Exploiting A PCI Compliant Network: A How-To Guide

Rob Havelt

Trustwave, SpiderLabs

Session ID: DAS-303

Session Classification: Intermediate

RSA CONFERENCE 2012

What I'm Here To Talk About

- Not an indictment of PCI itself
- Compliance defines a minimum standard, not an end goal
- PCI applies to a specific business process
- It is very easy to undermine your work and compliance investment
- When focus is too narrow, it is possible to compromise a fully compliant network

What You Need To Know

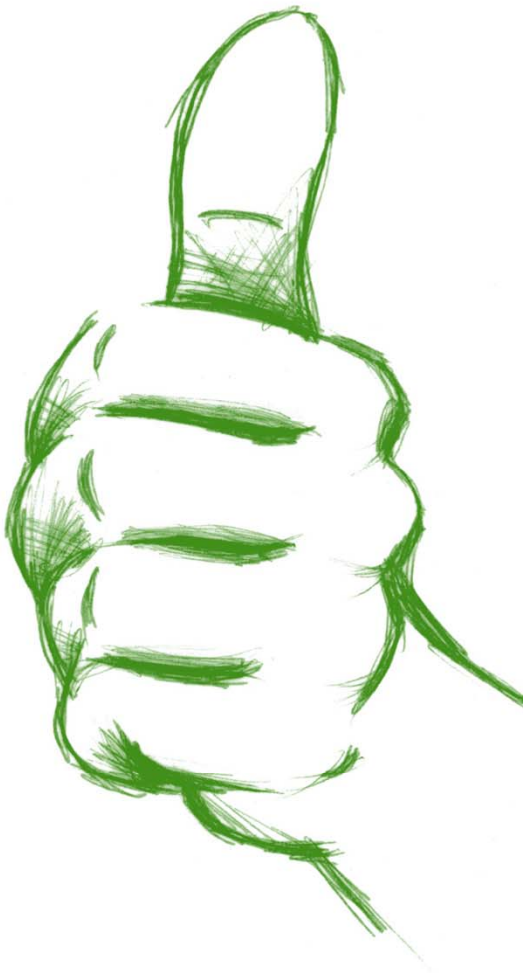
- There are traps you can fall into
- We will look at those traps and how attackers take advantage
- Hundreds of examples of organizations taking shortcuts to compliance and sacrificing integrity
- Easy ways those organizations can be compromised

A Quick Recap of PCI

- Card Brands / Council (PCI-SSC)
- 6 Focus Areas and 12 Requirements
- Just specific enough to be painful
- At the same time, just vague enough to be painful
- Standards need to be either prescriptive or interpretive

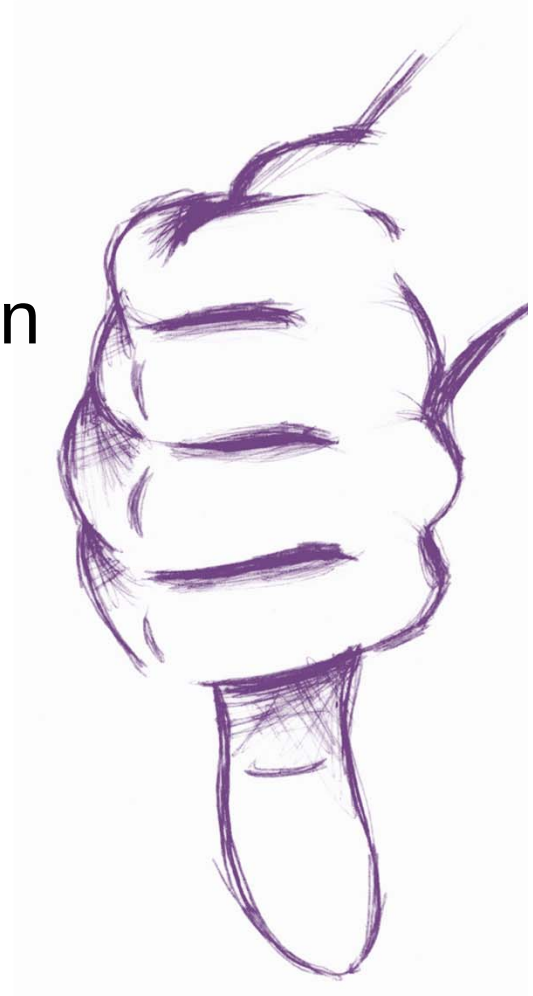
Why PCI Is Good...

- Many will say PCI is good due to specificity — *Not true*
- Some will say that PCI is good because its protecting precious credit card data — *Also not true*
- Why is it good?
  - Because it forces organizations that were previously doing nothing to do something



Why PCI Is Bad...

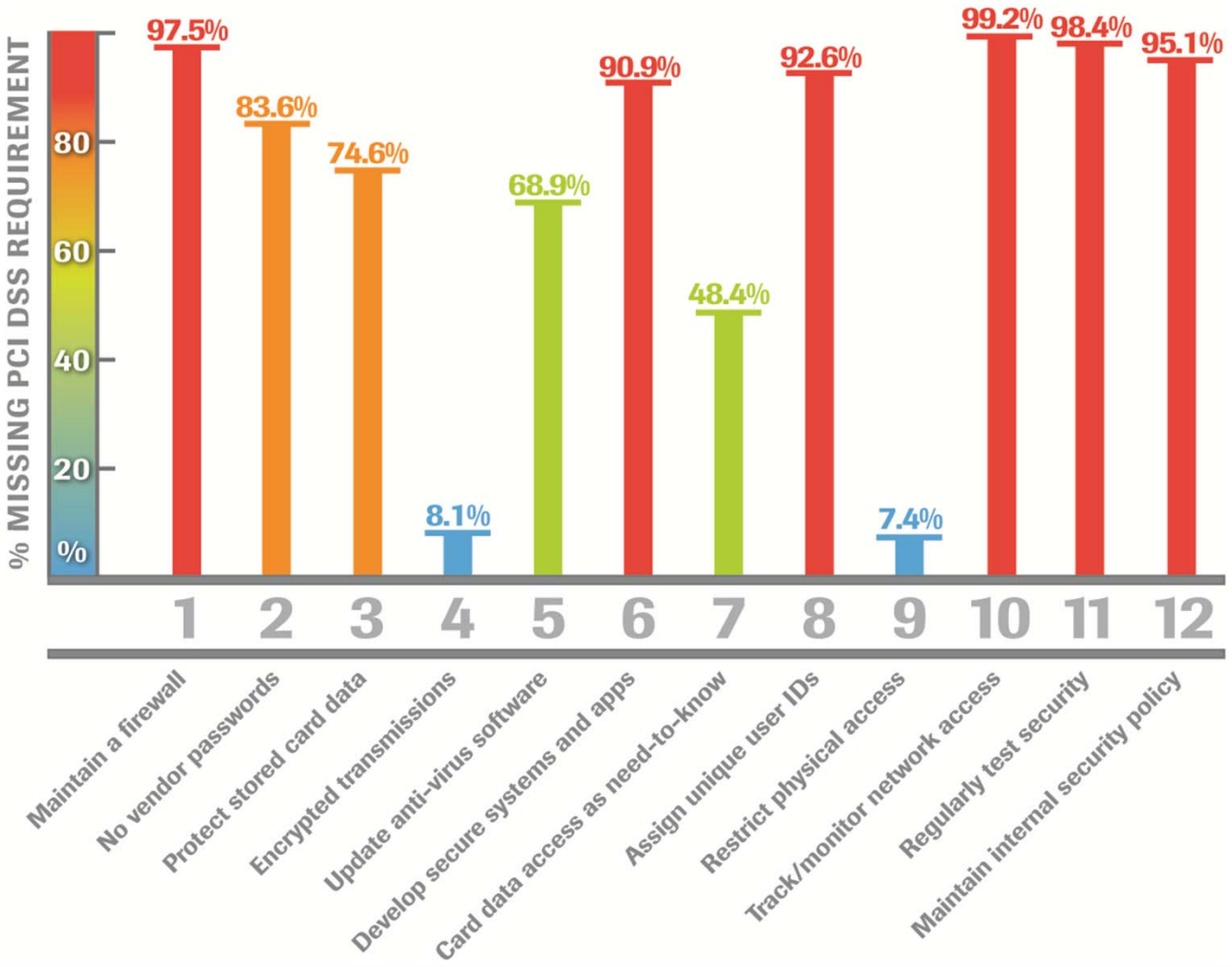
- Standards should be in one of two formats – stringent or loose
  - PCI is neither
- WAY too much room for interpretation
- Pressure on the wrong points frequently
- Things like: “No merchant has ever been found to be compliant at the time of compromise”
  - and other fairy tales…



The Numbers Tell A Story

- Number of merchants is not dramatically increasing
- According to VISA and The PCI-SSC, the number of compliant merchants goes up every year
- So does the number of compromises

The Numbers Tell A Story, cont.

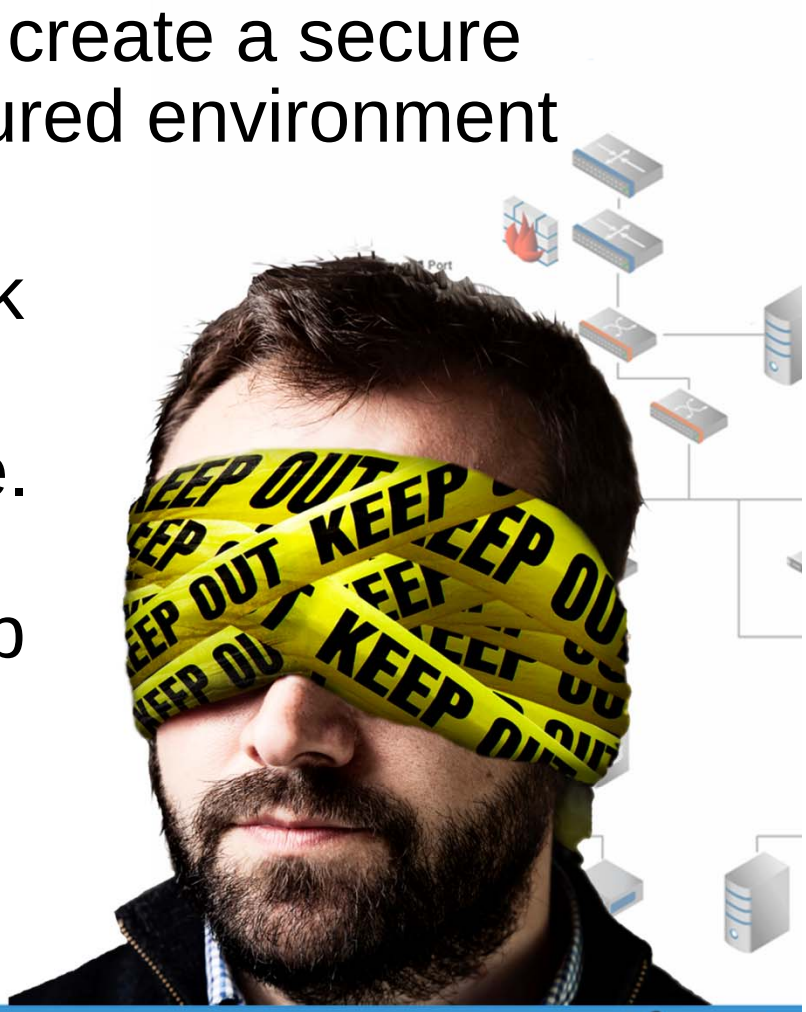


PCI Scope

- Defines a small portion of the network where one must apply these PCI rules
- Allows organizations to effectively “Draw a box” around part of the network
- If only systems knew they were inside a magic protective box

Magical Thinking

- It is EXTREMELY difficult to create a secure zone in an otherwise unsecured environment
- Organizations insist that the Out of Scope (OOS) network should not come into play
- Assessors cannot look there. Even if the organization is doing something really dumb

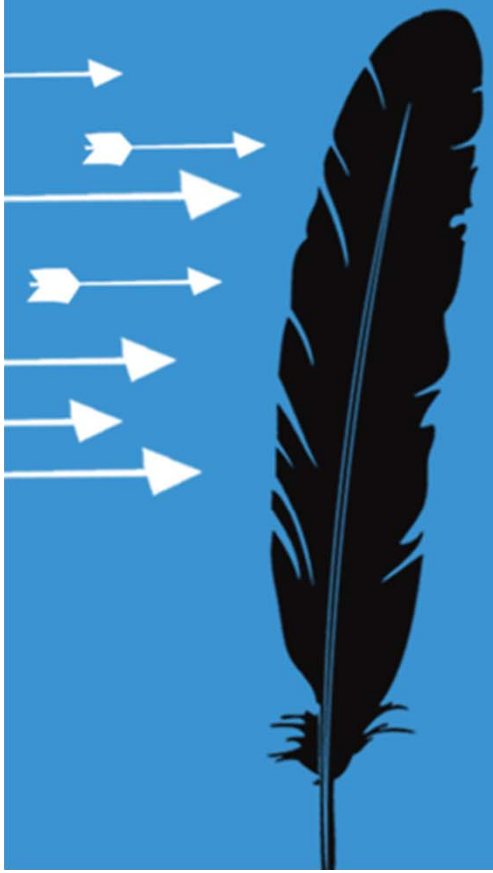


The OOS Network Matters!

- Thought Exercise:
  - Consider that building codes are implemented and enforced like PCI
  - Only rooms that store, move, or deliver water are in scope for a building inspector
- Questions:
  - How will this change building construction?
  - What can go wrong in this scenario?

The OOS Network Matters!

- How will this change building construction?
  - Plumbing done in odd ways to limit water delivery to the kitchens and bathrooms
  - Construction standards are strict in kitchens and bathrooms, not so much in dens, bedrooms, living areas
  - No one pays attention to the foundation!
- What can go wrong?
  - Building inspectors can only enforce standards for in-scope rooms



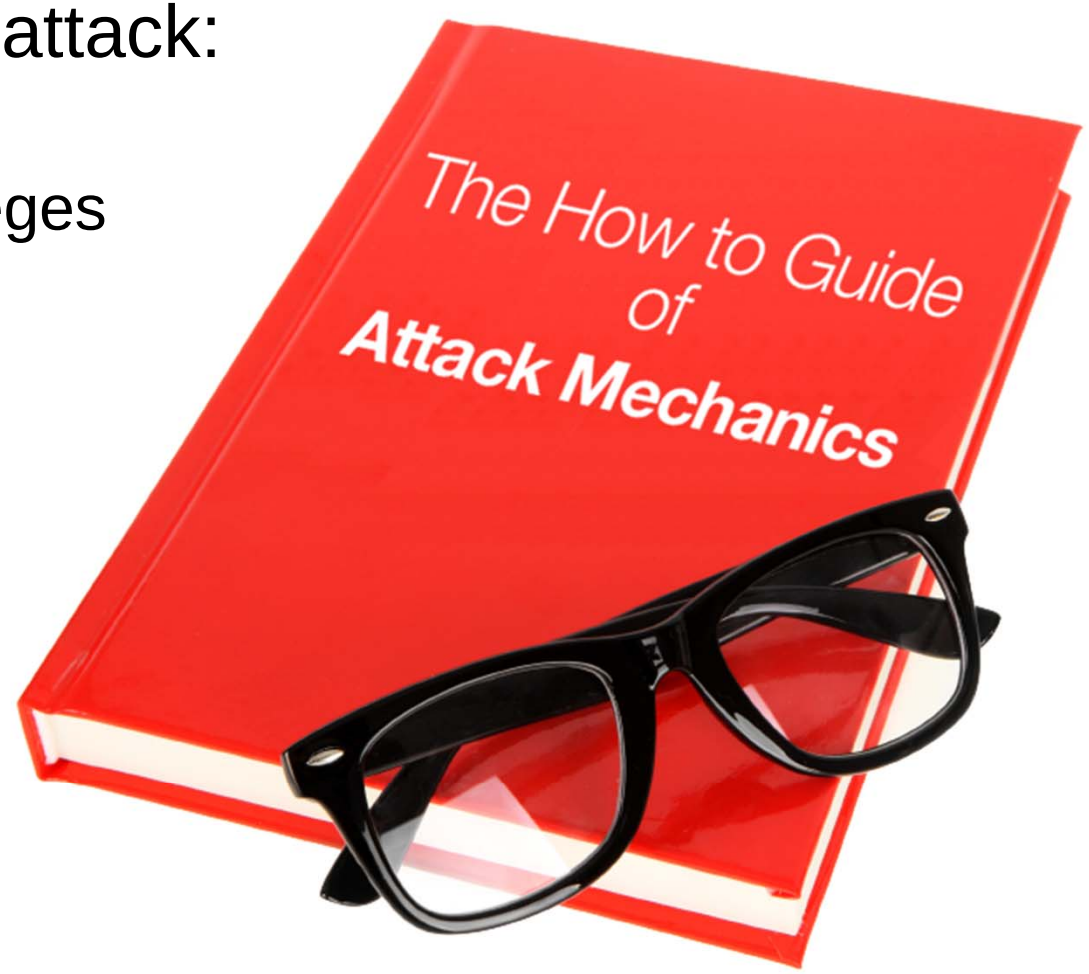
The How-To Guide

The How-To Guide: Attack Mechanics

- Security Professionals can develop a “scanner mentality”
- Completely overlook
  - configuration errors
  - poor architecture
  - implementation weaknesses
  - ill conceived human design flaws
- Do not look at issues in context of usefulness in an attack

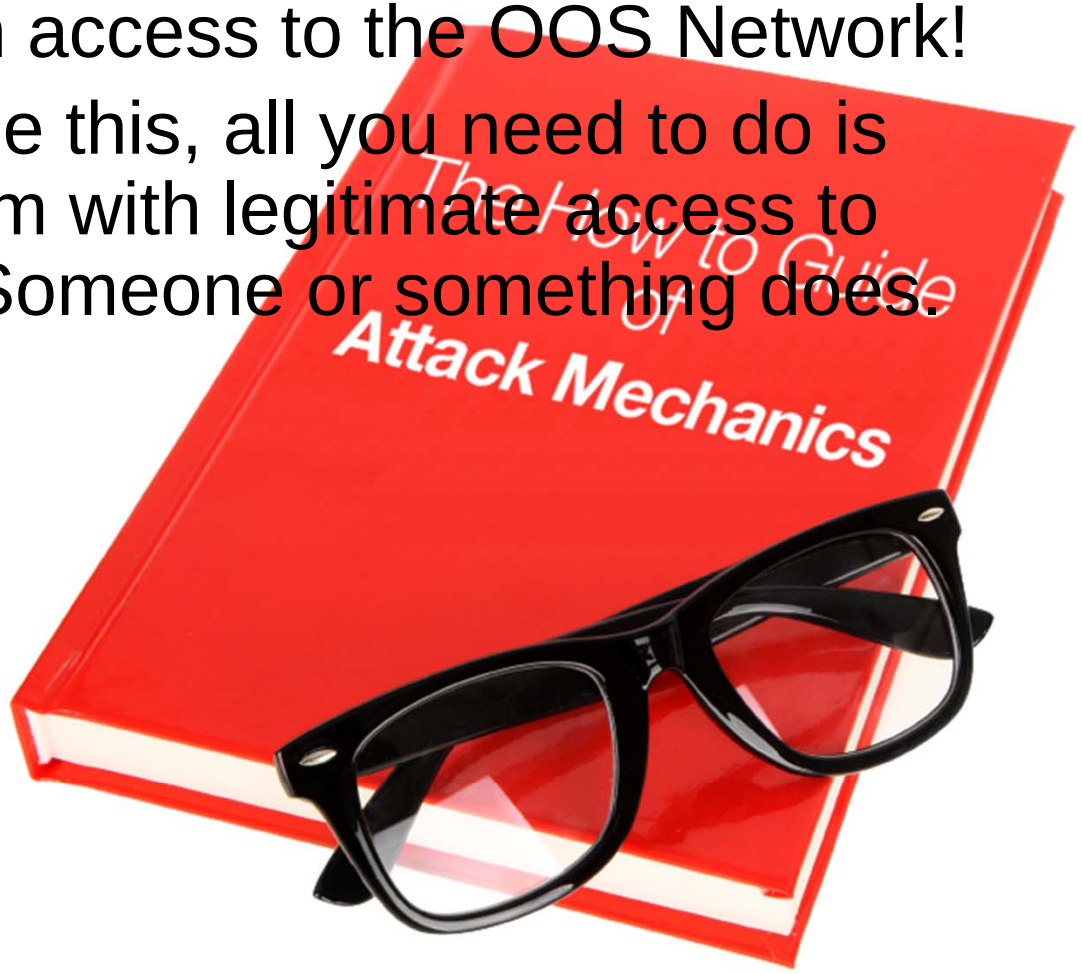
The How-To Guide: Attack Mechanics

- The 5 stages of an attack:
  - Gaining Access
  - Escalation of Privileges
  - Location of Data
  - Access Data
  - Exfiltration of Data



The How-To Guide: Gaining Access

- Normally starts with access to the OOS Network!
- Once you have done this, all you need to do is find a user or system with legitimate access to the CHD network. Someone or something does.

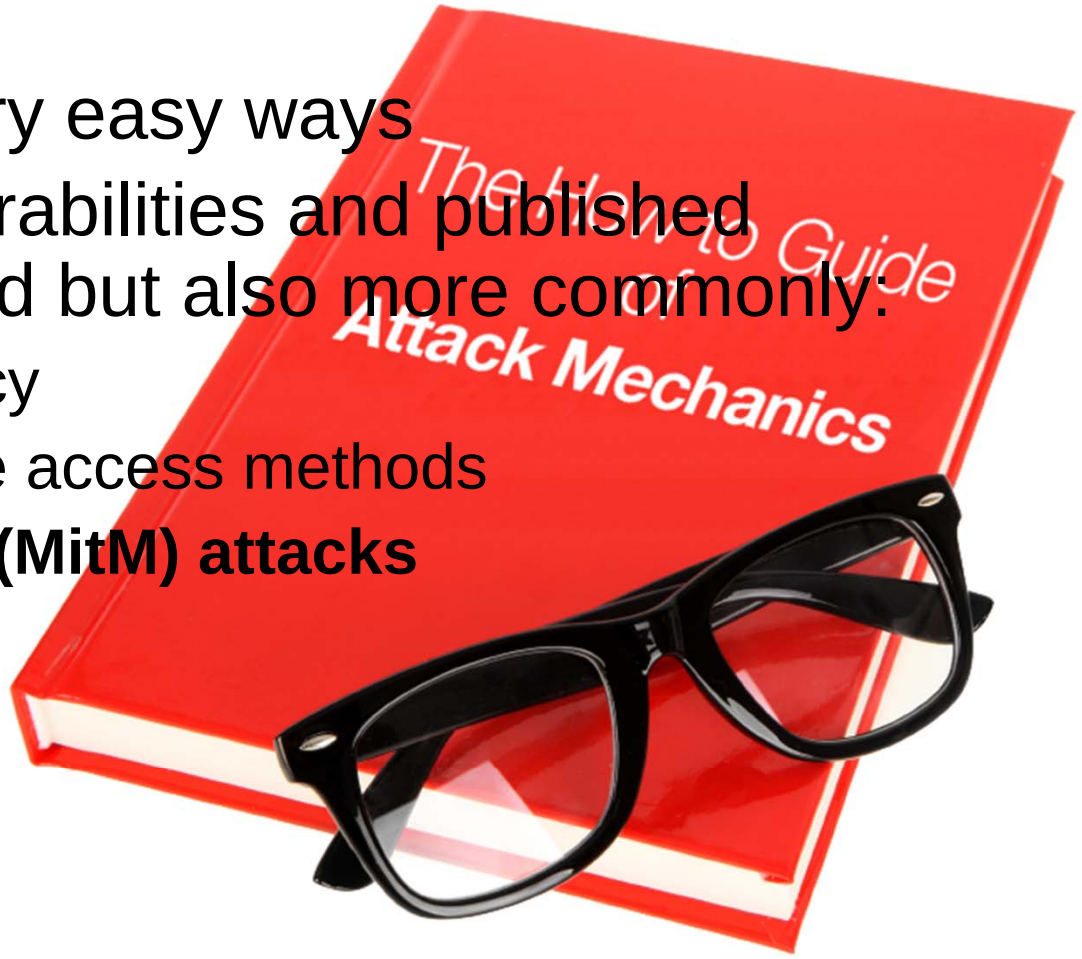


The How-To Guide: Escalate Privileges

- Who CAN access your protected/secure zone?
  - Probably someone
- Would it be bad if an attacker had their access level and privileges?
- If this can be accomplished its no longer "hacking"
  - its system administration
- Many detection systems will not alert you to this unauthorized use of legitimate methods

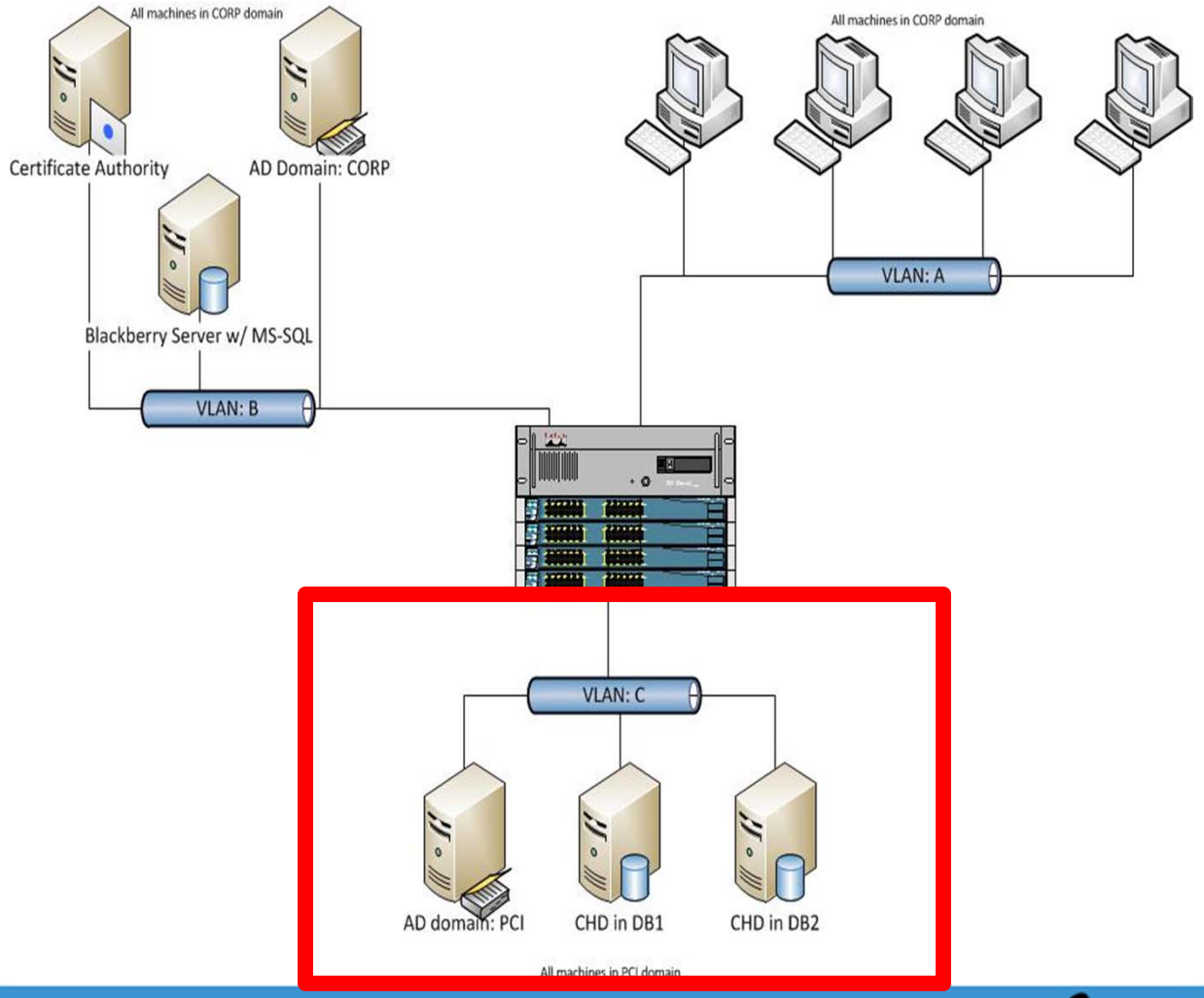
The How-To Guide: Escalate Privileges

- How?
- There are some very easy ways
- Yes Software vulnerabilities and published exploits can be used but also more commonly:
  - Bad Password Policy
  - Ill conceived remote access methods
  - **Man in the Middle (MitM) attacks**



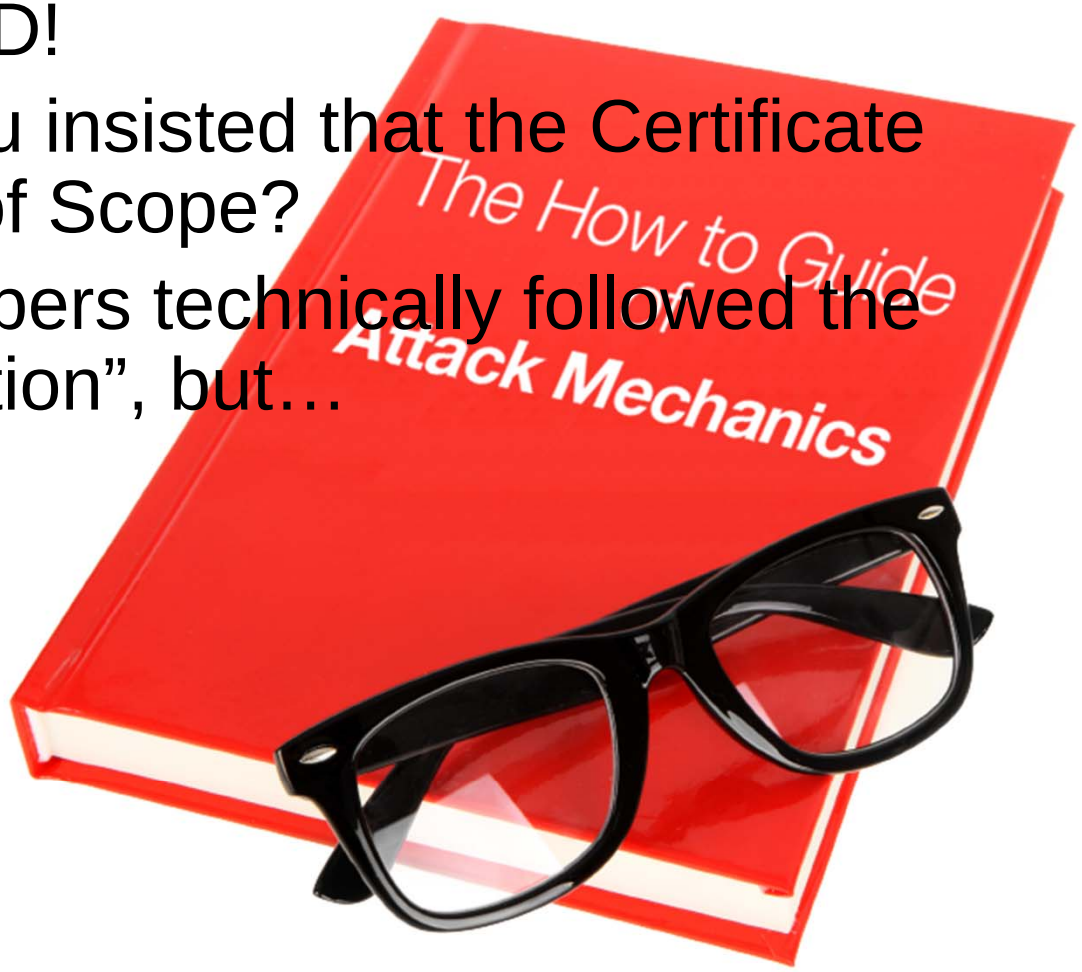
A Brief Interlude: MitM Attacks

- MitM: It's 2012 and we still don't have ARP Spoofing under control – we ignore it as an issue.



The How-To Guide: Data Access

- But its ENCRYPTED!
- Remember how you insisted that the Certificate Authority was Out of Scope?
- Maybe your developers technically followed the "letter of the regulation", but…

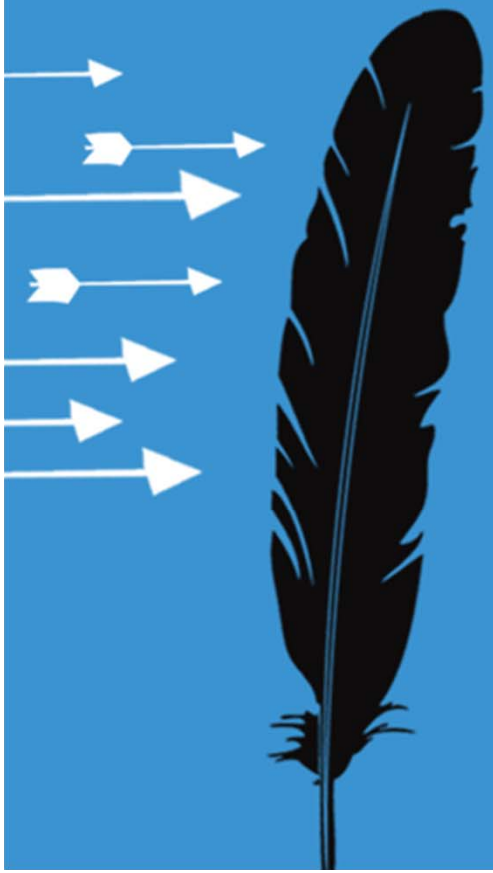


The How-To Guide: Data Access

- But I have AV/Desktop Security!
- Signature based systems don't deal well when you significantly alter known "bad" binaries
  - (this is NOT hard to do).
- Also – fairly useless against custom malware

The How-To Guide: Data Access

- What about FIM/HIPS? What about my disk encryption?
- Detection can still be bypassed.
- Exploitation with payloads direct in memory never touch the disk.
- If your payload has features like syscall proxying you can dump the whole memory or execute programs without ever touching the disk!



Putting It All Together

Scenario: PCI Compliant Company Exploitation

- In the scenario given what is done wrong?
  - Aggressively limiting scope
  - Following the letter of the requirement ignoring intent
  - Unwillingness to address anything out of scope

Recap: What Did We Learn?

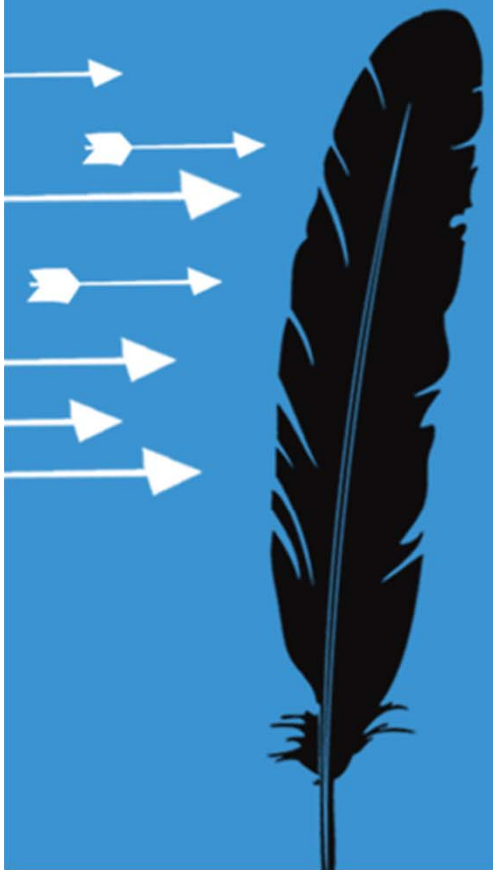
- Compliance defines a minimum standard, not an end goal
- PCI applies to a specific business process
- It is very easy to undermine your work and compliance investment
- It is entirely possible to compromise a fully compliant network

How Can This Be Applied?

- Immediately: Sit down and write down 4 different ways that you think PCI data can be accessed in your organization
  - Figure out who can access protected data
  - What controls protect them from attackers?
- Follow It Up: within 3-6 months run a test
  - Use the “malicious insider” scenario based testing
  - Use a third party that’s not invested in the outcome
  - Skilled testers test 100% of the time, they don’t do other things – ask the third party what percentage of the tester’s job is testing

How Can This Be Applied?

- Immediately: Consider if your security controls would prevent a system or network administrator from accessing sensitive data
  - Write down scenarios where an attacker might have their level of access
  - What is the likely outcome?
- Follow It Up: within 3-6 months run a test
  - Use a third party that's not invested in the outcome
  - Give a skilled 3rd party tester admin credentials and see what they can access
  - Adjust controls accordingly



Questions?