Penetration Testing Methods and Strategies

IT Audit Strategies to
Maximize Value of Penetration Testing

August 2015
ISACA Geek Week

Robert Morella
MBA, CISA, CGEIT, CISSP
Rob.morella@gmail.com

About Me

Been there done that....

- ✓ IT Systems Infrastructure
- ✓ IT Architecture & Security
- ✓ IT Auditor, Financial Services
- ✓ Cybercrime Investigation
- ✓ ISACA QAT (CISA Exam)
- ✓ CISA Exam Boot Camp (GSU)
- ✓ 2014 Reported security breach on TV
- ✓ Proposed SB386 Privacy Law
- ✓ Web developer, adjunct professor, HOA President, aspiring author, etc, etc, etc.
- ✓ Geek

LOCKHEED MARTIN

Coca-Cola Enterprises

Westinghouse

Agenda

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

1 Definition

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

Actual CISA Question*

The PRIMARY purpose and benefit of performing a penetration test is?

- A) Methodical specialized way to test and validate security defenses.
- B) Methodical specialized way for security vendors to make money.
- C) Method to prove that your audit findings were right all along.
- D) Exercise designed to make IT security and IT Audit look bad.

*not a real CISA question

Answer: all of the above?

- None of the above?

Formal definition

- A penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization.
- Using many tools and techniques, the penetration tester (ethical hacker) attempts to exploit critical systems and gain access to sensitive data.

2 Types of Tests

- 1) Define Pen Testing
- 2) Types of Tests
- 3) Benefits of Pen Testing
- 4) Management Expectations
- 5) Value for IT Audit
- 6) Pen Testing vs Vulnerability Assessment
- 7) Pen Testing Guidance and Standards
- 8) Plan, Manage, and Survive Pen Test
- 9) How to Stay Out of Jail
- 10) What Makes Successful Pen Test

White, Black and Gray

- “White box” uses vulnerability assessment and other pre-disclosed information.
- “Black box” is performed with no knowledge of the target system and tester must perform their own reconnaissance.
- Gray means partial knowledge.

But Wait, There's More: Red Team

Red Team exercise:

- "Anything* goes”,
- Physical tests
- Social engineering
- Applications
- Data extraction and exfiltration
- More time, more cost
- Most common at service providers
- (* typically does not involve US Navy Seals with Live Ammo, but YMMV)

Red Team tests

- Origin is from military tactics
- Red Team = Attacker
- Blue Team = Defender

Main Six "Normal" Types of Pen Tests

1) Network Penetration Testing
2) Application Penetration Testing
3) Website Penetration Testing
4) Physical Penetration Testing
5) Cloud Penetration Testing
6) Social Engineering

1. Network Penetration Testing

- Internal or External
- Black box, White box, Gray box
- Perimeter Infrastructure
- Wireless, WEP/WPA cracking
- Cloud Penetration Testing
- Telephony systems / VoIP
- Vulnerability scanning*
- PCI DSS Scanning*

*technically not pen testing, but will get to that

2. Application Penetration Testing

- Web applications – asp.NET, PHP, Java, XML, APIs, web
- Custom apps – CRM systems, SAP, logistics, finance and sales order systems
- Mobile applications – Android, IOS
- Industrial control systems – SCADA
- Databases – SQL, MySQL, Oracle

3. Website Penetration Testing

Website Pen Testing (Web App Security Testing)

- SQL injection and Cross-site scripting vulns
- Server configuration problems
- Hacking website or web server to access credit card details
- Use of hacked web server to distribute malware
- Use of hacked web server to gain deeper access to network (pivoting).

Really a subset of application penetration testing.

4. Physical Penetration Testing

Lock-picking, impersonation, bypassing other physical security measures:

- Sales premises and head offices
- Warehouses and storage facilities
- Data centers
- Bug sweeping
- CCTV systems
- Door entry systems
- Incident response

*

* (Typically doesn't involve Tom Cruise hanging from a wire, but YMMV)

5. Cloud Penetration Testing

- UK G-Cloud service
- The Federal Risk and Authorization Program (FedRAMP)
- AWS, Azure Requirements

6. Social Engineering

Assess resilience to attacks to ‘human network’

Methods include phishing, media drops, tailgating, pretexting

- Phishing attacks
- Password resets
- Imposters – fellow employee, or external authority
- Third party employees
- Tailgating
- Social networking scams – Facebook, LinkedIn

As well as discovering and fixing potential vulnerabilities, social engineering penetration testing will help to raise **security awareness** within organization.

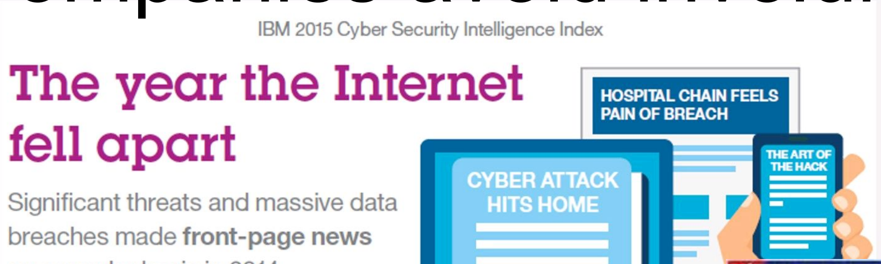
3 Benefits

- 1) Define Pen Testing
- 2) Types of Tests
- 3) Benefits of Pen Testing
- 4) Management Expectations
- 5) Value for IT Audit
- 6) Pen Testing vs Vulnerability Assessment
- 7) Pen Testing Guidance and Standards
- 8) Plan, Manage, and Survive Pen Test
- 9) How to Stay Out of Jail
- 10) What Makes Successful Pen Test

[Insert scary hacking statistic here]

Cybersecurity is Front Page News

- Penetration testing more popular than ever
- Companies avoid involuntary publicity



IBM 2015 Cyber Security Intelligence Index

The year the Internet fell apart

Significant threats and massive data breaches made **front-page news** on a regular basis in 2014

HOSPITAL CHAIN FEELS PAIN OF BREACH
CYBER ATTACK HITS HOME
THE ART OF THE HACK

FREE METRO 09.03.2011 metro.co.uk

It's all got Messi for Arsenal P56

Shot going out for a pizza

Hacking alert on Google phones

UK's BEST DEAL PHONE & BROADBAND £3.49 NOW HALF PRICE 0800 049 6288 talktalk.co.uk TalkTalk

Required for PCI, Cloud Providers, Federal Entities

- Not so much "if"
- When
- Who
- How much will it cost?

4 Expectations

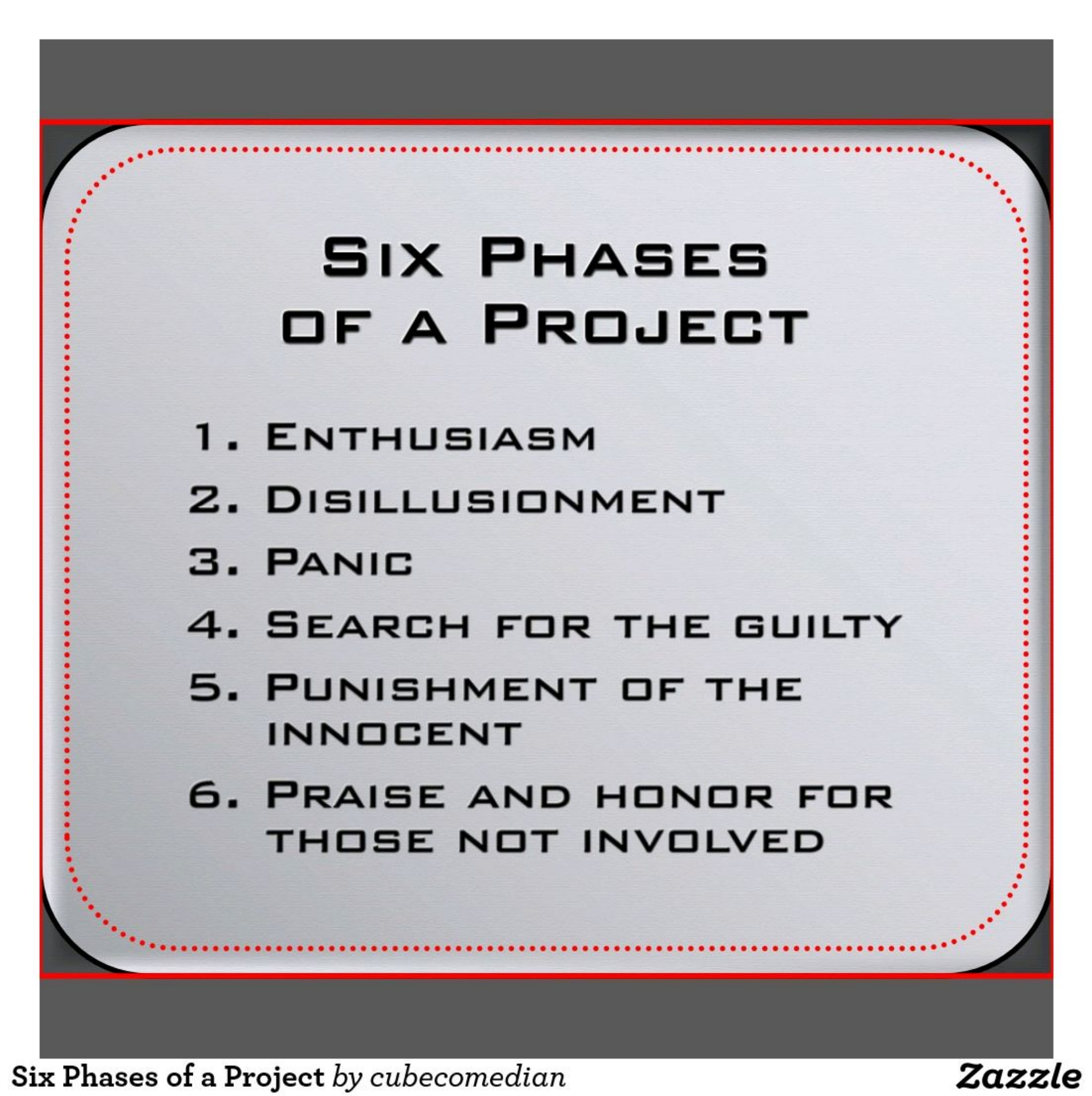
1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

Penetration Testing Project

Just another IT Project?

Penetration Testing as a Simple IT Project

- It Seemed Like a Great Idea at the Time



Six Phases of a Project

1. Enthusiasm
2. Disillusionment
3. Panic
4. Search for the guilty
5. Punishment of the innocent
6. Praise and honor for those not involved

Six Phases of a Project *by cubecomedian* **Zazzle**

Expectations

- Penetration Test:

Highly Anticipated

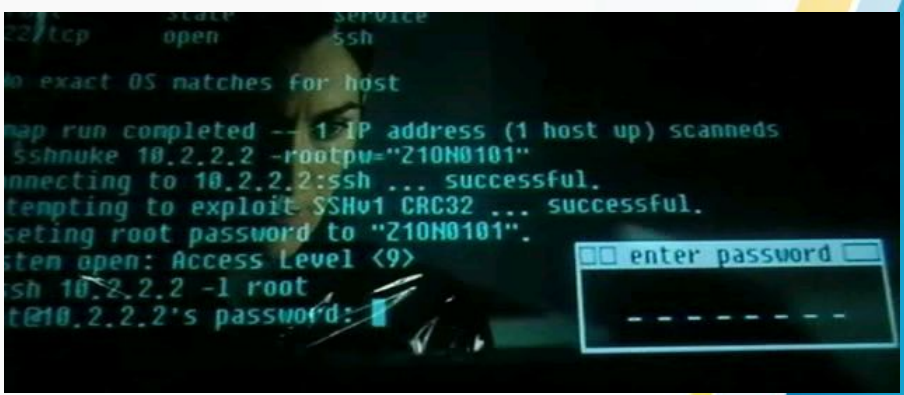
Typical IT Audit

(Not So Much)

Woo, it's a hacker!

Hollywood Films

- IT Auditors = 0
- Hackers = Many



```
       state          service
22/tcp      open           ssh

o exact OS matches for host

map run completed -- 1 IP address (1 host up) scanneds
 sshnuke 10.2.2.2 -rootpw="Z10N0101"
nnecting to 10.2.2.2:ssh ... successful.
tempting to exploit SSHv1 CRC32 ... successful.
seting root password to "Z10N0101".
sten open: Access Level <9>
sh 10.2.2.2 -l root
t@10.2.2.2's password:
```

Wah, it's like SOX

- Pen Testing = Compliance Testing
- Fast, Cheap, Automated
- Little value-add
- Scope and funding may be constrained.

Do a Pen Test and Our Job is Done Here!

Passing an easy test adds little value.

However a well managed test will:

- Yield valuable lessons
- Build awareness
- Add value

Expectations to Consider

Is main focus meeting compliance requirements? Or concern that intellectual property is at risk from a motivated and skilled attacker?

- IT Management
- IT Security & Technical
- IT Audit
- Business Units
- Senior Management
- Your own

Organization Expectation: Value

Teachable Moment* vs *Valuable Lesson

Successful Test Yields

- Corrective and improvement solutions.
- Both technical and process fixes.

Improve IT Skills and Knowledge

- In depth analysis of pen techniques.
- Constructive debrief with IT experts.

5 Value for IT Audit

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

Value of Penetration Testing for IT Audit?

CAUTION
THIS SIGN HAS
SHARP EDGES
DO NOT TOUCH THE EDGES OF THIS SIGN
ALSO, THE BRIDGE IS OUT AHEAD

Typical IT Audit Role

☑ Coordinate and Manage Pen Test

☑ Observe Pen Test

☑ Audit Pen Test

☒ Perform Pen Test?

Who here wants to be a pen tester?

Who here wants to be an IT Auditor?

What’s the difference?

6 Pen Testing vs Vulnerability Assessment

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

Penetration Test or Vulnerability Assessment?

- Terms often used synonymously (=confusion)
- Pen tests are Vulnerability Assessments
- Vulnerability Assessments are not Pen Tests
- Confused yet?

Definition of Vulnerability Assessment

A vulnerability assessment scans for and points out vulnerabilities but does not exploit them. Vulnerability assessments can be completely automated (e.g. Nessus, Retina).

- Can be easy to do
- Find more issues, typically
- Normally uses 'white box' mode
- Does not exploit the vulnerability.
- This is where you add value.

Penetration Testing General Steps

1. Determination of scope
2. Targeted info gather (reconnaissance)
3. Exploit attempts: access and escalation
4. Sensitive data collection testing

Vulnerability Assessment General Steps

1. Catalog assets & resources in a system.
2. Assign quantifiable value and importance to resources.
3. Identify security vulnerabilities or potential threats to each resource.
4. Mitigate or eliminate the most serious vulnerabilities for the most valuable resources.

(hmmm: sounds like an audit)

Vulnerability Assessment Adds Value

→

Penetration Testing Methods and Tools

Value for IT Audit is that it Improves:

- Vulnerability Assessment Process
- Management of Penetration Test
- Audit of Penetration Test

One Caution: Independence

Crossing the line from Vulnerability Assessment to Pen Testing

- Invalidate results
- End badly

Vulnerability Assessment Better Than Pen Test?

Maybe, IF:

- IT is confident in their security posture
- Has mature vulnerability management process in place

Advantages and Limits of Pen Testing

Pros

- Raise security awareness
- Independently show how easily an attack can happen
- Shows how attacker can escalate privileges
- Good way to test incident response
- Secure funding for technology, training, third-party help.

However

- Even successful test does not find all vulnerabilities
- False sense of security.
- May turn into "blame game" vs. Teachable Moment

Best Answer: Both

Vulnerability assessment:

- Improve security posture, security program,
- Start with Vuln Assessment then Pen Test
- First white box, then black box
- Ideally with different third party

7 Penetration Testing Guidance

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

Standards, Lots of Standards, Guidelines

Penetration Testing Execution Standard

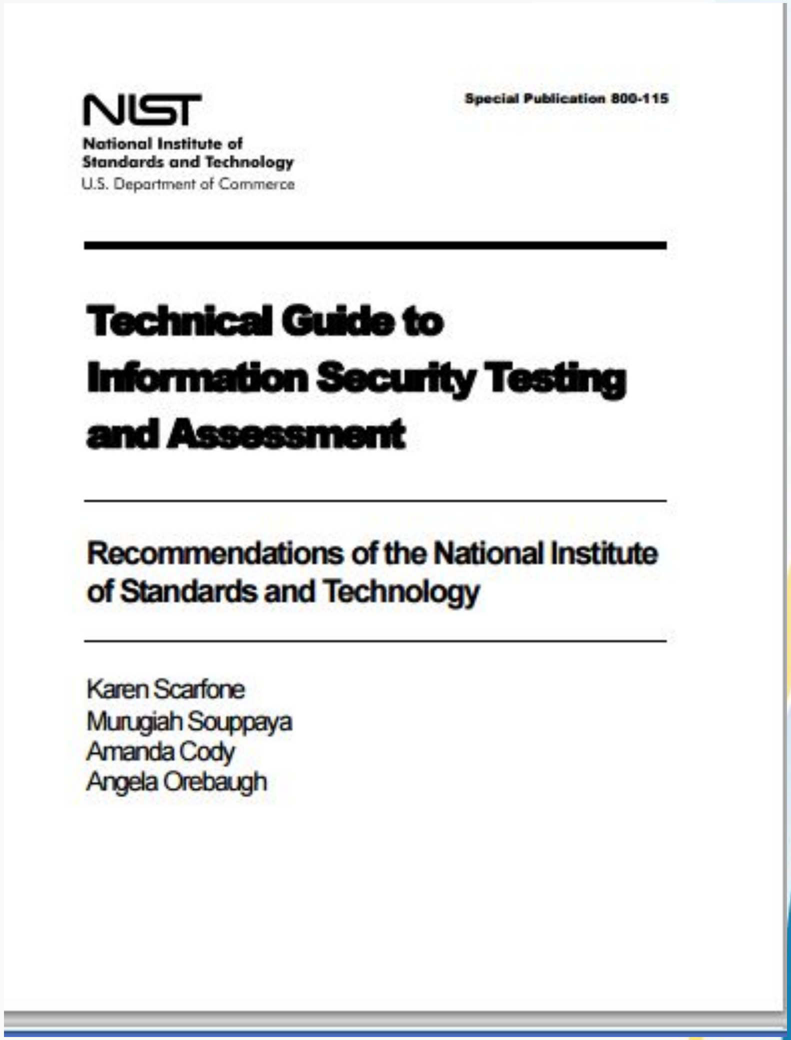
PTES (old but good)

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

http://www.pentest-standard.org

NIST SP800-115

- 2008
- Useful, though outdated



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-115

Technical Guide to Information Security Testing and Assessment

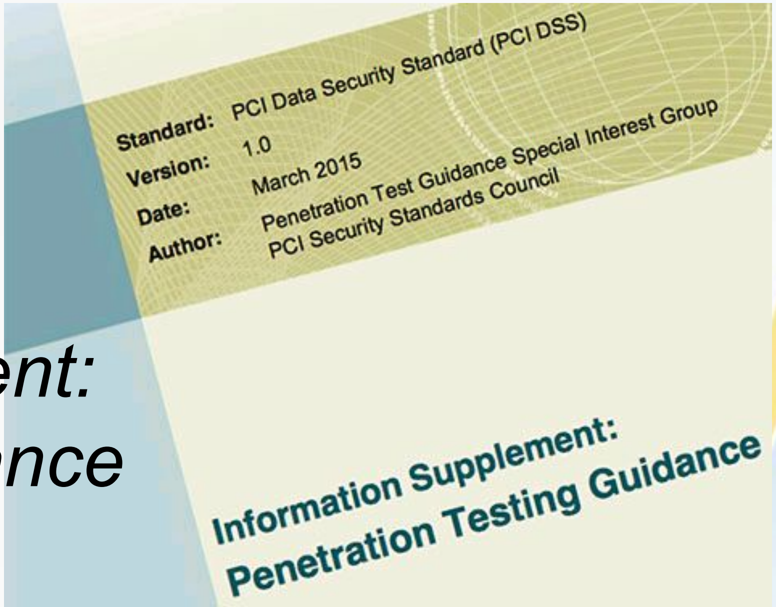
Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Murugiah Souppaya
Amanda Cody
Angela Orebaugh

New PCI DSS Guidance

- Excellent! Must Read!
- Even if you have no PCI requirements

- *PCI Information Supplement: Penetration Testing Guidance March 2015*



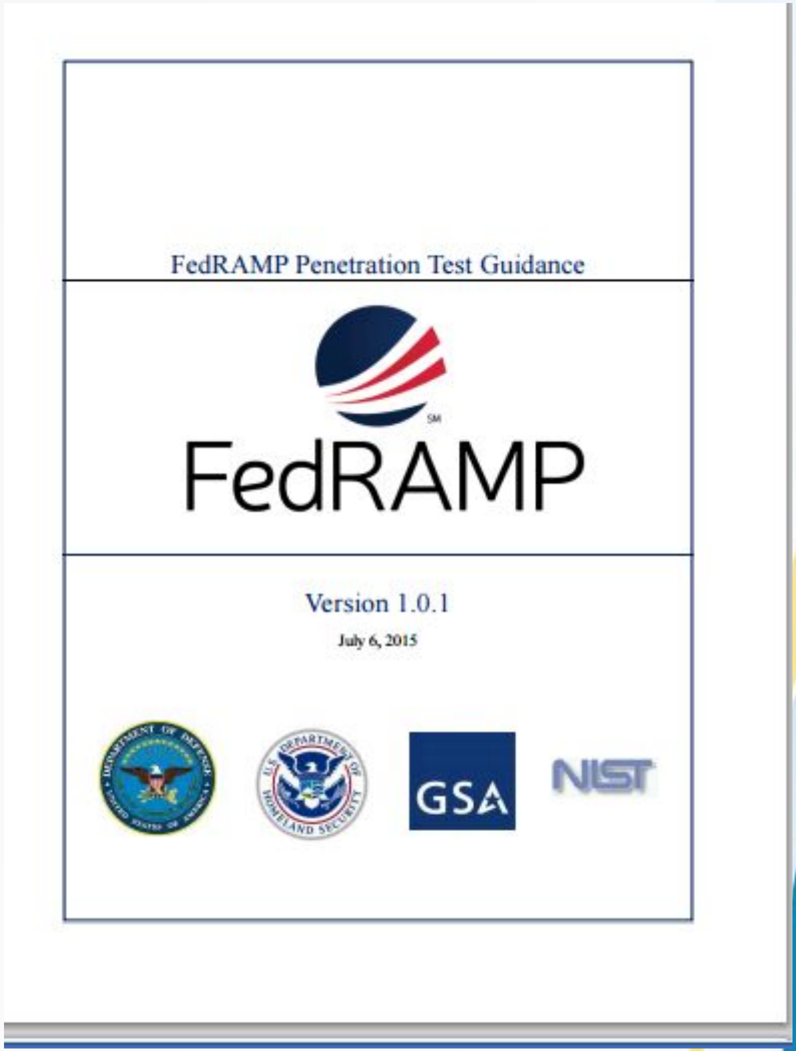
Standard: PCI Data Security Standard (PCI DSS)
Version: 1.0
Date: March 2015
Author: Penetration Test Guidance Special Interest Group
PCI Security Standards Council

Information Supplement:
Penetration Testing Guidance

FedRAMP

- Also Excellent!
- Even if you have no FedRAMP requirements

- FedRAMP Penetration Test Guidance 1.0.1



FedRAMP Penetration Test Guidance

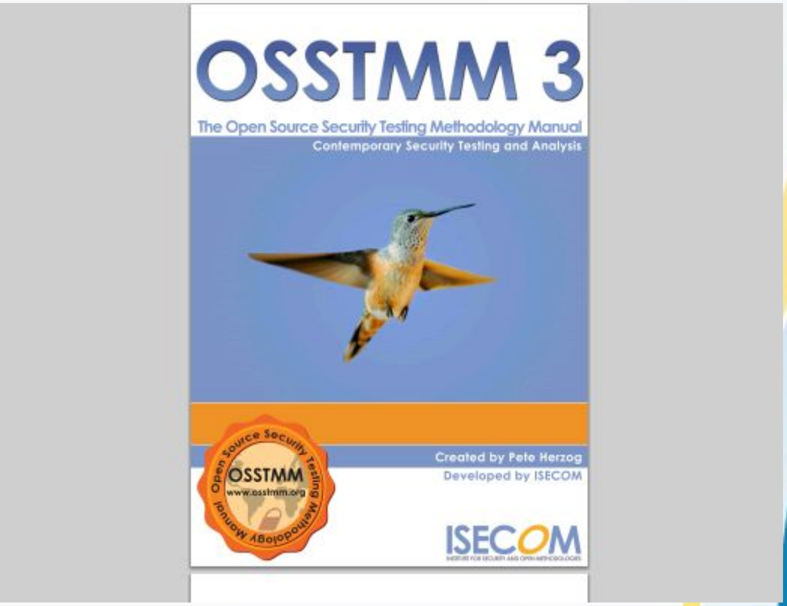
FedRAMP

Version 1.0.1

July 6, 2015

OSSTMM v3

- Goes way beyond Penetration Testing
- Valuable Guide
- Lots of Great Insights


OSSTMM 3
The Open Source Security Testing Methodology Manual
Contemporary Security Testing and Analysis
Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org
Created by Pete Herzog
Developed by ISECOM
ISECOM

OWASP Testing Guide

- Web Application Security
- Excellent resource
- Detailed, practical methods

OWASP
Open Web Application Security Project
Testing Guide
4.0
)release(
Project Leaders: Matteo Meucci and Andrew Muller
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

Pen Test Partner Use of Standards

- Awareness-of vs. Working Knowledge
- Some vendors more PTES, vs. FedRAMP, vs. OWASP, vs. others.
- Slightly different focus between/among standards and requirements.

Basic anatomy of PTES
Seven Key phases of Penetration Test

1 Pre-engagement Interactions

Pre-engagement Interactions:

- Often overlooked
- Logistics of testing can be difficult
- Tester not understanding your goals
- Not considering risks, culture, or best strategy (e.g. proposes more canned approach)
- True partnership vs. Customer
- **Key factor is need for more project planning expertise and less selling expertise.**

2 Intelligence Gathering

- Are you providing information, or is vendor going to research and provide you with their what they have found?
- Sometimes useful to have them find as much as they can on their own then provide info to fill in gaps.
- Amount of info given depends on nature of test (e.g. white box, black box, gray box).
- Scope depends on test type
- **Great way to assess security awareness.**

3 Threat Modeling

- Identify targets and map attack vectors.
- Security testers should be able to take info from intelligence gathering to inform you what type of attacks your organization is susceptible.
- Not a formal presentation, synopsis of "weak points" they see as vulnerable.
- **They may see something you do not.**

4 Vulnerability Analysis

- Finding what what vulnerabilities exist.
- More importantly, exploitable ones.
- These drive remediation efforts.
- Normally shared after the fact

5 Exploitation

- Shows how far an attacker can get (within scope of test).
- Security tester should be able to explain exploitation technique **and**:
- Why it worked.
- What exploit did.

6 Post Exploitation

- Many testers fail at this point
- Elevating privileges is not "**game over**".
- Goal is to understand methods used to gain access to valuable information.
- (eg: XSS on internal web site = so what?)

7 Reporting

The **most important part of the test**

- Value comes from findings and detailed explanation of what was found
- Well crafted recommendations that come from years of experience.
- Ask vendor about their reporting structure and how it’s written.
- Output directly from a scan tool = red flag.

8 How to Plan Manage and Survive Test

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

Goals

Have Goals and Targets:

- Get to PII
- Establish specific attack vectors
- Compromise specific systems or apps
- Bypass security / stealth attacks
- Identify most sensitive data
- Consider what data/access has material impact
- Include any hot buttons you want addressed.

Have Realistic Objectives

- Not all goals may be met during the test.
- Build flexibility into the plan

Consider Top Management Concerns

Who concerns you?

- Random individuals on the Internet
- State-sponsored attackers, criminals, hacktivists
- Individual or malware on corporate network?
- Your employees
- Your customers (or attackers using that attack vector).
- This drives the type of testing to be performed

Caution: Beware of Sabotage

If primary motivation is compliance, be on the lookout for those seeking better test result:

- Limiting scope of systems assessed.
- Control types of tools used.
- Limit duration of the test.
- Major changes just prior to testing.

Select Pen Test Partner

Qualifications of the organization and certifications of the **testers** (not just engagement managers)

- Age of those certs (six months vs six years)
- All white-hats, former black-hats, ex-military
- Size/depth of team (small team multiple projects).
- % Manual vs automated testing? (Ask for samples)
- Biased? Do they sell other products and services?

Ask them to explain **process** for:

- Building test plans
- Defining rules of engagement
- Post-test wrapup
- Crafting final report.(Ask for samples)

Define Location

- Where testers will sit? (Cost vs Secuity Risk)
- Some can be done remotely, some not
- Physical/social engineering engagements and wireless assessments
- Internal pen tests via VPN connection?
- Logical location in network (e.g. VLANs)
- Same state/country?
- **Data privacy laws, time zones, language, culture**

Define Scope

- Team should help to set scope
- IP addresses, URLs and IP addresses, and apps.
- Who is in-scope for social engineering.
- Physical access from roof to dumpsters defined
- Scope prioritized for high value assets
- Balance scope vs. budget
- Too narrow: **realism** suffers
- Too broad: false positives, **costly**

Adopt Rules of Behavior / Statement of Work

Rules of Behavior:

- Legally binding test agreement
- Limitations, constraints, liabilities, and indemnification.

At Minimum Address:

- Type of tests to be performed,
- Scope of the test and the risks involved
- Defined targets,
- Time frame
- Points of contact
- Authorization to proceed

Define Approach

Covert/Overt: Blackbox/Whitebox.

Whitebox (full knowledge or partial "gray”)

- Less time spent on discovery, more breaking into things
- Better assess insider threat (insiders did discovery)

Blackbox (zero knowledge)

- Most realistic external attack result.
- Better gauge of controls related to public info disclosure.
- Better test of social engineering awareness.
- Teach risks of **social engineering and public data**

Consider Timing

Scheduling

- Non-production times of day
- Red flag would be if test team did not ask

Frequency

- Annual assessment (VA or PT: YMMV)
- Before upgrades/patching?
- After upgrades/patching?
- Balance realism vs. desired end state.

Review Report & Recommendations

When choosing partner:

- Discuss how remediation recommendations will be made in report.
- Ask for a sanitized example of a report
- Are recommendations clear, actionable, realistic?
- Not ‘canned’ and generic

When reviewing your report:

- Does it show evidence of compromise and attack vectors?
- Screen shots, planted files, modified web pages are best.
- Eliminate false positives (confirm with IT before report)

How to Do it Wrong

- Vague scope
- Heavy scanning with automated tools
- Exploit with Metasploit
- Poke around with other tools
- Produce a generic report

Factors Leading to Less Effective Pen Tests

- Apathy in your organization
- “Checkbox” mentality
- Unskilled scanning/testing teams
- Assessment reports fail to assess risk

9 How to Stay Out of Jail

1) Define Pen Testing

2) Types of Tests

3) Benefits of Pen Testing

4) Management Expectations

5) Value for IT Audit

6) Pen Testing vs Vulnerability Assessment

7) Pen Testing Guidance and Standards

8) Plan, Manage, and Survive Pen Test

9) How to Stay Out of Jail

- 10) What Makes Successful Pen Test

Read this Article:
"Legal Issues in Penetration Testing"

http://www.securitycurrent.com/en/writers/mark-rasch/legal-issues-in-penetration-testing

by

Mark Rasch

November 26, 2013

SecurityCurrent.com

Legal Authority

- Computer crime laws and what constitutes “authorization” can quickly get muddy.
- Security expert performed pen test, results were bad, authorization unclear, GBI called to arrest and investigate.
- Houston security expert took news reporter on war-driving excursion, arrested, thousands in legal costs, acquitted.

Get Out of Jail Free Card

Great **in theory**, however:

- Pen tester can attack wrong target
- Service provider (e.g. Cloud Provider) may not approve.
- Reverse-engineering apps may violate license agreements.

Damage Control

- Reducing all production systems to smoking heap could happen.
- All damages even incidental/coincidental are customer's problem.
- Agreement needs to spell that out clearly.

Indemnification

- (def: compensation for damages)
- Contract needs to address liability for damage to third parties.
- Liability can be huge risk.

No Hack-backs

- Hacking is illegal.
- If pen tester attacks and organization launches counter-attack, that's not legal.
- If pen tester is attacking shared infrastructure, without permission they have no legal right to do that.
- All needs to be spelled out, scope carefully defined.

Scope of Work

- Pen test agreement needs to state clearly what is in-scope, or implied warranty may lead to bigger issues.
- Each term of scope must be defined, e.g. what does 'off peak' mean, and what internal vs internal means.

Professionalism

- Standard of care
- What is warranty
- Will find 'substantially all' issues?

Licensing and Certification

- Some jurisdictions require Pen Testers to be licensed private investigators.
- If pen test uncovers illegal activities, inadequate licensing or certifications will make evidence inadmissible in court.

Privacy Issues

- Pen tester may access sensitive personal information, credit card information, personally identifiable information (PII) or Private Health Information (PHI).
- Some jurisdictions could consider this a reportable breach, even though the testing was intentional.
- Pen tester overseas who accidentally moves PII may be breaking laws.

Venue and Jurisdiction

- If California pen-tester does work remotely for Ohio company, which laws apply?
- But if company damages systems of some other Ohio company, **whose laws apply?**

Data Ownership

- Pen tester owns methods/template
- Customer owns results
- If pen tester writes custom code while working for customer, who owns that?

Duty To Warn

- If pen tester discovers wider issue that could impact others, must they report it?
- Even if customer owns results, does pen tester own **knowledge of** dangerous issue?

10 What Makes Successful Pen Test?

1) Define Pen Testing
2) Types of Tests
3) Benefits of Pen Testing
4) Management Expectations
5) Value for IT Audit
6) Pen Testing vs Vulnerability Assessment
7) Pen Testing Guidance and Standards
8) Plan, Manage, and Survive Pen Test
9) How to Stay Out of Jail
10) What Makes Successful Pen Test

What Makes Successful Pen Test?

Shackleford Penetration Testing Maturity and Scoring Model

(see references slide)

Realism + Methodology + Reporting

Scoring system to measure/rate:

- How valid, realistic, up-to-date are attacker methods and approach
- How complete, logically consistent are methods
- How actionable, specific, and valuable is report.

see references slide

Takeaways

- ✓ 1) Define Pen Testing
- ✓ 2) Types of Tests
- ✓ 3) Benefits of Pen Testing
- ✓ 4) Management Expectations
- ✓ 5) Value for IT Audit
- ✓ 6) Pen Testing vs Vulnerability Assessment
- ✓ 7) Pen Testing Guidance and Standards
- ✓ 8) Plan, Manage, and Survive Pen Test
- ✓ 9) How to stay out of jail.
- ✓ 10) What Makes Successful Pen Test

Questions?

Thanks!

References

References

1) Dave Shackleford "A Penetration Testing Maturity and Scoring Model" RSA Security Conference 2014
2) Mark Rasch "Legal Issues in Penetration Testing" November 26, 2013
3) David A. Shinberg "A Management Guide to Penetration Testing" SANS Hacker Techniques, Exploits, and Incident Handling, 2003

Links

https://www.fedramp.gov/files/2015/03/Guide-to-Understanding-FedRAMP-v2.0-4.docx

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

http://dx.doi.org/10.6028/NIST.SP.80053Ar4

http://csrc.nist.gov/publications/nistpubs/800145/SP800-145.pdf

https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Mobile_Security_Testing

http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

https://azure.microsoft.com/blog/2014/11/11/red-teaming-using-cutting-edge-threat-simulation-to-harden-the-microsoft-enterprise-cloud/