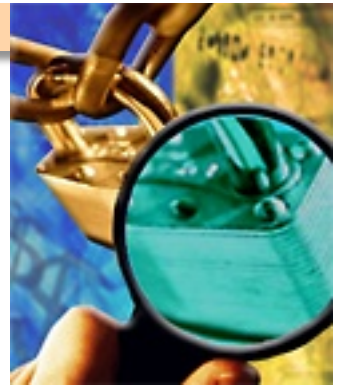
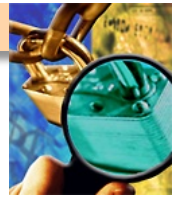


Findings

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

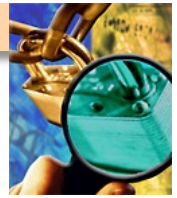
Under the following conditions:

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.

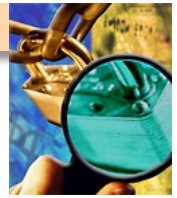
Agenda

- Developing the perfect finding
- Describing the Finding
- Describing the Impact of the Vulnerability
- Providing Actionable Recommendations
- Characterizing the Finding



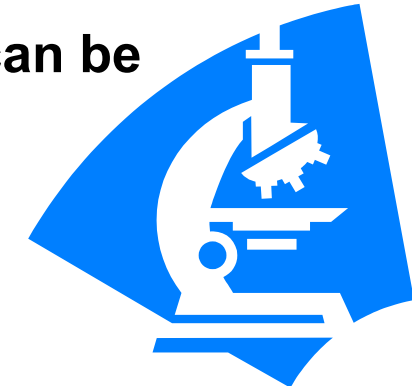
The Perfect Finding

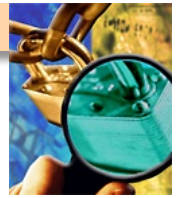
- Several different formats
- All typically provide three essential elements
  - Description
  - Impact
  - Recommendation
- Optional characterizations
  - Risk Level
  - Ease of Fix
  - Level of Effort
- Other Information



Description

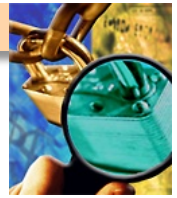
- The observation
- Describe the vulnerability, mis-configuration, or compliance issue that was observed
- How was the observation made?
  - Analysis of script output
  - Results of automated scanning
  - Manipulation of parameters
- Affected systems
- Provide enough information that the finding can be duplicated or retested





Impact

- Provide enough information to define the risk to the system or its components if the vulnerability is exploited
- Address important information security concerns
  - Confidentiality
  - Integrity
  - Availability
- Dependency on other conditions
- Transitive risk
- Describe the negative affect if the finding is left uncorrected



Recommendation

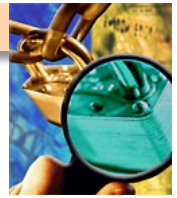
- Provide detailed actionable remediation
- Eradication versus Mitigation
- Provide alternatives if they are available
- Only the System Approving Authority can accept risk

Characterizations

Characterizations provide a means for prioritization, grouping, and management

- **Risk Level (or Severity Code)**
- **Ease of Fix**
- **Estimated Work Effort**
- **Other useful descriptors and tags**

Risk Level – Federal Civil Agencies

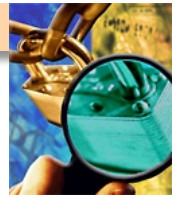


The Risk Level is, in actuality, an assessment of the priority with which each Business Risk shall be viewed

The Risk Level takes into account many factors including information at risk, ease of exploitation, exposure level of the vulnerability, and other situational factors

- **High**
- **Moderate**
- **Low**

High Risk Level



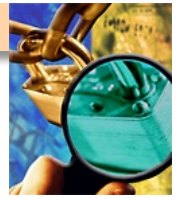
- Exploitation of the technical or procedural vulnerability will cause substantial harm
- Significant political, financial, and/or legal damage is likely to result
- The threat exposure is high, thereby increasing the likelihood of occurrence
- Security controls are not effectively implemented to reduce the severity of impact if the vulnerability was exploited
- Vulnerabilities that allow an attacker immediate access into a machine, allow privileged access, or bypass a firewall
- Vulnerabilities that provide information that has a high potential of giving access to an intruder

Moderate Risk Level

- Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data
- Exploitation of the vulnerability may cause moderate financial loss or public embarrassment
- The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence
- Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur
- Vulnerabilities that provide information that potentially could lead to compromise
- The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal

Low Risk Level

- Exploitation of the technical or procedural vulnerability will cause minimal impact to operations
- The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise
- Exploitation of the vulnerability may cause slight financial loss or public embarrassment
- The threat exposure is moderate-to-low
- Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur
- Vulnerabilities, when resolved, will prevent the possibility of degraded security
- The vulnerability is such that it would otherwise be considered Moderate Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal



Ease of Fix

The Ease of Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability

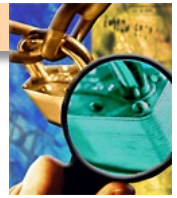
- **Easy**
- **Moderately Difficult**
- **Very Difficult**
- **No Known Fix**

Estimated Work Effort

The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions

- **Minimal**
- **Moderate**
- **Substantial**
- **Unknown**

Other Information



- Security Reference
- Source of the finding
- Numbering scheme
- Status

Questions