PEN TESTING AS AN AUDITING TOOL

With An Update On Regulations

Presented By:

Bryan Miller
CCIE, CISSP

Agenda

- Introduction
- Regulations Update
- Why Pen Test
- Why Not Pen Test
- Tools & Techniques
- Low Hanging Fruit
- Case Studies
- Questions

Introduction

- Biography
  - B.S. - Information Systems – VCU
  - M.S. – Computer Science - VCU
  - CCIE, CISSP
  - Former CCNA Instructor at John Tyler & J. Sargeant Reynolds Community Colleges
  - Current President, Syrinx Technologies LLC

Introduction

- Employment History
  - VCU – Academic Campus
  - Circuit City/DiVX
  - Cabletron
  - Started Dominion Systems Consulting
  - Dataline
  - SyCom Technologies
  - Packet360
  - Started Syrinx Technologies

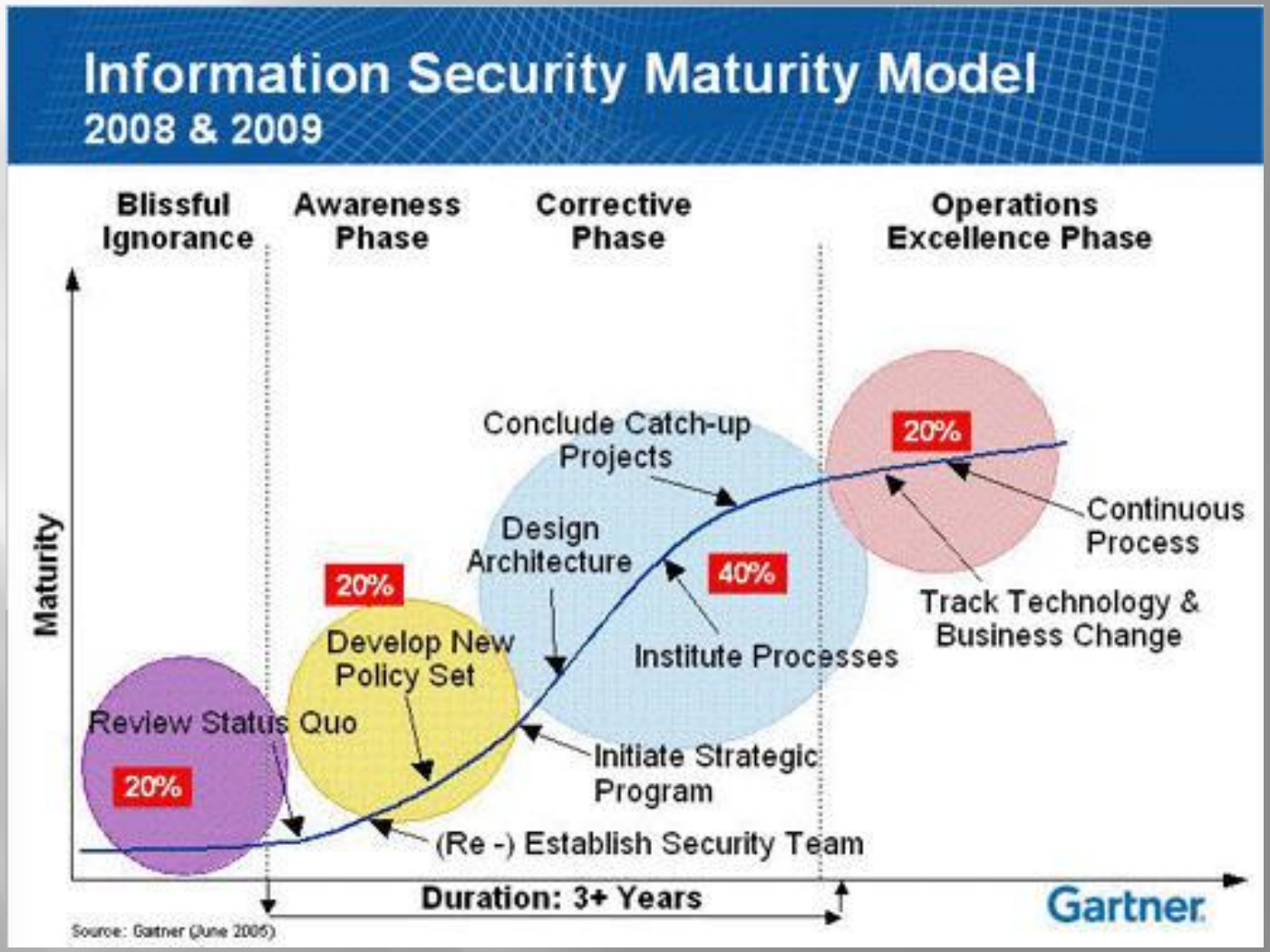
Regulations Update

- ID Theft Red Flags Rule
  - Part of the Fair and Accurate Credit Transactions (FACT Act) of 2003, instituted by the FTC
  - Requires companies to have identity theft prevention programs in place
  - Compliance date is November 1, 2008
  - Who must comply?
    - Financial institutions and creditors
    - OK, what's a creditor?
      - Any entity that extends, renews or continues credit, such as….
      - Finance companies, auto dealers, utility companies, mortgage brokers, telecommunications companies
  - Penalty for non-compliance: $2,500 per violation

Regulations Update

- PCI Version 1.2
  - Released on October 1, 2008
  - Clarifies a fair amount of verbiage
  - Several of the major changes are:
    - Removed requirement to disable broadcasting of wireless SSID.
    - For new wireless implementations after March 31, 2009, WEP is prohibited.
    - For existing wireless implementations, WEP is prohibited after June 30, 2010.
    - Included Unix-based systems in anti-virus requirement.
    - Under 11.3, clarified rule that both internal and external testing is required.

Why Pen Test



Why Pen Test

- Satisfy legal/governmental requirements (HIPAA, GLB, SOX, PCI).
- Raise overall security awareness.
- Often required by internal/external auditors.
- Test IDS/IPS systems, including incident handling procedures.
- New management: Provides a great security baseline.
- Because it's just damn fun doing it!

Why Not Pen Test

- We already know where everything is broken.
- If you tell us what's wrong, we'll have to fix it.
- We don't have anything that hackers want.
- We're too small to matter.
- We can't afford it.

Tools & Techniques

- Start with a methodology.
  - Reconnaissance
  - Scanning
  - Verification
- Use a variety of tools and don't trust any one tool too much.
- Test everything with an IP address.
- Every device is important, otherwise disconnect it.

Tools & Techniques

- Categories of tools:
  - Research
  - Port/Vulnerability Scanners
  - Wardialing/Wardriving
  - Application-specific scanners
    - Web Servers
    - OS specific
    - Database
    - Password cracking
  - Frameworks
  - Social Engineering

Low Hanging Fruit

- Things to check for in your own organization:
  - Blank or easily guessed SA password (MS SQL).
  - Blank or easily guessed "root" password (MySQL).
  - Default passwords in Compaq Insight Manager.
  - Patches (MS05-039, MS06-040 in particular).
  - Default SNMP read-write strings in Cisco gear.
  - Default Oracle passwords.
  - Obvious SQL Injection opportunities.
  - Unprotected wireless AP's.
  - Default passwords on infrastructure devices.

Low Hanging Fruit

- Things to check for in your own organization:
  - Remote control/access programs that don't require passwords.
  - VNC.
  - Common passwords across different platforms and/or architectures.
  - Lack of proper physical security for servers and other network infrastructure devices.
  - Sensitive configuration data stored on file shares without encryption.
  - Sensitive configuration data stored in email.

Case Studies

- Each of these 3 cases are real. There are many more.
- The names and specifics have been changed to protect the innocent and the clueless.
- Each case provides an example of the "domino effect".
- Note that in each case nothing alerted the client to what was going on.
- For each case identify the "LHF".

Case Study #1

- Large company running Notes with many branch offices. Each branch office had a BDC.
- One BDC had a blank administrator password.
- The VNC password was the domain admin password.
- Connected to AP via Telnet and viewed config.
- Same password provided access to HP and 3Com switches along with SNAP servers.
- While examining file systems a file was found with backup Cisco configurations.
- Full access to all Notes email and Oracle systems.

Case Study #2

- During wardialing, a Shiva LanRover was found using Novell authentication.
- Oracle servers were accessed using default passwords.
- Cisco infrastructure compromised due to default read-write SNMP community string.
- Connected via web browser to AP's.
- Connected via FTP to Novell server, viewing sensitive configuration files.
- Accessed many UNIX machines, decrypting several password files.

Case Study #3

- Entire Cisco infrastructure compromised from one device with default read-write SNMP community string.
- Several devices with PnP vulnerability provided access to local domain administrator password.
- VNC password also provided access to many MySQL server databases.
- A tool was uploaded to a SQL server providing the SA password, providing access to over 2 dozen SQL servers.
- Accessed databases containing student and faculty info, including SSN's. Other databases provided access to building control systems.
- One SQL server associated with the bookstore provided access to credit card information!

Case Study Recap

- What did we learn?
  - THE 3 P'S:
    - Policies & Procedures
    - Patch Management
    - Password Management
- The majority of the remediation doesn't have to cost a lot of money.
- The biggest changes often have to occur with the user community, systems administrators and developers.

Questions

Thank You Very Much for Your Time and Attention!