DKN1 TASK 1: Penetration Test Report Analysis

Tyra Austin

College of Cybersecurity, Western Governors University

December 3, 2024

“Evaluation and Recommendations for Western View Hospital’s Penetration Testing Engagement Plan”

A1. Client Goals

Goal: Western View Hospital’s primary goal is to ensure the security of its newly implemented medical and patients records system.

The hospital seeks to safeguard sensitive patient and financial data while maintaining compliance with HIPAA requirements. Additionally, they aim to validate that their IT infrastructure is robust enough to protect against attackers before launching the system into production.

Objective: Western View Hosiptal purpose is to identify and remediate vulnerabilities in its newly modernized IT infrastructure to ensure the system is secure before going live.

At the same time, the hospital aims to confirm compliance with HIPAA standards and protect sensitive patient data from unauthorized access or breaches. Achieving these objectives will allow the hospital to maintain patient trust and ensure uninterrupted service delivery.

Functions: Western View Hospital operates as a healthcare provider serving a rural community for over 80 years. Its primary function is to deliver patient care while managing sensitive medical and financial data.

Processes: Western View Hospital processes sensitive medical and financial data, relying on electronic health records (EHRs) and integrated IT systems to manage patient care efficiently.

Practices: Western View Hospital follows industry-standard practices for data security, including encryption, regular risk assessments, and adherence to HIPAA regulations to protect patient information.

A2. Penetration Testing Engagement Plan Structure

The penetration testing engagement plan focuses on identifying vulnerabilities in Western View Hospital's IT infrastructure, specifically targeting the newly implemented medical and patient records system.

The Scope: Includes network devices, servers, and applications critical to the system's operation.

The Test type: Primarily involves a vulnerability assessment followed by controlled exploitation to simulate real-world attacks.

The Approach: includes both external penetration testing to identify perimeter vulnerabilities and internal testing to uncover risks from within the network.

The Techniques: such as network scanning, phishing simulations, and application-level security testing are used to ensure comprehensive coverage.

A3. Misalignments

The penetration testing engagement plan includes a general scope of testing, but it may lack a comprehensive focus on all HIPAA-required safeguards, such as assessing administrative controls and verifying data encryption protocols.

Additionally, while external threats are a priority, the plan does not explicitly address insider risks, such as misconfigured user permissions or potential employee negligence, which are critical in a healthcare setting. The focus on network vulnerabilities without sufficient emphasis on application-level security testing, particularly for the hospital's electronic health records (EHRs), may leave critical areas untested.

Finally, the engagement plan does not outline how findings will be tied directly to HIPAA compliance practices, limiting its value in helping the hospital achieve its regulatory and operational goals.

B1. Best Practices and Frameworks

1. **Best Practices**
    - **NIST SP 800-115:** This guide provides a structured approach to information security testing, emphasizing phases like planning, discovery, attack simulation, and reporting, which are critical for penetration testing.
    - **OWASP Testing Guide:** Focused on application security, this gude ensures vulnerabilities in web applications and APIs, such as those used for patient records, are thoroughly assessed.

2. **Compliance Frameworks**
    - **HIPAA Security Rule:** This framework establishes safeguards for protecting electronic health information, including requirements for risk assessments and access controls.
    - **ISO 27001:** A global standard for managing information security, this framework ensures that the hospital's IT systems adhere to rigorous data protection practices.

B2. Comparison of Plan to Best Practices and Frameorks

The penetration testing engagement plan aligns with **NIST SP 800-115** by including a structured testing process that incorporates vulnerability assessment and simulated attack phases. However, the plan falls short in addressing the **reporting phase**, where findings should be explicitly tied to HIPAA compliance requirements.

While the plan's focus on external threats demonstrates alignment with the **OWASP Testing Guide,** it lacks sufficient emphasis on application-layer testing, which is critical for protecting the hospital's electronic health records (EHRs). Similarly, while the plan partially meets **HIPAA Security Rule** requirements by targeting technical safeguards, it does not address administrative controls, such as auditing user access permissions.

The absence of a clear strategy for continuous improvement and alignment with **ISO 27001's** risk management principles further indicates a gap in ensuring long-term security and compliance.

C1. Proposed Improvements

1. **Expand Testing Scope to include Application-Level Security**
    - The penetration testing plan should incorporate a detailed assessment of application-level vulnerabilities, especially focusing on electronic health records (EHRs) and patient portals. This addition will ensure critical application-layer threats, such as injection attacks and unauthorized access, are thoroughly evaluated.
2. **Integrate Compliance-Driven Reporting**
    - The engagement plan should include a comprehensive reporting phase that directly maps findings to HIPAA compliance requirements. This would not only help the hospital address vulnerabilities but also provide clear guidance for meaning regulatory standards, such as risk assessments and encryption protocols.

C2. Proposed Solutions

1. Implement User Behavior Analytics (UBA)

- To address the gap in detecting insider threats, the penetration testing plan should include user behavior analytics. UBA tools can monitor and identify unusual activity, such as unauthorized data access or privilege escalation, helping to mitigate insider threats effectively.

2. Conduct Training Simulations for Staff

- To reduce risks related to phishing and social engineering, the plan should include simulated phishing attacks and cybersecurity awareness training for hospital staff. This would strengthen the hospital's human firewall and ensure better adherence to security practices.

References

Dodd-Frank Act. CFTC. (n.d.). Retrieved February 7, 2023, from https://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm

Ferpa. FERPA | Protecting Student Privacy. (n.d.). Retrieved February 7, 2023, from https://studentprivacy.ed.gov/ferpa

Furneaux, N., & Hayes, J. (2019). Penetration testing: A guide for business and IT managers. BCS.

Health Information Privacy (2021). HIPAA for professionals. HHS.gov. Retrieved February 7, 2023, from https://www.hhs.gov/hipaa/for-professionals/index.html

The Penetration Testing Execution Standard. (n.d.). Retrieved February 7, 2023, from http://www.pentest-standard.org/index.php/Main_Page

PTES technical guidelines. PTES Technical Guidelines - The Penetration Testing Execution Standard. (n.d.). Retrieved February 7, 2023, from http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

- National Institute of Standards and Technology. (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. Retrieved from https://csrc.nist.gov/publications
- OWASP Foundation. (2024). *OWASP Testing Guide v4*. Retrieved from https://owasp.org
- U.S. Department of Health and Human Services. (2024). *HIPAA Security Rule: Protecting Electronic Health Information*. Retrieved from https://www.hhs.gov/hipaa
- International Organization for Standardization. (2013). *ISO/IEC 27001: Information Security Management*. Retrieved from https://www.iso.org