Penetration Testing Platinum Plan FAQ'S

What is Penetration testing?

Penetration testing (aka"Pen testing") is in the context we are suggesting here, a software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.

How is this done?

A specific target (vector) within your organization is defined and a plan is created to nondestructively attempt to breach your company.

Essentially a professional trained to use the same tools and processes used by cyber-hackers is given your target vector and permission to remotely or internally attack your office computer systems.

We gather Information about your company, locations, email service, Internet addresses, infrastructure, software, and personnel. Based on this information we schedule and plan an attack on your computer system over the Internet. Initially we will target the firewall and the email system. The intent is to attempt to access user passwords, elevate security credentials and exploit vulnerabilities using readily available hacker tools. If appropriate, we will test your company website for the latest basic security vulnerabilities (Google: "Heartbleed", "Bash").

We will issue a report showing exploitable vulnerabilities, if any, and suggestions for remediation.

I am HIPAA compliant, so why do I need this?

While a HIPAA Privacy & Security IT audit might check the box for a HIPAA requirement it does not necessarily equate to a secure IT or business environment.

Your IT security consultants will have likely protected your computer systems for IT best practices, risk analysis, audit, redesign and remediation the final IT system is not actually penetration tested. Pen testing is analogous to a hidden shopper service such as retail stores use to test their staff. In this context penetration testing simulates a hacker attempting to get to your PHI, Finances or IT resources.

What will a Pentest Reveal?

According to Shon Harris, one of the top experts and author for Security Certification study manuals, "A penetration test is carried out to emulate what a real hacker would do and it proves to the company that the organization can indeed be penetrated." If the CEO is presented with his or her password to their computer or the Server, then this would be the difference between assuming what to protect and actually knowing what must be protected.

http://searchsecurity.techtarget.com/answer/How-security-audits-vulnerability-assessments-and-penetration-tests-differ

Additional Items included from the Silver & Gold Plans:

What is meant by "Test your passwords for length of time it will take to crack each (30 max.)"?

This is a presentation with the use of an online resource to visualize the vulnerability of your passwords. It is interactive and will demonstrate an easier method of password creation and importance of password length. You will be given this resource for future use.

What is meant by "Internal (LAN) Password Hack to determine if passwords are exposed on your network internally."?

This is a test conducted on a computer inside your network. The purpose of the test is to determine the real world vulnerability to internal hacking. The test is conducted remotely by one of our engineers as to simulate someone inside your infrastructure and is non-destructive. We make a moderate effort to reveal user

login and passwords on the network. This is done with readily available free tools online.

What is a "Firewall Vulnerability Port Penetration Test with Pass or Fail Certificate?"

In this test we remote into your office on a workstation and perform a non-destructive attack on the firewall's most common access points (also called ports). The results are presented online with an immediate pass or fail reports. We explain the results verbally and discuss suggestions as appropriate.

What is "External Email Domain, Non-Destructive Diagnostic Attack"?

Depending on your email system we probe the email domain, which is exposed on the Internet by necessity. We retrieve the publicly accessible configuration and determine the vulnerabilities and potential exploits of your email system. This simulates the initial levels that a hacker might perform to begin to penetrating your email. We discuss the results and if appropriate provide suggestions

What is "10 Cyber Security Awareness Facts"?

This is a document of current cyber-security, physical security, malware and IT privacy basic information to help staff and management understand and protect themselves from computer risk.