STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Highly Restricted

Title:	**Testing Segregation of TRE Projects**
Effective Date:	**14 Feb 2019**
Reference Number:	**SOP-09-18**
Version Number:	**1.3**
Owner:	**TRE Infrastructure and Security Management Process Owner,**
Review Date:	**15 Jun 2020**

Table of Contents

1. Purpose

This document provides guidance for the testing of adequate isolation of virtual machines that form part of TRE projects.

The Trustworthy Research Environment (TRE), and all systems contained within, is involved in handling information that must be managed in a way that ensures its confidentiality, availability and integrity. Implementing security controls throughout the lifecycle of a system can help the TRE achieve its ISMS objectives, regulatory requirements and the needs of its users.

2. Scope

Threats corresponding with an established connection to a virtual machine running in the TRE.

3. Responsibilities

The ISMS Sponsor is responsible for:

- Providing authorisation for emergency decisions

The Information Security Manager (ISM) is responsible for:

- Escalating security incidents to IG SIRI if applicable

Members of the Information Security Steering Group (ISSG) are responsible for:

- Providing authorisation for emergency decisions in the absence of the ISM
- Providing sufficient resources to ensure continuity of information security.

The TRE Operations Manager is responsible for:

- Ensuring the TRE infrastructure record contains details of all tests conducted.

4. Procedure

4.1. Background

The TRE is a secure data analytics facility that hosts each research project within a secure and isolated environment. This environment, known as the 'TRE Project' comprises the following components:

- Encrypted data volumes
- Virtual workstations containing necessary data analysis software tools (data volumes are mounted on the virtual workstations)

Additionally, the TRE User end-points that connect to the TRE represent a potential TRE Project security vulnerability. However, the mechanisms that segregate TRE Projects are not dependant on these end-points and therefore they are out of scope of this document. The controls that secure external end-point connections are tested within the scope of the TRE Access Control ISMS process.

All TRE Projects use the same physical network. Segregation of virtual machines according to the TRE project is accomplished using firewalling and network access control. Segregation of data volumes is accomplished via encryption and filesystem permissions.

It is essential that each data volume is only accessible to users that are authorised to access data stored on that volume; therefore, it is necessary to test the security controls that provide this isolation.

4.2. TRE data access

All TRE data volumes are encrypted using key files. Each project's virtual workstations contain the key files needed to decrypt the data volumes belonging to that project. During boot-up, TRE virtual workstations automatically decrypt and mount allocated data volumes. Therefore, the only way of accessing data is to first connect to a virtual machine that has mounted and decrypted the data volumes. This narrows down the scope of the necessary testing to scenarios representing a user who is already logged onto a virtual machine within the TRE.

4.3. Testing methodology

A network scan exploits vulnerabilities such as network navigation, host discovery, and port status. Tools such as nmap are not installed on the standard TRE Project virtual workstations. However, to account for the worst-case scenario, the network scan tests will be conducted using an established penetration testing tool that incorporates nmap functionality.

4.4. Test Results

Each time an individual test is conducted, an entry will be placed in the TRE Infrastructure Record (REC-001). The full output of each test will be stored on Q-Pulse.

4.5. TRE Project Segregation Test

TEST:	$ nmap -vv -n -A --version-all 130.88.38.0/25
Positive Result:	[host down] status for all hosts within the range 130.88.38.0 to 130.88.38.127
Negative Result:	Anything status different to a [host down] and/or additional information such as host certificate etc.

4.6. Frequency of testing

This test 'regime' will be conducted following a *High-Impact/Criticality* change (categorisation of change is defined in SOP-03-08 TRE Change Control) to an existing TRE Project, or when a new TRE Project is created. Additionally, the testing will be routinely conducted every 6 months to ensure that segregation is maintained within existing TRE Projects.

5. Cross-referenced ISMS Documents

Number	Type	Title
REC-001	ISMS\Record	TRE Infrastructure Record

SOP-03-08	ISMS\SOP\TRE Operations - SOP	TRE Change Control

6. Appendices

None