D484

Penetration Testing

BY: Christobel Nweke

DATE: July 26, 2025

Penetration Test Report Analysis

Introduction

Penetration tests are attempts to evaluate the security of an IT infrastructure by safely trying to exploit operating system vulnerabilities, services and application flaws, improper configurations, or risky end-user behavior. These assessments have become common across varies industries, as they are useful in validating the efficacy of defensive mechanisms and end-user adherence to security policies.

Instead of approaching cybersecurity from the perspective of a defensive tactical team this assessment will require you to assume the role as a member of an offensive cybersecurity team.

In this task, you will be given a penetration testing engagement plan that you will evaluate based on the business goals and industry best practices and guidance. You will also propose solutions to the gaps in the plan.

Scenario

Western View Hospital is a 100-bed facility that has been serving the residents of a rural community for over 80 years. The administration recently completed an expansive modernization of the medical and patient records system in an attempt to provide better care for members of the community.

Before the new system can go live, the hospital administration has authorized your firm, Pruhart Tech, to test it for potential vulnerabilities and to ensure the IT infrastructure can secure sensitive patient medical and financial data according to HIPAA compliance requirements. A senior manager at Pruhart Tech has asked a member of your team to develop a penetration testing engagement plan for Western View Hospital that is in alignment with their goals and follows industry best practices. To ensure the penetration testing plan is appropriate for the hospital before it is put into action, your manager has asked you to evaluate the testing plan, provide recommendations for improvements, and propose solutions to any problems you identify.

Penetration Testing Plan

Overview

Western View Hospital (CLIENT) engaged Pruhart Tech to conduct penetration testing against the security controls within their information environment to provide a practical demonstration of those controls' effectiveness, as well as to provide an estimate of their susceptibility to exploitation and data breaches. The test will be performed in accordance with Pruhart Tech's information security penetration testing methods. Pruhart Tech's information security analyst (ISA) will conduct all testing in coordination with CLIENT's information technology (IT) staff members to ensure safe, orderly, and complete testing within the approved scope. CLIENT's information environment is protected by endpoint antivirus and administrative controls managed by an Active Directory. The environment contains numerous potential vulnerabilities, which makes CLIENT susceptible to data breaches and system takeovers. Highly important files that contain HIPAA and payment information may be easily accessible and very visible, putting CLIENT at great risk to compliance violation and potentially subject to large fines or loss of business reputation.

Extent of Testing

CLIENT engaged Pruhart Tech to provide the following penetration testing services:

- Network-level, technical penetration testing against hosts in the internal networks
- Network-level, technical penetration testing against internet-facing hosts
- Social engineering phone phishing against CLIENT employees

Internal Phase

Pruhart Tech's ISA will conduct various reconnaissance and enumeration activities. This will include port and vulnerability scanning, as well as other reconnaissance activities, to try to reveal any security holes, particularly vulnerabilities, that allow complete system takeover on important servers, most critically the McAfee security server for which a compromise could allow a potential attacker to render the endpoint security for the entire internal network inoperable or ineffective. If server compromise can be achieved, directory traversal will be conducted to search for important data such as private patient data. The ISA will use a Secure Sensor deployed inside CLIENT's facilities to conduct port, service, and vulnerability scanning, as well as other reconnaissance techniques within CLIENT's internal networks. EternalBlue will be used to gain root-level access to multiple critical systems including the McAfee security server.

External Phase

The external phase of the penetration test will focus on the assets that are publicly accessible. Reconnaissance and scanning will be conducted to identify opportunities for intrusion or malicious modification of the systems. Attacks will be launched from Pruhart Tech's network via internet to the externally accessible assets at Western View Hospital using Burp Suite and network scanner Nmap 4.2.

To determine and practically demonstrate the feasibility of gaining physical access to facilities' non-public and high-security zones or gaining unauthorized, authenticated access to CLIENT's workstations, the ISA will conduct phone-based social engineering. Pruhart Tech's social engineer will perform phone-based social engineering with the goal of getting credentials or having CLIENT staff perform tasks on their workstation. This is intended to simulate a malicious actor attempting to gain credentials and a foothold in the environment by a phone call. Pruhart Tech's social engineer will call CLIENT staff members claiming to be a technical support worker authorized to contact CLIENT's personnel to provide critical support. If challenged, the social engineer will then drop information security staff member names in a statement that they are working on their behalf. The social engineer's program will include the following activities:

- Requesting that the user provide their domain username
- Feigning an attempt to perform a technical operation on the user's behalf, and then requesting that the user provide their domain password when the operation "fails"

Pentest Plan Analysis

Evaluation of alignment between client and pentest plan

Western View Hospital (Client) is a moderately sized facility that had been serving residents of its rural community for over 80 years. It seems that they recently completed a mass upgrade to their medical and patient records system in order to provide higher quality care for members of their community. Before feeling confident in rolling out these new quality of life changes the client needed to be sure that the sensitive patient medical and financial data were secured according to HIPAA compliance requirements. So, they requested penetration testing to root out potential vulnerabilities with their current security controls in order to ensure confidential patient information isn't susceptible to exploitation and data braches. Prior to the start of the Pentest, it's noted that the client has an endpoint antivirus on their system while also having their administrative controls managed by an Active Directory.

Pruhart Tech's breaks divides their tests into 3 types. The first targets the clients internal networks. During this stage reconnaissance and enumeration activities are performed including but not limited to port and vulnerability scanning. Pruhart Tech plans on performing credentialied internal scans of the system during the reconaissance phase as well. To increase the likelihood of spotting critical systems vulnerabilities to aid in their exploitation attempts The results of the reconnaissance could aid in exploiting key areas such as the endpoint antivirus (Mcafee security server) the client has on their internal systems. There is also plans to leverage eternal blue to gain root level access to multiple critical systems.

The second type of test Pruhart Tech plans on performing is an external tests of the clients assets that are publicly accessible. Reconaissance and scanning will also be performed here to identify areas for exploitation of the systems. Pruhart Tech also has Plans to perform direct attacks on the clients public facing networks using tools such as burt suite and nmap 4.2

Lastly Pruhart Tech plans on performing phone based social engineering in an attempt to gain credential information and a foothold within the clients network by pretending to be a technical support worker on behalf of the client.

This penetration testing is a good baseline to start with but it does miss a couple of marks. It doesn't fully address The clients concerns. One of the few ways that it's unaligned with clients expectations is in regards to compliance frameworks. The client does specify that they want to "secure sensitive patient medical and financial data according to HIPAA compliance requirements." (Scenario Par 2) However, HIPAAA is more so focused on protecting the patients Physical and electronically accessible patient health information. It doesn't target the financial aspect. This would be a different compliance framework that the penetration testing plan should aim to also be compliant in. For example since the client most likely processes patient payment as well as store patient financial data the penetration testing plan should also aim at being compliant with the Payment Card Industry Data Security Standard (PCI DSS) as well as Sarbanes-Oxley Act (SOX). Another area of misalignment lies in the scope of Social Engineering (SE) to be performed to stay in compliance with HIPAA requirements. While the penetration testing plan does include SE tests like vishing that aims at exploiting the workers it falls short in including more Social Engineering scenarioes. For example scenarios in which an employee falls victim to email related phishing attempts. Another scenario could be a malicious actor gaining physical access to patient health information through tailgating/piggybacking. These are other high risk ways malicious actors could gain access to patient health Information that the penetration testing plan doesn't address which would also address the clients goals/objectives of remaining HIPAA compliant.

Evaluation of the pentest engagement plan

Some of the best practices that the penetration plan could employ that would help meet clients requirement includes but not limited to an extensive discussion on scoping requirements as well as an extensive discussion on rules of engagement prior to the start of the penetration test. Some frameworks that could also help meet the clients requirements are HIPAA, PCI DSS, and Sarbanes-Oxley Act (SOX).

The pentestration testing engagement plan lacks in areas of identifying scope of tests. It makes mention of the internal and external tests to be performed but doesn't identify what systems are legitimate targets nor does it also address issues related to what time of day to pentest and even how to handle patient data in the event of a successful breach.

The testing plan does aim to test some of the internal controls of the clients system as well as external which helps it fit overall into testing that helps in being HIPAA compliant. It does include social engineering tests as well which is great. The social engineering aspect though does lack and isn't very comprehensive. The pentest engagement plan also doesn't address the financial data protection aspect of the clients goals/objectives like being complaint in PCI DSS/SOX. While the client does seem to lump in the financial data with being compliant with HIPAA it is the duty of the pentester to be knowledgeable enough to know that HIPAA and finance related data fall under separate compliance frameworks.

Suggestions to improve the current Pentest engagement plan

The penetration testing plan doesn't do a very good job of identifying scope. The penetration testing plan needs to establish "explicitly what IP ranges are in scope for the engagement." (The Penetration Testing Execution Standard Scoping Meeting Par 3) While the client themselves might not understand the need for this, it should fall on the penetration tester to help guide the client in identifying this scope in such cases. There could be legal issues if scope is not defined. If the client does not own certain systems and the penetration tester isn't aware of that limitation and performs penetration testing on said systems this could land the Penetration tester/firm in serious legal trouble. Which is why it is very important that scoping is included in the penetration plan. What IP Addresses are in scope, what systems does the pentester have access to. If a system is outsourced to a third party in a different country, what are the rules and regulations of that company that could impact the penetration test etc. These are all scoping discussions that should happen and also be included in the penetration testing plan.

Another recommendation that would improve the penetration testing plan would be including clear rules of engagement. This is crucial given the importance of the data (Patient Health Information) being pen tested on. This data should in no circumstance be under the possession of the pen tester regardless of the fact that they are attempting to breach this data. This is one of many considerations that Rules of engagements aim to address. Patient data availability is something to also consider as well. Therefore rules of engagement that aim to address what time of day is permissible to perform testing that could affect customer data availability is a concern that also could be addressed via Rules of engagement specifications in the penetration testing plan. Given again the sensitivity of the data being handled there are various other legal considerations that a rules of engagement should address making it such an important needed addition to any penetration testing plan.

We established several client misalignment earlier from the lack of compliance frameworks that targeted financial data to a lack of social engineering tests that would help cover the bases for HIPPA compliance. One of the solutions to frameworks aimed at protecting client financial data which meets the clients goals/objectives would be implementaton of PCI DSS compliance frameworks as well as the Sarbanes-Oxley Act (SOX). PCI DSS compliance standard calls for establishing annual external and internal penetration testing as well as ensuring that the cardholder data environment is properly segmented from other areas of an organizations infrastructure. Checking for proper network segmentation is something that the penetration testing plan doesn't highlight and could benefit from including. The annual assessments that PCI DSS also calls for could be self assessed on this clients part since they more than likely don't make greater than 20,000 annual card transactions given how the client serves a rural community. Implementing SOX to meet the financial data compliance that the client requests is a bit more involved. The PCAOB organization which enforces SOX compliance does state that companies wanting to be SOX compliant need to ensure that that they have elements that encompass the five COSO. components on internal control. This framework includes common definitions of internal control and criteria against which companies can evaluate the effectiveness of their internal control systems. The 5 controls elements are:

- Control environment,
- Risk assessment,
- Control activities,
- Information and communication,
- Monitoring

Bibliography

[1] Jason Charalambous et al. *Payment Card Industry Data Security Standard (PCI DSS)*. 2014. URL: https://wgu.percipio.com/books/7612f29b-c2c5-495c-931b-f0c9244295c1#epubcfi(/6/52!/4/2%5Bepubmain%5D/2%5Bch003_s1_3%5D/2/2/1:0).

[2] PTES. *Pre-engagement - Introduction to Scope*. 2014. URL: http://www.pentest-standard.org/index.php/Pre-engagement%5C#Introduction%5C_to%5C_Scope.

[3] PTES. *Pre-engagement - Pre-engagement - Rules of Engagement - Legal Considerations*. 2014. URL: http://www.pentest-standard.org/index.php/Pre-engagement%5C#Legal%5C_Considerations.

[4] PTES. *Pre-engagement - Pre-engagement - Rules of Engagement - Time of the Day to Test*. 2014. URL: http://www.pentest-standard.org/index.php/Pre-engagement%5C#Time%5C_of%5C_the%5C_Day%5C_to%5C_Test.

[5] PTES. *Pre-engagement - Rules of Engagement - locations*. 2014. URL: http://www.pentest-standard.org/index.php/Pre-engagement%5C#Locations.

[6] PTES. *Pre-engagement - Scoping Meeting*. 2014. URL: http://www.pentest-standard.org/index.php/Pre-engagement%5C#Scoping%5C_Meeting.

[7] Lyn Spooner and George Lekatis. *The Sarbanes Oxley Act*. 2014. URL: https://sarbanes-oxley-act.com/.