Barbara Garcia

4/24/2024

**D484 – Penetration Testing Performance Assessment**

**A1.**

The goals of Western View Hospital for this penetration testing engagement are to test security controls and estimate the susceptibility of their new medial record IT systems to exploitation and data breeches. The objectives of the test are to ensure IT infrastructure can secure sensitive financial and medical data and measure compliance of their internal and external systems with HIPAA. The hospital’s main functions as it pertains to the penetration test are to secure patient medical and financial records as well as to provide a secure way for patients to make payments. Their processes consist of Active Directory which manages endpoint antivirus and administrative controls. They practice data privacy and client accessibility.

**A2.**

Pruhart Tech has proposed a structured penetration testing plan. The scope includes hosts in internal networks, internet-facing hosts, and employees. The type of test they are conducting is goal-based. The approach they are using is to conduct technical penetration testing against hosts on an internal network, technical penetration testing against internet-facing hosts and social engineering using the telephone (POTS). The techniques they are using are reconnaissance, enumeration and attempt to overtake servers on the internal network, using burp suite to attempt to hack into the external assets and calling employees and pretending to technical support from the hospital in order to elicit user login credentials.

**A3.**

Misalignments between the testing plan and the company’s goals, objectives, functions, processes, and practices exist. The test involves the entire IT department, which can limit the realistic measure of the hospital’s readiness against a real threat. Another weakness in the plan is that a credentialed scan of the network from a machine located in the internal network (not just a sensor) is not planned. A credentialed scan being conducted is important as it will identify vulnerabilities that a non-credentialed scan will not. Another misalignment is that the penetration test plan indicates a phone social engineering attack which is much less likely to result in credential disclosure than an email phishing attack. One other major shortfall is that the plan does not call for an attempt to physically access sensitive assets, like servers containing PHI and PII.

**B1.**

Best practices for a penetration test that would meet Western View Hospital Requirements include: “Asset vulnerabilities are identified and documented, threat and vulnerability information is received from information sharing forums and sources, internal and external threats are identified and documented, potential business impacts and likelihoods are identified, threats, vulnerabilities, likelihoods and impacts are used to determine risk, and risk responses are identified and prioritized.” (“2023-06-20 05:11 | Archive of HHS.gov”)

Frameworks that meet the hospital’s requirements are HIPAA, which is a government law that deals with keeping medical records secure and PCI DSS, which is a standard by the financial industry to ensure cardholder data and transactions are secure.

**B2.**

While the penetration testing engagement plan goes a long way toward complying with

penetration testing best practices and HIPAA and PCI DSS frameworks, it is missing some important elements. While the client requested a test for a specific business purposed, which appropriately makes it a goal-based test, since the infrastructure being tested deals with medical records, it is also necessary to conduct a compliance-based test. One important step that is missing is OSINT. The penetration testing team should conduct Open-Source Intelligence research, such as combing through social media accounts of both the company and key employees to identify information and weaknesses that can be used to conduct social engineering attacks. Also missing is a plan to identify the isolated VLANs and assets such as servers where PHI and Financial records are stored to make sure they meet compliance of the above frameworks. The plan also fails to attempt to physically access critical servers, which is necessary for compliance.

**C1.**

One recommendation for improving to the penetration testing plan is to conduct an email phishing exercise with a prompt to reset the employee’s enterprise password in order to collect their credentials.

A second recommendation for improvement work with the client to designate a single IT department contact instead of the entire department. This is a better measure of their response if an actual tack were to occur.

**C2.**

One solution to the problems identified in the current testing plan includes conducting a credentialed vulnerability scan on the internal network.

A second solution to the problems identified in the current testing plan is to attempt physical access to sensitive servers via badge cloning and tailgating. The current plan is lacking any physical testing.

**Works Cited**

“2023-06-20 05:11 | Archive of HHS.gov.” *Public3.Pagefreezer.com*, public3.pagefreezer.com/browse/HHS.gov/20-06-2023T05:11/www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.