**Penetration Testing**

Western Governors University

January 30, 2025

**A1: Client Goals**

Western View Hospital is requesting a penetration test to determine the overall security of their organization. Since they are dealing with sensitive patient health information it is important that this data is safeguarded. HIPAA has many guidelines in place to enforce the security of patient data.

Since Western View wants to remain compliant with HIPAA, there are many goals, objectives, functions, and processes in which we have discussed.

The goal of the client is to ensure that their patient’s data is secure and protected. They will do this by taking measures to validate security within the internal network, and any external web facing applications.

Their objective is identifying all security weaknesses and pinpoint vulnerabilities which could place the organization or patients’ information at risk of cyber threat. They would like our company to complete a penetration test to see if their current controls are effective. If we identify any weaknesses in the client’s security, they would like to enact remediations and take preventative measures.

The client functions as Healthcare Service Provider in a rural area. They are transitioning to a more modern system to provide a better experience for their patients. The introduction of new technology can potentially increase the attack surface and place the patients at risk. They will be maintaining digital health records with their new systems. They are also securing financial data which would require PCI DSS compliance. (UCSF Controllers office, 2023).

The client has several processes in which they would like us to test. We are to perform social engineering as a part of Employee Security Training. We will also examine Network Security Monitoring, to test the strength of firewalls and IDS. In addition, we will test for incident response and recovery. The recovery portion can be very important for hospitals as cybercriminals often target these atmospheres with ransomware, knowing patients’ information could be time sensitive,

For current practices, the client is using centralized anti-virus software. They are looking for ways to secure data at rest and data in transit. They understand the importance of regular employee training, advice from cyber security professionals, and remain compliant with HIPAA and todays standards for Hospitals. Safeguarding patients’ information is very important. In certain cases, it could even mean life or death.

**A2: Penetration Testing Engagement Plan Structure**

The scope of our Pentest encompasses the internal environment and the external environment. We are to conduct the test in a manner which does not disrupt normal operations of the client. In addition, we are to properly remove all created credentials, shells, tools, and any traces which a malicious actor can use to their advantage.

The Internal environment consists of a technical penetration test geared towards hosts in the internal network. The second phase of our test will be internet facing hosts. We will also be conducting social engineering on the employees to assess their level of understanding in regard to cyber threat. The social engineering portion will consist of phone calls and phishing emails to extract sensitive information and potentially gain access to host devices.

In order to ensure client security, we will be implementing several tests simultaneously. Our team will be communicating consistently to ensure situational awareness, those avoiding collision and interruption. We will operate as an outsider, with no knowledge the environment performing external scans and passive reconnaissance as a means obtaining enough information to gain foothold. We will be operating with partial knowledge to perform credentialed scanning as this will provide us with important system information which we can track back to a CVE database to assess various known vulnerabilities. We will also have a pentester operate with full system knowledge to operate as an insider as company employees can also be a threat. We will do this to ensure organization is operating based on the principles of least privilege.

Our approach will consist of consistent exploration and reconnaissance. We will start off with passive tools which will not alarm the employees as they will be unaware of the engagement at first. We will utilize OpenVas, WHOis, NMAP, NSlookup, Dig, and various tools which will allow us to enumerate the users and the assets. Once we have identified the assets and created basic understanding of the topology regarding accessible areas, we will start to identify the open insecure ports which can potentially be exploited by a malicious actor. Our goal is to highlight as many unnecessary services as possible so the client can decrease their attack surface and keep their patients safe.

We will also look for weak configurations and defaults as these can be common in new setups. We will simulate several social engineering attacks against the employees with the use of the Social Engineering Toolkit, and direct impersonation calls. We will likely use some of the common methods that malicious actors use such as: Urgency, likeness, fear, social proof, Quid pro quo, etc.

**A3: Misalignments**

The current penetration testing engagement is on the right path, however there are ideas mentioned in the plan which may not be aligned with the clients’ goals.

The current plan is suggesting the use of a powerful exploit known as Eternal Blue. This exploit, if used improperly, could cause significant damage to devices and could result in downtime or data loss. This creates unnecessary risk and could potentially harm the patients if they lose access to their data.

There is not a clear direction of how patient data will be handled if discovered. There is also no mention of fragile devices, IOT devices, or medical devices that might be discovered during the test. There should be a playbook on how those devices will be interacted with if discovered. In addition there should be a specific IP range within the scope. There should also be testing for MFA during the credentialed testing mentioned earlier.

**B1: Best Practices and Frameworks**

In order maintain the best practices for penetration testing there are a few actions that must take place. It is important that rules of engagement is as clear as possible. The scope of the penetration test should include more details. It is important that we clarify which devices are within the scope. The ip ranges, the locations, and the interactions that are possible with the employees. We also must determine how to properly handle sensitive data when discovered.

In order to meet the client’s objectives of securing their network we will utilize two frameworks which are suitable for the environment. We will reference the MITRE ATT&CK & OWASP Frameworks. MITRE ATT&CK is suitable for the environment as it will help to categorize different techniques and tactics that malicious actors commonly use. This will help the client prepare for attacks before they arise. OWASP will be great web application testing. We need to determine if there is any external threat to the internet facing servers and applications the client is utilizing. We will test for common vulnerabilities such as SQL injection and Cross Site Scripting. In addition, we will check for secure coding, input validation and parameterized queries.

**B2: Comparison of Plan to Best Practices and Frameworks**

There are currently some gaps in the penetration testing engagement plan and the desired best practices/frameworks. It is important that the team has clarity on scope before the engagement begins. The team is going to be interacting with sensitive health information, so it is important that they set boundaries on which files and devices are accessible. The manner in which pentesters interact with employees should also be clearly defined, as there are many in which social engineering can take place. Make sure that the employees sign an agreement acknowledging that these tests can take place and make sure they go through training before the engagement.

The Frameworks OWASP & MITRE ATT&CK are not mentioned in PTE. These should be referenced as they contain guidelines and a significant amount of information which can be utilized regarding the environment. While some of the tactics and methods are mentioned there is not a clear structure or information for the client to understand how the attack could take place. In addition, there should be clear hours of operation and instructions on how to interact with devices to avoid disruption.

**C1: Proposed Improvements**

There are two recommendations which I feel the current plan would benefit from substantially. If possible, the team should discuss the creation of a simulated environment that doesn’t impact devices which are holding PHI. This will reduce the risk of system interruption.

The plan would significantly benefit from in-depth scope, in relation to devices, locations, engagement with employees. Refining the scope will leave less room for error, which could be costly to both the penetration team and the client.

**C2: Proposed Solutions**

While there are problems identified in the current engagement plan, there a plenty of examples that would create an efficient solution.

It is very important to test the environment for any weaknesses to ensure that malicious actors are not able to access patient data. It is also important to discuss the scope of the test to ensure that the pentesters do not create new problems for the organization while doing the testing. Discussing time of day, what devices are accessible, how to interact with specific devices, and what data the pentesters can read and access is crucial to aligning with HIPAA and protecting the confidentiality patient PHI. It is important to discuss the tools that will be used and avoid tools that could cause significant damage to devices or create new vulnerabilities.

Another problem noted was misalignment with frameworks which could be very beneficial to the test. Utilizing the MITRE ATT&CK & OWASP framework the team will have guidelines which make it easier to achieve HIPAA compliance in safeguarding patient data. They will approach the test using tactics that malicious actors would be more likely to use making the time spent more efficient. The use of OWASP is recommended as the hospital is utilizing web applications and internet facing devices.

Exploring different possibilities of threat, following efficient frameworks, and communicating effectively with the client in order to understand the assets will lead to efficient test. As the client branches into more modern technologies, knowing their weaknesses and vulnerabilities early will protect their patients, their reputation, and help them to avoid fees for lack of compliance.

**D.  Sources**

UCSF Controllers Office. (2023). Understanding PCI DSS.

https://controller.ucsf.edu/how-to-guides/accounting-reporting/understanding-payment- card-industry-data-security-standard-pci