Vulnerability Testing Process

By Gregory Yhan CISSP, CISM

eMail: info@androidsecurity.com

TABLE OF CONTENTS

1. NETWORK SECURITY TESTING

1.1 Purpose

This document is a sample of a vulnerability testing process for a fictitious company, Company X. It outlines Company X's technical security testing process. The key deliverable is to take a risk base approach to identifying and validating system vulnerabilities.

To successfully obtain this key objective, any vulnerability testing must follow a standardized process methodology. The methodology must incorporate the following:

Adaptable: The Vulnerability Test Process is adaptable to various types of security testing, including password cracking, network discovery and penetration testing.

Auditable: The Vulnerability Test Process is documented and has defined objectives.

Repeatable: The Vulnerability Test Process is repeatable to ensure consistency across all vulnerability testing initiative.

2. ROLES AND RESPONSIBILITIES

2.1 I.T Manager

1. Authorize all security assessment activities.
2. Review all vulnerability-scanning reports.
3. Assign roles and responsibilities for performing security assessments.
4. Assign roles and responsibilities for mitigating risks.

2.2 Assessor

1. Inform the appropriate parties—such as information security, management, system administrators, and users—of security assessment activities.
2. Execute examinations and tests, and collecting all relevant data.
3. Conduct additional examinations and tests when needed to validate mitigation actions.
4. Collaborate with Information Security to develop an assessment plan for all vulnerability testing.
5. Keep a log that includes assessment system information.

2.3 Information Security

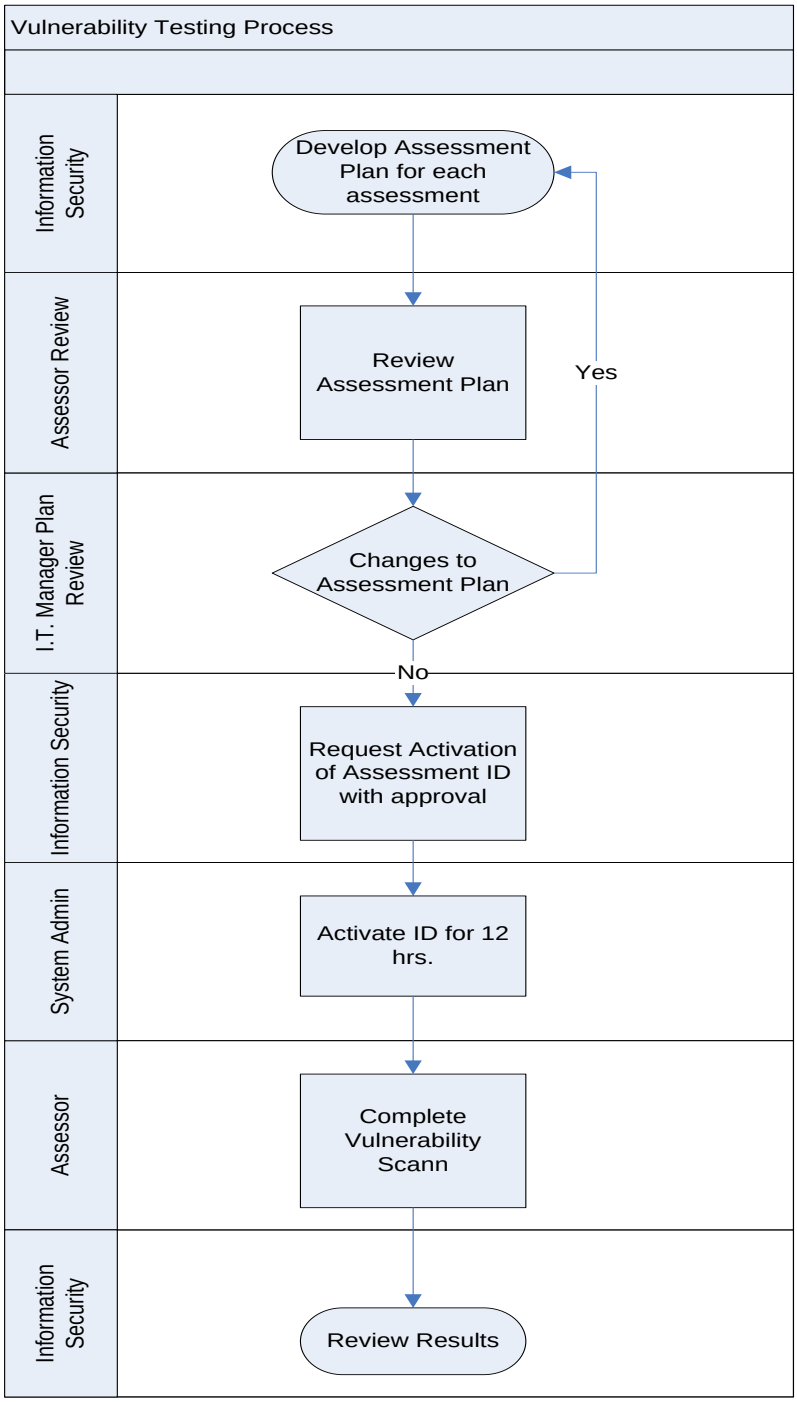
1. Analyze collected data and develop mitigation recommendations.
2. Develop an assessment plan for all vulnerability testing activity.
3. Determine system impact rating.
4. Develop an Assessment Plan for vulnerability testing.

2.4 System Administrators

1. Activate vulnerability scanning ID when vulnerability scans are scheduled.
2. Deactivate vulnerability scanning ID when a scheduled vulnerability scan is completed.
3. Fix vulnerabilities.

3. PROCESS

3.1 Process Flow



3.2 Assessment Plan

The assessment plan will provide structure and accountability to the vulnerability-testing program. Information Security function and the assessor will develop this plan for each vulnerability assessment test. This will be apart of the vulnerability testing documentation. Sign-off from the I.T Manager will be required.

The assessment plan will answer these basic questions:

- What is the scope of the assessment?
- Who is authorized to conduct the assessment?
- What are the assessment's logistics?
- How should sensitive data be handled?
- What should occur in the even of an incident plan?

3.3 Request ID activation

After sign-off of the Assessment Plan is received from the I.T. Manager, the information security function will request the vulnerability testing ID be activated for a period of 12 hours. Following this timeframe, the ID should be immediate deactivated.

3.4 Review Results

The Information Security function will review the results of any vulnerability testing. Results will be review with the assistance from various SME's. A recommendation regarding any vulnerabilities identified will be made to the I.T Manager. Resources will be assigned by the I.T manager to address vulnerabilities.

3.5 Remediation

A remediation plan will be developed and implemented for each scanned results. The plan will outline roles, responsibilities and deadlines for remediation. The I.T manager will assign the appropriate resources to address any vulnerability recommended for remediation by I.T security. The following is a schedule for remediating vulnerabilities base on impact and severity rating:

Remediation schedule:

Priority Matrix		Vulnerability Score		
		Low Severity	Medium Severity	High Severity
Impact	Low	Fix within One Year	Fix within One Year	Fix within Six Months
	Medium	Fix within One Year	Fix within Six Months	Fix within One Month
	High	Fix within Six Months	Fix within One Month	Fix within One Month

4. SCHEDULE

4.1 Testing schedule

Vulnerability testing is scheduled base on system impact and vulnerability score. In this context, impact means the overall affect on a Company X system, if such system was compromised. The vulnerability score is the result of the last vulnerability test.

Examples of **High impact** systems include:

- Firewalls, routers, and perimeter defense systems such as for intrusion detection,
- Public access systems such as web and email servers,
- DNS and directory servers
- Database servers with confidential client data.

The following table outlines the timing for the next review. The timing of the next review is dependent upon two things:

1. The criticality of the system.
2. The Vulnerability Severity rating

Priority Matrix		Vulnerability Score		
		Low Severity	Medium Severity	High Severity
Impact	Low	One Year	One Year	Six Months
	Medium	One Year	Six Months	One Month
	High	Six Months	One Month	One Month

5. ASSESSMENT PLAN TEMPLATE

Assessment Overview:	
What is the scope of the assessment?	
Who is authorized to conduct the assessment?	
Please list systems and networks authorized to be examined (e.g. system name, IP addresses or address ranges):	
Assessment Type:	
Please outline the type and level of testing being performed (e.g. port and service identification, vulnerability scanning):	
Logistical Details:	
Assessment schedule date:	
Physical location where assessment activities will originate:	
Please list equipment and tools that will be used to conduct the assessment:	
Are there any requirements to inform parent organization?	
Who is responsible for informing the parent organization?	
Incident Handling:	
Primary and alternate points of contact for the assessor:	
Sign off:	
Nenad Vitas or Fernando Da Silva _____	**I.T. Manager**
Sergei Myrox _____	**Assessor**
Gregory Yhan _____	**Information Security**