



IT Security Presentation
Vulnerability Assessments
October 16, 2002



Who I Am

Adrien de Beaupre - IT Security Specialist
(ISC)_ CISSP
SANS GSEC and GCIH
7+ Years IT and Security Experience
Sit on the SANS GCIH advisory board,
authorized grader for SANS GIAC
Member of www.whitehats.ca



Vulnerability Assessments

- ¥ Definition of vulnerability assessments
- ¥ What they are
- ¥ What they are not
- ¥ Penetration testing and security audits
- ¥ Tools, techniques and methodologies
- ¥ Conclusion



The problem

- ¥ The business issue: are the crown jewels properly protected?
- ¥ The technical issue: are the systems and networks protected as they should be?
- ¥ Audit perspective: do we meet regulatory or our own policy requirements?



Solution

- ¥ Locate the areas where an attack may be successful.
- ¥ Understand how your systems and networks look from a security perspective.
- ¥ Document and compare how things actually are as opposed to how they are supposed to be. Policy, procedures.



Formal Definition

- ¥ A vulnerability assessment is an effort to discover and document the current state of vulnerability for your environment.
- ¥ Discovering vulnerabilities with the intent to document and resolve problems.
- ¥ Improving your security



Contrast

¥ Assessment

—Locate and fix vulnerabilities

¥ Penetration testing

—An attempt to circumvent security features

¥ Auditing

—Comparing current policies and procedures for compliance with an established standard



VA

¥ An assessment is a snapshot in time.

¥ A vulnerability assessment project should not be a one time event, but an ongoing part of a security program.

¥ Over time assessments are compared with the initial baseline to evaluate success of security program.



Documentation

- ¥ The key concept is to document all aspects of your networked environment.
- ¥ You need to be aware of how vulnerable you are, where the vulnerabilities are, how to fix the problems, and have an accurate picture of systems and network security.



How to

- ¥ Plan and schedule
- ¥ Review documentation, policy and procedures
- ¥ Select tools and targets
- ¥ Run scans
- ¥ Analyze results and create report
- ¥ Fix identified problems
- ¥ Refine and repeat process



Planning

- ¥ What are we looking for?
- ¥ When and how often?
- ¥ Who should do the VA?
- ¥ From where and which tools?
- ¥ Analysis — the hard part.
- ¥ Reports, who reads them anyways?
- ¥ What next?



Methodology (1)

- ¥ Recon —network map and port scanning
- ¥ Target —key systems and services
- ¥ VA —run vulnerability scanners
- ¥ Detailed —confirm findings
- ¥ Research —Bugtraq, SANS, hack sites
- ¥ Dig deeper



Methodology (2)

- ¥ Advanced —penetration testing, war-dialing, war driving, password auditing, sniffing, running malicious code
- ¥ Analysis of results
- ¥ Reporting and recommendations
- ¥ Fix what you find
- ¥ Do it all again



Some Tools

- ¥ Port scanners:
 - nmap for *nix
 - Superscan for Windows
- ¥ Vulnerability scanners:
 - ISS, Retina, CyberCop for Windows
 - nessus for *nix
- ¥ Other specific scripts or tools
- ¥ Commercial tools VS. free



Scanners

- ¥ Running two different scanners on key systems is recommended
- ¥ Cannot rely on scanners only
- ¥ Confirm findings manually
- ¥ False positives are an issue
- ¥ What scanners don't find



Advanced

- ¥ Caveat emptor: use at your own risk
- ¥ Download and run the real exploits, malicious code, attack. Maybe test first?
- ¥ Results can be more accurate, but
- ¥ Denial of service? Buffer overflows? Trojans? Bad things can happen.
- ¥ Do you really need to actually break in?



Analysis

- ¥ What are you looking for?
 - Un-patched services
 - Badly configured servers
 - Rogue IP addresses
 - Holes in routers, firewalls and VPNs
 - Ports that shouldn't be there
 - Things that hackers/crackers are looking for
 - Anomalies
 - Systems that are already compromised (Oh Oh).



Report

- ¥ Technical or management?
- ¥ Detailed or summary?
- ¥ List all tests performed and targets
- ¥ List systems and services found
- ¥ List vulnerabilities and descriptions
- ¥ List solutions, big and small, recommended



Conclusion

- ¥ The key is not running the scanners, but analysis, documentation and problem solving
- ¥ All systems and networks should have vulnerability assessments run regularly.
- ¥ Part of a comprehensive defense in depth strategy security program.
- ¥ Should be done with proper planning, tools, methodology and expertise



Questions?



Web Resources

<http://www.cccure.org>

<http://rr.sans.org/audit/know.php>

<http://www.elytra.com>

<http://www.whitehats.ca>

<http://www.ideahamster.org>