

Maximising the benefits of Vulnerability Assessment

Neal Wise, CISSP CISA



a s s u r a n c e . c o m . a u

What we're covering today...

- Tips and tricks for effective Vulnerability Assessment exercises
- How to save on exercise costs
- Managing risks throughout exercise process
- Maintaining the investment made in your efforts



What is Vulnerability Assessment?

- A process by which an organization can identify and manage information security risk
- What this means in practical terms
 - Security Control analysis
 - Solution object analysis and testing of networks, systems, applications and data



VA Examples

- Penetration testing of Internet-facing network services
- Review of application code for security control adoption
- Compliance audit of technology against a defined criteria such as a public or organizational standard



Why conduct assessment?

- Obviously as a component of Risk Management
- Required by internal/external audit or regulatory body
- General Due Care
- Good technology management practice
- It's fun sometimes... :-)



When should assessment occur?

- Prior to “major change” events
- At appropriate points in the development lifecycle
 - On paper by reviewing solution designs
 - Testing during development releases (alpha, beta, etc)
 - Testing prior to production release or following production implementation (especially if staging occurs)
- Like other security maintenance efforts (patching, keeping up-to-date and informed) - on an ongoing, regular basis



The Assessment Process

- Planning for Vulnerability Assessment
- Conducting the effort
- Maintaining the effort



Planning your testing

- Determining the scope of your exercise
- Determining exercise output requirements
- Determining who will provide the exercise
- Choosing an appropriate methodology and depth of review
- Project and Risk Management and commercial considerations



Determining Scope

- The most difficult part - has a “knock on” effect on costs, progress and outcomes
- Deciding what’s in and out of scope can be an emotional and political exercise
 - Defensive Reactions & “Finger Pointing” (of all kinds)
 - Shared Infrastructure - “nobody’s problem”
 - Often ignored or accepted risk
 - Results in “Shoot the messenger” on outcomes
- Important to communicate the benefits of the outcome



Determining Scope II

- Risk Assessment helps
- If you've conducted organizational Threat & Risk Assessment you'll have a more complete understanding of your risk profile.
- Information Classification of organizational data/applications can help determine scope/review interval



Determining Scope III

- Attempt to assess the whole solution
- Assessment in parts can leave “gaps” in risk determination
- In a tiered solution assess all tiers and the environment containing the solution
- From the delivered solution function through to the solution “audience” (person, other application, 3rd party, etc) end-to-end
- Can be expensive... especially the first effort



Determining Scope IV

- If this isn't practical thoroughly assess the “riskiest parts”
 - Representative technology - 1 of n
 - Those facing uncontrolled environments (internal/external)
 - Sensitive or valuable information stores... follow the \$\$\$
 - Components which provide primary security controls
 - 3rd party solutions which make no security representations



Determining Output Requirements

- effort = time = money
- Exercise reporting will influence exercise effort
- Know your required output(s) - for example
 - Results Presentation
 - Report in assessor's format
 - Report in organization's format
 - Executive/Board reporting
 - Report for a third party (regulator, business partner, etc)



Who should conduct your review?

- Depends on the exercise “drivers” and audience for outcomes
- Some cases are pretty clear
 - Regulatory reporting usually requires an external, independent assessor
 - Regular (continuous, daily/weekly/monthly) review of the same target may be expensive to be externally provided
 - Specialist review (wireless, telephony and other enterprise infrastructure) requires specialist skills



Considerations for an internal assessor..

- “Cheaper”?
- Be wary of “conflict of interest” issues
 - Whose solution is it?
- Skill set issues
- Requires appropriate Risk Management for effort
- Often most suitable for
 - Supporting solution development effort
 - Confirmation prior to engaging external party
 - Ongoing Security Maintenance and compliance



Considerations for an external assessor...

- Also potential “conflict of interest” issues
 - Whose solution is it?
- An organization which invests in skill sets for professional services
- Liability and Risk Management more complex
- Most appropriate for
 - Independent Validation
 - Solution vetting at design phase
 - End solution confirmation



Important considerations

- Risk Management. That's what we're here for after all
 - Who is this assessor? What's their qualification, history and experience? Can I trust them with my environment?
- Perspectives
 - For external providers it's important to get a fresh perspective - not unlike a second opinion
 - Ongoing review of a stable environment will result in fewer issues over time. Is this because of maturity or a review factor such as skill depth?



Exercise Risk Management

- All Vulnerability Assessment has inherent risk. Key is recognizing it, identifying it and minimizing/monitoring
- Ensure appropriate authorization for the exercise is in place
- Ensure all 3rd parties are aware of activities and risks
 - Co-location of systems and services
 - Shared Infrastructure
 - Outsourced functions



Determining Exercise Approach

- Review vs. Penetration Test vs. Audit
 - Selection depends on what's “driving” the exercise
 - Often obvious based on goals
- Penetration Test – specific goals or targets using a “White Box” or “Black Box” methodology
- Security Review – “white glove” against best practice
- Security Audit – review using defined criteria or against frameworks/standards



Penetration Testing - “White Box”

- Intends to illustrate risks of “knowledgeable” attacker or internal fraud
- Most effective with access to knowledgeable personnel, documentation, privileged system access
- Usually conducted with organizational assistance
- Identifies/tests security controls and the state of their adoption



Penetration Testing - “Black Box”

- Intends to illustrate the ability of an outside party to gain an understanding of and access to the exercise target
- Meant to be “stealthy”
- Often conducted with 0 knowledge of exercise target
- Tests organizational reaction, event capture (logging, etc) quality and escalation more than controls



Security Review

- Utilize consensus documents, commissioning standards and other “best practice” as guidelines
- Can be technical or interview based
- Technical reviews range from remote, network-based services identification through to Build and Configuration reviews of device/system operating system build and application/functional configuration
- Examples - “best practice” Build and Configuration review of DMZ hosts and protection/detection infrastructure



Security Audits

- Audit requires thoroughness and is meant to provide a high degree of assurance.
- Most times what is called a security audit isn't
- Review against industry/international/public standards
- Review against build standards
 - Vendor recommendation
 - SANS, CSI, NSA hardening guides
 - Organisational standards such SOE



Conducting your exercise

- Managing the exercise
 - Define a schedule with aligns with the exercise scope. Follow this and notify “slippage” quickly
 - Have regular, brief updates with exercise stakeholders. A daily “heads up” of progress at the beginning or end of the day is often sufficient



Conducting your exercise

- Ongoing risk management
 - For everyone's benefit determine a suitable mechanism to capture exercise activity. This can be tricky.
 - Confidentiality - notify your assessor of who should be made aware of exercise findings and outcomes
 - Have an “information handling” process for the exercise



Maintaining the results of your efforts

- Security Maintenance
 - Remediation of Vulnerability Assessment findings
 - Patching, utilizing supportable/serviceable technology
- Building an effective internal review capability
 - Learn how to think like an attacker - lots of books and courses...
 - Learn to use tools that attackers (and security pros!) use... the basics can go a long way. Hone the “good edge” of these
 - Utilise the same approaches that work well for external providers - notification, authorization and communication



Example: Due Diligence

- Distributor approaches Assurance.com.au about supporting a product
- We receive an evaluation appliance
- 4 hours of “White Box” penetration testing later...
- more than one 0-day exploit of product resulting in remote privileged access



<see movie>

Conclusion - Savings and Benefits

- Back to basics... where is security in your development/solution design process
- Utilize a project management approach (even informal)
- Define a specific, risk-driven scope of review
- Define an exercise schedule which reflects the scope and any requirements for delivery



Conclusion - Savings and Benefits II

- Ensure those requirements (sites, documentation, access and people necessary for an exercise) are available on the scheduled dates
- Minimize out-of-hours effort
- Avoid creating scope variances if possible
- Does your organization foster a “security awareness” culture?



Conclusion

- Planning is the key to effective Vulnerability Assessment exercise
- Avoid “uncontained” scope and effort
 - Define the exact targets of review and the depth of review which is expected
 - If it isn't possible specify exactly how much time is to be utilized on each point of the scope
- Follow through on the results and manage your risk



Thank You! Questions?

