Security Assesment

by
Ramraj S ME.,
Assistant Professor
Department of Software Engineering

28 - Mar -2016

Agenda

- Introduction
- Methodology
- Technical Assesment Techniques
- Non-Technical

Introduction

An information security assessment is the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, personknown as the assessment object) meets specific security objectives. Three types of assessment methods:

- Testing
- Examination
- Interviewing

Methodology

Repeated and Documented Security Assesment Methodology is beneficial because it can

- provide consistency
- provide structure
- provide easy understanding for the new staff
- address various constraints.
- Easy to resuse the various resources

Phases

- Planning - information about assets, its security threats and security control mechanism
- Execution - identify vulnerabilities and validate
- Post-Execution - To identify the root cause of the vulnerabilities identified in the execution phase.

Techinical Assesment Techniques

- Review Technique
  - applications,networks, policies, and procedures are assessed
  - manual method

,

- Target Identification and Analysis Techniques
  - network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security examination.
  - automated method with tool (may be performed manually)
- Target Vulnerability Validation Techniques
  - password cracking, penetration testing, social engineering, and application security testing
  - automated method with tool (may be performed manually)

Non-Techinical Security assesment

- Security threats related to physical activity
- example - attempting to circumvent locks, badge readers, and other physical security controls, typically to gain unauthorized access to specific hosts

References I

[1] Karen Scarfone Murugiah Souppaya Amanda Cody Angela Orebaugh
"Technical Guide to Information Security Testing and Assessment "

Thank you