Penetration Test Report Analysis

Jamal Rizki

Western View Hospital Penetration Test Analysis

A1. Clients Goals, Objectives, Functions, Processes, and Practices

The clients' goals are to build and maintain an exemplary organizational reputation, ensure compliance with HIPAA and other pertinent regulatory bodies, and protect its clients' sensitive financial and personal health data. The client's objectives are to assess staff awareness of social engineering and to test both internal and external networks. The client operates in the healthcare industry and functions as a rural hospital serving the community for the past 80 years. As a provider in the healthcare space, the client's processes include sensitive data collection and storage, including financial data and health records. The practices it implements include organizational management through Active Directory, endpoint protection, and adherence to compliance frameworks such as HIPAA.

A2. Penetration Testing Engagement Plan Structure

The structure of the test will include testing internal assets, external assets, and social engineering across employees. The approach follows

the seven phases of the Penetration Testing Execution Standard (PTES): pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. Tools that will be used include Nmap, Burp Suite, Social Engineering Toolkit (SET), and Metasploit (PTES Technical Guidelines, n.d.)

A3. Misalignments

The period of active testing create a potential misalignment with the client's goals, as it could cause significant operational disruption at that time. The objectives of the client are also not fully aligned, as the current testing plan does not measure and assess compliance with regulatory bodies effectively. The hospital's function as a healthcare provider may also be adversely affected, as testing against production system infrastructure can ultimately disrupt operations. Critically, the incident response process of Western View Hospital is not being evaluated, which is a major flaw because it directly impacts the outcome of a data breach or security incident, should one occur. Finally, the client's practice of handling data in relation to PCI DSS requirements is being overlooked in this plan.

B1. Best Practices and Frameworks

Best Practices:

1. PTES – A penetration testing method that provides a structure and system for executing tests. (The Penetration Testing Execution Standard, n.d.)
2. NIST SP 800-115 – Provides a clear method for testing information systems. (National Institute of Standards and Technology [NIST], 2008)

Frameworks:

1. HIPAA – Establishes national standards to protect patient health information. (Health Information Privacy, 2021)
2. PCI DSS – A set of standards to protect cardholder data. (PCI Security Standards Council [PCI SSC], n.d.)

B2. Comparison of Plan to Best Practices and Frameworks

The plan partially aligns with PTES, but is missing key steps, most importantly the reporting phase, which is essential in any robust penetration test. Specifically, PTES requires comprehensive documentation of findings and recommendations, both of which are currently absent. NIST SP 800-115 details a well-defined scope, but in this current iteration the scope is not clearly defined. The plan currently specifies internal and external networks but is missing key information like accounts and IP addresses that are off-limits, specifics on testing timeframes, and system boundaries. HIPAA compliance requirements are also not up to par, as the protection of data is not being adequately assessed. For HIPAA compliance, data encryption, controls, and logs must be thoroughly assessed. PCI DSS is currently being completely ignored in this test, which is contrary to Western View Hospital's goal of securing financial data. Since the hospital processes payments, the plan should include testing of cardholder data and the company's payment processing procedures.

C1. Proposed Improvements

To create a more comprehensive and robust plan it is advised to:

1. Add a reporting phase to the penetration test. This should align with both PTES and NIST and will help clarify the risks involved, allowing for a more accurate security posture. The report should include an executive summary, technical findings, risks, and remediation steps.
2. More closely align testing to both HIPAA and PCI DSS. This is key in the healthcare industry and has real-world business impact, including legal and reputational consequences if not properly addressed. These tests should evaluate the handling of patient data and the processing of that data to ensure compliance with both HIPAA and PCI DSS requirements.

C2. Proposed Solutions

Solutions to problems identified:

1. The social engineering portion of the test is currently fairly limited. It is suggested to expand this to include other attack vectors such as email phishing campaigns and physical testing. For email testing, a tool like GoPhish could be used to run campaigns. For physical testing, methods such as USB drops in parking lots and break rooms, tailgating attempts at entrances and secure access

points, and testing badge access controls or cloning attempts should be included to evaluate on-site security.

2. Incident response plans should be written and tested frequently to assess their effectiveness and address any weaknesses. The incident response tests should include multiple formats and approaches, such as tabletop exercises and technical drills that simulate data breach scenarios. Running these regularly will help improve staff readiness, identify gaps, and increase the speed and effectiveness of response efforts.

References

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

National Institute of Standards and Technology. (2008). Technical guide to information security testing and assessment (NIST Special Publication 800-115). National Institute of Standards and Technology.

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

PCI Security Standards Council (PCI SSC). (n.d.). Retrieved February 25, 2025, from https://www.pcisecuritystandards.org/

PCI Security Standards Council (PCI SSC). (n.d.). Retrieved February 25, 2025, from https://www.pcisecuritystandards.org/