

Università degli Studi di Salerno



Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Tipi e Metodologie di Testing

Parte 2

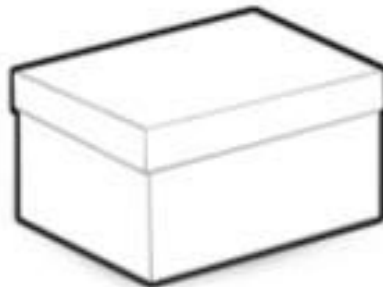
Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Terminologia
- Tipologie di Test di Sicurezza
- **Tipi di Penetration Testing**
- Metodologie di Testing
- Framework Generale per il Penetration Testing (FGPT)
- Penetration Testing Report

Tipi di Penetration Testing

- Tre approcci principali per il Penetration Testing
 - Black Box Testing
 - White Box Testing
 - Grey Box Testing



Tipi di Penetration Testing

Black Box Testing

- Simula nel modo più fedele possibile gli attacchi che potrebbero accadere nel mondo reale
- Opera allo stesso modo di chi è intenzionato ad attaccare un determinato asset (*Black Hat Hacker*)



Tipi di Penetration Testing

Black Box Testing

- Garantisce che
 - Tutte le componenti di un determinato asset siano correttamente enumerate
 - Server, client, switch, etc
 - Tutte le possibili vulnerabilità siano identificate
 - Sia tramite approcci automatici che manuali
 - Tutti i potenziali strumenti (*vettori*) di attacco siano utilizzati per (provare a) sfruttare le vulnerabilità identificate



Tipi di Penetration Testing

Black Box Testing

- Il pentester non ha alcuna conoscenza preliminare sull'asset da analizzare
- Il pentester non conosce
 - Architetture dei sistemi
 - Software
 - Hardware
 - Eventuali processi interni sottoposti a valutazione
 - Etc



Tipi di Penetration Testing

Black Box Testing

- Va usato solo quando necessario
 - Richiede molte risorse in termini di tempo e di costo
 - Rischia di causare interruzioni e/o danni all'asset sottoposto a valutazione



Tipi di Penetration Testing

White Box Testing

- Il pentester ha conoscenza approfondita dell'asset da analizzare
 - Sistemi, applicazioni, hardware, software, etc
- Il pentester potrebbe avere accesso a
 - Diagrammi di rete completi
 - Inventari dei sistemi operativi
 - Livelli di aggiornamento/patch
 - Codici sorgente e file di configurazione
 - Informazioni sul personale
 - Etc



Tipi di Penetration Testing

White Box Testing

- Il pentester
 - Non attacca l'asset così come lo farebbe una minaccia esterna
 - Valida i controlli di sicurezza dell'asset in esame
- Spesso rivolto a nuove applicazioni o sistemi in fase di sviluppo
- I pentester cercano le vulnerabilità nei sistemi in fase di sviluppo
 - Prima che questi siano messi in produzione e risultino esposti alle minacce del mondo reale



Tipi di Penetration Testing

Gray Box Testing

- Forma ibrida di penetration testing
- Il pentester ha a disposizione solo alcune informazioni sull'asset da valutare, ad esempio
 - Versioni del sistema operativo
 - Documentazione sull'architettura di rete interna
 - Etc



Tipi di Penetration Testing

Gray Box Testing

- Attività di portata limitata, con uno specifico obiettivo di valutazione
 - Specifico segmento di rete
 - Sottosistemi di un asset
 - Etc
- Lo scopo del Gray Box Testing è spesso la validazione dei controlli di sicurezza delle componenti di un asset
 - Senza la messa offline dell'asset stesso



Tipi di Penetration Testing

Come Scegliere il Tipo di Testing?

- Scelta spesso dettata dagli obiettivi del cliente o dell'organizzazione che ha commissionato il processo di penetration testing per il proprio asset



Tipi di Penetration Testing

Come Scegliere il Tipo di Test?

- In generale, un asset
 - Se vuole verificare la sicurezza di un **nuovo sistema** da mettere in produzione, spesso richiederà un **White Box Testing**
 - Se ha un **programma di sicurezza consolidato** e vuole valutare la propria sicurezza rispetto a possibili attacchi del mondo reale, spesso richiederà un **Black Box Testing**

Outline

- Terminologia
- Tipologie di Test di Sicurezza
- Tipi di Penetration Testing
- **Metodologie di Testing**
- Framework Generale per il Penetration Testing (FGPT)
- Penetration Testing Report

Metodologie di Testing

Motivazioni

➤ Permettono di

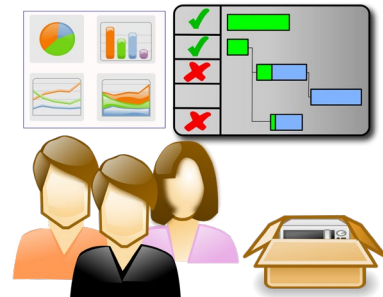
- Condurre il processo di penetration testing usando un approccio strutturato e ben definito
- Eseguire efficacemente un compito impegnativo e critico in termini di tempo
- Indipendentemente dalle dimensioni e dalla complessità dell'asset da analizzare



Metodologie di Testing

Motivazioni

- Formalizzare il processo di penetration testing mediante un framework strutturato è estremamente importante
 - Sia da un punto di vista tecnico che gestionale
- Un processo di penetration testing condotto in accordo ad una determinata metodologia consente di ereditare da essa
 - Caratteristiche
 - Processi
 - Conformità
 - Vantaggi
 - Svantaggi



Metodologie di Testing

Come Scegliere quella Migliore?

- Alcune metodologie si concentrano su aspetti tecnici, altre su criteri manageriali
 - Pochissime su entrambi
- La scelta della metodologia migliore richiede un'accurata selezione
 - Attraverso cui si potrà stimare il costo e l'efficacia del processo di penetration testing che si andrà a condurre



Metodologie di Testing

Come Scegliere quella Migliore?

- La scelta della metodologia migliore dipende da diversi fattori, tra i quali
 - Dettagli tecnici forniti sull'asset
 - Tipo di asset
 - Disponibilità di risorse (tempo, denaro, etc)
 - Competenza del/dei penetration tester
 - Obiettivi aziendali
 - Vincoli normativi
 - Etc



Metodologie di Testing

Quali sono quelle Principali?

- Esistono numerose metodologie per il penetration testing
- Alcune tra le principali metodologie sono le seguenti
 - **Open Source Security Testing Methodology Manual (OSSTMM)**
 - **Information Systems Security Assessment Framework (ISSAF)**
 - **Open Web Application Security Project (OWASP)**
 - **Web Application Security Consortium Threat Classification (WASC-TC)**
 - **Penetration Testing Execution Standard (PTES)**
 - **NIST Special Publication (SP) 800-115**



OWASP
Open Web Application
Security Project



NIST
National Institute of
Standards and Technology

Metodologie di Testing

Open Source Security Testing Methodology Manual (OSSTMM)

➤ Open Source Security Testing Methodology Manual (OSSTMM)

- Nata nel 2001
- Creata da Pete Herzog e sviluppata da *ISECOM (Institute for Security and Open Methodologies)*
- Versione Stabile: 3.0
- Versione Draft: 4.0
- Metodologia molto complessa



Metodologie di Testing

Open Source Security Testing Methodology Manual (OSSTMM)

➤ Open Source Security Testing Methodology Manual (OSSTMM)

- Metodologia completa che permette di
 - Gestire penetration testing, vulnerability assessment e security audit
 - Definire le «migliori difese di sicurezza possibili» per un determinato asset



Metodologie di Testing

Open Source Security Testing Methodology Manual (OSSTMM)

OSSTMM 3

The Open Source Security Testing Methodology Manual
Contemporary Security Testing and Analysis



Created by Pete Herzog
Developed by ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

<https://www.isecom.org/OSSTMM.3.pdf>

Metodologie di Testing

OSSTMM – Aspetti Chiave

- Alcuni **aspetti chiave** della **metodologia OSSTMM** sono
 - **Focus Operativo:** identificazione e valutazione delle vulnerabilità tecniche, dei processi operativi, della sicurezza fisica e dei fattori umani, fornendo una visione completa della sicurezza di un determinato asset
 - **Test dei Canali:** analisi dei canali di comunicazione in entrata ed in uscita da/verso un asset, ad es., Bluetooth, Wi-Fi, VoIP, SMS, E-mail, Web, etc
 - **Metriche e Misurazioni:** introduzione di misurazioni e metriche oggettive nel processo di valutazione della sicurezza, consentendo un'analisi quantitativa, anziché una semplice valutazione di tipo *pass/fail*
 - **Risk Assessment Value (RAV) Score** – Maggiori dettagli in seguito...
 - **Previsioni sulla Sicurezza:** stima di quanto l'asset rimanga sicuro nel tempo in base ai suoi controlli di sicurezza
 - **Superficie di Attacco:** identificazione dei punti tramite cui un utente malintenzionato potrebbe inserire o esfiltrare dati da un sistema



Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

➤ Un test di sicurezza secondo OSSTMM prevede 7 passi

1. Definire le **Risorse** che si intende proteggere (*asset*)

➤ I meccanismi di protezione per queste risorse sono detti **Controlli**, i quali saranno valutati per identificare le **Limitazioni** dal punto di vista della sicurezza (i.e., *vulnerabilità*)

2. Identificare l'**Area (o Zona) di Ingaggio**

➤ È qui che avrà luogo l'interazione con gli asset

➤ Tale area può includere, oltre ai meccanismi di protezione, anche i processi ed i servizi utilizzati o erogati dagli asset



Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

- Un test di sicurezza secondo OSSTMM prevede 7 passi
- 3. Identificare tutto ciò che è necessario, al di fuori dell'**Area di Ingaggio**, per mantenere operativi gli asset
 - Ciò potrebbe includere elementi
 - Che non possono essere controllati direttamente dall'asset, come elettricità, fattori climatici, legislazione, regolamenti, etc
 - Con cui l'asset si potrebbe trovare ad interagire, come appaltatori, colleghi, branding, partnership, etc
 - Bisognerebbe considerare anche altri elementi che mantengono operativi gli asset, come processi, protocolli, risorse, etc
- Ciò che è stato identificato dai punti 2. e 3. rappresenta l'**Ambito di Valutazione**



Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

- Un test di sicurezza secondo OSSTMM prevede 7 passi
- 4. Definire come avvengono le «*interazioni*» sia all'interno dell'**Ambito di Valutazione** che verso il suo esterno
 - Compartimentare logicamente le risorse appartenenti all'**Ambito di Valutazione**, basandosi sulla «*direzione*» delle interazioni effettuate da tali risorse
 - Ad es., dall'interno dell'asset verso l'esterno, dall'esterno verso l'interno, dall'interno verso l'interno, dalla risorsa A alla risorsa B, etc
 - Ad es., la ricezione di una e-mail da parte di una persona appartenente all'asset, sarà una interazione dall'esterno dell'asset verso il suo interno.
 - Tali interazioni sono chiamate **Vettori**
 - Ciascun vettore dovrebbe essere valutato da un test di sicurezza separato, così da mantenere breve la durata di ciascun test prima che possano verificarsi cambiamenti significativi nell'asset



Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

- Un test di sicurezza secondo OSSTMM prevede 7 passi
- 5. Identificare i **Canali** da valutare per ogni test
 - All'interno di ciascun **Vettore** le *interazioni* possono avvenire utilizzando cinque **Canali**: *Human, Physical, Wireless, Telecommunications e Data Networks*
 - Maggiori dettagli in seguito...
 - Ogni **Canale** deve essere valutato separatamente per ciascun **Vettore**



Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza – Canali

Class	Channel	Descrizione
Physical Security (PHYSSEC)	Human	<i>"Comprises the human element of communication where interaction is either physical or psychological"</i>
	Physical	<i>"Physical security testing where the channel is both physical and non-electronic in nature"</i>
Spectrum Security (SPECSEC)	Wireless	<i>"Comprises all electronic communications, signals, and emanations which take place over the known EM spectrum"</i>
Communications Security (COMSEC)	Telecommunications	<i>"Comprises all telecommunication networks, digital or analog, where interaction takes place over established telephone or telephone-like network lines"</i>
	Data Networks	<i>"Comprises all electronic systems and data networks where interaction takes place over established cable and wired network lines"</i>

Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

- Un test di sicurezza secondo OSSTMM prevede 7 passi
- 6. Determinare le informazioni che si vogliono acquisire dal test
 - Ad es., se verranno valutate solo le interazioni con l'asset (i.e., valutazione di ciascun **Canale** per ciascun **Vettore**, etc) o anche le misure di sicurezza poste a protezione dell'asset (*firewall, IDS, etc*)
 - I tipi di test da condurre: la metodologia OSSTMM definisce sei **Tipi di Test**: *Blind, Double Blind, Grey Box, Double Grey Box, Tandem e Reversal*
 - Maggiori dettagli in seguito...
 - Etc



Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

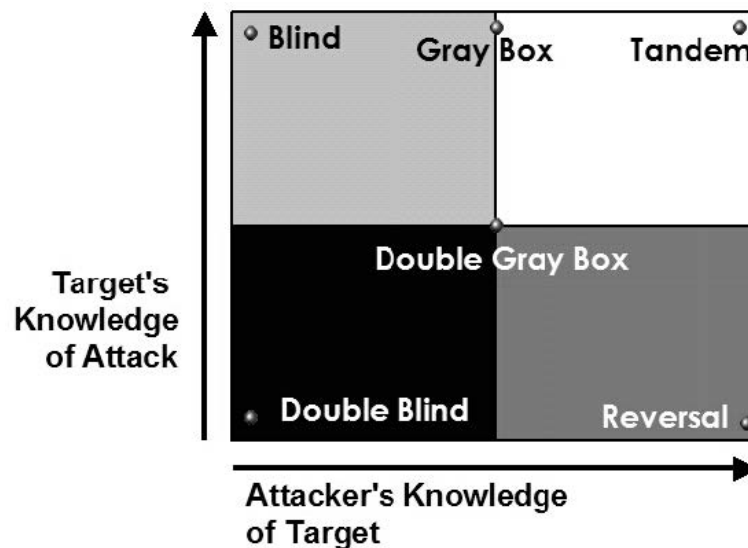
- Un test di sicurezza secondo OSSTMM prevede 7 passi
- 7. Assicurarsi che i test di sicurezza definiti tramite i passi precedenti siano conformi alle **Regole di Ingaggio**
 - **Regole di Ingaggio:** Linee guida per garantire che il processo di valutazione della sicurezza sia autorizzato, adeguato, e non crei incomprensioni, idee sbagliate o false aspettative
 - Maggiori dettagli in seguito...
- Il risultato finale, dato dall'esecuzione dei test di sicurezza, fornirà informazioni quantitative (i.e., *misurazioni* date dal RAV Score) sulla **Superficie di Attacco**
 - La **Superficie di Attacco** rappresenta la parte non protetta dell'**Ambito di Valutazione**



Metodologie di Testing

OSSTMM – Tipi di Test

- I tipi di test si differenziano in base alla quantità di informazioni che
 - Il pentester possiede sull'asset (Asse X)
 - L'asset possiede sul pentester (Asse Y)



Target = *asset*
Attacker = *pentester*

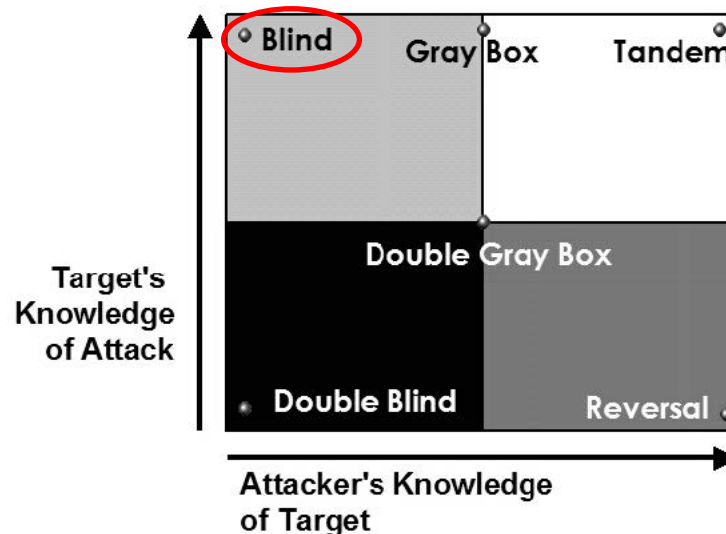


Metodologie di Testing

OSSTMM – Tipi di Test

➤ Blind

- Non richiede al pentester alcuna conoscenza preliminare sull'asset da valutare
- L'asset viene informato prima dell'esecuzione del test
- Ciò rende questo tipo di test ampiamente accettato

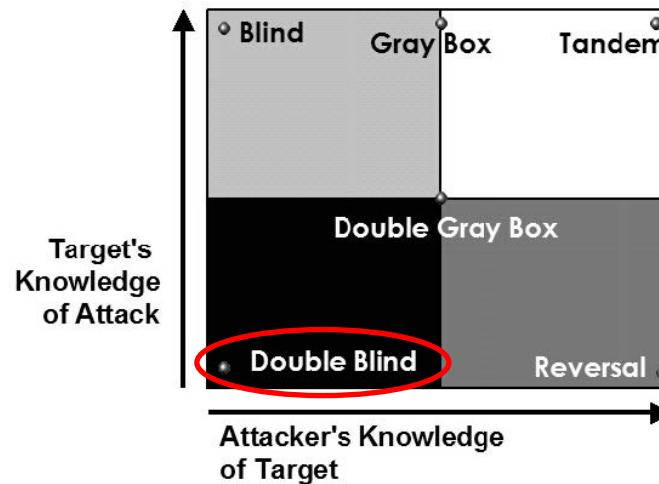


Metodologie di Testing

OSSTMM – Tipi di Test

➤ Double Blind

- Né il pentester ha alcuna conoscenza dell'asset né l'asset viene informato prima dell'esecuzione del test
- **N.B.** La maggior parte delle valutazioni di sicurezza oggi viene eseguita utilizzando questa strategia

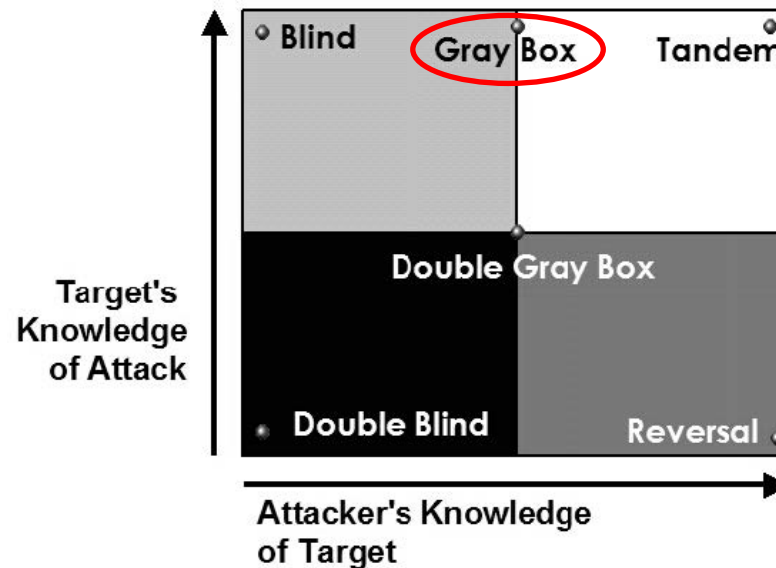


Metodologie di Testing

OSSTMM – Tipi di Test

➤ Gray Box

- Il pentester ha conoscenza limitata sull'asset
- L'asset viene informato prima dell'esecuzione del test

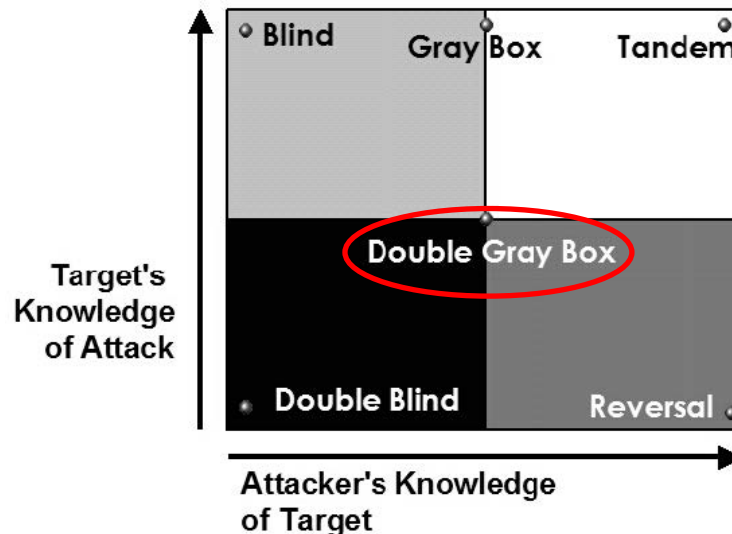


Metodologie di Testing

OSSTMM – Tipi di Test

➤ Double Gray Box

- Opera in modo analogo al Gray Box testing: il pentester ha conoscenza parziale sull'asset e l'asset viene informato solo parzialmente sull'esecuzione del test
- Pone generalmente specifici vincoli sulla durata del test

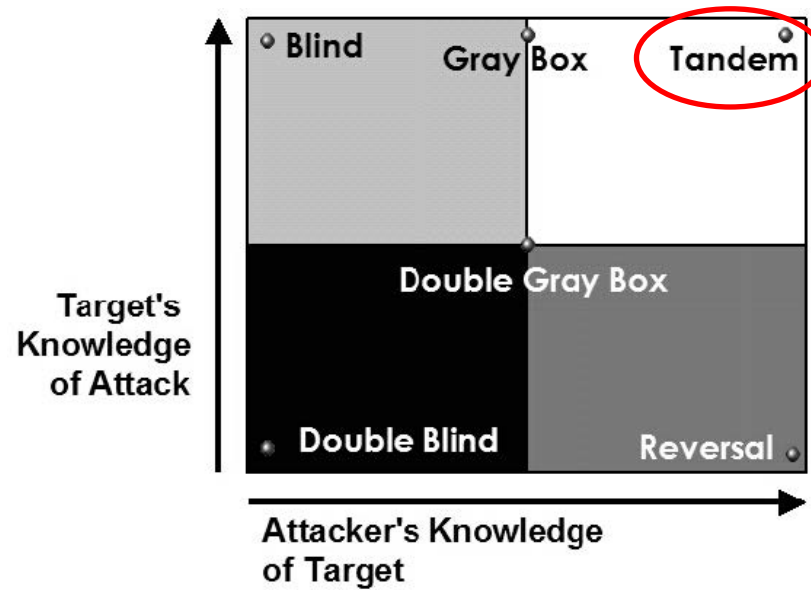


Metodologie di Testing

OSSTMM – Tipi di Test

➤ Tandem

- Il pentester ha piena conoscenza dell'asset
- L'asset è informato su come e quando verrà condotto il test

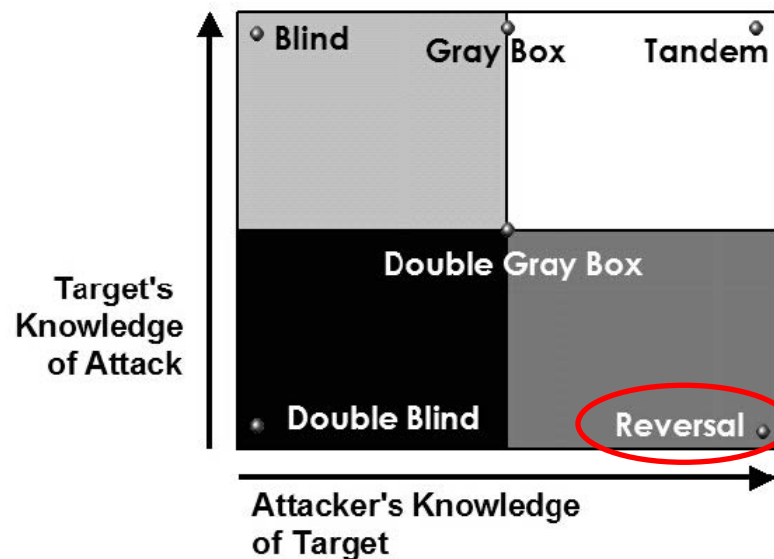


Metodologie di Testing

OSSTMM – Tipi di Test

➤ Reversal

- Il pentester ha piena conoscenza dell'asset
- L'asset non ha alcuna conoscenza del pentester



Metodologie di Testing

OSSTMM – Casi e Procedure di Test

- OSSTMM permette anche di definire **Casi di Test**, che generalmente valutano aspetti quali
 - Sicurezza del controllo accessi
 - Sicurezza dei processi
 - Controllo dei dati
 - Protezione perimetrale
 - Livello di consapevolezza della sicurezza da parte del personale
 - Etc



Metodologie di Testing

OSSTMM – Casi e Procedure di Test

- Le **Procedure di Test** si concentrano su
 - Cosa deve essere valutato (asset)
 - Come deve avvenire la valutazione
 - Quali azioni devono essere messe in atto prima, durante e dopo la valutazione
 - Come devono essere interpretati e correlati i risultati ottenuti al termine della valutazione



Metodologie di Testing

OSSTMM – Risk Assessment Value (RAV) Score

- Al termine del processo di valutazione viene calcolato un valore (*metrica*) di sicurezza
 - **RAV (Risk Assessment Value) Score**
- **RAV Score**
 - Rappresenta lo stato dell'asset in termini di sicurezza
 - Può essere usato
 - Dal pentester per fornire un'idea precisa sulla sicurezza di un asset
 - Da un'organizzazione per ottimizzare la quantità di investimenti richiesti per la messa in sicurezza del proprio asset



Metodologie di Testing

OSSTMM – Risk Assessment Value (RAV) Score

- Mostra quanto un asset sia sicuro
- È un valore quantitativo, di tipo numerico
 - Un **RAV Score** pari a **100** denota una «sicurezza perfetta»
 - Equilibrio «ottimale» tra **Vettori** e **Controlli**
 - Un **RAV Score inferiore a 100** evidenzia quali **controlli** sono **insufficienti o assenti**
 - Quando il **RAV Score** è 100 e vengono aggiunti ulteriori controlli esso **supera 100**
 - Ciò denota che si stanno «**sprecando**» **risorse**: «inutile» investire risorse per migliorare qualcosa che è già «perfettamente sicuro»




Metodologie di Testing

OSSTMM – Risk Assessment Value (RAV) Score

➤ RAV Calculator

- Foglio di calcolo che permette di ottenere un **RAV Score**
 - Metrica standard per misurare la **Superficie di Attacco** di un asset
- Necessario per completare il **Security Test Audit Report (STAR) Sheet**

Attack Surface Security Metrics					
OSSTMM version 3.0					
Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.					
OPSEC					
Visibility	0				
Access	0				
Trust	0				
Total (Porosity)	0				
					
					OPSEC 0.000000



https://www.isecom.org/rav_calc_OSSTMM3.xls

Metodologie di Testing

OSSTMM – Security Test Audit Report (STAR) Sheet

➤ **Security Test Audit Report (STAR) Sheet**

- Riepilogo, in formato standard, dei risultati prodotti da unsecurity audit, vulnerability assessment o penetration testing OSSTMM
- Fornisce in maniera strutturata
 - Indicazioni precise sulla **Superficie di Attacco**
 - Dettagli su cosa è stato valutato e come
- Il Security Test Audit Report (STAR) Sheet è richiesto quando la sicurezza di un asset deve essere certificata secondo la ISECOM OSSTMM



Metodologie di Testing

OSSTMM – Security Test Audit Report (STAR) Sheet – Esempio



Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

STAR Sheet

Report ID

Date

Lead Auditor

Test Date Duration

Scope and Index

Vectors

Channels

Test Type

I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE

COMPANY STAMP/SEAL

OPST Certification #

OPSA Certification #



Metodologie di Testing

OSSTMM – Principali Vantaggi

- Si adatta a molti tipi di test di sicurezza
 - Penetration Testing, Vulnerability Assessment, Security Audit
- Riduce il verificarsi di falsi positivi e falsi negativi
- Fornisce metriche di sicurezza riproducibili
- Garantisce che
 - La valutazione di sicurezza sia condotta in maniera accurata
 - I risultati siano raccolti in modo coerente, quantificabile ed affidabile



Metodologie di Testing

OSSTMM – Principali Vantaggi

- «Aggiornata» in base alle nuove tendenze dei test di sicurezza, alle regolamentazioni ed alle questioni etiche
- Si adatta facilmente alle *best practice* del settore, alle politiche aziendali ed alle norme
- Una verifica di sicurezza certificata in base alla metodologia OSSTMM può essere accreditata direttamente dall'*ISECOM (Institute for Security and Open Methodologies)*



Metodologie di Testing

Open Source Security Testing Methodology Manual (OSSTMM)

- Fornisce varie tipologie di certificazione
- <https://www.isecom.org/certification.html>



OSSTMM Professional Security Analyst

The OPSA is a technical, skills-based certification designed to accredit professional security analysts.



OSSTMM Professional Security Tester

The OPST is a technical, skills-based certification designed to accredit professional penetration testers.



OSSTMM Professional Security Expert

The OPSE is an introductory, knowledge-based certification designed to accredit security professionals working with the OSSTMM.



Metodologie di Testing

Open Source Security Testing Methodology Manual (OSSTMM)

- Fornisce varie tipologie di certificazione
- <https://www.isecom.org/certification.html>



OSSTMM Wireless Security Expert

The OWSE is a technical, knowledge-based certification designed to accredit professional penetration testers.



OSSTMM Certified Trust Analyst

The CTA is a knowledge-based certification designed to accredit professionals measuring trust or making trust-based decisions either in a business or security capacity.



Certified Security Awareness Instructor

The SAI is a knowledge-based certification designed to accredit professionals teaching cybersecurity awareness.

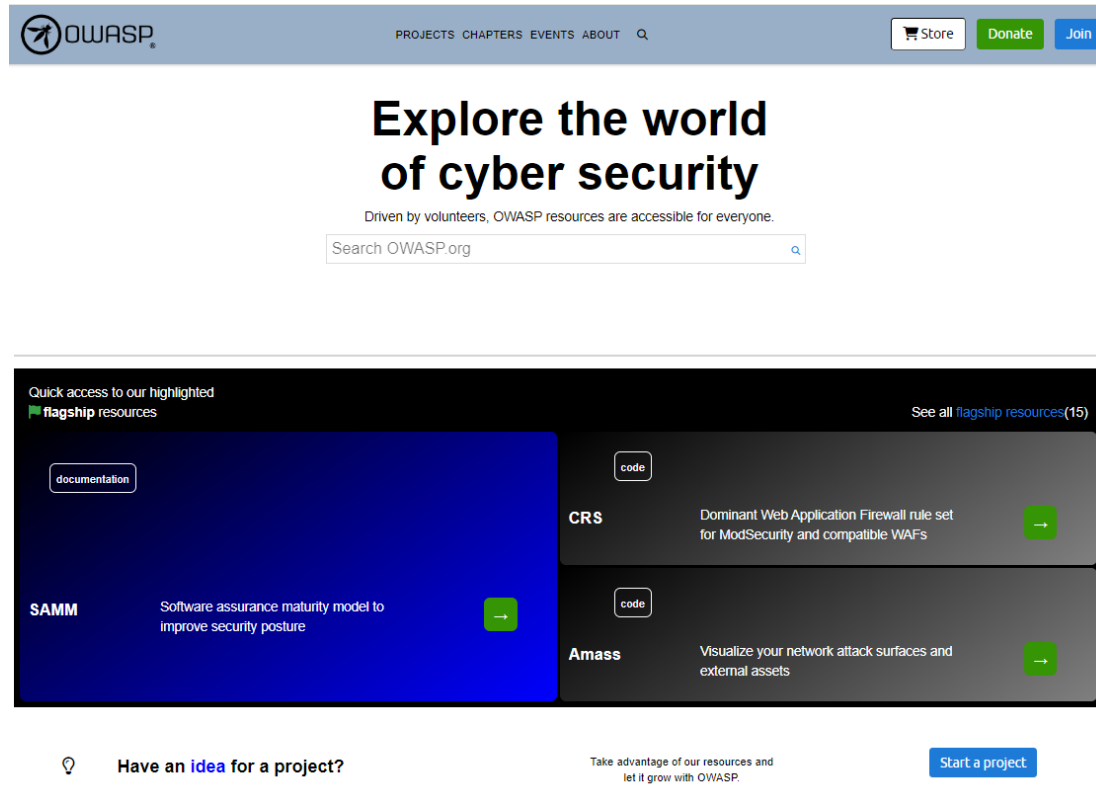


Metodologie di Testing

Open Web Application Security Project (OWASP)

➤ **Open Web Application Security Project (OWASP)**

➤ <https://owasp.org/>



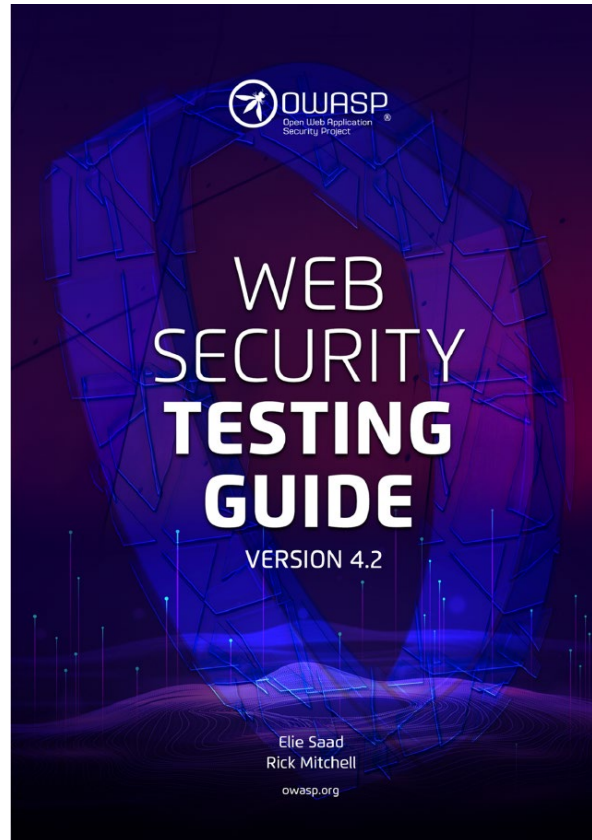
Metodologie di Testing

OWASP – Caratteristiche

- Fornisce
 - **Linee guida a sviluppatori e pentester** per gestire la sicurezza in diversi settori (applicazioni Web e mobile, sistemi IoT, firmware, etc) mediante vari progetti
 - **OWASP Web Security Testing Guide (WSTG)**
 - **OWASP Mobile Application Security (MAS)**
 - **OWASP Internet of Things Project**
 - **OWASP Top 10 Project**
 - **OWASP Top 10 for Large Language Model Applications**
 - Etc
 - **Numerosi strumenti** (tipicamente Open Source) per valutare la sicurezza in vari contesti
 - https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools

Metodologie di Testing

OWASP – Web Security Testing Guide (WSTG)



OWASP Web Security Testing Guide 4.2



Metodologie di Testing

OWASP – Web Security Testing Guide (WSTG)

- Fornisce linee guida per
 - Integrare la sicurezza nelle Web Application e nei Web Service attraverso principi e pratiche di programmazione sicura
 - Effettuare il penetration testing di Web Application e Web Service
- È costituita da due sezioni principali
 - **Web Security Testing Framework**
 - **Web Application Security Testing**

Metodologie di Testing

OWASP – WSTG – Web Security Testing Framework

- Definisce generiche linee guida ed attività da utilizzare per il controllo della sicurezza nelle varie fasi del ciclo di vita di un software
 - Può anche essere utilizzato per sviluppare testing framework ad hoc
- Utilizzato per valutare la sicurezza di un software durante le sue fasi di analisi dei requisiti, progettazione, sviluppo, distribuzione, configurazione e manutenzione
 - Evitando così di attendere fino al completamento della creazione di un software per poterne valutare la sicurezza
- Non definisce una particolare metodologia di sviluppo e non fornisce indicazioni specifiche appartenenti ad una determinata metodologia
 - Modello di sviluppo generico, che può essere seguito e adattato in base alle proprie esigenze

Metodologie di Testing

OWASP – WSTG – Web Security Testing Framework

- Definisce una serie di attività che dovrebbero essere condotte
 - Prima che inizi lo sviluppo del software
 - In fase di definizione e progettazione del software
 - Durante lo sviluppo del software
 - Durante la distribuzione del software
 - Durante la configurazione, il funzionamento e la manutenzione del software

Metodologie di Testing

OWASP – WSTG – Web Application Security Testing

- Si concentra sulla valutazione della sicurezza di una Web application (già creata)
- Consente di effettuare *analisi* di sicurezza *passive o attive* di una Web application per rilevare eventuali punti deboli, difetti tecnici o vulnerabilità
- Eventuali problemi di sicurezza riscontrati verranno presentati al committente, insieme a
 - Una valutazione dell'impatto
 - Una proposta di mitigazione o una soluzione tecnica

Metodologie di Testing

OWASP – WSTG – Web Application Security Testing

- Raccoglie e descrive numerose tecniche di analisi della sicurezza per le Web application, mantenendosi costantemente aggiornato
- Si basa su un approccio «black box»
 - Il pentester non sa nulla (o ha pochissime informazioni) sull'applicazione da testare
- Tale framework è costituito da tre elementi principali
 - *Tester*: chi esegue le attività di testing
 - *Strumenti e Metodologie*: la parte più importante del Web Application Security Testing, che stabilisce in che modo deve essere condotta l'analisi
 - *Applicazione*: la «black box» da valutare

Metodologie di Testing

OWASP – WSTG – Web Application Security Testing

➤ L'attività di **testing** può essere di tipo **attivo** o **passivo**

➤ **Testing Passivo**

➤ Il pentester cerca di comprendere la logica dell'applicazione, utilizzandola ed esplorandola così come farebbe un normale utente

➤ **Testing Attivo**

➤ Il pentester effettua un insieme di test, raggruppati in 12 categorie

- | | |
|---|-----------------------------------|
| 1. <i>Information Gathering</i> | 9. <i>Cryptography</i> |
| 2. <i>Configuration and Deployment Management Testing</i> | 10. <i>Business Logic Testing</i> |
| 3. <i>Identity Management Testing</i> | 11. <i>Client-side Testing</i> |
| 4. <i>Authentication Testing</i> | 12. <i>API Testing</i> |
| 5. <i>Authorization Testing</i> | |
| 6. <i>Session Management Testing</i> | |
| 7. <i>Input Validation Testing</i> | |
| 8. <i>Error Handling</i> | |

Metodologie di Testing

OWASP – Web Security Testing Guide (WSTG)

- La *OWASP Web Security Testing Guide* fornisce anche dettagli sulla valutazione specifica delle tecnologie
- Visione ampia e collaborativa di numerose tecnologie
 - Per supportare il pentester nella scelta della procedura di testing più adeguata