What Audits Miss and How Penetration Testers Abuse Those Gaps		[*picture here*]
Rick Redman KoreLogic		
Governance, Risk & Compliance – G24		

Session Abstract

During penetration tests, a penetration tester's job is to abuse systems to gain access to sensitive data. But almost all the resources that are abused have been audited. Then why are penetration testers successful? For example, password complexity introduces vulnerabilities that can be abused. In this talk, Rick (a penetration tester for KoreLogic and founder of the **Crack Me If You Can** password cracking contest) will discuss methods of attack used in a penetration test, and relate the techniques used, to methods auditors can use to be aware of the risk. If you don't audit for X, an attacker can abuse X. Solve for X.

Target Audience

- Skill Level – Beginner, Intermediate, and Advanced
- Occupational Experience – Entry to Senior level Auditors, Managers, and Directors in all industry verticals

COBIT Objectives or Practices

PO1 – Define a Strategic IT Plan

PO3 – Determine Technological Direction

PO9 – Assess and Manage IT Risks

DS5 – Ensure System Security

Speaker Bio

Rick Redman

Creator/plaintext-creator of DEFCON's "Crack Me If You Can" - password cracking contest

Professional Penetration Tester since 1999

Owner/Possesses 0 (Zero) security certificates

Graduate from Purdue's COAST/CERIAS program

Password researcher since 2009

"Author" of many published password cracking tools/rulesets/tips

Cracked over 2.038 million *unique* password hashes from internal corporate networks

Speaker Details (optional):

Company	KoreLogic
Title	Senior Security Consultant
Email	rredman@korelogic.com
Facebook URL	
Twitter URL	@CrackMeIfYouCan
LinkedIn URL	
Website	*Www.korelogic.com*