Mighty Guides



PENETRATION TESTING CHANGES THAT WOULD MAKE FINDINGS MORE ACTIONABLE

Sponsored by

RISKSENSE

INTRODUCTION

Experts agree pen testing is highly effective at identifying an assessing vulnerabilities. The key to making pen testing more integral to ongoing vulnerability management programs is for pen testing organizations to offer faster, more flexible testing, speedier reporting, and more meaningful reports.

This eBook looks at strategies such as making some aspects of pen testing can be frequent and automated, and reporting that focuses on the greatest threats to the security posture and business needs of the organization.

Regards,
David Rogelberg
Publisher, Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

MEET THE EXPERTS

KOUSHIK SUBRAMANIAN
Strategic Security Advisor, DMDII

CLIFTON KRAHENBIL
Lead Faculty for the Information Security/ Cybersecurity Program, Columbia Southern University

WOLF HALTON
CISO/ Cybersecurity Analyst/ Disaster Recovery Specialist, Atlanta Cloud Technology

Koushik Subramanian, Strategic Security Advisor, DMDII

Koushik Subramanian is a global security expert and seasoned veteran with experience across many industries. Specialities include data privacy, risk and compliance, identity and access management, application security, and penetration testing.

"Reports need to be digestible and in business terms that business managers understand, not technical terms only meaningful to security experts."

For many organizations, pen testing is a cumbersome process that fulfills a compliance requirement. However, focused penetration tests are highly effective at identifying critical exposure and remediation priorities. As the number of vulnerabilities in complex environments grows, pen testing can play a greater role in vulnerability management. But what would make pen testing a more practical tool for regular or even continuous use as part of a vulnerability management practice?

Several things need to change, including the security team's attitude toward pen testing itself. Wolf Halton, CISO/cybersecurity analyst/disaster recovery specialist at Atlanta Cloud Technology, underscores this point when he says, "Even when 99% of successful attacks come from exploiting known vulnerabilities, most organizations are a little scared about offering up their production network to the devious attentions of a full-on penetration test."

Cliff Krahenbill, lead faculty for the information security/cybersecurity program at Columbia Southern University, makes the point that pen testing should not be a black box operation; rather, security personnel need to be involved. "Security personnel need to be engaged from the beginning to better understand the context of what makes penetration testing such an integral part of any organization's internal security framework," he says.

Clifton Krahenbil, Lead Faculty for the Information Security/ Cybersecurity Program, Columbia Southern University

Clifton Krahenbill (aka Prof. K) has worked in technology since 1998 working as a Microsoft Support Technician, a Microsoft Certified Trainer, a Technology Support Specialist, a Senior Networking Technology Consultant, and as an IT Auditor and Network Security Professional. Prof. K has a Master of Science in Cyber Security from UMUC (2015) and Master of Science in Information Technology from Capella University (2007).

"Automating the first steps … enables more frequent check-ups and allows skilled pen testers to focus on issues requiring in-depth pen tests."

"Having security personnel engaged through the entire penetration testing process allows them to 'buy in' to the importance of vulnerability testing. This early-on engagement allows the team to make better-informed decisions about how to best to utilize their limited resources and improve the security posture of the organization."

Some experts note that attitudes and practices around pen testing are already changing through the use of tools that enable faster turnaround of testing and results. Koushik Subramanian, strategic security advisor for DMDII, says, "This change is already underway. Organizations are getting hacked more often, and new regulations are leading them to test their environments more frequently. Just a few years ago, organizations had to wait weeks while settling on scope and contracts, in addition to waiting for their assigned pen tester. This process required a lot of patience on both sides of the table. These days, pen test firms continue to grow their workforce and procure more tools to help reduce the time between contract execution and kickoff. The entire industry will continue its march toward on-demand testing. This enables organizations to pen test after each change and receive more feedback in real time, which they can use to direct security resources more effectively."

Wolf Halton, CISO/ Cybersecurity Analyst/ Disaster Recovery Specialist, Atlanta Cloud Technology

Wolf Halton is a tested Senior Executive and Principal Security Architect, who works with clients in the Finance, Healthcare, Hospitality, and Entertainment industries. A Best-Selling author with five books on Computer and Internet Security. Leveraging extensive experience in cloud migrations, security architecture, disaster recovery, and global operations, he is a valuable advisor for an organization that need to tighten up their cybersecurity profile.

The key to making pen testing more integral to ongoing vulnerability management programs is for pen testing organizations to deliver faster testing, speedier reporting, and more meaningful reports. Koushik Subramanian goes on to say, "Some pen test firms have secure portals where you can input information about your environment, testing hours, sensitive systems, and in general, make the rules of engagement a click-through process. This helps tremendously because it ensures both sides are on the same page. I would also recommend a standardized reporting format. I've seen hundreds of pen test reports. They all look different even though they prioritize vulnerabilities and results in a similar manner. Why not include potential cost of remediation or the potential fine if information is breached? Organizations need to use the report as a one-stop shop. These reports need to be digestible and in business terms that business managers understand, not technical terms only meaningful to security experts."

Cliff Krahenbill agrees about the need for more meaningful reports. "The value of any pen testing report is in the delivery of the information," he says. "Canned exports taken verbatim from the scanning tool are of little value and minimize the potential benefit. The results of the pen test should be translated and customized specifically for those that will need to understand and work with pen test results. Vulnerability issues should be clearly annotated in the report with extensive recommendation on how best to remediate any discovered vulnerabilities. The report findings of the pen test should focus on the specific concerns identified as the greatest threat to the security posture of the organization. The report will have the greatest impact if it is tailored to the specific business needs of the organization."

Wolf Halton notes that some aspects of pen testing can be frequent and automated. He says, “A pen testing organization could lead the engagement with basic compliance testing (vulnerability checking, and further attempts to exploit what is discovered). A good approach is to automate the first steps. This enables more frequent check-ups and allows skilled pen testers to focus on issues requiring in-depth pen tests.”

With a third party validation service, pen testing can become a practical, easy-to-deploy tool in the vulnerability management toolbox. The key is more flexible and automated pen testing services, faster reporting, and more meaningful reports that are useful to business leaders as well as security personnel. ■

CLOSING THOUGHTS

Without a doubt, you struggle with prioritizing the plethora of threats and vulnerabilities that hit your organization. Penetration testing findings add to the problem. There are never enough hours in the day, nor enough staff to remediate all of the possible exposure on both your internal and external IT infrastructure.

Shift your thinking. Narrow down the threats and vulnerabilities to the ones that have active exploits, are dangerous with remote code execution capabilities, and are trending with active threats in the wild. This is impossible if you don't have a platform that takes in all of your vulnerability scanner data, across your dynamic attack surface: network, endpoints, database, applications, cloud, and IoT devices. Leverage human intel, combined with AI and machine learning to achieve prescriptive prioritization in minutes. Security and IT teams can focus on what matters the most with a new efficiency to manage cyber risk.

This article illustrates the value of risk-based vulnerability management to predict, prioritize, and take control of your most dangerous vulnerability and risk findings.

Regards,
Srinivas Mukkamala
CEO and Co-Founder, RiskSense

RISKSENSE

RiskSense®, Inc. provides vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness.

The company delivers a fully-informed picture of group, department, and organizational cybersecurity risk with our credit-like RiskSense Security Score (RS3). The RiskSense platform continuously correlates customer infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities to achieve security risk goals.

By leveraging RiskSense threat and vulnerability management solutions, organizations significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, lower costs, and ultimately reduce attack surface and minimize cyber risks. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.