

THE TEXAS A&M UNIVERSITY SYSTEM



TACUA Show and Tell
**Alternate Information Gathering
and Analysis Techniques**

Presentation to TACUA Attendees
April 2010

Copyright © 2010 Paul Wiggins

Agenda

- **My Background...**
- **Typical IA Information Gathering in the Past...**
- **My Approach**
- **Findings...**
- **Tools**
- **Moving Forward**
- **Current Obstacles**

My Background...

- A little about me...
- So no, I'm not a traditional auditor. 😊

Typical Information Gathering in the Past...

- All work may be performed by non-technical personnel;
 - May not know the 'right' questions to ask in a given situation;
 - Unaware of system or application specifics/nuances;
 - Not knowing when you are being buffaloed...
- Manual, and possibly time-intensive information gathering process;
- Work may not have been technical or in-depth enough;
- May have been primarily Policy and Procedure driven.

Current Approach

- Enhance the Audit process with additional skills:
 - Personnel with deeper IT and security experience and certifications are now being used to assist with IT audit/review work.
- Leveraging systems administration, networking, and security skill sets. Personnel with:
 - A familiarity of various products, operating systems, databases, etc.;
 - Executed a number of vulnerability assessments and penetration engagements; and
 - Experience with compliance reviews.

Current Approach

- Configuration reviews, vulnerability assessments, and penetration tests compliment one another and provide a more comprehensive approach to validating controls and mitigating risks...
- Each activity has its own merits, strengths and weaknesses (e.g. a pen test may not reveal a weaker password policy, whereas a configuration review may)- combined give a more comprehensive approach to risk management.

Current Approach

- Automating the process of gathering system information as much as possible...
- Why?
 - Repeatable
 - Consistent
 - Time efficient
 - You know exactly what was executed
 - No accidental typos... ☺
 - Requires little effort from client personnel versus previous method.

Current Approach

- How?
 - By using what is already there to get system-generated output in a more automated fashion:
 - System calls
 - Built-in tools
 - Queries
 - Configuration files (UNIX/Linux especially)
 - ...and screenshots where necessary.
 - IT/Security personnel collect and oversee...
 - <Examples>

Current Approach

- And they let you do this?
- Getting Buy-in:
 - Building relationships with System members and ISOs;
 - Vetting and testing on both sides;
 - Demonstrated competency;
 - Being transparent, and having a process;
 - Show value;
 - Ongoing collaboration and assurance mechanisms...

Findings...

- Probably what you've been finding...
- For my work, the findings are supported by the output generated by the systems themselves.

Findings...

- Patch management for operating systems, databases, and applications.
- System defaults left in place;
- Lack of baseline system hardening;
- Poor password controls and/or enforcement;
 - Not just for operating systems, but for appliances and database accounts as well...
 - Think about Oracle used for Banner, etc.
<EXAMPLE>

Findings...

- Obsolete products in use;
- Not updating virtualization platforms;
- Lack of automated monitoring and alerting;
 - You do not know what you do not know...
- Wireless-related:
 - Primarily with one-offs;
 - Weak encryption mechanism if any;
 - Personnel being connected both by wire and wirelessly to the network.

Findings...

- Weak physical security and/or practices.
 - Not just protection of servers.
 - Information storage assets.
 - Outsiders being able to gain access to facilities.
- Lack of DLP solutions or measures where they may make sense...
 - Little due diligence performed initially regarding data loss prevention (DLP) of protected data types.
- Entity cannot demonstrate compliance with nor due diligence to comply with regulatory requirements (e.g. HIPAA)

Findings...

- Other issues...
 - Lack of [forced] encryption (e.g. websites where policy or regulation would require, Oracle, etc.)
 - Non-hardened modem-connected devices;
 - Misconfigured multi-function 'smart' printers;
 - Patch management;
 - Open shares.
 - Web application penetration testing, for some, may not have gone far enough... <EXAMPLE>
 - Personnel not enforcing policies (susceptible to social engineering)
 - Money / Training / Skill sets...

Tools

- **Hardware**
 - A multi-homed router of some sort with VPN access built-in or provided in another way;
 - E.g. pfSense (www.pfsense.org) or m0n0wall (m0n0.ch)
 - Small switch;
 - Multi-core system (e.g. Core i7-based) with a lot of memory that is capable of supporting a virtualized 'test environment' and WoL.
- **Virtualization software**
 - VMWare (www.vmware.com)
 - VirtualBox (www.virtualbox.org) [Free]

Tools

- **Operating systems – you need to test as many as you can that you clients use...**
 - UNIX/Linux
 - Many are freely available
 - Subtle differences between some variants
 - MSDN Subscription
 - Access to Microsoft operating systems and applications;
- **Freely available code and tools**
 - Security tools;
 - VB code, shell code, example commands, etc. can be found online;
 - Don't' forget dictionaries...

Tools

- Specialized hardware where practical and necessary to test against;
 - Sun/SPARC, Apple
- Leverage vendor's products via demos;
- Iron Key (www.ironkey.com) for collecting and transporting data / output;
- System-member surplus
 - Usable old hardware...

Tools

- Hand-held GPS (for use in wireless surveys)
- Software capable of finding protected data types or that leverage regular expressions for searches...
- Gray matter and experience can be a great tool...
 - Certain hash characteristics, for example...
 - Tools that we've seen work, and have used, we can offer as examples of ways to improve security awareness or aid in IT management in some way.
 - e.g. denyh0sts

Tools

- While onsite...
 - Passive network information gathering
 - Snort and WireShark can aid in identifying anomalies...
 - Active network information gathering if in-scope and with authorization.
 - nmap can leveraged for targeted service discovery...

Moving Forward...

- Adding more Information Security-related Services...
- Additional personnel with IT and/or Information Security experience...
- IT and Security Professionals add value to the audit and controls validation process, as they bring complimentary skills and different experiences to the table...

Current Obstacles

- Probably nothing new:
 - Clients trying to limit audit/review scope;
 - Not providing complete information...
 - Altering systems as your audit/review is underway;
 - <EXAMPLE> Comparing stale password ages to account inactivity time and comparing to password rules... Sometimes it doesn't add up.
 - Time stamp changes.
 - Clients not having a good understanding of the support or licensing of certain products they use... but they'll argue it.
 - This is where CISO support can help...
 - And so on...

Advice for Security Personnel...

- Learn to link findings to business risks;
- Keep abreast of new regulatory requirements and technologies;
- Always look for new tools and methods;
- Interact with other security professionals;
- Keep active or self-obliterate...

Thank You for Your Time!

Any Questions?