CyberSecurity

VESTIGE
Digital Investigations

I.T. Penetration Testing Options

There's A Difference

Penetration Testing (aka, Pen Test) is NOT the same thing as Vulnerability Scanning (VS). In fact, VS is a "tool" and one which we may actually employ as part of our Pen Testing, but not necessarily.

Determine Weaknesses In An I.T. System

For Vestige, Penetration Testing is about identifying vulnerabilities which can be exploited and then take it the next level to confirm and see if those vulnerabilities can actually be exploited. While part of the goal of a penetration test is for us to gain access to the system, the real goal of a penetration test is to systematically test the environment in a realistic fashion to determine if there are weaknesses that should be addressed. For a well-controlled, well-secured environment, we may not be able to gain access to the environment. However, the steps that are taken, the information learned and items identified as being in-place and working can offer an organization value in confirming that the environment is well-controlled.

On-Going Evaluation Is Important

However, CyberSecurity is an ever-changing world. New vulnerabilities are discovered, new exploits are developed, systems get configured and reconfigured over time, new equipment and resources are deployed, updates and patches to systems continue to be made—all of these things can have an impact on the organization's CyberSecurity. Therefore, on-going evaluation of an environment should be undertaken.

Do No Harm

Vestige follows Best Practices as it relates to Penetration Testing. Our mantra is to "Discover...But Do No Harm". That means that we may, during our assessment, identify potential weaknesses, that based upon our knowledge and experience, we recognize as a risk and also know that it could do damage to the environment. This can include such things as creating a Denial Of Service (DOS) attack, deleting data, documents, user accounts or configurations, or even taking a system off-line. Vestige will never knowingly pursue such activity. Instead, we will identify these items, testing them as close as we can, but stopping short of performing any type of activity that would or could result in harm.

Vestige **Benefits**

- Realistic Assessment of the organization's critical infrastructure.
- Options provide good balance between realism and ensuring focus is on the "right" assets.
- Gain insight as to how an attacker views your environment.
- Receive advice on how to further strengthen your environment.

Get Started with Vestige

Contact us today to learn how Vestige can partner with your Organization to provide proactive or reactive CyberSecurity Penetration Testing of your I.T. environment.

You'll be glad you did!

Vestige Digital Investigations

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

info@VestigeLtd.com | **800-314-4357** | www.VestigeLtd.

OVER

Vestige **CyberSecurity**

Three Realistic Approach Options

Organizations hire us for a number of reasons – hopefully tied to well thought-out goals of the organization. As such, we offer three types of Penetration Tests.

Black Box Option

Black Box penetration tests are the most realistic in terms of approaching the environment from an attacker that knows little to nothing about the organization. In essence, this simulates the impact that an outside attacker could have on the environment using only information that is in the public, is discovered by the attacker or gained by incrementally and sequentially infiltrating the organization.

While our approach is to be as thorough as possible, depending on the organization's complexity, configuration, attention to ensuring there's a well-controlled environment, etc., a Black Box pentest may miss some areas, as the idea is to assess the environment and gain access. Gaining access is generally viewed as success and along the way the items that we test and identify as weaknesses can be addressed.

+ **PROS:** Most realistic approach

- **CONS:** May not identify or focus on all areas or the areas of most concern to the organization

White Box Option

On the other end of the spectrum is a White Box penetration test, whereby we work hand-in-hand with the organization to identify the scope, specific systems of concern, and the overall plan of attack. Most organizations have a relatively good feel for their environment and know where their weaknesses are. As such, a White Box approach directs us to those areas that are of highest concern and ensures that the organization gains the value of focus on those areas.

+ **PROS**: Focus on the areas of highest concern

- **CONS:** Less realistic

Hybrid Option

Vestige's Hybrid approach is a combination of the two. It starts with a Black Box approach, followed by a reconvening of our Experts and the organization's stakeholders. During that meeting we share what we have found and determine areas where we may not have had visibility and discuss the organization's priorities for where they want to direct the testing.

+ **PROS:** Good balance between realistic and focus on highest concern areas

- **CONS:** More expensive

Contact Vestige today to discuss your Pen Testing needs.

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com