Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Nota Informativa dello Schema N. 1/20

Condizioni per l'effettuazione di test da remoto in valutazioni Common Criteria

Versione 1.0

6 aprile 2020

1 Sommario

2 Scopo del documento

Il presente documento ha l'obiettivo di fornire agli LVS indicazioni riguardo le misure procedurali e di sicurezza minime per poter effettuare le attività operative di test funzionali e di intrusione interagendo con l'ODV esclusivamente da remoto.

Tali indicazioni si intendono applicabili nei casi in cui per il Valutatore non sia possibile, per motivazioni di natura eccezionale (ad es., gravi ragioni di sicurezza fisica, restrizioni sugli spostamenti imposte dalle autorità, ecc.), accedere fisicamente all'ambiente di esercizio dell'ODV, agli strumenti utilizzati per eseguire le verifiche e all'ODV stesso.

3 Introduzione

I principi generali espressi dai Common Criteria riguardo alle attività di valutazione operative prevedono che il Valutatore debba avere sotto controllo l'ODV e l'ambiente nel quale esso è installato.

In particolare, il Valutatore deve essere in grado di ottenere garanzie sulla validità dei risultati delle attività operative che si accinge a svolgere e sulla ripetibilità delle stesse.

Tali garanzie prevedono la capacità del Valutatore di:

- determinare lo stato noto dell'ODV e dell'ambiente operativo prima dell'esecuzione di ogni attività;
- osservare lo stato dell'ODV e dell'ambiente operativo al termine dell'esecuzione delle attività;
- poter controllare le eventuali influenze esterne durante l'esecuzione delle attività.

È importante sottolineare che, per ottenere le suddette garanzie, il Valutatore deve effettuare un'analisi indipendente che, caso per caso, porti a stabilire quali siano le attività richieste.

I controlli specifici da effettuare per determinare lo stato noto e le eventuali misure da porre in atto affinché tale stato sia ricostruibile durante il corso delle attività di valutazione operative sono dipendenti dalla tipologia e dall'architettura dell'ODV e dall'architettura dell'ambiente di test.

Lo scenario ideale è quello in cui il Valutatore esegue le necessarie verifiche da una postazione direttamente connessa all'ODV. In questo caso si presuppone che il Valutatore abbia installato e configurato sia l'ODV, sia l'ambiente di test, sia la strumentazione di test.

Nei capitoli successivi vengono fornite alcune indicazioni da seguire nel caso, non ideale, in cui il Valutatore è chiamato ad effettuare tutte le attività operative sopra descritte da una postazione remota rispetto all'ODV e all'ambiente di test, connessa a questi ultimi attraverso una rete potenzialmente non sicura.

4 Scenario di riferimento

Ai fini del presente documento, si considera unicamente la situazione in cui l'ODV (o il *test bed* predisposto dallo Sviluppatore) è ospitato in una sede differente dalla sede in cui opera il Valutatore e questi accede all'ODV solo tramite una rete pubblica (Internet).

Si presuppone altresì che il Valutatore operi fisicamente nella sede dell'LVS[1] e che siano garantite le misure di sicurezza IT e fisiche atte a preservare la confidenzialità e l'integrità delle informazioni raccolte e utilizzate durante le attività di valutazione, nel rispetto delle procedure esaminate dagli ispettori OCSI in fase di visita ispettiva di accreditamento.

La postazione da cui il Valutatore esegue i test può essere un computer situato presso l'LVS, e quindi sotto il completo controllo del Valutatore, o una macchina remota direttamente collegata alle interfacce dell'ODV, alla quale il Valutatore accede mediante connessione privata.

Ciascuna deroga alle modalità "standard" di esecuzione delle attività oggetto di questo documento, individuate in modo esplicito nei Criteri di Valutazione e nella relativa metodologia, rende comunque necessaria l'individuazione di specifiche soluzioni e modalità operative *ad hoc* da sottoporre caso per caso all'approvazione del Certificatore.

5 Misure di sicurezza minime

Per poter effettuare le attività operative da remoto nello scenario di riferimento, mantenendo il più possibile le stesse condizioni e garanzie dello scenario ideale, il Valutatore deve mettere in atto alcune misure di sicurezza per:

- proteggere il canale di comunicazione fra la postazione del laboratorio e l'ambiente remoto di test
    - da compromissioni dell'integrità dei messaggi che transitano in esso;
    - da compromissioni della riservatezza delle informazioni in transito ove tale compromissione possa recare danni al Fornitore dell'ODV;
    - da minacce alla disponibilità dell'oggetto delle verifiche operate tramite la rete pubblica;
- assicurarsi che durante le attività di verifica eventuali altre comunicazioni da e verso il sistema che ospita l'ODV (o la macchina di test remota) non interferiscano con le verifiche in corso, invalidandone i risultati;
- assicurarsi che prima, durante e dopo le attività di verifica l'ODV e l'ambiente di test si trovino nello stato che il Valutatore si aspetta sulla base della documentazione di valutazione, in particolare sulla base della guida all'installazione e configurazione sicura.

Come esempio pratico, nel caso in cui il Valutatore accede da remoto allo strumento di test tramite un elaboratore posizionato nel proprio laboratorio, la connessione privata dedicata sulla rete pubblica può essere realizzata mediante una connessione VPN alla rete di test dove è istallato e configurato l'ODV.

[1] Qualora, sempre per motivi eccezionali, il Valutatore si trovasse ad operare in un sito diverso dall'LVS (ad es. in regime di lavoro a distanza), dovrà essere sottoposto a misure di sicurezza fisiche, procedurali e tecniche adeguate a garantire la protezione delle informazioni allo stesso livello del sito dell'LVS. Tali misure dovranno essere comunicate all'Organismo di Certificazione per approvazione.

6 Attività di verifica da remoto

L'attività di verifica della corretta implementazione eseguita da remoto consiste nell'esecuzione di specifici test funzionali (sulla base ad esempio di quanto richiesto dai componenti di garanzia della famiglia ATE_IND) utilizzando le interfacce dell'ODV stimolate dalla postazione remota del Valutatore senza la possibilità di accedere fisicamente all'ODV e di osservarne lo stato se non attraverso la connessione instaurata.

Allo stesso modo, l'attività di prove di intrusione da remoto consiste nell'esecuzione della sequenza di operazioni previste per lo sfruttamento delle vulnerabilità in esame dalla postazione remota del Valutatore accedendo all'ODV attraverso la connessione instaurata.

Per lo svolgimento delle verifiche da remoto, le attività del Valutatore si possono dividere nelle seguenti quattro fasi:

- attività di verifica dell'ambiente operativo;
- attività di preparazione sicura dell'ODV;
- attività di connessione preliminare al sistema remoto;
- attività di monitoraggio del sistema durante le verifiche da remoto.

6.1 Attività di verifica dell'ambiente operativo

Il Valutatore deve accertarsi che l'ambiente di test dell'ODV sia una corretta istanza dell'ambiente operativo ipotizzato per l'ODV e che quindi realizzi gli obiettivi di sicurezza ad esso associati.

Rispetto al caso ideale il Valutatore deve collezionare una serie di parametri che caratterizzano l'ambiente al fine di poter stabilire lo stato del sistema e quindi poter verificare lo stato noto dell'ODV in fase di attività di verifica da remoto.

Esempi di parametri che il Valutatore dovrebbe collezionare, per ciascun componente presente nell'ambiente operativo, sono i seguenti:

- informazioni di configurazione dell'HW a supporto dell'ODV, ad es.:
    - numero dei processori;
    - identificativo dei processori;
    - identificativo dei dischi;
    - identificativo delle schede di rete;
    - dimensione totale della RAM;
    - numero partizioni e identificativo partizioni;
- informazioni di configurazione del Sistema Operativo e del SW/FW a supporto dell'ODV (ad esempio le informazioni estratte dal *policy manager* di Windows, le informazioni di configurazione del Web Server, le informazioni di configurazione della scheda di rete).

6.2 Attività di preparazione sicura dell'ODV

Il Valutatore deve accertarsi che l'ODV sia installato nell'ambiente di test e configurato in accordo alla documentazione di valutazione (TDS e guide).

Rispetto al caso ideale, in particolare ove il Valutatore non sia in grado di testimoniare direttamente l'installazione e la configurazione dell'ODV, questi deve collezionare parametri aggiuntivi al fine di poter verificare lo stato noto dell'ODV in fase di attività di verifica da remoto.

Oltre ai parametri elencati per l'ambiente operativo, esempi di parametri relativi all'ODV che il Valutatore dovrebbe collezionare sono i seguenti:

- informazioni di configurazione dell'ODV (incluso un *hash* dei file binari dell'ODV);
- copia dei file di log al termine dell'istallazione per eseguire verifiche successive.

6.3 Attività di connessione preliminare al sistema remoto

Prima di iniziare la vera e propria attività di verifica il Valutatore deve essere in grado di accedere da remoto al *test bed* sul quale è installato l'ODV con privilegi di amministratore (o comunque sufficientemente elevati per le operazioni da svolgere) tramite un canale protetto (autenticazione di origine, riservatezza e integrità), possibilmente diverso da quello che verrà usato per le attività di verifica.

Il Valutatore dovrebbe ad esempio predisporre assieme al Fornitore una connessione VPN con certificato fra la macchina del proprio laboratorio e il sistema operativo remoto dell'ODV o della macchina predisposta per i test.

Esempi di attività concrete che il Valutatore dovrebbe compiere sono le seguenti:

1. predisporre sul sistema operativo remoto un utente con privilegi di amministratore;
2. predisporre il sistema operativo remoto equipaggiandolo con un servizio VPN IPSec (configurato per autorizzare connessioni protette e autenticate tramite certificato).

A tale scopo è chiaro che in fase di preparazione sicura dell'ODV sarà necessario configurare opportunamente il sistema.

Tali operazioni effettuate in fase di installazione non fanno parte della preparazione sicura dell'ODV come da guida per l'amministratore, ma sono solo propedeutiche ai test effettuati dal Valutatore e devono essere documentate solo nei rapporti di attività corrispondenti.

6.4 Attività di monitoraggio del sistema durante le verifiche da remoto

Prima, durante e dopo ciascuna verifica svolta da remoto sul sistema, il Valutatore deve monitorare i parametri individuati sul sistema in fase di preparazione sicura al fine di determinarne lo stato noto.

Tramite l'accesso privilegiato descritto in precedenza il Valutatore dovrebbe aprire, ad esempio, una istanza di desktop remoto e un terminale per verificare:

- i parametri del sistema collezionati in fase di verifica dell'ambiente operativo e preparazione sicura dell'ODV;
- gli utenti connessi all'ODV e al sistema operativo;

- le porte aperte e le connessioni tramite interfaccia di rete all'ODV e ad altri servizi del sistema operativo (tramite *tool* come netstat, ntop, ecc.);
- il traffico in ingresso ed uscita;
- la qualità del canale, verificando per esempio il tempo di percorrenza dei pacchetti TCP.

Il Valutatore dovrebbe anche verificare che la connessione privilegiata al sistema remoto non interferisca in modo da invalidare l'esito delle verifiche eseguite.

Infine, il Valutatore dovrebbe verificare se esistano altre connessioni attive all'ODV e in caso valutare se queste connessioni possano inficiare il risultato delle verifiche condotte. In caso positivo, il Valutatore dovrebbe gestire la presenza di tali connessioni eventualmente prendendo contromisure per limitarle/bloccarle (ad esempio servendosi di strumenti di filtraggio del traffico).

7 Note conclusive

Fatto salvo l'impegno degli LVS ad ottemperare alle linee guida illustrate nel presente documento, ove applicabile, questo Organismo di Certificazione si riserva la facoltà di attuare le opportune verifiche sui Rapporti di Attività e sulla documentazione relativa ai test prodotta dagli LVS e di specificare ulteriori requisiti e condizioni ove ciò si riveli necessario.

Allo scopo di consentire una verifica preliminare, le informazioni sulle modalità di esecuzione dei test in modalità remota e di attuazione delle misure di protezione aggiuntive richieste, unitamente al piano di test, dovranno essere inviate all'OCSI con congruo anticipo rispetto alla data prevista per lo svolgimento delle attività connesse.

I responsabili degli LVS e i Committenti/Fornitori accettano implicitamente le conseguenze di eventuali inosservanze delle condizioni e dei principi espressi in questo documento, nello standard Common Criteria e nelle Linee Guida dell'OCSI, che possono comportare a seconda dei casi l'invalidazione delle attività svolte, la richiesta di ripetizione in parte o in tutto delle attività, fino alla conclusione con esito negativo della valutazione e alla mancata emissione del Certificato.