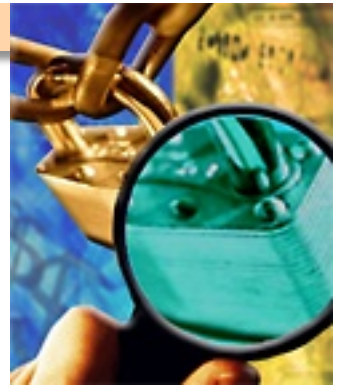
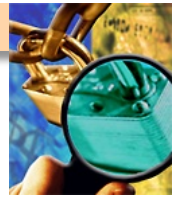


Terms, Methodology, Preparation, Obstacles, and Pitfalls

Vulnerability Assessment Course

All materials are licensed under a Creative Commons “Share Alike” license.



- **http://creativecommons.org/licenses/by-sa/3.0/**

You are free:

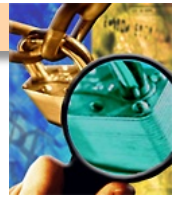
to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.



Agenda

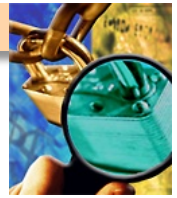
- Terminology
- Methodology
- Preparations
- Obstacles and Pitfalls

Terminology

- A constant source of confusion
- The need to use commonly understood terms
- What does the system owner want to accomplish?

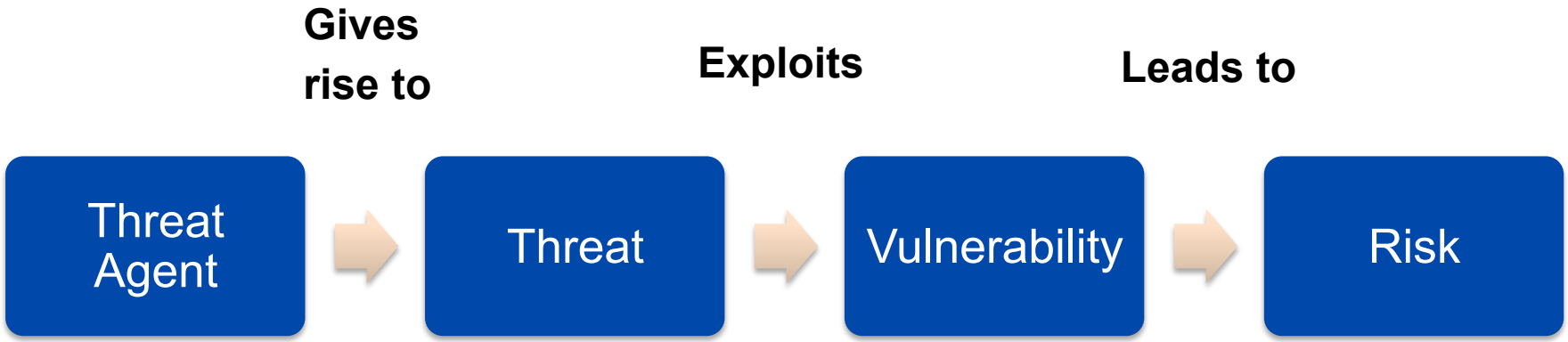
Let's attempt to clarify what each of these are:

- Vulnerability Assessment
- Security Test and Evaluation
- Penetration Testing
- Compliance Assessment



Before We Get Started

- Threat – any potential danger to information or systems
- Vulnerability – software, hardware, procedural, or human weakness that may provide an attacker unauthorized access to resources
- Risk – likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact



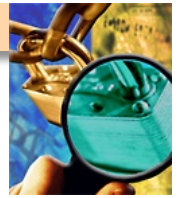
Vulnerability Assessment

- Focused assessments on the adequacy and implementation of technical, operational, and management security controls
- Based on an assessment methodology
- Strives to identify all vulnerabilities present in the system and its components
- Contributes to risk management
- Full knowledge and assistance of systems administrators
- No harm to systems

Security Test and Evaluation

- Linked to Authorization to Operate
- Set of specific tests designed to evaluate the security requirements of the system
- Based on Security Requirements Traceability Matrix (SRTM)
- Governed by a formalized test plan
- Full knowledge and assistance of systems administrators
- No harm to system

Penetration Testing

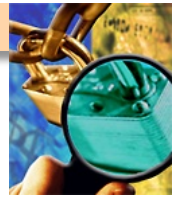


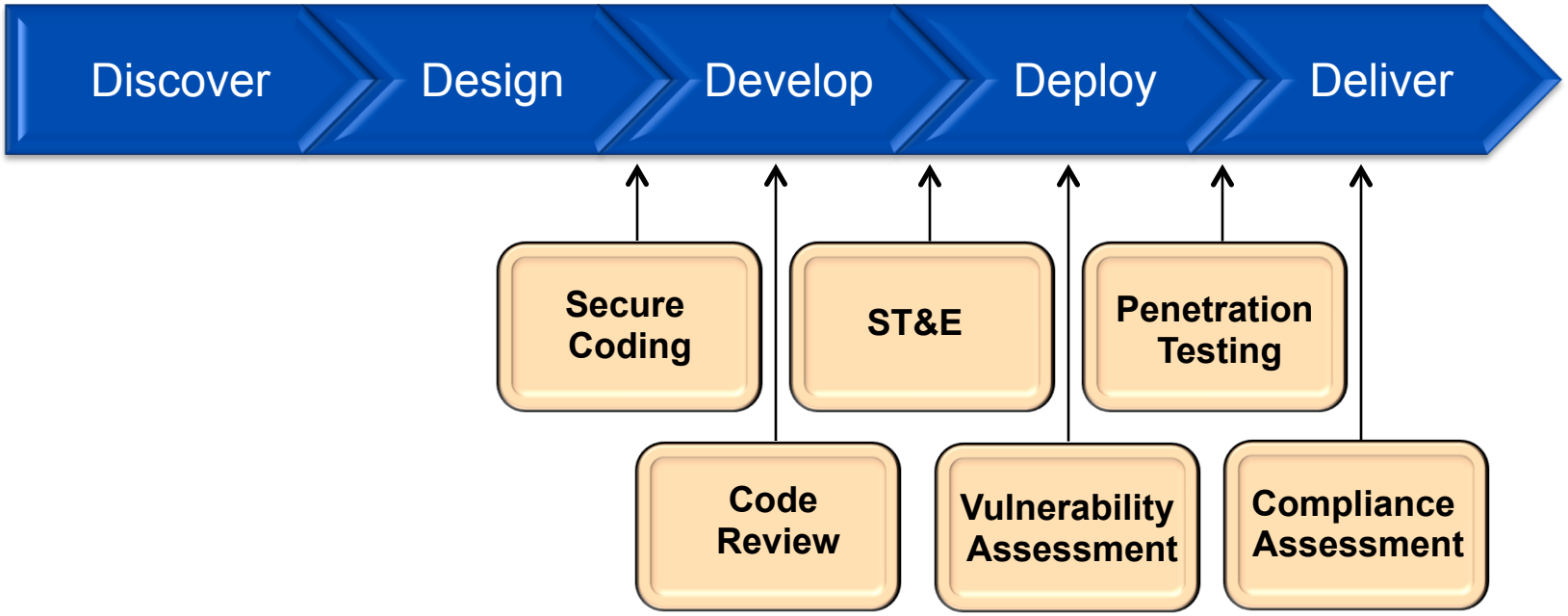
- Most often misused term
- A number of different meanings
  - Product-focused vulnerability assessment
  - Role-based assessment
- Potential Goals
  - Develop network defenders
  - Develop an understanding of the inherent weaknesses of a technology
  - Develop a risk profile based on an individual or group
  - Warm fuzzy feeling
- Limited or no knowledge of systems administrators
- May harm systems and components
- Clean up may be necessary

Compliance Assessment

- An evaluation designed to determine the system's compliance with a body of regulation
- Based on:
  - IT Policy
  - Security Policy
  - Security Technical Implementation Guides (STIGs)
  - Security Catalogs
- Internal Control Reviews (OMB Circular A-123)
- Compliance can be determined by multiple methods
  - Hands-on testing
  - Interview key personal
  - Examination of relevant artifacts

Security in the SDLC



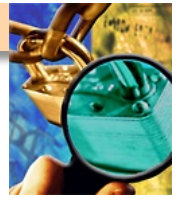


Vulnerability Assessment Methodology

- A disciplined process, not a game
- A predictable, repeatable process

- Methodology
  - Phase 1 – Planning
  - Phase 2 – Information Collection
  - Phase 3 – Enumeration
  - Phase 4 – Testing and Evaluation
  - Phase 5 – Reporting

Phase 1 – Planning



Defines the goals and activities of the assessment, and requires coordination of all involved parties

- **Security Policy Review**
- **Security Requirements Review**
- **Threat Assessments**
- **Premise and Scenario**
- **Goals and Timelines**
- **Rules of Engagement**
- **System and Network Review for Scope and Resources**

May include one or more meetings with security personnel, functional business owners, system owners, developers, operators, etc.

It is just as important to communicate requirements for systems information

Phase 2 – Information Collection

Before any meaningful assessment can be conducted, thorough research must be performed against the target

Data gathered is analyzed as the assessment proceeds and when the assessment is complete

- Information Gathering & Reconnaissance
- Information Analysis
- Exploit Research
- Request Additional Information

Phase may be revisited as necessary

Phase 3 – Enumeration

Activities provide specific information about targets of the assessment

Depending on the scope of the activity, enumeration can be conducted at the application and/or network level

- Network Discovery
- Port Scanning
- OS Fingerprinting
- Services Probing
- Vulnerability Scanning
- Host-based Scripts
- Manual Vulnerability Testing & Verification
- Applications Enumerating

This information is often collected using software tools

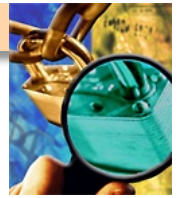
Phase 4 – Testing and Analysis

Activities typically involve both automated testing of security vulnerabilities via software tools and evaluation of particular aspects of the organization's security policies and practices by assessment team members

- **Applications Testing**
- **DBMS Testing**
- **Web Server & System Review**
- **Firewall & IDS Testing**
- **Other Network Component Configuration Review**
- **Network Services**
- **Anti-Virus Software and Patch Distribution**
- **Results and Script Output Analysis**

Goal is to apply experience and insight to identify security vulnerabilities

Phase 5 – Reporting



Phase consolidates all findings into the final output

Output includes reports providing detailed findings, the impact of each vulnerability and actionable recommendations

May include summary briefings

- Development of Findings
- Characterization of Findings
- Prioritization of Findings
- Consolidation and Ordering
- Reports Generation

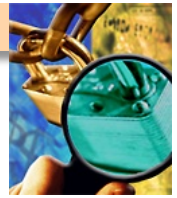
Preparations

- Initial estimate and feasibility
- Information gathering
- Developing scope and timeline
- Team development and staffing
- Rules of Engagement
- Individual preparation and analysis

Initial Estimate and Feasibility

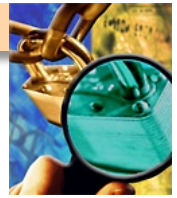
- A management function
- Gather enough information to determine
  - What the system owner wants or needs
  - Availability of resources
- Used to create a technical proposal and cost estimate
- Select a test lead
- Initial staffing assignment
- A cause of many problems

Information Gathering



- Develop a list of needed information
  - Systems Security Plans
  - Security Concept of Operations
  - Threat Assessments
  - Relevant certification and accreditation artifacts
  - Inventories
  - Network diagrams
  - Accounts
- Relevant policies and regulations
- Reconnaissance
  - On-site visits or interviews
- Needed to develop scope
  - A source of many problems and misunderstandings
  - Essential to the success of the assessment

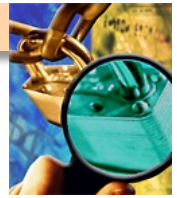
Developing Scope



- A critical exercise that affects
  - Team size
  - Staffing
  - Duration of test
  - Rules of engagement
- Must be developed as soon as possible
- Define what needs to be assessed
- Precursor to detailed assessment timeline
- Need for system owner agreement
- Eliminates confusion
- Contributes to the success of the engagement
- Often poorly defined

Team Development and Staffing

- Based on test scope
- Numbers of test personnel required
- Skill sets needed
- Time required on site
- Limited by time, money, availability



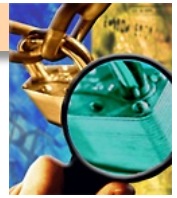
Rules of Engagement

- Authority to test
- Authorized assessment activities
- Assessment limitations
- Test schedule
- Test duration
- Personnel involved
- Location of testing
- “Get Out of Jail Free Card”

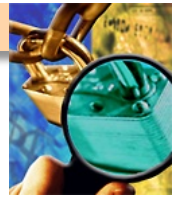
Individual Preparation and Analysis

- Prepare for the assessment in advance
- Review relevant documentation
- Research vulnerabilities and known exploitations
- Develop a list of additional information and documents
- Practice phases of the assessment
- Prepare for interviews
- Analyze script outputs, if available
- How much time is needed?
- Back-to-back assessments hinder individual preparation

Obstacles and Pitfalls

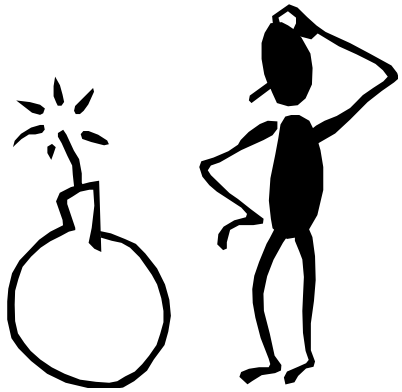


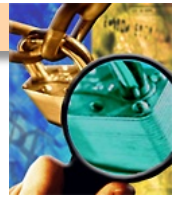
- To discuss common impediments to completing the vulnerability assessment
  - Obstacles – created by the environment, system owner, or vendor
  - Pitfalls – self-inflicted wounds and mistakes
- To discuss possible methods of avoiding or overcoming common obstacles and pitfalls



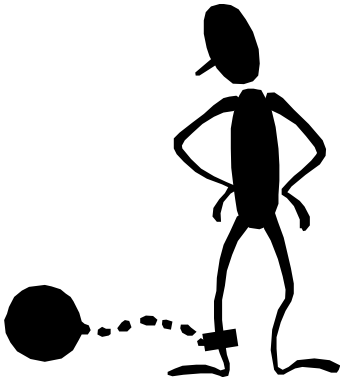
Obstacles

- The “Waiting Game”
- “I don’t understand”
- Scope is inaccurate
  - More systems than previously reported
  - Unanticipated technology
- Inaccurate network diagrams
- Documentation not available
- Data not provided
- Appropriate connectivity not provided
- Systems administrators lying, changing data outputs, or making corrections and re-running scripts
- Argumentative systems owners and administrators
- Asked to change a finding
- *Others...*





Pitfalls



- Poorly defined scope
- Coming in blind
- Not anticipating common delays
- Relying too heavily on tools
- Relying on a checklist
- Relying on a script
- Reporting false positives
- Not providing the impact of a finding
- Inaccurately characterizing the risk
- No network cable, power cord, other equipment
- Temptation to change a finding
- Arguing with a systems administrator
- *Others...*

Questions