SACM Vulnerability Assessment Scenario

IETF 94

11/05/2015

What is it?

- Walks through an automated enterprise vulnerability assessment scenario
- Begins with an enterprise ingesting a vulnerability report (i.e., security advisory) and ends at the point of identifying affected endpoints
- Aligns with the SACM "Endpoint Security Posture Assessment: Enterprise Use Cases" [RFC7632] and builds upon the usage scenarios described in the RFC
- The term "vulnerability report" is intended to mean: "A publication intended to alert enterprise IT resources to the existence of a flaw or flaws in software, hardware, and/or firmware, which could potentially have an impact on enterprise functionality and/or security."

Purpose

- Provides a detailed scenario and vision for enterprise vulnerability assessment that can be used as a core narrative
- Identifies aspects for use in the development of the information model
- Defines the classes of data, major roles, and a high-level description of role interactions
- Helps to further inform engineering work on protocol and data model development
- Part of the overall goal of breaking the SACM problem space into smaller and more manageable pieces

Scope and Assumptions

- Does not attempt to cover the security disclosure itself and any prior activities of the security researcher or discloser
- Assumes the vulnerability report contains all information necessary to identify affected endpoints within an organization
- Assumes the vulnerability report data has been processed into a format that the enterprise security software tools can understand and use
- Assumes the enterprise has a means of identifying and collecting information from their enterprise endpoints

Endpoint Identification and Initial (Pre-Assessment) Data Collection

- First step of the process
- Identifies and collects basic information from enterprise endpoints
  - Network identity
  - Operating system and patch level
  - Installed software inventory
  - …
- Occurs before receiving and processing any vulnerability reports
- Information should be stored within a CMDB
- Information obtained could be used by other enterprise processes, such as configuration and license management

Vulnerability Reports and Endpoint Applicability and Assessment

- Vulnerability reports are received and tagged (e.g., internal ID) by the enterprise and stored for immediate or later use within a CMDB
- Report versions are tracked in the event that reports are updated at a later date
- In many cases, applicable or affected endpoints can be determined using the previously collected basic information and software inventory. No further assessment of data collection needed.
- If required, a secondary assessment is used to collect additional information such as:
  - Files and their attributes
  - Text configuration file settings
  - Windows registry queries
  - …

Assessment Reports

- The results that determine which enterprise endpoints are applicable to the vulnerability report

- Essential data items include (not the complete list):
  - Endpoint ID
  - Vulnerability report
  - Date of assessment
  - Age of collection data
  - …

Appendix

- Additional processes that have not been integrated into the overall document
  - Continuous Vulnerability Assessment – timing of assessments (e.g., initial assessments, reassessments, etc.)
  - Priority – vulnerability reports and the remedies
- Data attribute table and definitions
  - A table of all discussed data attributes and where they are used, followed by their definitions
- Alignment with other works
  - The Council on CyberSecurity's Critical Security Controls
    - CSC 1 Inventory of Authorized and Unauthorized Devices
    - CSC 2 Inventory of Authorized and Unauthorized Software
    - CSC 4 Continuous Vulnerability Assessment and Remediation

Appendix (continued)

- Alignment with SACM Usage Scenarios
  - Automated Checklist Verification (2.2.2)
  - Detection of Posture Deviations (2.2.3)
  - Asynchronous Compliance/Vulnerability Assessment at Ice Station Zebra (2.2.5)

- Future SACM work items
  - See next steps and technical standards development on the following slide

Next Steps

- Get feedback and thoughts on the current draft

- Develop technical standards to support automation of facets of this scenario
  - Software inventory (e.g. ISO SWID)
  - Endpoint applicability (e.g. NIST CPE)
  - Vulnerability Report Data Format (e.g. ICASI CVRF)
  - Assessment Result Reporting (e.g. NIST ARF, ASR)
  - Human-assigned endpoint attributes (e.g. NIST AI)
  - Others?