Implement Effective Penetration Testing

Ed Verdurmen
Visa - Moderator

Navid Jam
FireEye

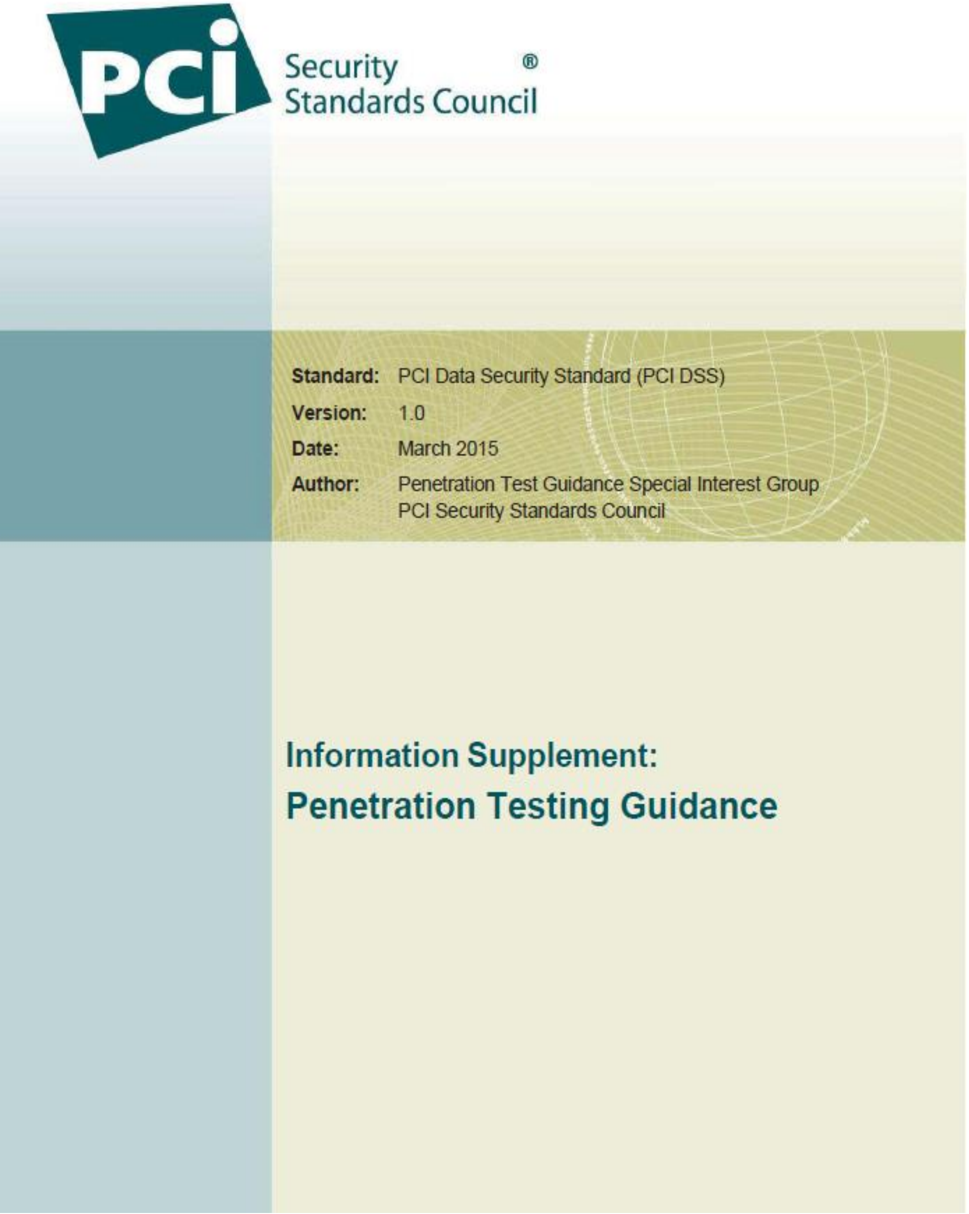
Rob Chahin & Kevin Dunn
NCC Group

Ryan Wakeham & Scott Sutherland
netSPI

Notice of Disclaimer

The information, recommendations or “best practices” contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance.

Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.



PCi Security Standards Council®

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

What's Changed in 2015?

The PCI SSC Issued Pentest Guidance

Q: How has the PCI guidance improved assessments?

A: Alternate guidance is exhaustive (read: expensive), the previous PCI requirement set a low bar

What’s Changed in the Past Five Years?

Penetration testing has emerged as a mature market niche in the U.S, Western Europe, and parts of Asia

Q: How do you find a top tier pentester?

A: Good pentesters remain hard to identify. Examine the company’s hiring process. It must include testing, and the company must be able to describe their approach to testing tools.

OFFENSIVE®
security

Q: How do I prepare for a pentest?

A: People don’t do this everyday, so:

- **Start with an overview of the company,**
- **Ensure your QSA helps prepare your pentester,**
- **Set high-level goals, and**
- **Collaborate, Collaborate, Collaborate**

Have a Threat Model Ready

It needn’t be detailed nor technical, cybercrime and POS malware may be sufficient

Q: How do I prioritize my first technical pentest or first investment in a more expensive pentesting firm?

A: Merchant breaches tend to exploit the POS and remote access, Fortune 500 breaches tend to exploit website vulnerabilities, and most breaches involve compromised privileged accounts. Start with these areas, share diagrams and access information, and suggest systems to use and examine

Single linux\ AIX Console

RDP

LogMeIn Free

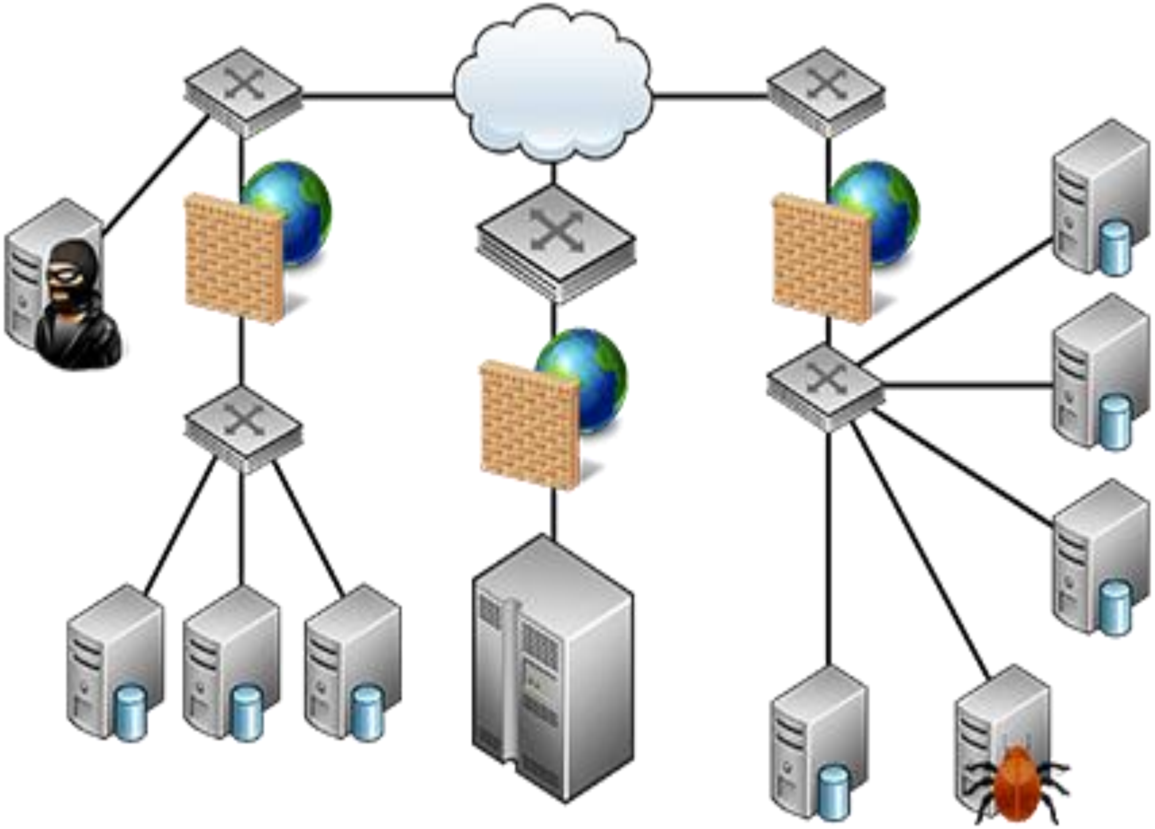
Single Active Directory Domain

BEWARE

Large Companies Are Strict and Complex

Q: How do I scope a test that provides system access to the tester without creating undue risk?

A: REPEAT POINT: Use your QSA to help negotiate and provide appropriate detail to your pentester



Q: This sounds basic, do companies really struggle with performing detailed PCI penetration tests?

A: Yes.

Although Fortune 500 companies tend to have more experience, many firms set low standards for pentests

Q: Our company is deploying encryption, tokenization, and upgrading hardware between 2015 and 2017. How can a pentester help?

A: A good pentester can help identify implementation errors. Implementation errors can render most technologies ineffective.

Q & A

Thank you