Marco Ivaldi
Mediaservice

La certificazione della sicurezza ICT con OSSTMM.
(ICT Security Certification with OSSTMM)

Sommario

Le verifiche di sicurezza ricoprono un ruolo fondamentale all'interno del processo di gestione della sicurezza ICT.

Tuttavia, esse sono soggette a numerose problematiche che possono limitarne la reale utilità. La metodologia scientifica OSSTMM si propone come una soluzione a queste problematiche, fornendo un processo concreto per la verifica funzionale e la certificazione della sicurezza.

Abstract

Proactive security testing is a critical element within the ICT security governance process.

However, its effectiveness might be affected by many potential problems. The OSSTMM is a scientific methodology that has been created to address those problems. It provides a concrete process to thoroughly evaluate and certify operational security.

"Grazie alla metodologia OSSTMM non è più necessario affidarsi a best practice generiche, riscontri aneddotici o superstizioni, poiché essa fornisce evidenze scientifiche su cui basare le decisioni che impattano sulla sicurezza." – Open Source Security Testing Methodology Manual 3.0.

1. Sicurezza proattiva e OSSTMM

La disciplina della sicurezza proattiva comprende tutte le attività finalizzate a rilevare e valutare il grado di efficacia, efficienza e robustezza delle contromisure di sicurezza tecnologiche o organizzative adottate all'interno di un ambito definito. I più comuni servizi di sicurezza proattiva sono:

- Vulnerability Assessment, che prevede l'esecuzione di scansioni automatizzate o semi-automatizzate non invasive, condotte avvalendosi di strumenti software al fine di rilevare la presenza di vulnerabilità note.
- Penetration Test, che si basa su tecniche di attacco inferenziali finalizzate all'identificazione delle criticità non note o comunque non rilevabili tramite i soli strumenti di scansione ed analisi automatizzata.

L'esecuzione di verifiche di sicurezza richiede l'intervento di analisti specializzati (ethical hacker) in grado di comprendere non solo le tematiche di sicurezza ICT, ma anche le normative, le leggi, le premesse, le operazioni, i processi e le specifiche tecnologie coinvolte nel contesto oggetto di analisi. Tra le tecnologie che possono essere oggetto di verifica figurano: reti IP pubbliche e private, reti Wi-Fi, piattaforme applicative, servizi VPN, infrastrutture telefoniche tradizionali e VoIP, dispositivi hardware, sistemi di controllo degli accessi e videosorveglianza, etc.

A causa dell'elevato grado di specializzazione richiesto agli analisti e al fine di garantire una valutazione di sicurezza indipendente e slegata dalle dinamiche aziendali, le verifiche sono di norma condotte da una terza parte. A seconda degli accordi, il team di specialisti può o meno avvalersi di informazioni di dettaglio relative al contesto oggetto di analisi, oltre che di credenziali valide per l'accesso ai servizi applicativi in caso di verifica da posizione privilegiata.

Al termine delle attività viene redatta la reportistica, solitamente organizzata in due livelli distinti:

- Executive Summary, destinato allo staff dirigenziale del Cliente, che fornisce indicazioni strategiche e di facile lettura sullo stato complessivo della sicurezza riscontrato a seguito delle attività di analisi.
- Technical Report, che costituisce la documentazione formale dei test eseguiti e riporta in

modo particolareggiato i risultati emersi dalle attività svolte, i dettagli tecnici e le evidenze più significative.

L'esecuzione periodica di verifiche di sicurezza consente di identificare in modo preventivo eventuali inadeguatezze o non conformità, al fine di fornire le indicazioni necessarie alla formulazione del piano correttivo di rientro. La disciplina della sicurezza proattiva ricopre pertanto un ruolo estremamente importante all'interno del processo di gestione della sicurezza ICT. Tuttavia, il valore di una verifica di sicurezza dipende fortemente dal valore degli analisti che la effettuano. Le verifiche di sicurezza sono inoltre storicamente soggette alle seguenti classi di problematiche, che possono limitarne l'utilità:

- I risultati della verifica non sono esaustivi, poiché il perimetro di analisi o l'approccio di test non è stato correttamente e formalmente definito.
- I risultati della verifica includono numerosi falsi positivi e negativi, dovuti a limitazioni negli strumenti o nei metodi di test adottati.
- I risultati della verifica non sono consistenti, ripetibili, misurabili e quantificabili secondo precise regole.
- La priorità degli interventi correttivi da effettuare nell'ambito del piano di rientro non è definita sulla base di un metodo condiviso con il Cliente.
- La verifica di sicurezza non tiene conto delle politiche, delle normative e delle leggi vigenti applicabili al contesto oggetto di analisi.
- La reportistica non è fruibile e facilmente confrontabile.

Al fine di ovviare alle problematiche descritte, l'associazione no-profit ISECOM ha realizzato l'Open Source Security Testing Methodology Manual (OSSTMM), che nel corso degli anni è divenuto lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza. OSSTMM (scaricabile gratuitamente dal sito ufficiale www.osstmm.org) è una metodologia scientifica sviluppata da numerosi volontari in tutto il mondo tramite il modello peer review. Essa ha introdotto numerosi concetti innovativi nella disciplina della sicurezza proattiva, quali: regole di ingaggio precise, OpSec (Porosity, Controls, Limitations), metrica rav per misurare la superficie di attacco, reportistica certificata STAR.

La versione 3.0 della metodologia, pubblicata nel dicembre 2010, è frutto di ben 10 anni di lavoro ed è pertanto considerata molto matura. Tanto che persino l'International Standard Organization ha recentemente manifestato interesse a creare uno standard ISO basato su OSSTMM, dando inizio al processo formale di studio che costituisce il primo passo del percorso di normazione.

ISECOM

ISECOM (Institute for Security and Open Methodologies) è un'organizzazione internazionale di ricerca senza scopo di lucro fondata nel 2001 da Pete Herzog, al fine di sviluppare e condividere metodologie aperte nel campo della sicurezza delle informazioni. Oltre ad OSSTMM, ISECOM promuove numerosi altri progetti, quali: SCARE (Source Code Analysis Risk Evaluation), HHS (Hacker HighSchool), HPP (The Hackers Profiling Project), BPP (The Bad People Project). Ha inoltre curato la terza edizione del libro Hacking Linux Exposed, pubblicato da McGraw-Hill Osborne Media.

ISECOM è inoltre un'autorità di certificazione riconosciuta e sostenuta da partner istituzionali (Università La Salle). In quanto tale offre certificazioni per professionisti ed aziende, tra cui le più note sono: OPST (OSSTMM Professional Security Tester), OPSA (OSSTMM Professional Security Analyst), OWSE (OSSTMM Wireless Security Expert), ILA (ISECOM Licensed Auditor).

Per ulteriori informazioni è possibile consultare il sito ufficiale dell'organizzazione: www.isecom.org.

2. Regole di ingaggio, tipologie di test e definizione del perimetro

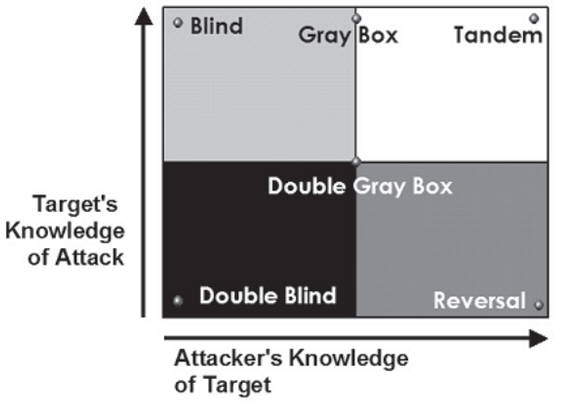
La metodologia OSSTMM definisce esattamente quali elementi devono essere verificati, che cosa occorre fare prima, durante e dopo i test di sicurezza e come misurare i risultati ottenuti. Essa non indica esplicitamente gli strumenti da impiegare durante le verifiche, ma dettaglia i metodi da utilizzare per valutare sul campo in modo consistente e ripetibile la superficie di attacco (*attack surface*) relativa al contesto oggetto di analisi, tramite il calcolo del *rav*.

Tutte le fasi di verifica, dalla prevendita alla formulazione dell'offerta, dalla firma del contratto alla definizione del perimetro di analisi, dall'esecuzione dei test alla stesura della reportistica, sono soggette a specifiche regole di ingaggio (*rules of engagement*), chia-

ramente definite all'interno della metodologia e sottoscritte da tutti gli analisti certificati presso ISECOM.

OSSTMM prevede differenti tipologie di test, che si differenziano tra di loro per il grado di conoscenza del target da parte degli analisti e per il grado di conoscenza dei dettagli della verifica di sicurezza da parte del target stesso.

Tipologie di test



1. **Blind**. Gli analisti simulano le azioni di un agente di minaccia all'oscuro dei dettagli implementativi del contesto oggetto di analisi. Il target è a conoscenza di tutti i dettagli della verifica.
2. **Double Blind**. Gli analisti simulano le azioni di un agente di minaccia all'oscuro dei dettagli implementativi del contesto oggetto di analisi. Il target non è informato sul perimetro di test.
3. **Gray Box**. Gli analisti simulano le azioni di un agente di minaccia in possesso di informazioni limitate sulle componenti e sulle difese presenti nel contesto oggetto di analisi. Il target è a conoscenza di tutti i dettagli della verifica.
4. **Double Gray Box**. Gli analisti simulano le azioni di un agente di minaccia in possesso di informazioni limitate sulle componenti e sulle difese presenti nel contesto oggetto di analisi. Il target è a conoscenza del perimetro di test, ma non di tutti i dettagli della verifica.
5. **Tandem**. Gli analisti ed il target sono entrambi in possesso di informazioni di dettaglio relative al contesto oggetto di analisi ed alla verifica di sicurezza.
6. **Reversal**. Gli analisti sono in possesso di informazioni di dettaglio relative al contesto oggetto di analisi. Il target non è informato sul perimetro di test.

Contestualmente alla definizione della tipologia di test desiderata, è necessario stabilire il perimetro della verifica. Al fine di garantire la massima copertura, OSSTMM comprende 3 classi di ambienti che possono essere analizzati. Tali classi sono a loro volta suddivise in 5 canali (channels), come riportato all'interno della seguente tabella:

Classe	Canale	Descrizione
Physical Security (PHYSSEC)	Human	Comprende il fattore umano della sicurezza (persone e loro interazioni)
	Physical	Comprende l'elemento tangibile dalla sicurezza (edifici, porte, etc.)
Spectrum Security (SPECSEC)	Wireless	Comprende le emissioni nello spettro elettromagnetico
Communications Security (COMSEC)	Telecommunications	Comprende le reti telefoniche digitali o analogiche
	Data Networks	Comprende i sistemi elettronici e le reti di trasmissione dati cablate

3. Verifica della sicurezza operativa

La metodologia OSSTMM fa ampio riferimento al concetto di sicurezza operativa (*operational security* o *OpSec*), che viene definito come la "combinazione di separazione e controlli".

Nel dettaglio, per essere efficace una minaccia deve essere in grado di interagire direttamente o indirettamente con il target. E' possibile impedire questa interazione separando la minaccia dal target, in uno dei seguenti modi:

- Spostando il target in modo da creare una barriera fisica o logica che lo protegga dalla minaccia.
- Rendendo inoffensiva la minaccia.
- Eliminando la minaccia.

Se si vogliono offrire servizi interattivi, tuttavia, non è possibile realizzare una separazione completa tra minacce e target, ma è necessario mantenere un certo livello di esposizione, che OSSTMM definisce con il termine *Porosity*.

La Porosity è calcolata sulla base dei seguenti elementi, che concorrono ad abbassare il livello di sicurezza complessivo:

Elemento	Descrizione
Visibility	Opportunità di attacco, ovvero target visibili all'interno del contesto oggetto di analisi (sistemi, componenti applicative, edifici, persone, etc.).
Access	Punti tramite i quali è possibile stabilire un'interazione all'interno del contesto oggetto di analisi (servizi di rete, funzionalità applicative, accessi fisici raggiungibili, etc.).
Trust	Relazioni di fiducia presenti tra target facenti parte del contesto oggetto di analisi (interazioni non autenticate tra differenti target).

Al fine di mitigare l'impatto delle minacce residue che sono in grado di interagire con il target, bisogna ricorrere ad opportune contromisure (*Controls*), che forniscono protezione da varie tipologie di interazioni non valide o inaspettate. Tali contromisure, che innalzano il livello di sicurezza complessivo, sono suddivise in controlli interattivi (che influenzano direttamente le interazioni in termini di Porosity) e di processo (che proteggono i target dalle minacce presenti):

Controllo	Descrizione
Authentication	Controllo interattivo di accesso basato sulla richiesta di credenziali. Include i processi di Identification e Authorization.
Indemnification	Controllo interattivo realizzato tramite una forma di contratto tra il proprietario del target e gli utenti che vi interagiscono.
Resilience	Controllo interattivo effettuato allo scopo di mantenere la protezione del target anche in caso di errore o disservizio.
Subjugation	Controllo interattivo finalizzato ad assicurare che le operazioni abbiano luogo unicamente sulla base di processi definiti.
Continuity	Controllo interattivo effettuato allo scopo di mantenere l'operatività del target anche in caso di errore o disservizio.
Non-Repudiation	Controllo di processo che impedisce agli utenti di negare il proprio ruolo nell'ambito delle interazioni con il target.
Confidentiality	Controllo di processo che garantisce la confidenzialità delle comunicazioni e delle informazioni in transito sulla rete o memorizzate su supporto fisico.
Privacy	Controllo di processo che garantisce la confidenzialità dei metodi di accesso, di visualizzazione o di scambio dati disponibili per il target.
Integrity	Controllo di processo che informa gli utenti degli eventuali cambiamenti che interessano il target ed i processi con cui esso interagisce.
Alarm	Controllo di processo che registra il verificarsi di interazioni che coinvolgono il target ed eventualmente invia opportune notifiche.

Le criticità di sicurezza (Limitations), infine, possono interessare sia i punti di interazione dati dalla Porosity che gli stessi controlli, e concorrono ad abbassare ulteriormente il livello di sicurezza complessivo del contesto oggetto di analisi. OSSTMM adotta la seguente classificazione delle criticità:

Criticità	Descrizione
Vulnerability	Criticità che nega l'accesso agli utenti autorizzati, consente l'accesso privilegiato ad utenti non autorizzati, o permette ad utenti non autorizzati di occultare la propria presenza.
Weakness	Criticità che interrompe, riduce o annulla l'effetto di uno o più dei cinque controlli interattivi: Authentication, Indemnification, Resilience, Subjugation, Continuity.
Concern	Criticità che interrompe, riduce o annulla l'effetto di uno o più dei cinque controlli di processo: Non-Repudiation, Confidentiality, Privacy, Integrity, Alarm.
Exposure	Criticità o azione non giustificata che provoca la visibilità diretta o indiretta di target all'interno del contesto oggetto di analisi, tramite il canale preso in esame.
Anomaly	Elemento inaspettato, sconosciuto o comunque non giustificabile nell'ambito delle normali operazioni che hanno luogo all'interno del contesto oggetto di analisi.

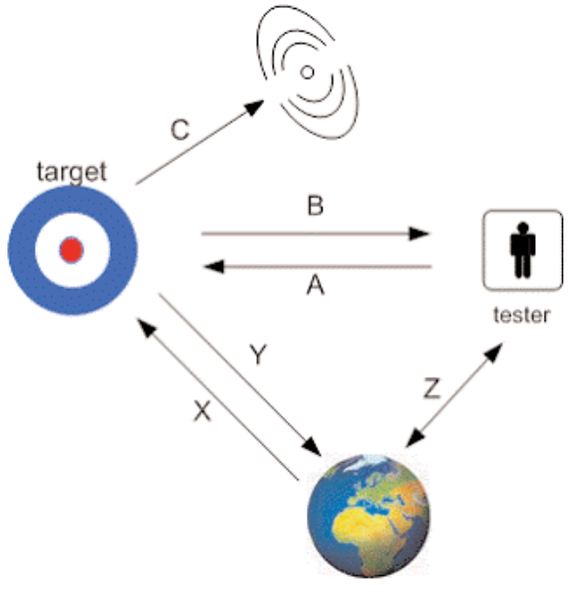
Tramite gli elementi descritti viene calcolata la superficie di attacco, che è definita come la "quantità di interazioni non controllate con il target" riscontrata a seguito di una specifica verifica di sicurezza. Secondo la metodologia OSSTMM è possibile raggiungere lo stato di *Perfect Security*, ovvero l'esatto bilanciamento di separazione e controlli con l'esposizione e le criticità.

Four point process

La metodologia OSSTMM definisce un processo di verifica della sicurezza operativa che consente di fornire le risposte alle seguenti domande fondamentali:

1. Come funzionano le operazioni?
2. In che cosa differiscono da come chi le gestisce pensa che funzionino?
3. Come dovrebbero funzionare?

Poiché il contesto oggetto di verifica è per definizione dinamico e non risponde sempre con lo stesso output al medesimo input, per derivare i dati necessari a popolare il modello di OpSec definito dalla metodologia OSSTMM è necessario applicare un processo più articolato del semplice "inviare uno stimolo, registrare e analizzare la risposta". Tale processo prende il nome di Four Point Process (4PP).



1. **Induzione** (Z). Derivare informazioni sul target osservando l'ambiente in cui esso risiede.
2. **Indagine** (C). Investigare le emanazioni del target, elettromagnetiche o di altra natura.
3. **Interazione** (A/B). Interagire in modo standard e non al fine di stimolare delle risposte.
4. **Intervento** (X/Y/Z). Modificare le interazioni tra il target e l'ambiente circostante.

4. Metrica di sicurezza e reportistica certificata STAR

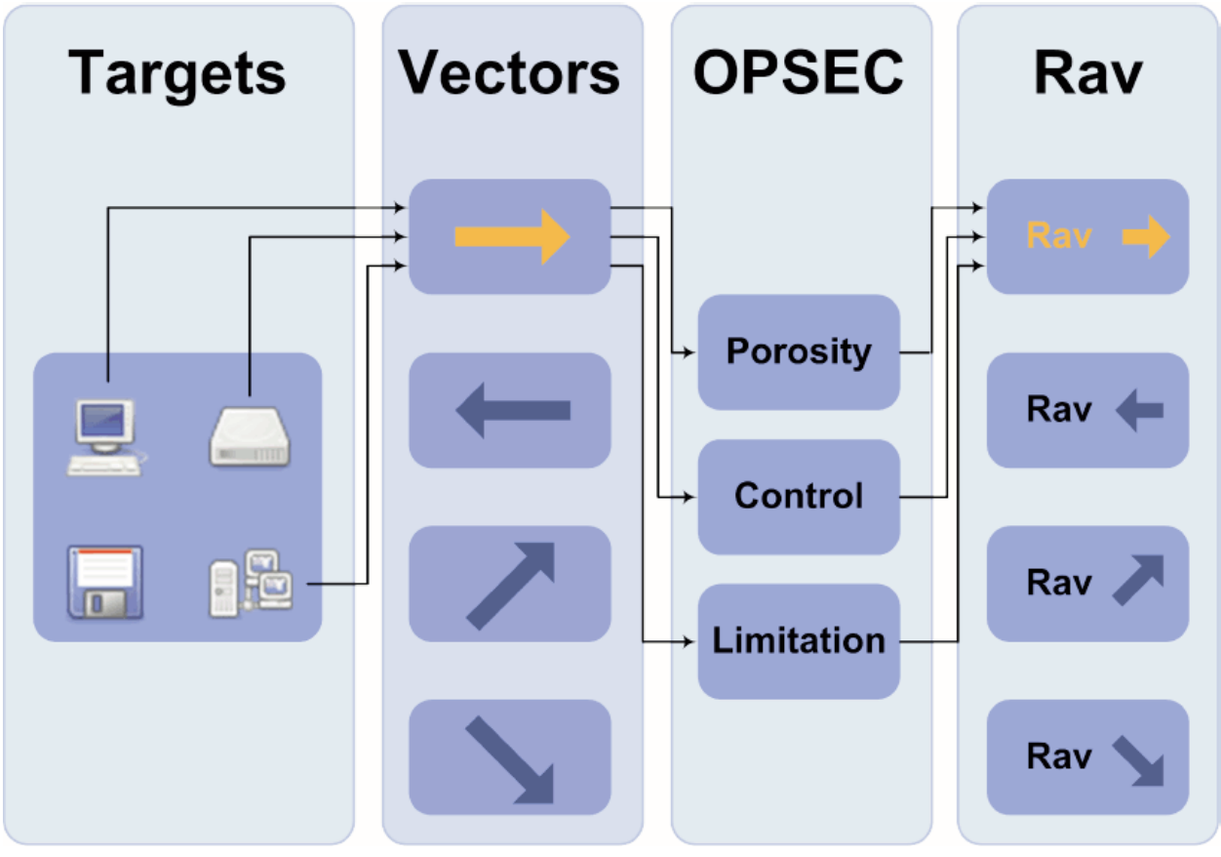
La metodologia OSSTMM fornisce una metrica accurata (rav) per valutare il livello di sicurezza operativa del contesto oggetto di analisi. Il rav misura la superficie di attacco tramite il calcolo bilanciato di Porosity, Controls e Limitations: l'esatto bilanciamento di questi valori è rappresentato da un valore di rav pari a 100 (Perfect Security).

Il rav non rappresenta una misurazione di rischio: non è in grado di prevedere se un particolare target sarà attaccato da un agente di minaccia, tuttavia evidenzia i punti deboli e i punti di forza di ogni target, e consente di misurare in modo efficace l'impatto reale di un possibile attacco. Grazie a queste informazioni, facilmente confrontabili nel tempo e ricalcolabili in base all'attuazione di differenti interventi correttivi, è possibile valutare i rischi con maggiore accuratezza.

Analogamente, il rav non è un indicatore di conformità. In generale, il concetto di conformità è molto diverso ed indipendente da quello di sicurezza: in altre parole, è possibile essere conformi e non sicuri o essere relativamente sicuri ma non conformi. L'utilizzo del rav e più in generale di OSSTMM, tuttavia, riveste un ruolo importante nell'ambito di qualsiasi iniziativa di conformità, perché consente di ottenere l'evidenza della governance della sicurezza ICT.

Il rav è quindi uno strumento molto concreto che permette di prendere decisioni supportate da numeri e non viziate da impressioni fallaci o pressioni commerciali. In particolare, esso consente di ottenere le risposte alle seguenti domande:

- Quanto dobbiamo investire nella sicurezza?
- Su quali aspetti dobbiamo concentrarci in modo prioritario?
- Di quali soluzioni di sicurezza abbiamo bisogno?
- Quanto migliora il livello di sicurezza a seguito dell'adozione di specifiche contromisure?
- Come possiamo misurare i risultati dei piani correttivi?
- Come possiamo sapere se stiamo riducendo l'esposizione alle minacce?
- Quanto è resistente un determinato componente?
- Come possiamo ottenere conformità e sicurezza?

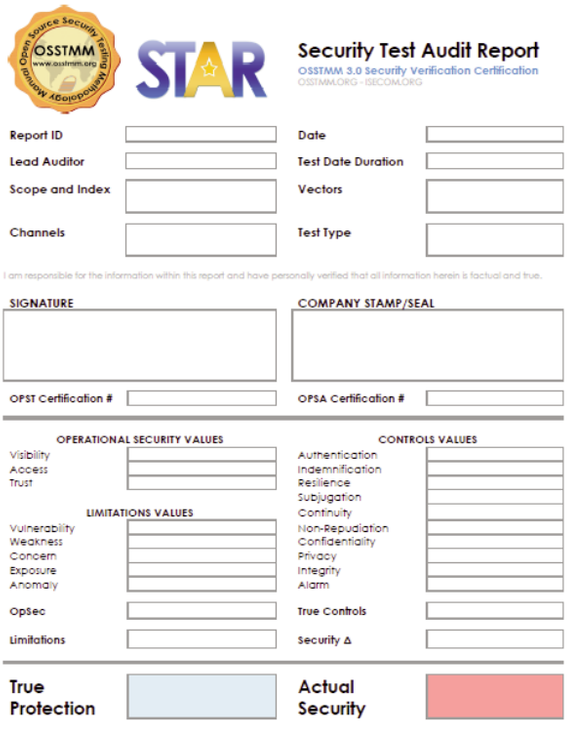


OSSTMM riporta la formula per il calcolo del rav, spiegandone in modo dettagliato i differenti passaggi. Per semplificare il lavoro degli analisti, inoltre, ISECOM distribuisce gratuitamente tramite il proprio sito web dei fogli di calcolo preimpostati, in entrambi i formati Excel e OpenDocument, insieme al modello di report STAR (Security Test Audit Report) che deve essere compilato al termine delle attività.

Lo STAR rappresenta l'Executive Summary della verifica e non sostituisce il Technical Report. Esso include le seguenti informazioni:

- Data e ora della verifica.
- Durata della verifica.
- Nominativi degli analisti coinvolti.
- Tipologia di verifica.
- Perimetro di analisi.
- Canali e vettori di attacco analizzati.
- Metrica di sicurezza (rav).
- Checklist dei test effettuati e non.
- Eventuali anomalie riscontrate.

Dopo essere stato sottoscritto dagli analisti responsabili, lo STAR può opzionalmente essere sottoposto al processo di accreditamento e certificazione presso ISECOM. Un rav superiore a 90 dà diritto ad un certificato di eccellenza della durata di un anno solare dalla data di chiusura dei test.



In conclusione, l'obiettivo finale di una verifica conforme allo standard OSSTMM è fornire un processo per essere funzionalmente sicuri, garantendo:

- Esaustività e profondità dei test, con riduzione sostanziale dei falsi positivi e negativi.
- Conclusioni oggettivamente derivate dai risultati dei test stessi, tramite applicazione del metodo scientifico.
- Rispetto di politiche, normative e leggi vigenti applicabili al contesto oggetto di analisi.
- Risultati consistenti e ripetibili.
- Risultati misurabili e quantificabili secondo precise regole.
- Valutazione immediata dei possibili interventi correttivi.

Infine, la reportistica STAR certificata, oltre ad essere fruibile e facilmente confrontabile, costituisce la prova di un test basato sui fatti e rende gli analisti responsabili della verifica.

GLOSSARIO

Agente di minaccia (*threat agent, attacker*): persona o cosa che agisce al fine di realizzare una minaccia.

Canali (*Channes*): classificazione degli ambienti che possono essere oggetto di analisi. OSSTMM prevede i seguenti canali: Human, Physical, Wireless, Telecommunications, Data Networks.

Falso negativo (*false negative*): il risultato di un test che appare negativo, non evidenziando la presenza di una criticità esistente.

Falso positivo (*false positive*): il risultato di un test che rappresenta un falso allarme, evidenziando la presenza di una criticità non esistente.

Metrica di sicurezza rav: misura quantitativa della superficie di attacco del contesto oggetto di analisi.

Modello peer review: modello di sviluppo che si basa sulla valutazione esperta eseguita da specialisti del settore per verificare la correttezza dei contenuti.

Sicurezza operativa (*operational security, OpSec*): combinazione di separazione e controlli. L'esatto bilanciamento dei valori di Porosity, Controls e Limitations rappresenta la Perfect Security.

STAR (*Security Test Audit Report*): reportistica Executive Summary conforme alla metodologia OSSTMM, opzionalmente certificabile presso l'ente internazionale ISECOM.

Superficie di attacco (*attack surface*): mancanza di separazione e controlli per un determinato vettore, ovvero quantità di interazioni non controllate con il target.

Target: obiettivo di una verifica di sicurezza presente all'interno del perimetro di analisi definito, costituito da una risorsa (asset) e dai suoi meccanismi di difesa.

Vettore di attacco (*attack vector*): direzione dell'interazione presa in esame nell'ambito di una verifica di sicurezza.

Breve biografia di Marco Ivaldi

Marco Ivaldi è un ricercatore e consulente con esperienza decennale nel campo della sicurezza informatica. Lavora con la qualifica di Senior Security Advisor presso @ Mediaservice.net (www.mediaservice.net), azienda leader del settore in Italia. Fa parte dell'ISECOM Core Team e partecipa attivamente allo sviluppo dell'Open Source Security Testing Methodology Manual (OSSTMM), lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza. La sua homepage è www.0xdeadbeef.info.

Marco Ivaldi is an experienced ICT security researcher and consultant. He is employed as Senior Security Advisor at @ Mediaservice.net (www.mediaservice.net), a leading consulting firm based in Italy. He is an ISECOM Core Team member, actively involved in the development of the Open Source Security Testing Methodology Manual (OSSTMM), the international standard for performing security testing and metrics. His homepage and playground is www.0xdeadbeef.info.