauthorized Access to Sensitive Information:

* **Access Controls:** Establishing strong access control measures, such as multi-factor authentication and role-based access controls, to ensure only authorized personnel can access sensitive data.
* **Monitoring and Detection:** Implementing continuous monitoring and intrusion detection systems to quickly identify and respond to potential security threats.

##### Maintain the Trust and Confidence of the Community and Patients:

* **Transparency:** Communicating openly with patients and the community about the steps being taken to protect their data and the quality of care being provided.
* **Trust-building Initiatives:** Implementing initiatives that reinforce the hospital’s commitment to patient privacy and security, such as regular updates on security improvements and patient satisfaction surveys.

### Functions

##### Medical Care and Treatment for Patients:

* **Diagnosis and Treatment:** Providing medical services including diagnosis, treatment, surgery, and rehabilitation to meet the health needs of patients.
* **Patient Education:** Educating patients about their health conditions, treatment options, and preventive measures to promote better health outcomes.

##### Management of Patient Records and Medical Data:

* **Record Keeping:** Maintaining comprehensive and accurate records of patient visits, medical history, treatment plans, and outcomes.
* **Data Analysis:** Analyzing patient data to identify trends, improve treatment protocols, and support clinical research.

##### Financial Management, Including Patient Billing and Insurance Processing:

* **Billing:** Generating and sending bills to patients and insurance companies for services provided.
* **Insurance Claims:** Managing the submission, processing, and tracking of insurance claims to ensure timely payment and resolution of any issues.

### Processes

##### Collection, Storage, and Management of Patient Information:

* **Collection:** The process of gathering patient data, including personal details, medical history, treatment plans, and other relevant health information.
* **Storage:** Ensuring that collected patient data is securely stored in electronic health records (EHR) systems, which are designed to protect sensitive information and make it easily accessible to authorized personnel.
* **Management:** Regular updates, organization, and maintenance of patient records to ensure accuracy and compliance with regulatory standards. This includes implementing access controls to limit who can view and modify patient information.

##### Medical Treatment Documentation and Retrieval:

* **Documentation:** Recording details of patient visits, diagnoses, treatments, prescriptions, and outcomes. This documentation must be thorough, accurate, and timely to support ongoing patient care and legal requirements.
* **Retrieval:** Efficiently accessing patient records when needed, whether for ongoing treatment, emergency situations, or administrative purposes. This process ensures that healthcare providers have all the necessary information to deliver appropriate care and make informed decisions.

##### Financial Transactions and Records Management:

* **Financial Transactions:** Handling billing processes, including generating invoices for services rendered, processing payments from patients and insurance companies, and managing any outstanding balances.
* **Records Management:** Keeping detailed records of all financial transactions, including billing, payments, insurance claims, and reimbursements. This ensures transparency, accuracy, and compliance with financial regulations and facilitates audits and financial reporting.

### Practices

##### Implementation of Administrative and Technical Safeguards for Data Protection:

* **Administrative Safeguards:** These include policies and procedures designed to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information (ePHI). Examples include assigning a security responsibility, developing and enforcing a data protection policy, and conducting regular security risk assessments.
* **Technical Safeguards:** These involve the technology and related policies that protect ePHI and control access to it. Examples include encryption, secure access controls, regular software updates, and implementing firewalls and intrusion detection systems.

##### Regular Reviews and Updates to Security Policies and Procedures:

* **Policy Review:** Conduct systematic evaluations of security policies and procedures to ensure they remain effective and relevant in light of new threats, technological changes, and regulatory updates.
* **Updates and Improvements:** Making necessary adjustments based on review findings, incident reports, and best practices in cybersecurity. This may involve updating access control measures, revising incident response plans, and improving data backup protocols.

##### Staff Training on Security Protocols and HIPAA Compliance:

* **Initial Training:** Providing comprehensive training for new employees on the hospital’s security protocols and HIPAA compliance requirements. This ensures all staff members understand their responsibilities in protecting patient information.
* **Ongoing Education:** Offering regular refresher courses and updates on new security threats, changes in regulations, and best practices for data protection. This can include simulated phishing attacks, security awareness campaigns, and regular testing of staff knowledge and compliance.

## Structure of the Penetration Testing Engagement Plan

### Overview

* **Conducted by Pruhart Tech:** Pruhart Tech, a cybersecurity firm, is tasked with carrying out a comprehensive penetration test on the hospital's information systems. Their role involves assessing the hospital's cybersecurity posture by actively exploiting vulnerabilities.
* **Testing the Effectiveness of Security Controls:** This involves evaluating how well the hospital's current security measures prevent, detect, and respond to attacks. The assessment will identify weaknesses in both the hardware and software components of the IT infrastructure.
* **Coordination with CLIENT's IT Staff:** Effective penetration testing requires close cooperation with the hospital's IT team. This coordination ensures that the testing is safe, controlled, and informative, preventing any unintended service disruptions or data breaches.

### Extent of Testing

* **Network-level Technical Penetration Testing (Internal and External):** This includes probing the hospital’s internal network (the network inaccessible from the internet) as well as external services (those exposed to the internet) to discover vulnerabilities that an attacker could exploit from both inside and outside the organization.
* **Social Engineering Phone Phishing Against Employees:** Phishing simulations targeting hospital employees by phone will test their awareness and response to social engineering threats, which are common vectors for breaches.

### Internal Phase

* **Reconnaissance and Enumeration Activities:** Initial steps include gathering publicly available information about the hospital’s network and identifying operational details, such as IP addresses, network services, and device types, which can pinpoint vulnerable systems.
* **Port and Vulnerability Scanning:** Systematic scans of network ports and services to identify open ports and associated vulnerabilities that could be exploited.
* **Directory Traversal on Compromised Servers:** Testing the ability to access unauthorized directories and files on a server, which might reveal sensitive information.
* **Use of Secure Sensor and EternalBlue for Gaining Access:** Utilizing advanced tools like Secure Sensor for detailed vulnerability scanning and EternalBlue exploit to test the robustness of network defenses against known vulnerabilities.

### External Phase

* **Focus on Publicly Accessible Assets:** Targeting resources that are accessible over the internet, such as the hospital's public website, external email servers, and remote access portals.
* **Reconnaissance and Scanning Using Burp Suite and Nmap:** Employing well-known tools such as Burp Suite for web vulnerability scanning and Nmap for port scanning to discover exploitable vulnerabilities in publicly exposed systems.
* **Attacks Launched from Pruhart Tech’s Network:** Simulated external attacks are launched from Pruhart Tech's infrastructure to mimic the techniques of real-world attackers.

### Social Engineering

* **Phone-based Social Engineering to Gain Credentials:** Simulated calls to employees pretending to be IT support or other trusted figures to trick employees into providing sensitive information like usernames and passwords.
* **Pretending to be Technical Support Workers:** Social engineers will use pretexts, such as urgent technical issues requiring immediate action, to manipulate staff into bypassing normal security protocols.
* **Activities Include Requesting Domain Usernames and Passwords:** These activities are designed to assess the readiness of the staff to respond to social engineering and help strengthen the organization's training and response strategies.

## Potential misalignments and recommendations

### Misalignments

##### Focus on Internal vs. External Threats:

* **Current Plan:** The plan emphasizes internal server takeovers, focusing on gaining access to internal systems and exploiting vulnerabilities within the hospital’s network.
* **Misalignment:** This focus may not align with the primary goal of protecting patient data from external breaches, as many threats originate from outside the organization. While internal security is important, external threats pose significant risks to patient data privacy and the hospital’s reputation.
* **Impact:** Neglecting external threats could leave the hospital vulnerable to common attack vectors such as web application attacks, remote code execution, and external network breaches, potentially resulting in data breaches and HIPAA violations.

##### Social Engineering Scope:

* **Current Plan:** The plan includes phone-based social engineering, simulating attacks where malicious actors impersonate IT support to obtain sensitive information.
* **Misalignment:** This approach may not fully encompass the range of social engineering tactics, particularly phishing emails, which are a common and effective method used by attackers.
* **Impact:** Failing to test other social engineering methods could result in insufficient preparedness against these types of attacks, increasing the risk of successful social engineering exploits.

##### Technique Specificity:

* **Current Plan:** The plan uses specific techniques, such as EternalBlue, to exploit vulnerabilities.
* **Misalignment:** Focusing on a limited set of techniques may not cover the full spectrum of potential vulnerabilities, especially newer or more sophisticated threats that have emerged since the development of these techniques.
* **Impact:** A narrow focus could leave the hospital’s systems exposed to vulnerabilities not tested by the specified techniques, potentially allowing attackers to exploit unaddressed weaknesses.

##### Coordination and Communication:

* **Current Plan:** The plan mentions coordination with IT staff but lacks detailed communication strategies or incident response plans.
* **Misalignment:** Without a clear communication and incident response framework, the testing process may not be well-aligned with hospital operations, leading to potential disruptions or misunderstandings.
* **Impact:** Poor coordination could hinder the effectiveness of the penetration test, cause unnecessary operational interruptions, and delay the hospital’s ability to respond to actual security incidents.

### Recommendations

##### Expand External Threat Focus:

* + **Action:** Increase emphasis on external penetration testing, including testing of web applications, external network interfaces, and remote access points.
  + **Benefit:** Ensures comprehensive coverage of all possible entry points for unauthorized access, aligning to protect patient data from external threats.

##### Broaden Social Engineering Tactics:

* + **Action:** Include additional social engineering methods such as phishing emails, physical security tests (e.g., tailgating), and simulated insider threats.
  + **Benefit:** Provides a more realistic and comprehensive assessment of the hospital’s susceptibility to social engineering attacks, enhancing overall security awareness and preparedness.

##### Update Testing Techniques:

* + **Action:** Incorporate a variety of up-to-date techniques and tools, including those for detecting zero-day vulnerabilities and advanced persistent threats (APTs).
  + **Benefit:** Ensures the testing process covers a broader range of potential vulnerabilities, improving the overall security posture and resilience against sophisticated threats.

##### Enhanced Communication Plans:

* + **Action:** Develop detailed communication and incident response plans, including regular updates to stakeholders, predefined incident response procedures, and thorough documentation of all findings and actions during the test.
  + **Benefit:** Ensures smooth coordination with hospital staff, minimizes operational disruptions and enhances the hospital’s ability to respond effectively to security incidents.

##### Regular Updates and Training:

* + **Action:** Incorporate regular updates to the penetration testing plan to address emerging threats and evolving security practices. Implement continuous training programs for staff to keep them informed about the latest security protocols and threats.
  + **Benefit:** Maintains the relevance and effectiveness of the penetration testing plan, ensuring staff are well-prepared to handle current and future security challenges.

By addressing these potential misalignments and implementing the recommendations, the penetration testing engagement plan can better align with the hospital’s goals, objectives, functions, processes, and practices. This alignment will enhance the overall security posture and ensure HIPAA compliance, ultimately protecting patient data and maintaining the trust and confidence of the community and patients.

# Penetration Testing Engagement Plan Evaluation

## Best Practices and Frameworks for Penetration Testing Engagement Plans

### Best Practices:

1. **Comprehensive Scope and Objectives:**
   * Define the scope and objectives clearly, including all systems, networks, and assets to be tested. This should cover both internal and external assets to ensure a holistic assessment of security.
2. **Compliance and Legal Considerations:**
   * Ensure the testing aligns with all relevant compliance requirements, such as HIPAA for healthcare institutions, to protect sensitive patient information legally and securely.
3. **Methodical Planning and Preparation:**
   * Prepare a detailed plan that outlines the methodology, tools, and techniques to be used, including both automated and manual testing approaches.
4. **Execution with Defined Protocols:**
   * Conduct the testing using a mixture of white box and black box testing approaches to simulate both insider and outsider threats comprehensively.
5. **Detailed Reporting and Remediation Guidance:**
   * Provide clear, actionable reports that categorize vulnerabilities by severity and suggest remedial actions. This helps prioritize fixes based on potential impact.
6. **Follow-Up and Continuous Improvement:**
   * Include provisions for re-testing post-remediation and regular updates to the testing plan to adapt to new threats and changes in the IT environment.

### Frameworks:

1. **NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment):**
   * This guide provides a comprehensive approach to security testing, including strategies for planning, conducting, and evaluating tests. (Souppaya, Scarfone, Cody, & Orebaugh, 2008)
2. **OWASP Testing Guide:**
   * A framework for web application penetration testing that includes a detailed methodology for identifying and exploiting web application vulnerabilities (OWASP Testing Guide v4, 2017).
3. **Penetration Testing Execution Standard (PTES):**
   * A standard that defines phases of a penetration test from pre-engagement to post-engagement, ensuring thorough coverage and professional conduct during the test. (PTES Technical Guidelines, 2012)

## Comparison of the Penetration Testing Engagement Plan to Identified Best Practices and Frameworks

1. **Scope and Objectives:**
   * The current plan covers both internal and external threats but places a strong emphasis on internal threats. Best practices suggest a balanced approach to equally address both internal and external vulnerabilities.
2. **Compliance and Legal Considerations:**
   * The plan recognizes HIPAA requirements; however, ensuring continual alignment with HIPAA through all phases of testing is critical (HIPAA for Professionals, 2024). Best practices recommend ongoing compliance checks throughout the testing process.
3. **Planning and Preparation:**
   * While the plan mentions using specific tools like EternalBlue, Burp Suite, and Nmap, there is a need for a broader range of tools and techniques as per OWASP and PTES (PTES Technical Guidelines, 2012) guidelines to cover more types of vulnerabilities.
4. **Execution Protocols:**
   * The plan includes coordination with IT staff and the use of advanced testing techniques. Best practices would also recommend clear protocols for incident handling during testing to minimize disruptions, which seems underdeveloped in the current plan.
5. **Reporting and Remediation:**
   * The current engagement plan lacks detailed descriptions of reporting formats. According to best practices, the report should include detailed vulnerability descriptions, reproducible proofs-of-concept, and prioritized remediation steps.
6. **Follow-Up and Continuous Improvement:**
   * There is no mention of follow-up testing or ongoing adjustments to the testing plan in the document. Best practices and frameworks like NIST (Souppaya, Scarfone, Cody, & Orebaugh, 2008) and PTES (PTES Technical Guidelines, 2012) advocate for post-remediation testing and periodic reassessment to adapt to new threats.

By addressing these gaps and aligning more closely with established best practices and frameworks, the penetration testing engagement plan for Western View Hospital can be significantly enhanced to ensure comprehensive coverage, effective identification and mitigation of vulnerabilities, and improved security posture in line with compliance requirements.

# Remediation of Potential Issues

## Recommendations for Improvements

### Expand the Range of Social Engineering Techniques:

* + **Current Plan:** Focuses primarily on phone-based social engineering.
  + **Recommendation:** Incorporate additional social engineering methods such as phishing emails, pretexting, and physical security assessments (e.g., tailgating and unauthorized access attempts). This will provide a more comprehensive assessment of the hospital’s vulnerability to social engineering attacks and better simulate real-world scenarios.

### Enhance Detailed Communication and Incident Response Plans:

* + **Current Plan:** Mentions coordination with IT staff but lacks detailed communication strategies and incident response protocols.
  + **Recommendation:** Develop a comprehensive communication plan that includes regular updates to key stakeholders, predefined incident response procedures, and thorough documentation of all findings and actions during the test. This should also involve training for staff on how to respond to incidents discovered during the testing process to minimize operational disruptions.

## Solutions to Identified Problems

### Problem: Limited Focus on External Threats

* + **Solution:** Increase the emphasis on external penetration testing to ensure comprehensive coverage of all possible entry points for unauthorized access. This includes testing web applications, external network interfaces, and remote access points. By expanding the focus on external threats, the hospital can better protect patient data from common attack vectors that originate outside the organization.

### Problem: Use of Specific Techniques Without Broad Coverage

* + **Solution:** Update the testing techniques to include a variety of tools and methodologies that cover a broader range of vulnerabilities, including zero-day threats. Incorporate tools like Metasploit for exploitation, Nessus for vulnerability scanning, and OWASP ZAP for web application security (OWASP Testing Guide v4, 2017). This approach ensures that the penetration testing plan can identify and address both known and emerging vulnerabilities, providing a more robust security assessment.

## Implementation of Recommendations and Solutions

### Expanding Social Engineering Techniques:

* + Develop a detailed plan for executing additional social engineering tactics.
  + Conduct training sessions for the penetration testing team on the new methods to be used.
  + Simulate real-world attack scenarios using these methods to test the hospital’s defenses comprehensively.

### Enhancing Communication and Incident Response:

* + Create a detailed communication plan that outlines who needs to be informed at each stage of the penetration test.
  + Establish clear incident response procedures that the IT staff can follow when vulnerabilities are found.
  + Hold workshops and training sessions for hospital staff to ensure they understand and can execute the incident response plans effectively.

### Increasing Focus on External Threats:

* + Schedule additional external penetration tests focusing on internet-facing systems and applications.
  + Use advanced tools and techniques to simulate sophisticated external attacks.
  + Review and update firewall configurations, intrusion detection systems, and other perimeter defenses based on the findings from the external penetration tests.

### Updating Testing Techniques:

* + Regularly review and update the penetration testing toolkit to include the latest tools and techniques.
  + Perform continuous training for the penetration testing team to keep them updated on the latest vulnerabilities and attack methods.
  + Conduct a thorough review after each penetration test to identify areas for improvement in the testing techniques used.

By addressing these improvements and solutions, the penetration testing engagement plan for Western View Hospital can be more comprehensive, align better with the hospital's goals and objectives, and adhere to industry best practices. This will enhance the hospital’s overall security posture, ensuring better protection of patient data and compliance with regulatory requirements like HIPAA (HIPAA for Professionals, 2024).

# Conclusion

The evaluation of the penetration testing engagement plan for Western View Hospital reveals several areas for enhancement to better align with the hospital's goals, objectives, and industry best practices. The current plan provides a strong foundation by addressing both internal and external threats and incorporating social engineering. However, expanding the scope of social engineering techniques, enhancing communication and incident response plans, and updating testing techniques to cover a broader range of vulnerabilities will significantly strengthen the plan.

By increasing the emphasis on external threats and ensuring comprehensive coverage of all possible entry points for unauthorized access, the hospital can better protect sensitive patient data from common attack vectors. Furthermore, implementing regular updates and continuous training will ensure that the penetration testing plan remains relevant and effective in the face of evolving security threats.

These improvements will not only enhance the hospital’s overall security posture but also ensure HIPAA compliance, thereby protecting patient data and maintaining the trust and confidence of the community and patients (HIPAA for Professionals, 2024). Through these targeted recommendations and solutions, Western View Hospital can achieve a more robust and resilient IT infrastructure, ready to support its mission of providing exceptional care to the community.

# References

*HIPAA for Professionals*. (2024, 07 19). Retrieved from Health IT: Privacy, Security, and HIPAA: https://www.hhs.gov/hipaa/for-professionals/index.html

*OWASP Testing Guide v4*. (2017). Retrieved from Open Web Application Security Project: https://owasp.org/www-project-web-security-testing-guide/stable

*PTES Technical Guidelines*. (2012, 04 30). Retrieved from Penetration Testing Execution Standard: http://www.pentest-standard.org/index.php/PTES\_Technical\_Guidelines

Souppaya, M., Scarfone, K., Cody, A., & Orebaugh, A. (2008, 9). *Technical guide to information security testing and assessment (NIST SP 800-115).* Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

*Summary of the HIPAA Security Rule*. (2022, 10 19). Retrieved from U.S. Department of Health and Human Services. (n.d.): https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html