**Standard Operating Procedure**

**Procedures for Security Penetration Testing**

**1.0 Introduction**

A Penetration test is an activity in which a test team attempts to evade the security processes and controls of a computer system. Posing as either external or internal unauthorised intruders, the test team will try to obtain access, extract information and also demonstrate the ability to manipulate the target computer in unauthorised ways.

Due to the delicate nature of the testing, specific rules of engagement are necessary to ensure that testing is done in a manner that minimises impact on the Bank’s operations to the barest minimum while maximizing the importance of the test results.

The tool Kali Linux will be used to perform this exercise, Kali Linux contains a large amount of penetration testing tools from various different niches of the security and forensics fields.

**1.1 Purpose**

The purpose of this SOP is to lay out the procedures and establish the rules of engagement for when penetration tests are performed on the Bank’s assets.

**1.2 Scope**

The scope of the penetration test is all the Bank’s I.T asset ranging from servers, workstations and network devices, this can also differ with the nature of the test.

**1.3 Roles and Responsibilities**

|  |  |  |
| --- | --- | --- |
| **S/N** | **Role** | **Responsibility** |
| 1 |  | * Be responsible for coordination/supervising of the penetration test activities and schedules, and notify of planned activities. * Coordinate the penetration test with the Penetration tester. * Be the recipient of all data generated by and related to the Security Penetration test. * Shall be responsible for ensuring that all data related to the IT Security Penetration test for each site are removed from the Pen Tester's computer(s) by a method approved by the Bank (in the case where an external party performs a white box test). |
| 2 |  | * Develop the documentation and plans for the penetration test. * Identify estimated dates upon which the milestones will be completed, and indicate the critical path. * Identify the steps that will be taken to protect the Test Plan, results, and final deliverables. * Assure that all pertinent reports, logs, test results, working papers and data related to the penetration test are being generated and maintained, and are being stored appropriately. |

* 1. **Process**

1. **Planning and Enumeration**

• Identify Scope and Goals of the Exercise

• Enumerate the Boundary of the Testing

• Develop Rules of Engagement

• Conduct penetration testing with the pen test team, red team. (e.g. reconnaissance, exploitation of vulnerabilities, intrusion, compromise, analysis and recommendations)

• When a vulnerability is exploited, describe the actions to be taken such as: issuing a "Stop Report" stopping further exploiting the system unless the approved

• How findings, risk impacts, and recommended corrective actions will be reported: such; daily and weekly reports unless high risk which will be report immediately

• Conduct technical presentation to CISO on test findings, methods, and approaches.

1. **Vulnerability Analysis**

• Identify Targets

• Identify Potential Vulnerabilities

• Perform Vulnerability Scans

• Buffer overflows

• Improperly configured network services

• Improperly configured trust relationships

• Insecure authentication mechanisms

• Outdated network services that have known vulnerabilities

• Apply enumeration data in searching vulnerable databases

• Perform manual tests

• Password guessing

• IP spoofing

• Social engineering

**C. Penetration Testing**

• Research and develop attack scenarios

• Execute attacks

• Record results

• Report exploitable vulnerabilities

• Analyse penetration testing results and if indicated, perform additional exercises

• Recommend counter measures

1. **Analysis and Reporting**

* Summary of any successful penetration scenarios
* Detailed listing of all information gathered during penetration testing
* Detailed listing of all vulnerabilities found
* Description of all vulnerabilities found
* Suggestions and techniques to resolve vulnerabilities found

1. **Cleaning Up**

The cleaning up process is done to clear any mess that has been made as a result of the penetration test. A detailed and exact list of all actions performed during the penetration test must be kept. This is vital so that any cleaning up of the system can be done.