HITACHI
Inspire the Next

Penetration testing:

THINKING LIKE YOUR ENEMY YIELDS WORLD-CLASS SECURITY

Hitachi Systems Security Inc.

TABLE OF CONTENTS

INTRODUCTION

If the fifth century, Sun Tzu mapped out the miliary strategies the world's great armies have long following. His "Art of War" treatise also holds wisdom for those trying to ward off cyber enemies. "If ignorant of your enemy and yourself," wrote Sun Tzu, "you are certain to be in peril."

In a constantly shifting threat landscape, you can't always be knowledgeable about your enemy – *making it imperative that you are knowledgeable about your own organization and its security weaknesses.*

This is where penetration testing, or pen testing, comes in. A pen test answers the question Sun Tzu might have asked, had he faced DDoS attacks, Mirai, phishing and ransomware.

Will my security controls hold against an ***active, skilled attacker?***

In order to answer that question, there are several others every organization should ask about pen testing.

We dive into each of these in the following pages.

WHAT IS A PENETRATION TEST?

A penetration test is a simulated attack on a computer system. The goal is to find your own security weaknesses – ***before attackers do*** – so you can fix them. With pen testing, you can assess the strength of all attack vectors, including your operating system, network devices and application software.

PEN TESTING IN FIVE STEPS:

1 ▶ Find a vulnerability that could significantly affect your organization.
(You can expose these through regular vulnerability assessments and experts can help you determine how to interpret and prioritize the findings.)

2 ▶ Design an attack to exploit a worrisome weakness.

3 ▶ Appoint a red team of ethical hackers to carry out the attack.

4 ▶ Task the team with determining what kind of data they could steal from your servers and applications once they breach your defenses.

5 ▶ Act on your findings.

DO WE NEED TO PEN TEST?

In a word, **YES**.

If that word is not enough, consider some numbers:

5.3 million

Data records lost or stolen since 2013

$4 million

Average cost per incident globally

60%

of small businesses close within six months of a cyber attack

93%

of small to medium-sized businesses say that breaches significantly affected operations

You have to be right ***every time***. The attacker only has to be right ***once***.

IF WE’RE COMPLIANT, CAN WE SKIP PEN TESTING?

You can be 100 percent in compliance with your industry regulations – ISO 27001, NIST, FISHMA, HIPAA, Sarbanes-Oxley or PCI DSS. That doesn’t mean you’re ready to withstand a skilled human threat.

Compliance ≠ defense

66%

of breaches take months or years to discover*

*Verizon 2016 Data Breach Investigation Report

> “Victorious warriors ***win first*** and then go to war, while defeated warriors go to war first and then seek to win. – *Sun Tzu*”

HOW DOES A PEN TEST BENEFIT MY TEST?

While the main goal of pen testing is to assess the depth of a vulnerability and how much pain attackers could inflict by exploiting it, there are other benefits to your team. Beyond learning hard truths about your organization's weaknesses, your pen test partner can help you use the results to:

- *Justify resources to your C-suite*
  If you've already asked upper management for the means to plug security gaps, a pen test provides the evidence to get the resources you need.

- *Identifying training needs*
  If your ethical hackers compromise your systems, but your team doesn't notice the breach, you'll learn a lot about where they need further security monitoring training.

- *Spot gaps that need closing*
  If you have gaps in your security defense, pen testing will expose critical vulnerabilities, so you can improve your security posture.

- *Save time and money*
  It's a lot easier to test and modify new technology before anyone starts relying on it. Perform your pen tests on applications and environments before they go into production.

WHAT HAPPENS IF WE DON'T PEN TEST?

Some of the highest profile breaches of the last several years could have been avoided through high-quality, comprehensive pen testing.

TARGET BREACH

Compromise private data of
70 million
customers

11 Gigabytes
of data stolen

$200 million
in credit card fraud / replacement costs

SONY BREACH

11 Terabytes
of data compromised

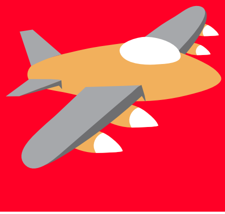
Private information of
4,000
employees exposed

100,000
Downloads of unrelased movies

What happens if you don't pen test? ***60% of small businesses close within six months of a cyberattack.***

HOW OFTEN SHOULD WE PEN TEST?

In high-visibility, high-target industries, vulnerability assessments should happen regularly, and should work with trusted, knowledgeable security partners to identify which weaknesses warrant pen companies testing. With attackers focused 24/7 on their next breach victims and constantly devising new attack methods, organizations cannot view pen testing as a one-and-done activity.



> The general who wins the battle makes many calculations in his temple ***before the battle is fought.*** The general who loses makes but few calculations beforehand. – *Sun Tzu*

62%
of cyber attack victims have been SMB's.*

**Verizon 2016 Data Breach Investigation Report*

WHAT DO WE DO AFTER PENETRATION TESTING?

If your red hat team beats your security systems, you have to move beyond the binary labels of “secure” and “not secure.”

Engage a partner to help you map out a plan to fortify all the critical systems implicated in your simulated attack, like:

- ***Customer databases***
- ***Applications***
- ***Servers***
- ***Networks***

About Hitachi Systems Security

Since 1999, Hitachi Systems Security has helped companies identify and repair their vulnerabilities to secure their most sensitive IT assets. Ready to talk to an IT security specialist about your defense strategy?

Hitachi Systems Company is a Global IT Security Service Provider who builds and delivers customized services for monitoring and protecting the most critical and sensitive IT assets in our clients' infrastructures 24/7. With a relentless focus on risk management, and continuous improvement of our technology and incident response processes, our clients count on us to provide the right solutions for their businesses -quickly, effectively and with expertise beyond the industry standards. Our mission is to deploy information security solutions that protect our customer's brand, and allow them to harness the full potential of connecting people and businesses together to build trusting relationships that can be catalyst of worry-free collaboration and limitless potential.

Being ISO 9001:2008 certified for its Managed Security Service delivery from its World Headquarters, Hitachi Systems Security is also an accredited member of FIRST (Forum of Incident Response and Security Teams) and a Certified QSA (Qualified Security Assessor) for Canada, the United States, Latin America and the Caribbean from the Payment Card Industry Security Standards Council (PCI SSC).

www.hitachi-systems-security.com | **info@hitachi-systems-security.com**
+1 (450) 430-8166 | **+1 (866) 430-8166** (toll free)

Contact us.

Hitachi Systems Security Inc.

> “The opportunity to ***secure ourselves against defeat*** lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself. – *Sun Tzu*”