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"