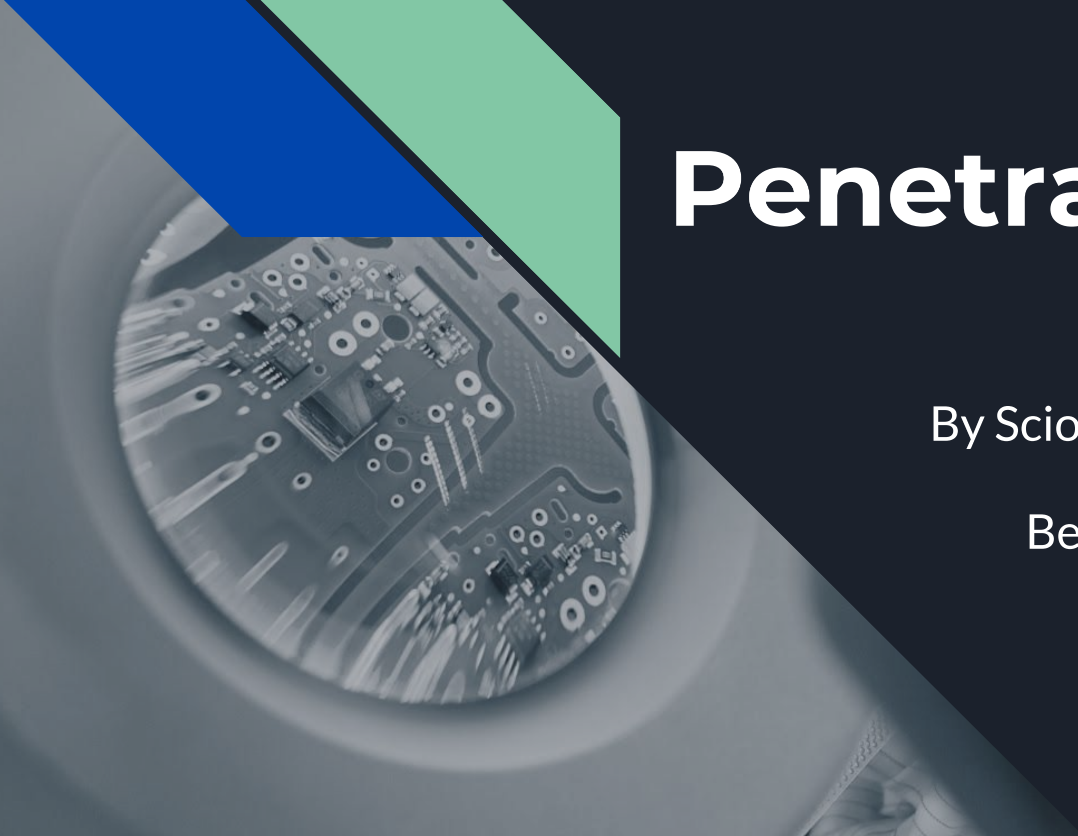


Penetration Testing

By Scion Li and Yingzi Ma

Bentley University

IPM723

Agenda

I. Introduction

II. Purpose of Penetration Testing

III. The Importance of Penetration Testing

IV. Process of Penetration Testing

V. Types of Penetration Testing

VI. Best Practices for Penetration Testing

VII. Key Challenges of Penetration Testing

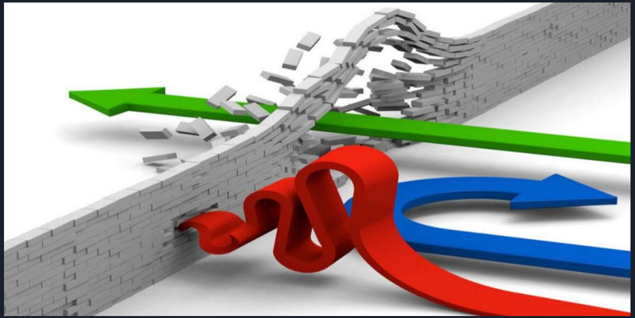
VIII. The Future of Penetration Testing

IX. Conclusion

Introduction

What is Penetration Testing?

Penetration Testing is the practice of **simulating an authorized simulated attack** on a computer system, network or web application to find vulnerabilities that an attacker could exploit.



~ Since the Mid 1960's

James P. Anderson's 1972 report titled
"The Anderson Report"

Purpose of Penetration Testing

Protect your House!

The House Analogy

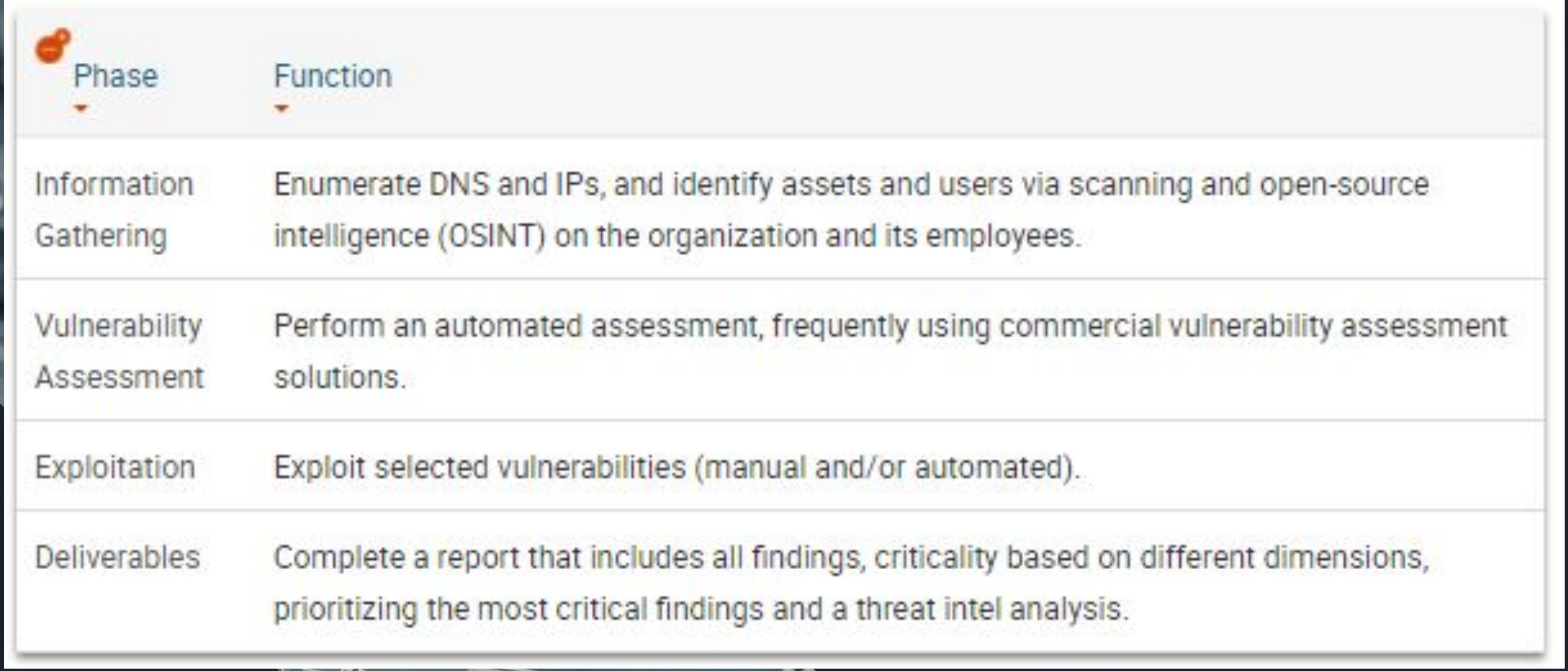
- Network/System/Assets = House
- Vulnerability Assessment = Home inspector
- Penetration Testing = Ninja

The Importance of Penetration Testing

Why is it important for organizations to use Penetration Testing?

- Prevent Data Breaches (protect data)
- Test security controls (see if they’re working)
- Ensure System Security (new systems)
- Baseline (CISOs, where spend security dollars)
- Compliance (PCI requirement)

Process of Penetration Testing



Phase	Function
Information Gathering	Enumerate DNS and IPs, and identify assets and users via scanning and open-source intelligence (OSINT) on the organization and its employees.
Vulnerability Assessment	Perform an automated assessment, frequently using commercial vulnerability assessment solutions.
Exploitation	Exploit selected vulnerabilities (manual and/or automated).
Deliverables	Complete a report that includes all findings, criticality based on different dimensions, prioritizing the most critical findings and a threat intel analysis.

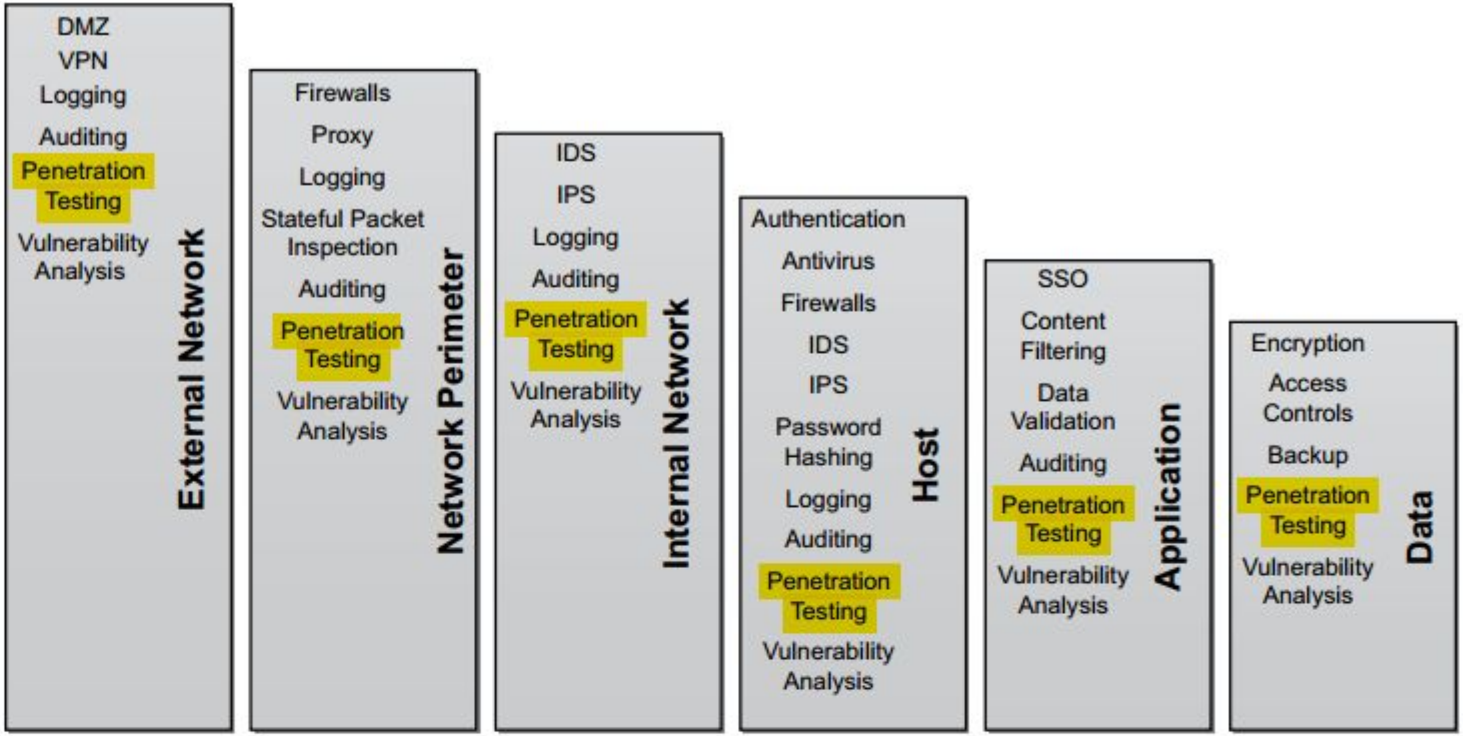


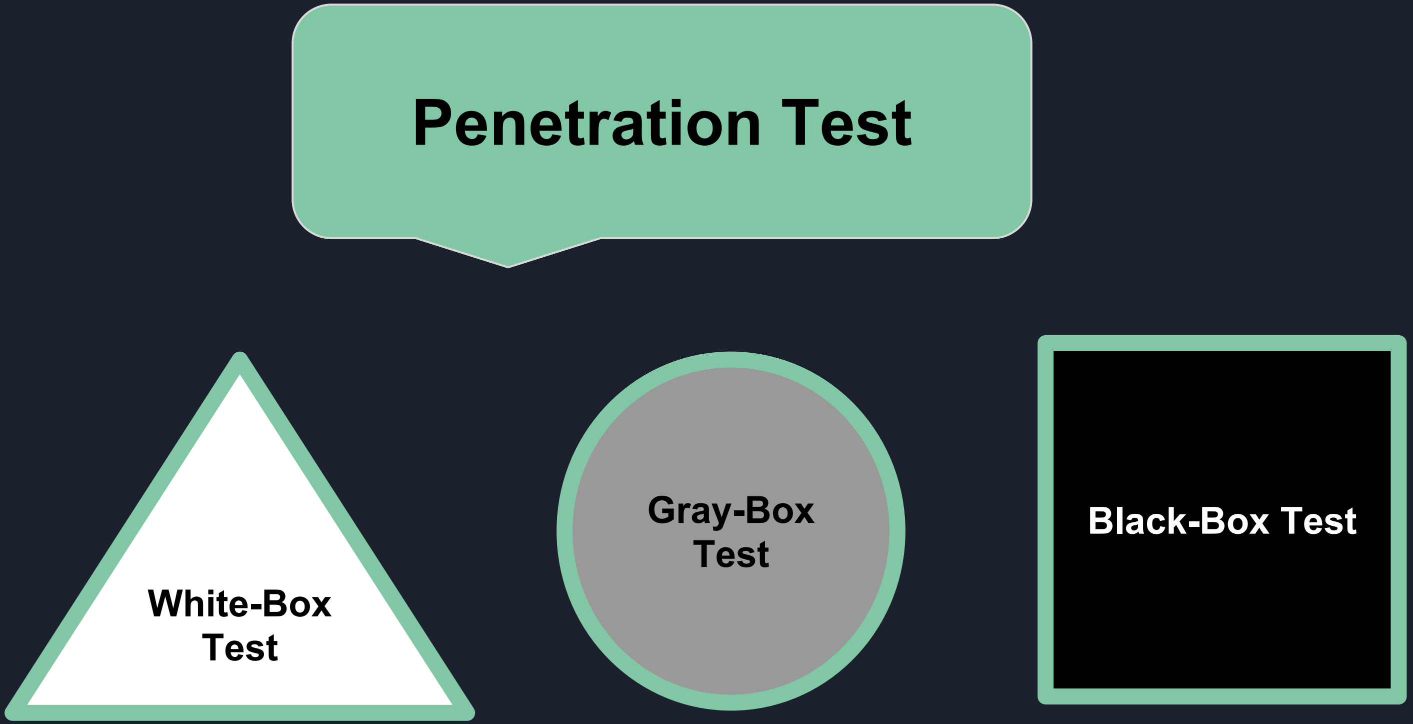
FIGURE 1.5
Defenses in Each Layer

Types of Penetration Testing

Penetration testing has three main use cases for businesses:

- Compliance - Control audits
- Risk Reduction - Gray-box, white-box and code review
- Attacker Simulation - Black-box and red team

Types of Penetration Testing



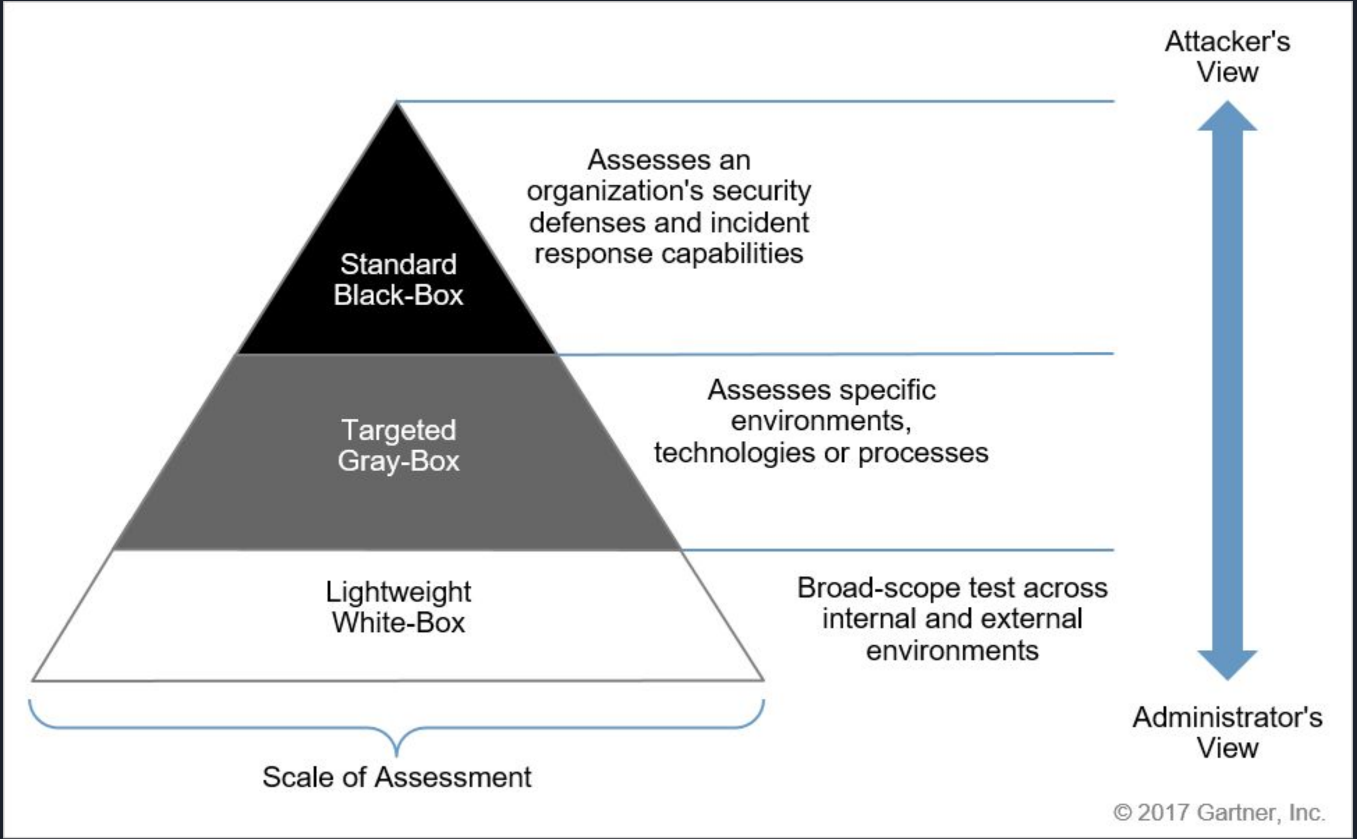
Penetration Test

White-Box Test

Gray-Box Test

Black-Box Test

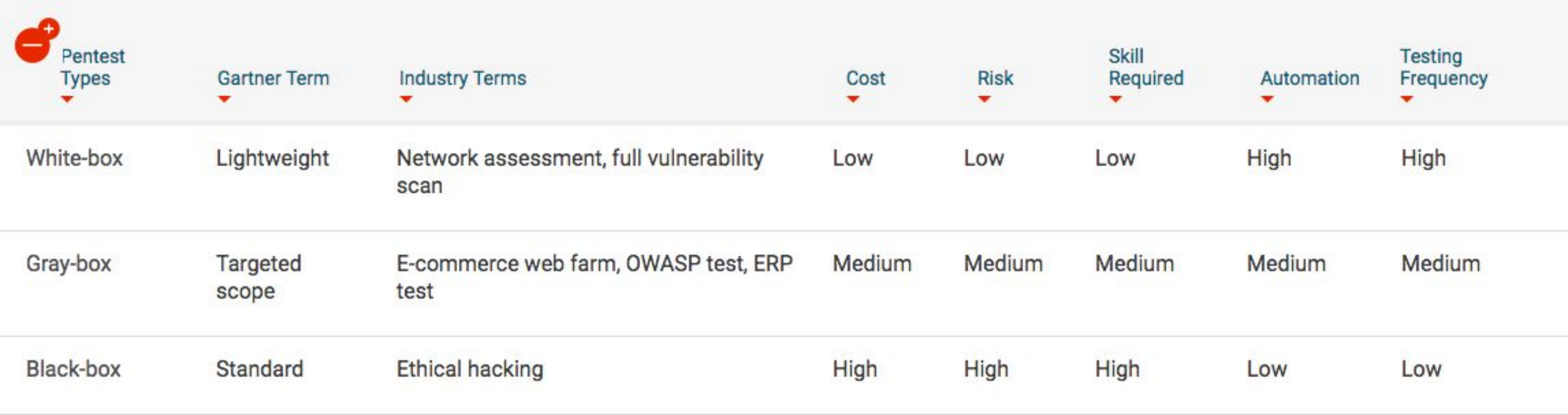
Types of Penetration Testing



Attacker's View
Standard Black-Box
Assesses an organization's security defenses and incident response capabilities
Targeted Gray-Box
Assesses specific environments, technologies or processes
Lightweight White-Box
Broad-scope test across internal and external environments
Administrator's View
Scale of Assessment

© 2017 Gartner, Inc.

Types of Penetration Testing



Pentest Types	Gartner Term	Industry Terms	Cost	Risk	Skill Required	Automation	Testing Frequency
White-box	Lightweight	Network assessment, full vulnerability scan	Low	Low	Low	High	High
Gray-box	Targeted scope	E-commerce web farm, OWASP test, ERP test	Medium	Medium	Medium	Medium	Medium
Black-box	Standard	Ethical hacking	High	High	High	Low	Low

Best Practices for Penetration Testing

- Select the Right Type of Assessment
    - Differences between pentest and vulnerability scanning
- Differentiate Assets and Environments, and Prioritize Focus
- Use Alternate Pentest Vendors to Balance the Cost and Rotation of Pentesters
- Weigh the Benefits of Post-Test Remediation Against the Cost of Implementing Changes

Key Challenges of Penetration Testing

- ★ Organizations are not fully aware of the differences between a penetration test and a vulnerability assessment, which results in a mismatch of expectations.
- ★ There are many types of pentests in use, which can be confusing for security and risk management (SRM) leaders tasked with selecting the best option for their situation.
- ★ SRM leaders show a limited awareness of the various testing models and their relevance to specific security needs.
- ★ Bug bounty programs are now viable alternatives to a traditional pentest for organizations, but require identification of major issues from the less critical findings.

18 APR 2018 NEWS

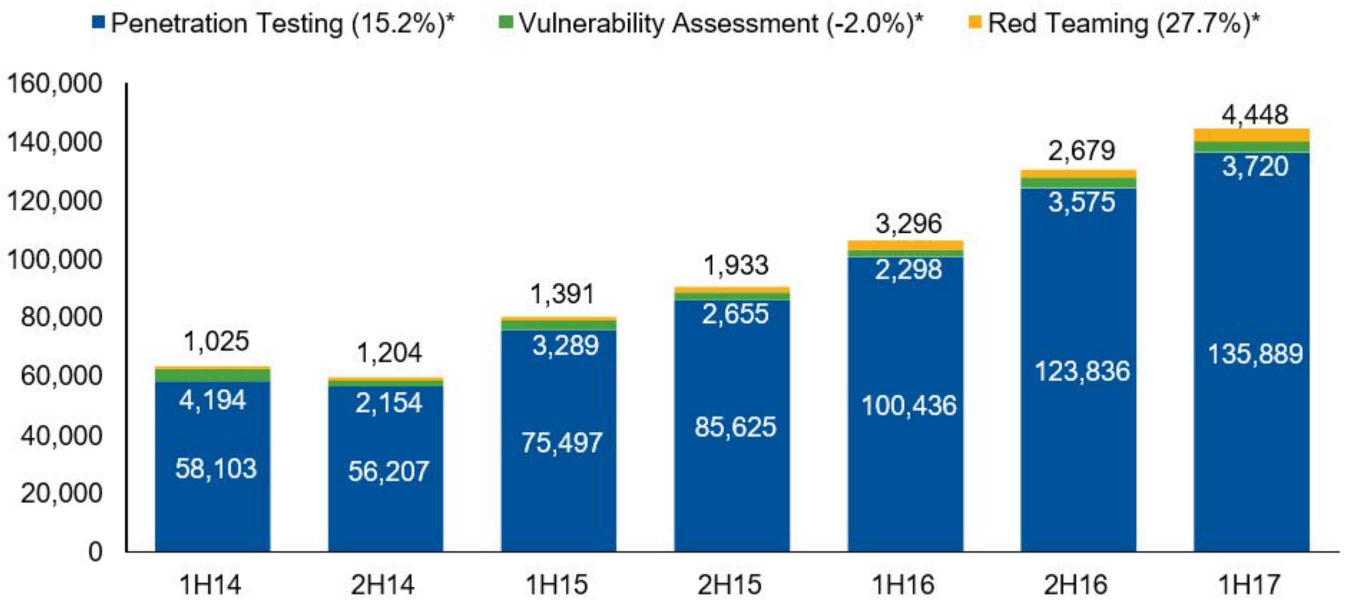
#RSAC: It's Time to Kill the Pen Test

At RSA 2018 in San Francisco today Adrian Sanabria, director of research at Savage Security, presented a session on why he believes it's time to kill the network pen test.

Pentest is not working because…

- ➔ Focus on symptoms, not root causes
- ➔ Focus on preventative controls, not detection
- ➔ Focus on depth, not breadth
- ➔ Focus on finding issues, not fixing them
- ➔ Have a lack of improvement metrics

The Future of Penetration Testing



* Represents CHGR Growth
Percentages in brackets represent the compounded Half-Yearly Growth Rate from 1 January 2014 through 30 June 2017.
Source: Social Media Listening Tool. Date Range: 1 January 2014 – 30 June 2017

The Future of Penetration Testing

FOREVER 21
BEST BUY
WHOLE FOODS MARKET
adidas
f
sears
GameStop POWER TO THE PLAYERS
DELTA
Panera BREAD
Arby's
UNDER ARMOUR
macy's
Lord & Taylor
Saks Fifth Avenue
kmart
SONIC
timehop
ticketfly

Closing Thoughts

How does Penetration Testing relate to our Information Security, Controls, & Ethics?

- Penetration Testing and information security is more important and relevant today than ever before, with increasing sophistication.
- We live in a world where ethical white hats and unethical black hats coexists.
- Social Engineering is also an important aspect of Penetration testing.
- Even with Penetration Testing, we will never be 100% safe.
- Companies need to take control and responsibility for the customer’s data to prevent exposure to personal and financial risk.

That is why penetration testing is so important.

Thank you!