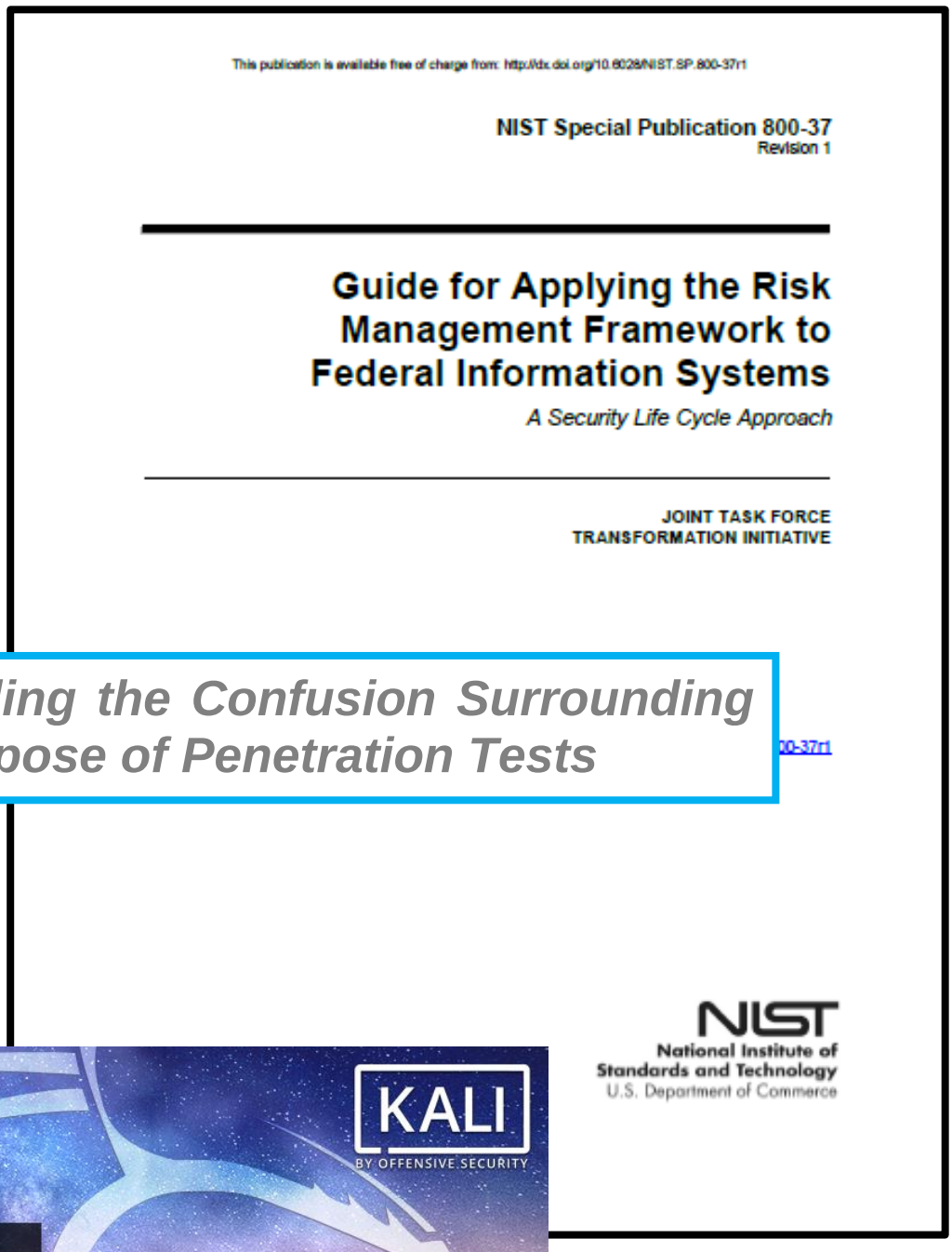
CYBER FORWARD

We Are Passionate About Helping Secure Your Sensitive Data & Infrastructure.



Unraveling the Confusion Surrounding the Purpose of Penetration Tests

Bo Birdwell
04.12.2018

Edited By: Jason Hays

CONTENTS

The Purpose for a Penetration Test

Many organizations look to Penetration Tests to serve as their Risk Assessments. When something bad happens at an organization and when we sit down with their IT[1] staff, too many conversations go like this: "When did you last conduct a Risk Assessment?" "We paid for a penetration test[2] [within the last 12 months]." *This is a problem because penetration tests primarily address the symptoms of the underlying problems, rather than their root causes*.

What is the Purpose of a Risk Assessment? A Risk Assessment should initiate the six steps within the Risk Management Framework (see top of next page). It identifies what is critical within cyberspace for an organization to operate. It then looks to find if any of these critical items (e.g. data, processes, people, hardware, etc.) are vulnerable. The Risk Assessment also studies the environment to identify, prioritize and understand the threats facing the organization. *A Risk Assessment should clearly identify risks to an organization and aid in their management, helping prioritize resource allocation to either mitigate, transfer or accept identified risks.*

Penetration Tests are not synonymous with Risk Assessments. A Penetration Test is a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.[3] Compare to the Risk Assessment definition: "The process of identifying, estimating, and prioritizing risks to operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations…resulting from the operation of an information system."[4] *Simply put, a penetration test serves a very different purpose than a Risk Assessment*.[5]

Purpose of a Penetration Test. A Penetration Test mimics specific adversary actor (script kiddies, nation-state actors, etc.) tactics to gain access to your network.[6] Used correctly, it addresses questions such as:

- Network vulnerability to different threat-actor classes.
- Identify time required for classes of actors to penetrate defenses.
- Network defenses vulnerability to human, rather than simply automated, attacks.

A Penetration Test can best serve an organization in helping identify the effectiveness of utilized security controls. Using a Penetration Test to serve as a Risk Assessment is roughly akin to starting the process from the middle rather than the beginning. *It identifies how well your intended action performed (i.e. assess security controls) rather than did you perform the correct actions (i.e. select the correct security controls)?*

---

[1] IT refers to Information Technology.
[2] The term Penetration Test is often shortened to Pen Test for brevity.
[3] Although there are many sources of technical definitions available, the author selected the National Institute of Science and Technology's (NIST) definition found in NIST Special Publication (SP) 800-53 Revision 4 (r4), *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, Includes Updates as of 01-22-2015, p. B-16.
[4] NIST SP 800-39, *Managing Information Security Risk,* March 2011, p. 8.
[5] The NIST provides detailed guidance on both Risk Assessments (NIST SP 800-30r1, Guide for Conducting Risk Assessments) and Penetration Tests (Chapter 5 of NIST SP 800-115, Technical Guide to Information Security Testing and Assessment).
[6] NIST SP 800-53r4, p. F-62.

When to Conduct a Penetration Test. The NIST[7] recommends all organizations conduct risk assessments. However, it only recommends organizations with high-impact information systems, where loss of information availability, integrity, or confidentiality would equate to severe or catastrophic adverse effect (think total mission failure), conduct Penetration Tests.[8] *This indicates the NIST believes many organizations can secure their cyber presence effectively without conducting Penetration Tests, so then why the widespread appeal?*

Why Are Penetration Tests So Popular?[9]

"Pen Test Just Sounds Cool"—Austin Justice

It may be a legal requirement. The primary reason many organizations conduct annual Penetration Tests is to comply with PCI-DSS.[10] PCI-DSS requires Penetration Tests for the reasons discussed above and not to serve as a Risk Assessment, while FINRA recommends firms conduct Third-Party Penetration Tests for the same reasons.[11] SOX is more complicated, but large financial institutions would benefit from Penetration Tests for security control assessment activities.[12] Neither DFARS, FERC, GBLA, GDPR nor HIPAA

[7] NIST refers to National Institute of Science and Technology.
[8] Impact standards definitions can be found in Federal Information Processing Standards (FIPS) Publication (Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems,* on pages 1 and 2. FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006, explains the process by which impact levels are determined. NIST SP 800-53r4, p. F-62 identifies Penetration Testing as a Priority #2 control measure and only recommended for High Impact systems.
[9] Toney Jennings, the Chief Executive Officer for *Encryptics*, aided the author develop this section.
[10] PCI-DSS refers to Payment Card Industry-Data Security Standard. The volume is entitled, *Requirements and Security Assessment Procedures,* current version is 3.2 dated April 2016. The Penetration Testing Requirement is 11.3.
[11] FINRA refers to Financial Industry Regulation Authority. FINRA published a report on Cybersecurity Practices in February 2015. The report is not legally binding, but does make recommendations to all FINRA entities.
[12] SOX, or Sarbanes-Oxley, section 404 requires financial institutions with an aggregate worldwide market value of the voting and non-voting common equity held by its non-affiliates of $75 million or more to draft an annual report. The annual report will "contain an assessment, as of the end of the

cybersecurity laws direct (or recommend) organizations to conduct Penetration Tests. *The issue primarily arises when organizations look to Penetration Tests to serve as Risk Assessments or to recommend improvements following a cybersecurity incident*.

Because it appears to bring legitimacy. When management asks the IT staff if the network is secure, it really helps IT to be able to say an external source came in and identified vulnerabilities, which we (IT staff) have addressed…so the organization is secure. This is a valid organizational requirement; however, the response simply paints an incomplete picture. A Penetration Test asks "thieves" to show you how they would rob your house. A better question might be: *Do we know all the locations where sensitive data is stored?* Or, *Is our Configuration Change Management process effective (assuming we have one)?* You could also ask, *When was our Incident Response process last tested and what did we learn?* Another equally important question to answer: *How effective are we at balancing functionality with security within security control measures?* This list is not intended to be exhaustive, rather it points out: *Penetrations answer some questions, but often not the most critical ones.*

Because it appears to show action. Sometimes people do things simply to demonstrate action rather than solve problems. A Penetration Test is an effective way to make discreet improvements to security without having to tackle more challenging issues, such as process optimization or personnel issues. Unfortunately, those same inefficient processes or other priorities placed upon IT personnel are usually the root cause of the issues where discreet changes were made. *A Penetration Test can thereby recommend discreet actions, which simply serve as proverbial band-aids…covering up the underlying problem.*

Because it is finite, if not effective. Penetration Tests follow a controllable process and produce predictable reports. It is very likely that several vulnerabilities will be found that can be patched and closed. *However, unless the underlying problems are addressed, these problems will arise again, probably within 30-60 days.*

You Conducted a Penetration Test, But…

Plugging holes in the dam does not really work. Penetration Tests often equate to closing the barn door after the horse escaped. Should a Penetration Test identify underlying policy, procedural, or data classification issues, the organization can just patch vulnerable systems instead. Organizational management will rest easier knowing something has been done, but likely does not realize the underlying issues have not been properly addressed.

$15,000 and 30 days later, are you any safer? The reader may ask: Could I have spent $15,000 and within 30 days instead made substantive improvements to processes and procedures? Although no entity desires to spend non-revenue generating income, and perhaps the Penetration Test was required because of PCI-DSS; unfortunately, the threat is not going away because band-aids were applied**.** The sheer number of cyber-attacks within public awareness today makes what should be frightening appear routine. Recent examples include Russian attacks against our critical infrastructure[13], Chinese theft of our intellectual property[14], Iranian state-sponsored hacking into our universities[15], as well as

most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." While not explicitly required, a Penetration Test could support the assessment of the security controls.

[13] https://www.us-cert.gov/ncas/alerts/TA18-074A

[14] https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

[15] https://home.treasury.gov/news/press-releases/sm0332

North Korea & Wannacry[16]. Each one in and of itself, is indicative of a significant threat to our nation, in both the public and private sector. The White House released a report in February 2018, estimating malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[17] Corporate entities can no longer consider cybersecurity as simply another non-revenue generating expenditure, it must become part of core business operations. *Was there a viable alternative? Could an organization have spent less money and less time, while improving their cybersecurity posture?*

What is the Alternative Solution?

"Instead of starting in the middle, maybe we could start at the beginning?"—Dowell Stackpole

The NIST Risk Management Framework. The NIST Risk Management Framework provides corporate entities a thoroughly-vetted Best Practice methodology to address cybersecurity concerns. It uses a systematic approach to identify what is important, determine how to protect it, validate that the protections work, and monitor everything to ensure nothing malicious occurs. Using the Risk Management Framework is a very different approach from conducting a Penetration Test. *It is more complete in approach, not expensive, and addresses underlying issues.*

This is a different approach altogether. Cybersecurity is much more about people and process than it is about technology. Technology enables processes to operate smoothly and frees people's time, but it is not a panacea. The Risk Management Framework integrates policy, plans, assessments, with technology and individual training to provide a complete solution. *The Risk Management Framework will integrate itself within your business, and not solely IT, processes.*

The Solution includes your people. No matter which source you listen to, you will find that social engineering[18] plays a prevalent role in cyber-attacks. For this reason, the NIST recommends user awareness and role-based focused training for all organizations. Most organizations train their members to not click on links or open attachments in emails; however, *few organizations emphasize properly marking documents, reporting potential cyber incidents, or the dangers of storing sensitive data on local (or personal) machines*.

Data classification is paramount. Frederick the Great was correct when he famously said, "He who defends everything defends nothing." Most organizations easily recognize their proverbial "crown jewels"; however, rarely are these digital items securely segregated from non-critical, (and necessarily, more accessible) less important data. *The Risk Management Framework can help an organization identify, segregate, and protect its sensitive data*.

Things rarely end well when one skips the first three steps of a six-step process. The Risk Management Framework has a: beginning; middle; and end; making it a finite process. Like any well-thought-out process, it flows naturally from start to finish. By confusing a Penetration Test for a Risk Assessment, an organization starts the process in the middle (Step 4) rather than the beginning (step 1). As previously stated, the purpose of a Penetration Test is to identify how well your intended action performed (i.e. assess security

[16] https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

[17] https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, p. 1.

[18] A useful definition of social engineering is "tricking people into divulging personal information or other confidential data." Definition from The Tech Terms Dictionary, https://techterms.com/definition/social_engineering

controls) rather than did you perform the correct actions (i.e. identify, select and implement the correct security controls). The Risk Management Process is iterative in nature and does not recommend simply skipping the first three steps in subsequent years and assume the identified, selected and implemented security controls are still correct. The threat evolves and so must an organization's security controls. An organization significantly increases the risk of subsequent cyber incidents by not following the process as designed. *A Penetration Test will identify vulnerabilities in specific systems without addressing what process caused them to arrive there in the first place.*

Wrapping It Up

The right way neither must cost a lot nor take a long time. A Penetration Test will identify holes in your firewall, unpatched systems, and vulnerabilities within website interfaces. Assuredly, these problems must be addressed. However, few organizations leverage a Penetration Test to address the underlying root causes, such as, "How did this happen?" Or, "What processes need improvement?" Alternatively, the Risk Management Framework frames cybersecurity within a term the Board will understand: risk. It emphasizes process and procedure over specific technologies. The Risk Management Framework improves your situation quickly because its processes already exist, necessary procedures have templates, and the configurations all have Best Practice exemplars. Most importantly, it can correct deficiencies to avoid future problems, rather than simply fix today's problems.

About the Author

Bo Birdwell co-founded Cyber Forward in June of 2017. He has over a dozen years of experience defending the largest public and private networks on the planet. He led elite technical teams of cyber operators within both the Citi Security Operations Center and United States (US) Department of Defense. At Citi, he led 20 analysts in monitoring, detecting and escalating potential malicious or fraudulent activities to appropriate investigative services.

He joined Citi after completing a twenty-year career within the US Air Force, where he served as one of the Air Force's premiere experts on offensive cyber operations. He represented the Air Force to US Cyber Command, commanded an elite 140-member network warfare squadron and directed a team of 120 individuals conducting intelligence activities for Air Force air mobility operations.

Bo led several organizations and teams, which were recognized as best in kind within the Department of Defense and Air Force. Awards included: Best Threat Working Group in the Department of Defense, recognition as one of the Top 10 organizations for best use of human resources within the Air Force and commanding the Best Air Force cyber organization. Individually, Bo was recognized as the person who best improved US Air Force and Japanese relations in 2007 and as multiple organizations' Officer of the Year. He was a Superior Performer in several Air Force-level audits. Bo served in several countries including: Afghanistan, Germany, Japan, Pakistan, Saudi Arabia, South Korea, Spain and Turkey.

EDUCATION & TRAINING

1996 Bachelor of Science in History, US Air Force Academy, Colorado Springs, CO
2001 USAF Intelligence Weapons Instructor Course, US Air Force Weapons School, Nellis Air Force Base, NV
2003 Squadron Officer School, Maxwell Air Force Base, AL, Distinguished Graduate
2003 Master of Arts in Strategic Intelligence, American Military University, Manassas, VA
2009 Master of Science in Cyber Warfare, Air Force Institute of Technology, Dayton, OH, Distinguished Graduate

PUBLICATIONS

"*Demystifying Cyber Battle Damage Assessment*," USAF Weapons Review Summer 2009: 9-18.
"*Apples & Oranges: Operating and Defending the Global Information Grid*," Information Assurance Newsletter 13, no. 2 (Spring 2010): 39-40.
"*Warfighting in Cyberspace: Evolving Force Presentation and Command & Control*" Air and Space Power Journal Spring 2011: 26-35.

THANK YOU.

FOR MORE INFORMATION CONTACT BO BIRDWELL
Bo@cyber4ward.com
https://www.linkedin.com/in/bobirdwell/
https://www.cyber4ward.com