

Performing a Comprehensive Network Security Review

November 3, 2009

Timothy Agee, CISA, CGEIT
Jacob Arthur

*FDH Consulting
Frasier, Dean & Howard, PLLC*



What is included in a “Security Assessment?”

- For SOX...
- For HIPAA...
- For PCI...



Performing a Comprehensive Network Security Assessment:

- Vulnerability Assessment / Penetration Test
- Security Policies (Change Control Policies)
- Security Configuration
- User Account Provisioning
- Security Monitoring
- Employee Training
- Social Engineering

Vulnerability Assessment Penetration (“Pen”) Test

What is it?

Vulnerability Assessment / Pen Test

Using a variety of third-party tools, a vulnerability assessment includes mapping hosts and services within a specified public address space or internal network and scanning them for potential vulnerabilities. During penetration testing, third party tools are used to exploit security weaknesses for the purpose of identifying and correcting means of unauthorized access.

Why a Vulnerability Assessment / Pen Test?

SOX “compliance” is not enough

Why? (Examples) - *130 Million Total Cards*

- Barnes & Noble
- Office Max
- BJs Wholesale
- JC Penny
- Target
- Forever21
- DSW
- Sports Authority
- Boston Market
- Dave and Busters
- TJ Maxx
 - *47 Million Cards*

Why? (Vulnerabilities)

- Patching
 - *Servers, workstations, firewalls, etc.*
- Old technology
 - *Windows 2000 (beware if using WSUS)*
 - *WEP encryption*
- Poor design
- Poor configuration
- Unapproved devices or services
 - *Change control*

Vulnerability Assessment / Pen Testing

- Internal vs. External
- Black Box vs. Crystal/White Box
 - *What are the advantages & disadvantages*
- Start with tool, but interpretation is key

Vulnerability Assessment / Pen Test (Rules for Engagement)

- Determining scope
- *Exploits that could crash systems or services*
- Timing / notification requirements
- Defined stop points
- Stealth requirements
- Get out of jail free card

Vulnerability Assessment Pen Test - Demos

Proceed at your own risk!

Vulnerability Assessment / Pen Test (BackTrack 4 pre-release)

- www.remote-exploit.org



- Bootable DVD Image (iso) / VMWare Image
- Linux distribution built for the sole purpose of testing security

Vulnerability Assessment / Pen Test (Scanning - nMap)

- www.insecure.org
 - *Linux (Unix) / Windows / Mac OS X / etc*
- Internal vs. External
- Finding potential targets
 - *What are we looking for?*

Vulnerability Assessment / Pen Testing (Wireless Scanning)

- AirPcap / Kismet (AirCrack)
 - www.cacotech.com (AirPcap) – Hardware
 - www.kismetwireless.net (Kismet)
 - *Linux / Windows (requires AirPcap for Win)*
 - www.aircrack-ng.org (AirCrack)
 - *Linux / Windows (requires AirPcap for Win)*
- Finding potential targets
 - *What are we looking for?*

Vulnerability Assessment / Pen Test (Vulnerability Scan - Nessus)

- www.nessus.org
 - *Free & commercial versions*
 - *Linux / FreeBSD / Windows / Mac OS X*
- Internal vs. External
- Pros & Cons (Why it's not enough)

Vulnerability Assessment / Pen Test (Exploit - Metasploit)

- www.metasploit.com (Just acquired by Rapid7)
 - *Linux (Unix) / Windows*
- Various uses
- Internal vs. External
- Can generate stand-alone files

Vulnerability Assessment / Pen Test (Exploit - What Now)

- View permissions of exploited user
- Migrate to other processes, view available tokens
- Enabling shell access

Vulnerability Assessment / Pen Test (Standard User)

- Review standard permissions assigned to users
- Must determine the potential risky users
- Begins with exploring the infrastructure

Security Policies (Change Control)

- Acceptable Use
- User Provisioning
- Password
- Network Access
- Incident Response
- Remote Access
- Guest Access
- Wireless
- Configuration Standards
- **Configuration Changes**
- Third Party Connection
- Network Security
- Encryption
- Confidential Data
- Data Classification
- Mobile Device
- Retention
- Outsourcing
- Physical Security
- Monitoring

Configuration / Design Review

- Firewall
- Wireless
- IDS
- Remote access
- Active Directory Group Policy / Accounts
 - *Local admin accounts*
- iSeries System Values / Profiles
- Standard configurations / deployment

User Provisioning

- New Hires / Transfers / Terminations
- Administrative access
- Consultants / Contractors / Vendors

Security Monitoring

- Security Logs
- Log Aggregation / Filtering / Alerts
- IDS Indicators / Alerts

- Use of powerful accounts
- Excessive failed login attempts
- Access to sensitive data
- Use of unapproved IP services

Employee Training

- Documents and Posters only?
- New employee orientation?
- Regular updates / reinforcement?
 - *Emails / Newsletters / Classroom (frequency)*
 - *Incorporate with other meetings*
 - *Make it personal*

Social Engineering

- Contact a sample of employees and attempt to obtain passwords or contact lists. *Impersonate IT Support personnel.*
- Contact the IT Help desk and attempt to have password reset for known employee
- Send an outside person into the office to walk around. Assess the length of time it takes for personnel to identify this unauthorized entry.

Social Engineering

- Place forged memos into a sample of company mailboxes with instructions that would facilitate unauthorized intrusion.
- Examine trash in a sample of offices to determine if sensitive material is being improperly disposed of that could lead to unauthorized access.

Social Engineering

- Randomly leave USB flash drives throughout the office, which are loaded with malicious files (hidden). Evaluate whether employees will attempt to use these drives.
- Impersonate a known company vendor at central or remote locations. Attempt to gain access to company network.

Online Resources

- ***Proceed at your own risk***
- www.packetstormsecurity.org
- www.cve.mitre.org
- www.smashthestack.org
- www.securityfocus.com
- www.osvdb.com
- www.infosecnews.org
- www.undergroundnews.com

Questions?

Timothy Agee, CISA, CGEIT
tim.agee@fdhconsulting.com
615-330-8652 (Mobile)

Jacob Arthur
jacob.arthur@fdhconsulting.com
615-852-8540 (Mobile)