

Information Security Vulnerability Assessment

UCLA Extension x417.86

Reg #: T5507

Instructor:

Vincent LeVeque

vleveque@sbcglobal.net

Class 1

1

Preliminaries

- Lecture notes available from UCLA bookstore
- In addition to the lecture notes, includes:
 - FFIEC Information Security Booklet, Appendix A: Examination Procedures
 - Open Source Security Testing Methodology Manual (OSSTMM) 3.0
 - NIST Special Publication 800-42, Guideline on network Security Testing

Class 1

2

Resources - Books

- **Hacking Exposed**, McClure, Scambray and Kurtz, McGrawHill Osbourne, ISBN 0-07-226081-5
- **Penetration Testing and Network Defense**, Whitaker and Newman, Cisco Press, ISBN 1-58705-208-3
- **Network Security Assessment**, McNab, O'Reilly, ISBN 0-596-0061-x
- **Inside Network Security Assessment**, Gregg and Kim, SAMS Publishing, ISBN 0-672-32809-7
- **A Practical Guide to Security Assessments**, Kairab, Auerbach, ISBN 0-8493-1706-1

Class 1

3

Resources – Web Sites

- <http://www.auditnet.org> - auditnet
- <http://www.securityfocus.com> – home of BugTraq
- <http://csrc.nist.gov/publications/index.html> - NIST publications on information security
- http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html - FFIEC publications
- <http://sectools.org/> - List of 100 top network security tools
- <http://www.nsa.gov/snac/> - NSA security site
- Others mentioned throughout

Class 1

4

Class Outline

- Security and Risk
- Security Management
- Security and Technology
- Types of Assessment
- Audits
- Security Assessments
- Vulnerability Scans
- Penetration Tests

Class 1

5

Class Scope

- Principles of information security
- Risk analysis – threats, vulnerabilities, countermeasures
- Standards for security assessments
- How different types of assessment support a security policy
- Practical methods for conducting assessments
- How to present assessment findings

Class 1

6

Security and Risk

Class 1

7

Information Security Concepts

- Information has value
- This value must be protected
- A risk analysis helps determine how much protection of what type
- Protection is multi-layered
- Protection includes:
 - Human behavior
 - Technical protections
 - Physical security
 - Good management practices for all of the above

Class 1

8

Assessments and Risk

- Information has value
- This value must be protected
- A risk analysis helps determine how much protection of what type is necessary
 - What's broken
 - How should it be fixed

Class 1

9

Assessments and Risk

- Protection is multi-layered
 - Failure of one protection by itself should not leave systems at risk
 - “Defense in depth”
- Related – compensating controls
 - Compensate for lack of countermeasures in one area by different countermeasures in another

Class 1

10

Assessments and Risk

- Protection includes:
 - Human behavior
 - Technical protections
 - Physical security
 - Good management practices for all of the above
- A security plan should cover all relevant protections
- A security assessment should evaluate all relevant protections

Class 1

11

Information Value

- Information is protected because it has value
- You should not spend more protecting something than what it is worth
- It is foolish to save pennies while risking thousands of dollars in value
- If information was without value, you wouldn't be taking this class

Class 1

12

Information Value

- What is information worth?
 - Replacement value, what would it cost to replicate the information
 - Market value, what could the information be sold for
 - Utilitarian value, how does the information facilitate value creating processes
 - Criminal value, what would it be worth to someone who steals it

Class 1

13

Protecting Information - CIA

- In what ways must information be protected?
 - Confidentiality – prevent unauthorized disclosure
 - Integrity – ensure information is internally consistent and reflects the real world accurately
 - Availability – information is there when you need it

Class 1

14

Protecting Information - CIA

- Some additional protection categories
 - Non-repudiation – Sender of information can't deny having
 - Accountability – Ability to trace actions to a specific individual
 - Authentication – Ability to verify identity (of individual, system, program, etc.)
 - Utility – Information or system maintains its usefulness
 - Possession – Control over information

Class 1

15

Protecting Information

- A security assessment will review
 - Why information has value to the organization
 - What are the sources of that value
 - How that value can be attacked
 - Confidentiality
 - Integrity
 - Availability
 - What protections (“countermeasures”) are in place to counter attacks
 - How effective are these protections
 - What could be done to improve these protections

Class 1

16

Risk Assessment

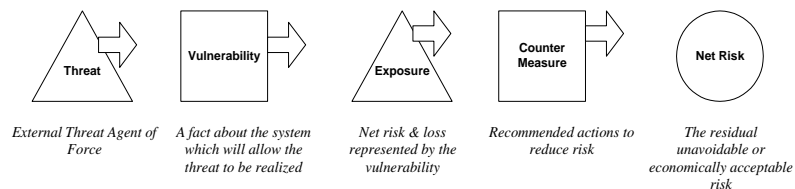
- A security assessment implies a risk assessment
- The assessment includes answers to these questions:
 - To what extent are your information resources at risk?
 - What are the sources of risk?
 - What are the consequences of risk? What can you lose?
 - What will it cost to mitigate risks?

Class 1

17

Risk Assessment

- Classic model:



Class 1

18

Risk Assessment

- Threat
 - An event that can compromise a system's security
 - Intentional threats are planned and executed by threat agents
- Vulnerability
 - A weakness in security controls that allows a threat to be realized
- Exposure
 - Extent to which information may be exposed due to existing threats and associated vulnerabilities
- Countermeasure
 - Controls that reduce exposure, by countering either vulnerabilities or threats
- Net Risk
 - What you have to live with after implementing all feasible countermeasures.

Class 1

19

Risk Assessment Example

- Threat
 - Criminals want to break into our ecommerce server, steal the customer database, and sell the credit card numbers on the black market
- Vulnerability
 - Flaw in Web server software allows downloading back end data
- Exposure
 - While source code for exploit of flaw has not been published, it is reasonable to assume a criminal organization could figure out how to do it
- Countermeasure
 - Encrypt credit card numbers
 - Keep credit card numbers entirely off line
- Net Risk
 - Encryption could be flawed
 - An exploit unknown to us could be used
 - An insider could steal off line data

Class 1

20

Risk Assessment Example

- Threat
 - What threats are credible? What resources do these threat agents have at their disposal
- Vulnerability
 - Given a thorough review of our technology, management systems, and culture, what flaws exist that a threat agent could exploit?
- Exposure
 - Given the resources available to a threat agent and their goal, can they feasibly exploit the vulnerability?
- Countermeasure
 - Given the value of the information at risk and the consequences of a compromise, what resources should we expend protecting it?
- Net Risk
 - After implementing all feasible counter-measures, what remaining methods could be used by the threat agent to accomplish their goals? How have our protections made a successful exploit less likely?

Class 1

21

Process-based Risk Models

- More detailed process-based models:
 - An attack is a sequence of activities
 - Countermeasures can guard against any point in this sequence
 - Helps to model:
 - Defense in depth
 - Compensating controls



Class 1

22

Risk Assessment

- Example Attack Methods
 - Malicious software distributed by email
 - Guessing a password to a service
 - Using a software flaw to obtain unauthorized access
 - Digging through trash to find sensitive hardcopy information
 - Using a pretense to talk sensitive information out of its possessor

Class 1

23

Risk Assessment

- Example Vulnerabilities
 - Easily guessed passwords
 - Software flaws that allow unauthorized access
 - Critical systems in physically unsecured places
 - Sensitive documents thrown away in public trash bins
 - Users that open all email attachments

Class 1

24

Risk Assessment

- Example Countermeasures
 - Enforce strong passwords
 - Have a program to patch software flaws promptly and consistently
 - Move all critical systems to a secure facility
 - Shred sensitive documents before trashing
 - Train users not to open unexpected email attachments

Class 1

25

Risk Assessment

- Some risk assessment methodologies
 - OCTAVE, Developed by CERT (Carnegie Mellon SEI)
 - NIST SP 800-30, Risk Management Guide for Information Systems

Class 1

26

Risk Assessment

- OCTAVE
 - Developed by CERT (Carnegie Mellon SEI)
 - Risk based approach to security strategy
 - Identify information assets and vulnerabilities, assess risks, develop security plan
 - See http://www.cert.org/octave/approach_intro.pdf

Class 1

27

Risk Assessment

- NIST SP 800-30, Risk Management Guide for Information Systems
 - Guidance for risk assessment across entire system lifecycle
 - Very similar in approach to Octave, but not quite as detailed and more suited to a government environment

Class 1

28

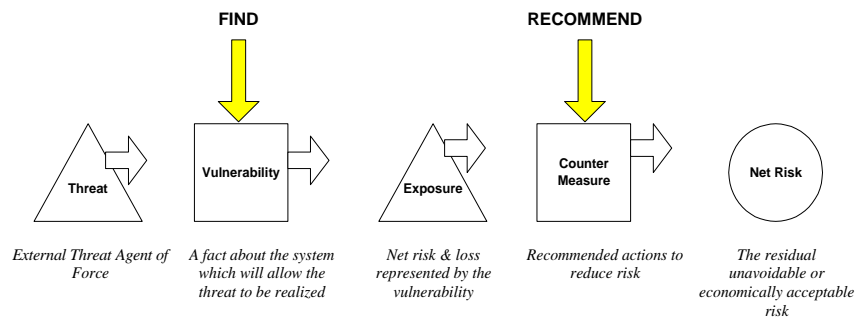
Risk Assessment

- Assessments of all types boil down to an evaluation of risk:
 - For feasible threats, what are the vulnerabilities the threat agent could exploit?
 - For each vulnerability, what are recommended countermeasures?
- Even assessments driven by standards compliance are implicitly threat based

Class 1

29

Risk Assessment



Class 1

30

Audits, Assessments, and Risk

- Find vulnerabilities that can leave information at risk
- Different types focus on different types of risk
- Vary in terms of breadth and depth
- Standards compliance vs. custom risk profile

Class 1

31

Audits, Assessments, and Risk

- Audit
 - Failures in management systems
- Security assessment
 - Failures in the technical configuration of components
- Vulnerability Scan
 - Failures in the network-visible configuration of large groups of components
- Penetration test
 - Failures that allow a dedicated attacker to achieve a specific goal

Class 1

32

Audits, Assessments, and Risk

- Find vulnerabilities that can leave information at risk
- Different types focus on different types of risk
- Vary in terms of breadth and depth
- Standards compliance vs. custom risk profile