National scheme for security evaluation and certification of ICT systems and products
(Prime Ministerial Decree of 30 October 2003 - G.U. no. 93 of 27 April 2004)

Scheme information note no. 1/20

Conditions for performing tests remotely in Common Criteria evaluations

Version 1.0

6 April 2020

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Table of contents

2 Scope of the document

This document aims at providing LVSs with indications regarding the minimum procedural and security measures to be put in place in order to carry out operational evaluation activities, i.e., functional and penetration testing, while interacting with the TOE exclusively remotely.

These indications are applicable in cases where it is not possible for the Evaluator, for exceptional reasons (e.g., serious safety concerns, travel restrictions imposed by authorities, etc.), to physically access the operating environment of the TOE, the tools used to perform the checks, and the TOE itself.

3 Introduction

The general principles expressed by Common Criteria with regard to operational evaluation activities provide that the Evaluator must have control over the TOE and the environment in which it is installed.

More specifically, the Evaluator must be able to gain assurance on the validity of the results of the operational activities that he is about to carry out and on their repeatability.

Such assurance require that the Evaluator is able to:

- determine the known status of the TOE and the operational environment before carrying out each activity;
- observe the status of the TOE and of the operational environment at the end of the execution of the activities;
- control any external influences during the execution of the activities.

It is important to emphasize that, in order to obtain the aforementioned assurance, the Evaluator must carry out an independent analysis which, on a case by case basis, leads to establishing what the required activities are.

The specific checks to be carried out to determine the known status, and any measures to be put in place so that this status can be reconstructed during the evaluation activities, depend on the type and architecture of the TOE and on the architecture of the test environment.

The ideal scenario is one in which the Evaluator performs the necessary checks from a location directly connected to the TOE. In this case, it is assumed that the Evaluator has installed and configured the TOE, the test environment and the test instrumentation.

The following sections provide some indications to be followed in the non-ideal case in which the Evaluator is requested to carry out all the operational activities described above from a location remote to the TOE and the test environment, connected to both through a potentially insecure network.

4 Reference scenario

For the purposes of this document, it is considered only the situation in which the TOE (or the test bed prepared by the Developer) is hosted in a different location from the location in which the Evaluator operates, and the Evaluator only accesses the TOE through a public network (Internet).

It is also assumed that the Evaluator operates physically at the LVS premises[1] and that IT and physical security measures are guaranteed to preserve the confidentiality and integrity of the information collected and used during the evaluation activities, in compliance with the procedures examined by the OCSI auditors during the accreditation site visit.

The workstation from which the Evaluator performs the tests can be a computer located at the LVS, and therefore under the complete control of the Evaluator, or a remote machine directly connected to the interfaces of the TOE, which the Evaluator accesses from his own PC through private connection.

Each derogation from the "standard" methods of carrying out the activities covered by this document, explicitly identified in the Evaluation Criteria and in the related methodology, still requires the identification of specific solutions and *ad hoc* operating methods to be submitted case by case to the approval of the Certifier.

5 Minimum security measures

In order to carry out remote operational activities in the reference scenario, maintaining as much as possible the same conditions and assurance as in the ideal scenario, the Evaluator must implement some security measures to:

- protect the communication channel between the laboratory workstation and the remote test environment
    - from compromise of the integrity of the messages passing through it;
    - from compromise of the confidentiality of information in transit where such compromise could cause damage to the TOE's Supplier;
    - from threats to the availability of the subject of the checks carried out via the public network;
- make sure that during the evaluation activities any other communications to and from the system hosting the TOE (or the remote test machine) do not interfere with the checks in progress, invalidating their results;
- make sure that before, during and after the evaluation activities, the TOE and the test environment are in the status expected by the Evaluator on the basis of the evaluation documentation, in particular on the basis of the installation and secure configuration guide.

[1] If, still for exceptional reasons, the Evaluator operates in a site other than the LVS (e.g., in remote working mode), he must be subjected to physical, procedural and technical security measures, which are adequate to assure protection of information at the same level of the LVS site. These measures must be communicated to the Certification Body for approval.

As a practical example, in the event that the Evaluator remotely accesses the test tool through a computer located in his laboratory, the private dedicated connection on the public network can be made through a VPN connection to the test network where the TOE is installed and configured.

6 Remote assessment activities

The assessment of the correct implementation performed remotely consists in the execution of specific functional tests (on the basis, for example, of what is required by the assurance components of the ATE_IND family), accessing the TOE interfaces from the Evaluator's remote location, without the possibility to physically access the TOE, and to observe the TOE status only through the established connection.

Similarly, performing remote penetration tests consists in carrying out the sequence of operations needed for the exploitation of the vulnerabilities under assessment from the Evaluator's remote location by accessing the TOE through the established connection.

For remote checks, the Evaluator's activities can be divided into the following four phases:

- assessment of the operational environment;
- secure preparation of the TOE;
- preliminary connection to the remote system;
- system monitoring activities during remote checks.

6.1 Assessment of the operational environment

The Evaluator must ensure that the TOE test environment is a correct instance of the TOE operational environment, and that it therefore achieves the security objectives associated with it.

With respect to the ideal case, the Evaluator must collect a series of parameters that characterize the environment in order to establish the status of the system and therefore be able to verify the known status of the TOE during the remote assessment activity.

Examples of parameters that the Evaluator should collect, for each component which is present in the operational environment, are the following:

- information on the configuration of the HW supporting the TOE, for example:
  - number of processors;
  - processor identifiers;
  - drive identifiers;
  - network card identifiers;
  - RAM size;
  - number of partitions and partition identifiers;
- information on the configuration of the Operating System and SW/FW supporting the TOE (for example, information extracted from the Windows policy manager, Web Server configuration information, network card configuration information).

6.2 Secure preparation of the TOE

The Evaluator must ensure that the TOE is installed in the test environment and configured in accordance with the evaluation documentation (ST and guides).

Compared to the ideal case, in particular where the Evaluator is not able to attend the installation and configuration of the TOE, additional parameters must be collected to allow the verification of the known status of the TOE during the remote assessment.

In addition to the parameters listed for the operational environment, examples of parameters relating to the TOE which the Evaluator should collect are the following:

- TOE configuration information (including a hash of the TOE binary files);
- copy of the log files at the end of the installation to perform subsequent checks.

6.3 Preliminary connection activities to the remote system

Before starting the actual assessment activity, the Evaluator must be able to access remotely the test bed on which the TOE is installed with administrator privileges (or in any case sufficiently elevated for the operations to be carried out) through a protected channel (authentication of origin, confidentiality and integrity), possibly different from the one that will be used for assessment activities.

For example, the Evaluator should set up with the Supplier's help a VPN connection with certificate authentication between the machine in his laboratory and the remote operating system of the TOE or the machine set up for testing.

Examples of actual activities that the Evaluator should carry out are the following:

1. set up a user with administrator privileges on the remote operating system;
2. set up the remote operating system by equipping it with an IPSec VPN service (configured to authorize secure and authenticated connections via certificates).

For this purpose, it is clear that during the secure preparation of the TOE, it is also necessary to configure the system appropriately.

These operations carried out during the installation are not part of the secure preparation of the TOE, as described in the guide for the administrator, but are only preparatory to the tests carried out by the Evaluator and must be documented only in the corresponding activity reports.

6.4 System monitoring activities during remote checks

Before, during and after each check carried out remotely on the system, the Evaluator must monitor the parameters identified on the system during the secure preparation phase in order to determine its known status.

Using the privileged access described above, the Evaluator should open, for example, a remote desktop instance and a terminal to check:

- the system parameters collected during the assessment of the operating environment and secure preparation of the TOE;

- users connected to the TOE and the operating system;
- open ports and connections via network interface to the TOE and to other operating system services (through tools such as netstat, ntop, etc.);
- incoming and outgoing traffic;
- the quality of the channel, for example verifying the travel time of the TCP packets.

The Evaluator should also verify that the privileged connection to the remote system does not interfere and invalidate the outcome of the performed checks. Finally, the Evaluator should check whether there are other active connections to the TOE, and in this case evaluate whether these connections can affect the result of the performed checks. If so, the Evaluator should manage the presence of these connections, possibly taking countermeasures to limit/block them (for example using traffic filtering tools).

7 Final remarks

In addition to the guidelines described in this document, that LVSs undertake to follow, where applicable, this Certification Body reserves the right to carry out the appropriate checks on the Activity Reports and on the test documentation produced by the LVSs and to specify additional requirements and conditions where necessary.

In order to allow a preliminary check, the information on how to carry out tests remotely and to implement the required additional protection measures, together with the test plan, must be sent to OCSI well in advance of the date scheduled for the related evaluation activities.

The managers of the LVSs and the Sponsors/Developers implicitly accept the consequences of any failure to comply with the conditions and principles expressed in this document, in the Common Criteria standard and in the OCSI Guidelines, which may lead to invalidation of the activities carried out, request for repetition of the activities in part or in whole, up to the conclusion with a negative outcome of the evaluation and the failure to issue the Certificate.