Compliance Based Penetration Testing: You're Doing it Wrong

James Edge
Attack & Penetration Testing
Practice Manager

datadiscovery

Agenda

- About Mainstream Security
- About Me
- What is a Penetration Test / What it is Not
- What is Compliance / What it is Not
- What is Compliance “Penetration Testing”
- Why Compliance Penetration Testing is Wrong
- Compliance Penetration Tests Done Wrong: Examples
- What you can do to fix it
- Questions

About Mainstream

www.mainstreamsecurity.com

About Me

James Edge

Attack & Penetration Testing Practice Manager

- CISSP
- CISM
- CISA
- CPTE
- MCSE

James Edge

Attack & Penetration Testing Practice Manager

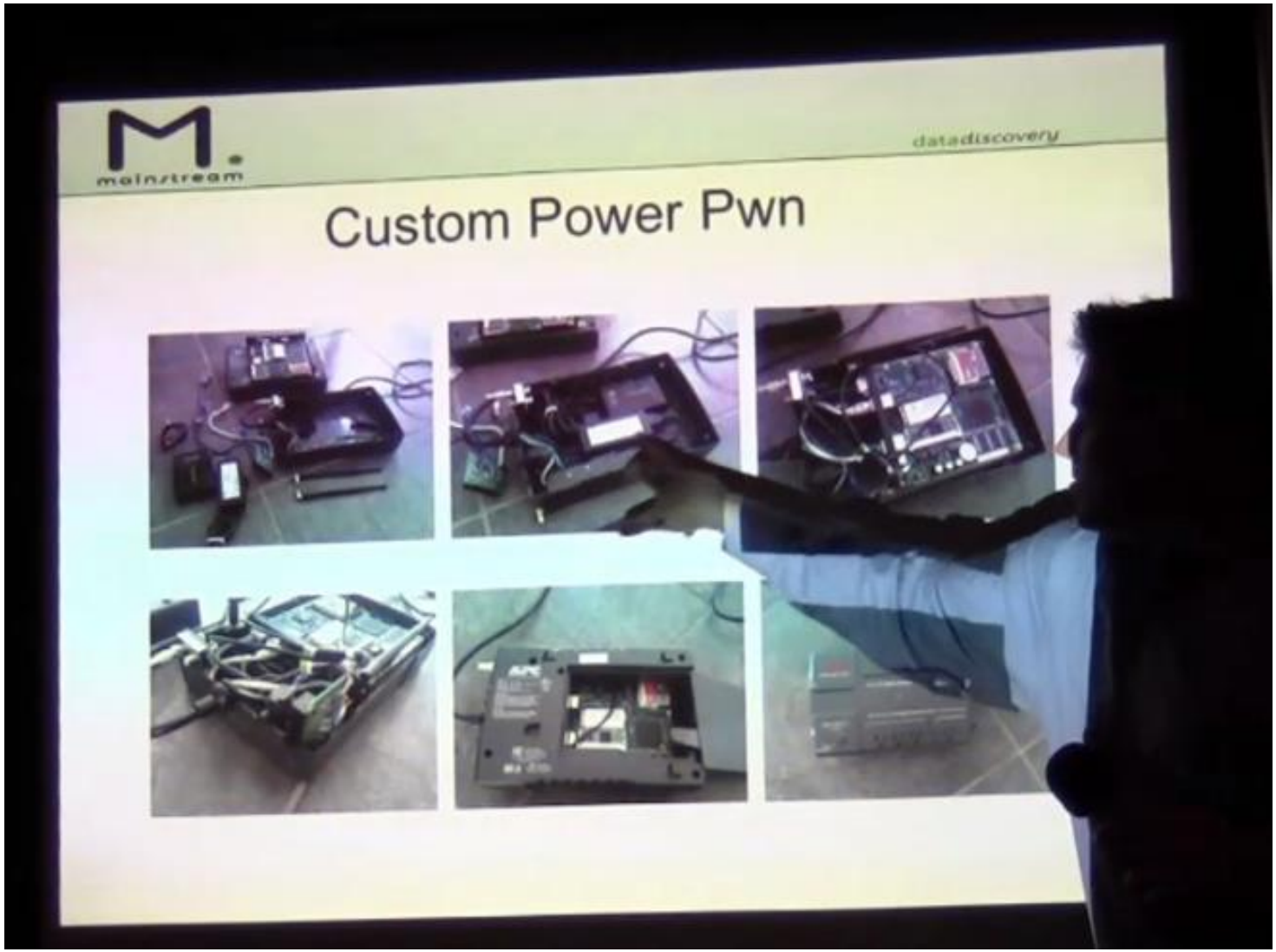
- CISSP
- CISM
- CISA
- CPTE
- MCSE

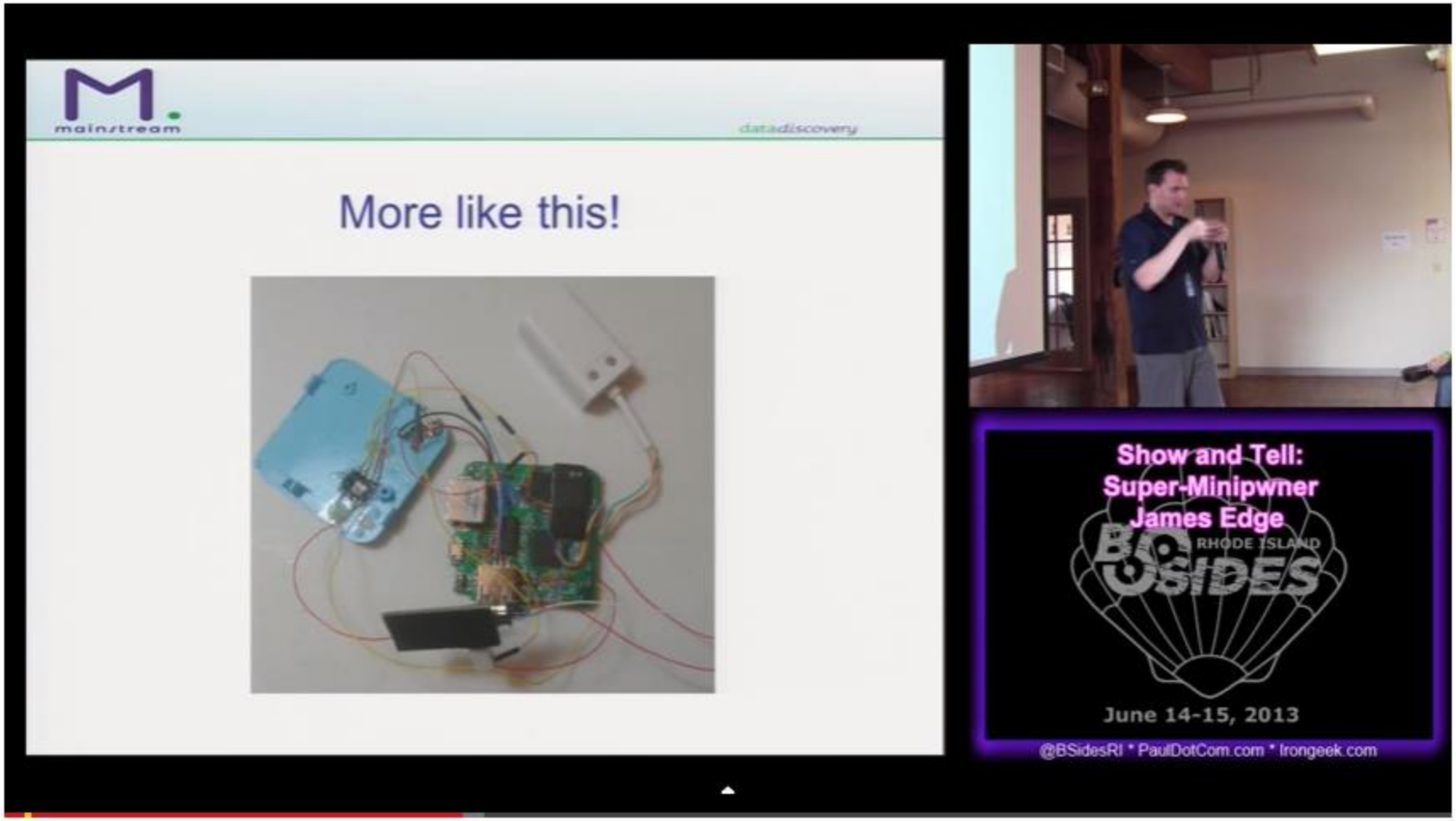
Great Test Taker

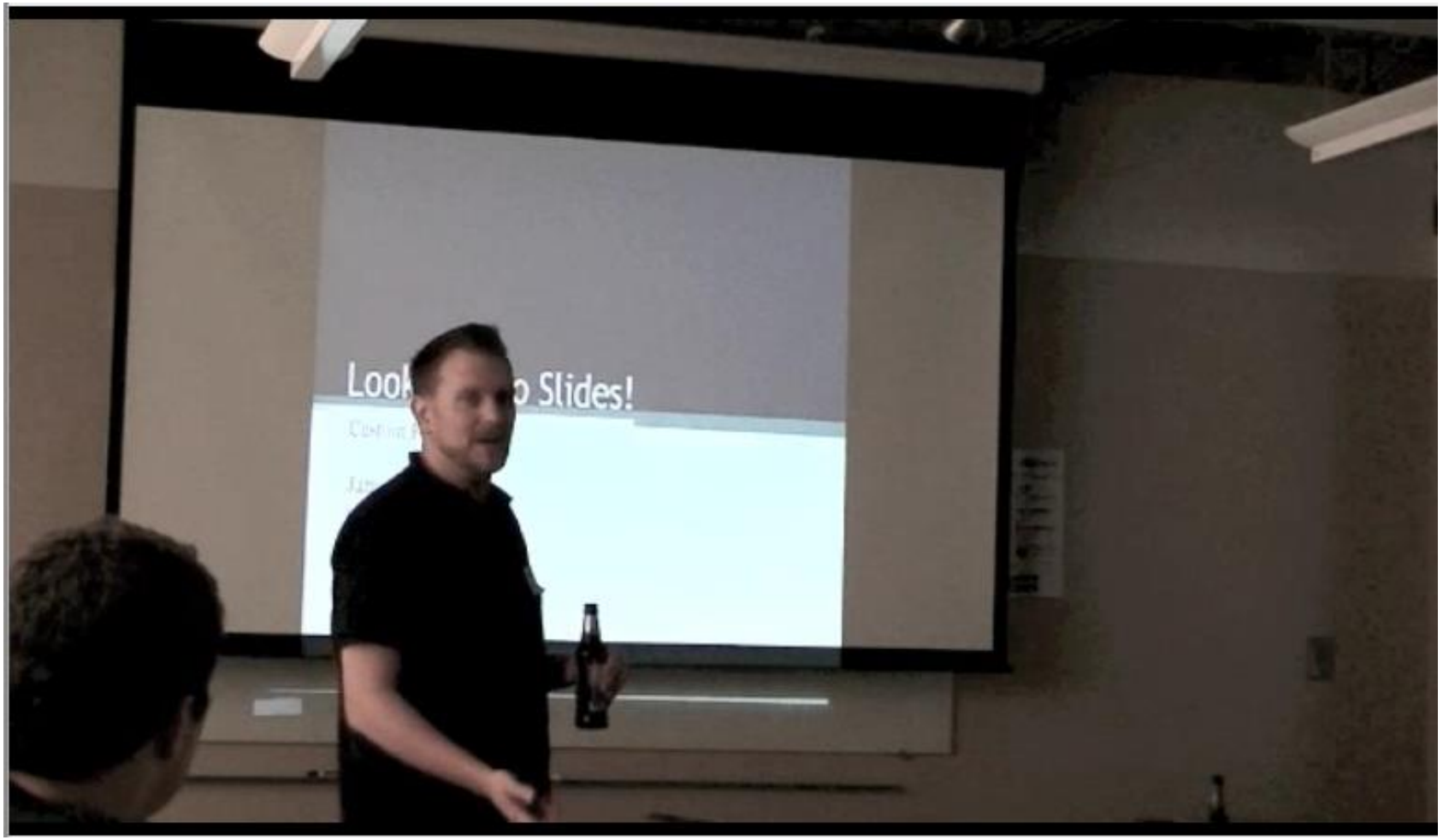
James Edge

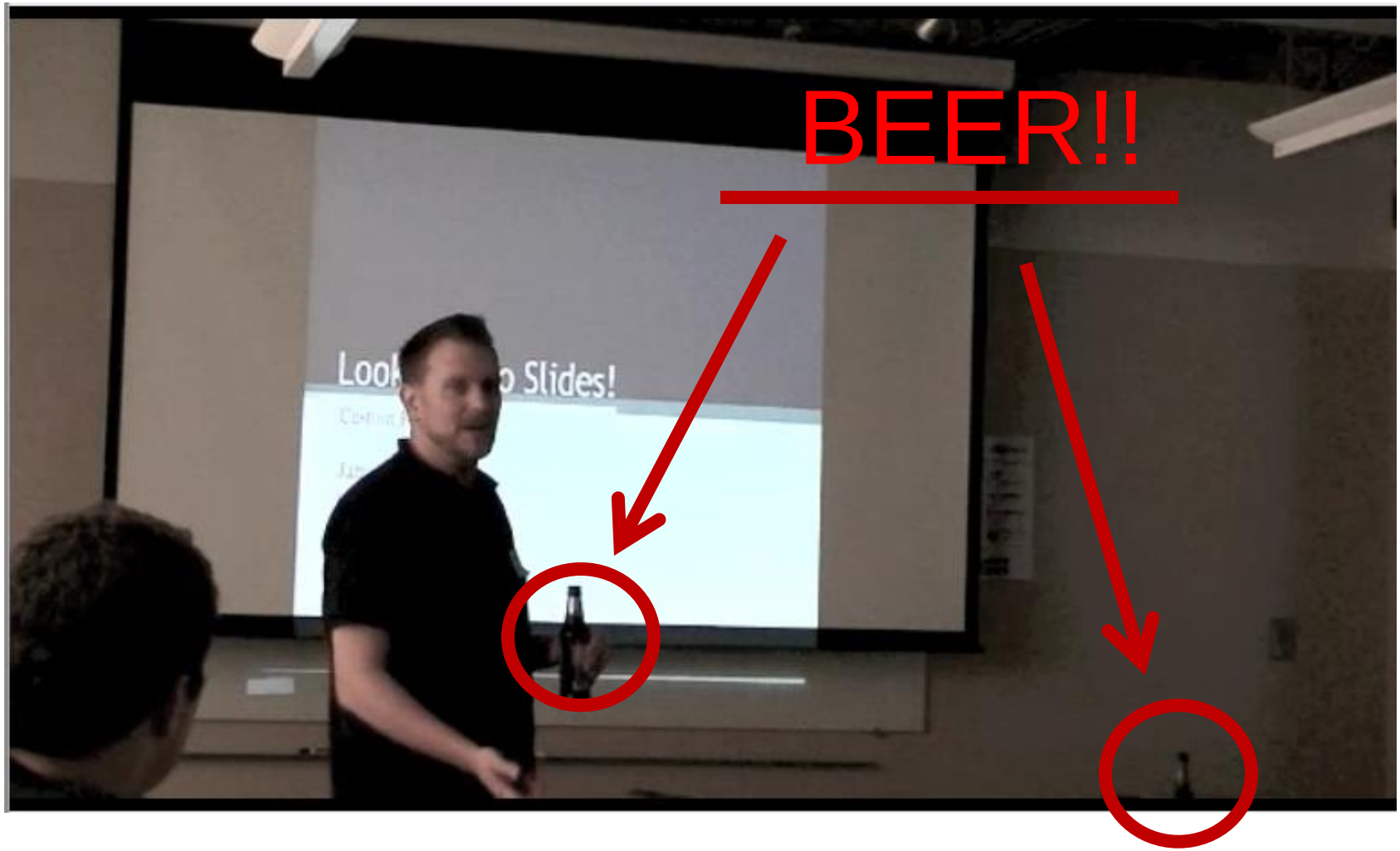
Information Systems Auditor


BSIDES


mainstream
datadiscovery
Custom Power Pwn


mainstream
datadiscovery
More like this!
Show and Tell:
Super-Minipwner
James Edge
RHODE ISLAND
BSIDES
June 14-15, 2013
@BSidesRI * PaulDotCom.com * Irongeek.com


Look
o Slides!


BEER!!
Slides!

What is a Penetration Test / What it is Not

Penetration Testing: What it is

"Successful penetration testers don't just throw a bunch of hacks against an organization and regurgitate the output of their tools. Instead, they need to understand how these tools work in-depth, and conduct their test in a careful, professional manner." - Ed Skoudis (SANS Instructor)

Penetration Testing – NIST Definition

A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Penetration Testing: What it is

- From position of a potential attacker
- active exploitation of ANY security vulnerabilities
  - Web Application
  - Social Engineering
  - Physical Security
  - Phone Systems

Penetration Testing: What it is not

- Nessus, Nexpose, Qualys (insert other vulnerability scanner) Report
- Vulnerability Assessment

Penetration Testing: What we have to live with

- Time constraints
- Budgets
- Morals

What is Compliance / What it is Not

Compliance means conforming with stated requirements.

Management processes identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies) and assess the state of compliance.

Compliance: what it is

- Definition: adhering to principles required by an entity
  - Government
  - Industry Standard
  - Internal Requirements
- largely industry specific (education, finance, healthcare)
- privacy and confidentiality focused

Compliance: What it is not

- A check box!!!!!

Compliance: What we have to live with

- Time constraints
- Budgets
- Morals (see Enron)

What is Compliance "Penetration Testing"

HIPAA

- HIPAA Security Rule (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/)
- NIST 800-66 revision 1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

HIPAA

- Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
- 142.308a.8.iv - Security Testing – **Deleted**

PCI-DSS

Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 2.0 October 2010

PCI-DSS

Page 6

PCI DSS Applicability Information

PCI DSS applies wherever account data is stored, processed or transmitted. Account Data consists of Cardholder Data plus Sensitive Authentication Data, as follows:

Cardholder Data includes:	Sensitive Authentication Data includes:
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full magnetic stripe data or equivalent on a chip • CAV2/CVC2/CVV2/CID • PINs/PIN block

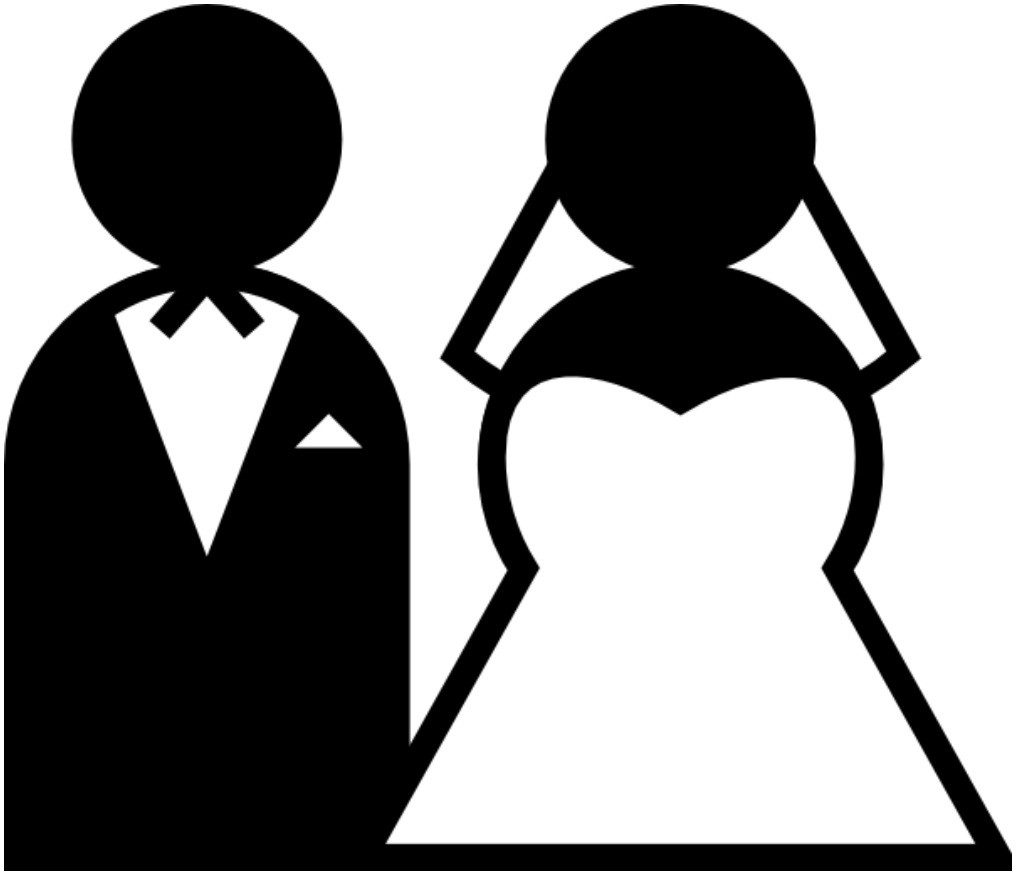
PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

Penetration Testing Requirement

Penetration testing should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification.

Why Compliance Penetration Testing is Wrong

Compliance and Penetration Testing



"Compliance is the biggest driver for the security industry right now"- Ron Gula

CEO & CTO, Tenable Network Security

Future Trends in IT security – Bsides Rhode Island 2013

"It is not stopping hackers" – Ron Gula

the biggest driver for the security

Gula

CEO & CTO, Tenable N

Future Trends in IT security – Bsid

2013


Security Fail
failblog.org


FAIL
failblog.org

Compliance Penetration Tests Done Wrong: Examples

What you can do to fix it?

Try to Expand the Scope

The scope of penetration testing is the cardholder data environment and **all systems and networks connected to it**. If network segmentation is in place such that the cardholder data environment is isolated from other systems, and such segmentation has been verified as part of the PCI DSS assessment, the scope of the penetration test **can be limited** to the cardholder data environment.

Try to Expand the Scope

Penetration testing should be performed **at least annually** and anytime there is a significant infrastructure or application upgrade or modification.

Try to Expand the Scope

Penetration testing should be performed at least annually and **anytime there is a significant infrastructure or application upgrade or modification.**

Try to Expand the Scope

Penetration testing should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification.

- addition of a web server
- addition of a sub-network
- new system component installations

https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Ask the Questions

- Do you know where your data is?
  - Trust but verify
    - examine the workstations of employees who work with the data
    - You may find 4GB of data on an employee's desktop
- How do you protect the data?
  - Examine those protections

Questions?

Contact Information

James Edge
james@mainstreamsecurity.com
www.mainstreamsecurity.com

datadiscovery