Vulnerability Assessment

CSH6 Chapter 46

"Vulnerability Assessment"

Rebecca Gurley Bace

Copyright © 2015 M. E. Kabay. All rights reserved.

Topics in CSH6 Chapter 46

- Scorekeeper of Security Management
- Taxonomy of VA Technologies
- Penetration Testing

Copyright © 2015 M. E. Kabay. All rights reserved.

Scorekeeper of Security Management

- Introduction to Vulnerability Management
- What is Vulnerability Management?
- What is Vulnerability Assessment (VA)?
- Where does VA Fit into Security Management?
- History of VA

Copyright © 2015 M. E. Kabay. All rights reserved.

Introduction to Vulnerability Management

- Information security tightly integrated into risk management
- Vulnerability management critical component of risk management
- Significant evolution from 1960s through 2000s

Copyright © 2015 M. E. Kabay. All rights reserved.

What is Vulnerability Management?

- Assessing deployed IT systems
- Determine security status
- Determine corrective measures
- Manage application of corrections
- Vulnerability assessment (VA): critical element in vulnerability management
- Synergy between VA & other elements of security
- Four key functions (see next slide)

Copyright © 2015 M. E. Kabay. All rights reserved.

Four Key Functions of Vulnerability Management

- Inventory
  - ❑Identify all systems in domain of interest
  - ❑Operating systems, platforms, topology
- Focus
  - ❑Determine data required for assessment
  - ❑Tune vulnerability assessment tools
- Assess
  - ❑Run automated & manual trests
  - ❑Evaluate (assess) results to judge risk
  - ❑Use security policy + best practices
- Respond
  - ❑Execute changes as required by assessment
  - ❑Fix specific weaknesses

Copyright © 2015 M. E. Kabay. All rights reserved.

What is Vulnerability Assessment (VA)?

- Analysis of security state of system
  - Gather data sample (e.g., parameters on selected firewalls)
  - Store data for future reference
  - Compare with reference standards
  - Identify discrepancies between current state & recommended standards or goals
- Examples of tools
  - MS Baseline Security Analyzer
    - ✓For Windows 2000/XP & NT4
    - ✓See http://www.techspot.com/tweaks/mbsa/index.shtml
  - Server VAM http://www2.stillsecure.com/products/svam/svam1.html

Copyright © 2015 M. E. Kabay. All rights reserved.

Sample Screen Shots from Baseline Security Analyzer

FAB (Features and Benefits) of a VAS (Server VAM)

Special features	Benefits
Intelliscan™	Delivers appropriate scans for range of devices
Scan Power Technology™	Optimizes scanning, saving time and network resources
Workflow Management Engine™	Provides accountability and control throughout the remediation process
Systematic and continuous vulnerability assessments	Reduce risk and liability from security vulnerabilities
Customizable scan policies and rules	Utilizes IT resources efficiently
Comprehensive reporting engine	Provides actionable information and historical data for compliance
Latest vulnerabilities updated as often as hourly	Eliminates manual effort required to protect against the latest vulnerabilities
Multi-user access	Allows tasks to be split among multiple users and provides for redundant support
At-a-glance Web-based interface	Reduces management time
Comprehensive glossary of vulnerabilities	Educates and informs regarding the latest issues in network security
Subscription-based payment structure	Provides affordable, cost-effective protection

http://www2.stillsecure.com/products/svam/svam1.html

Where does VA Fit into Security Management? (1)

- When systems 1st deployed, can establish baseline security state
- When security breaches suspected, can focus on likely attack paths
- May be able to see if vulnerabilities have been exploited
- VA can identify areas where newly reported vulnerabilities should be patched
- Records of VA scans can be archived
  - Serve for audits
  - Compliance with certifications

Copyright © 2015 M. E. Kabay. All rights reserved.

Where does VA Fit into Security Management? (2)

- Support *auditability*
  - Independent review of system records
  - Determine adequacy of controls
  - Ensure compliance with policy & procedures
  - Detect breaches of security
  - Recommend changes or guide recommendations
- *Auditability* in turn supports
  - Incident handling & recovery
  - Adjustment of security policies to meet needs

Copyright © 2015 M. E. Kabay. All rights reserved.

Brief History of VA (1)

- Manual security audits established in 1950s
- Auditability defined 1970s for USAF study
- Eugene Spafford and Dan Farmer (Purdue)
  - COPS VAS for UNIX
  - Late 1980s
- Internet Security Scanner (ISS) – early 1990s
  - http://www.cert.org/advisories/CA-1993-14.html

Some Famous Security Experts

Brief History of VA (2)

- SATAN (Security Administrator Tool for Analyzing Networks)
  - Farmer & Wietse Venema
  - Posted 1995
  - http://www.porcupine.org/satan/
  - http://www.cerias.purdue.edu/about/history/coast/satan.php
- NESSUS
  - http://www.tenable.com/products/nessus
  - Free for individual use
    http://www.tenable.com/products/nessus/nessus-homefeed
- NMAP
  - NetMAPper
  - http://nmap.org/

See "Alphabetical List of Vulnerability Assessment Products"
http://www.timberlinetechnologies.com/products/vulnerability.html

Taxonomy of VA Technologies

- VA Strategy & Techniques
- Network Scanning
- Vulnerability Scanning
- Assessment Strategies
- Strengths & Weaknesses of VAS
- Roles for VA in System Security Management

Copyright © 2015 M. E. Kabay. All rights reserved.

VA Strategy & Techniques

- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checking
- Virus detection
- War dialing
- War driving
- Penetration testing

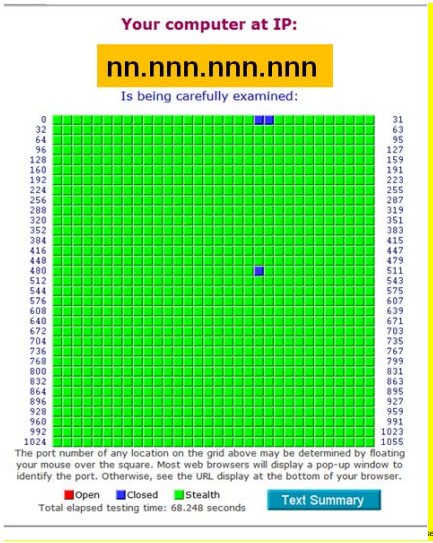
Copyright © 2015 M. E. Kabay. All rights reserved.

Network Scanning

- Port scanner
  - ICMP feature
  - Identify hosts in network address range
  - E.g., GRC ShieldsUP! (see next slide)*
  - Identify visible & open ports
  - Can spot undocumented equipment on network

*** https://www.grc.com/x/ne.dll?bh0bkyd2**

Copyright © 2015 M. E. Kabay. All rights reserved.



GRC ShieldsUP! Port Scanner

- Explanations of each *visible* (blue) port available
  - Risky because can be *seen* by attackers
- Open ports shown in red
  - Dangerous
  - May be exploited

Vulnerability Scanning (1)

- Heart of VA systems
- Beyond port scanning
  - Analyze data to recognize known vulnerabilities
  - May also attempt to correct problems
- Identifies deeper details
  - Software versions
  - Applications
  - Configurations
- Current DB of known vulnerabilities especially valuable

Copyright © 2015 M. E. Kabay. All rights reserv

Vulnerability Scanning (2)

- Typically slower than simpler port scanners
- Some scanning / testing may disrupt operations; e.g.,
  - DDoS testing
- False positive rates
  - May be high
  - Require more human judgement
- Vulnerability DB must be updated frequently

Copyright © 2015 M. E. Kabay. All rights reserved.

Assessment Strategies

- Credentialed monitoring
  - System data sources
    - ✓File contents
    - ✓System configuration
    - ✓Status information
  - Nonintrusive
  - Host-based
- Noncredentialed monitors
  - Simulate system attacks
  - Record responses
  - "Active" approaches superior for network-related vulnerability assessment

Copyright © 2015 M. E. Kabay. All rights reserved.

Strengths & Weaknesses of VAS (1)

Benefits

- Save time & resources
- Training novices
- Updated for new info
- Address specific problems
- Benchmark security of systems to document progress toward goals
- Systematic & consistent
  - Serve as quality assurance measures
  - Routinely applied after making changes

Copyright © 2015 M. E. Kabay. All rights reserved.

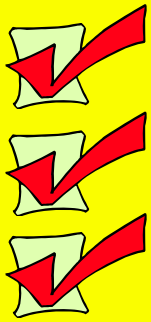
Strengths & Weaknesses of VAS (2)

- Weaknesses
- Not sufficient to secure system
- May diagnose, not fix
- If not up to date, may mislead users
- May reduce performance of operational / production network or system
- May be abused for malicious purposes

Copyright © 2015 M. E. Kabay. All rights reserved.

Roles of VA in Security Management

- When new programs are installed
- After significant changes
- During or after security incidents



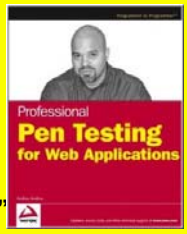
Copyright © 2015 M. E. Kabay. All rights reserved.

Penetration Testing

- Introduction to Pen Testing
- Penetration Test Goals
- Attributes of Pen Testing
- Social Engineering
- Managing Pen Testing

Copyright © 2015 M. E. Kabay. All rights reserved.

Introduction to Pen Testing



- VAS offer partial evaluation of vulnerabilities
- Actually testing for vulnerabilities by penetrating barriers is useful adjunct
- Penetration testing aka "pen testing"
- Pen testers aka "Red Team" from US Government parlance in capture/defend computer games
- Pen tests must be carefully planned & executed
- ALWAYS and ONLY with full authorization!

Copyright © 2015 M. E. Kabay. All rights reserved.

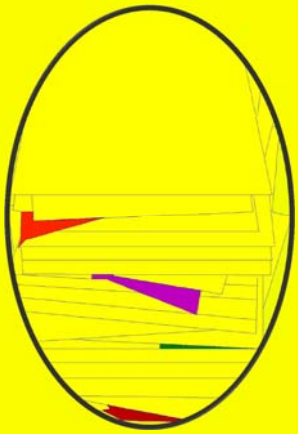
Penetration Test Goals

- Model real-world attacks closely
  - Break out of policy bounds
  - Out-of-the-box thinking
  - Criminal-hacker techniques
- Test simultaneous security measures
- Identify potential access paths missed by VAS
- BUT
  - Must not compromise production
  - Should produce unambiguous results for management

Copyright © 2015 M. E. Kabay. All rights reserved.

Attributes of Pen Tests

- Testing models
  - Zero knowledge
  - Full knowledge
- Scope
  - Physical
  - Communications
  - Systems
  - Social engineering
- Sophistication
  - Wide range of techniques



Copyright © 2015 M. E. Kabay. All rights reserved.

Social Engineering

- Trickery & deceit applied to employees
  - Often used by real criminals
  - But may have serious legal, psychological, & morale implications
- Obtain legally binding authorization
- STRONGLY RECOMMEND that organization's staff be *fully prepared to defend against social engineering attacks*
  - Otherwise will waste resources (too easy)
  - Cause guilt, embarrassment, anger, and distress in tricked employees

Copyright © 2015 M. E. Kabay. All rights reserved.

Managing Pen Testing

- Document & approve scenarios in advance
- Minimize damage to production / operations
- Do not cause distress
- Do not target / humiliate employees who have been involved in security failures!
- Don't strive to "win" at all costs:
  - "To leave a tested organization in worse condition than the test team found it is a hollow victory for all involved."

Copyright © 2015 M. E. Kabay. All rights reserved.

Review Questions

1. Distinguish between an IDS and a VAS.
2. If you wanted to check a system to see if it were protected against known attacks, would you use an IDS or would you use a VAS?
3. How do VAS support security audits?
4. In which decade were the first automated VAS developed?
5. Explain why the data store and analytical engine of an IDS should be situated off the system being monitored.
6. Compare and contrast credentialed vs. noncredentialed VAS monitoring.
7. Why should pen testers be careful in their use of social engineering?

Copyright © 2015 M. E. Kabay. All rights reserved.