Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Tipi e Metodologie di Testing
Parte 2

Arcangelo Castiglione
arcastiglione@unisa.it

Tipologie di Test di Sicurezza
Vulnerability Assessment

- Identifica, tipicamente tramite strumenti automatici (ma anche manuali), tutte le potenziali vulnerabilità che potrebbero essere sfruttate da un attaccante

- Utilizzato per valutare
  - La Sicurezza Fisica
  - Il Personale (attraverso tecniche di *Social Engineering* e similari)
  - La Sicurezza dei Sistemi
  - La Sicurezza delle Reti
  - Etc

Tipologie di Test di Sicurezza
Vulnerability Assessment

- Valuta i controlli di sicurezza interni ed esterni
- Indica i «potenziali» rischi nelle difese esistenti
- Raccomanda e dà priorità alle strategie per porre rimedio ai rischi

Tipologie di Test di Sicurezza
Vulnerability Assessment

- Due tipologie di Vulnerability Assessment
  - **Vulnerability Assessment Interno** si occupa della sicurezza dei sistemi interni
  - **Vulnerability Assessment Esterno** si occupa della sicurezza delle difese perimetrali

- In entrambe le tipologie, ogni componente dell'asset (informatica, umana e fisica) è valutata usando più modalità e strumenti di attacco
  - Così da poter rilevare eventuali minacce e quantificare le misure da intraprendere per far fronte a tali minacce

Tipologie di Test di Sicurezza
Vulnerability Assessment

- **Osservazione**
  - La scoperta di una vulnerabilità non implica che si tratti di un problema di cui preoccuparsi
  - Tale vulnerabilità potrebbe non essere sfruttabile o, qualora essa venisse sfruttata, potrebbe non causare danni all'asset in cui essa risiede

Tipologie di Test di Sicurezza
Penetration Testing

- Processo che emula fedelmente le azioni (malevole) che potrebbe effettuare un attaccante
  - Violare un sistema sfruttando le sue vulnerabilità
  - Ottenere i massimi privilegi possibili nel sistema violato (ad es., *root*, *Administrator*, etc), assumendone il totale controllo
    - Furto di dati, spionaggio, etc
  - Causare malfunzionamenti al sistema
  - Etc

- Processo anche noto come *Ethical Hacking*

Tipologie di Test di Sicurezza
Penetration Testing

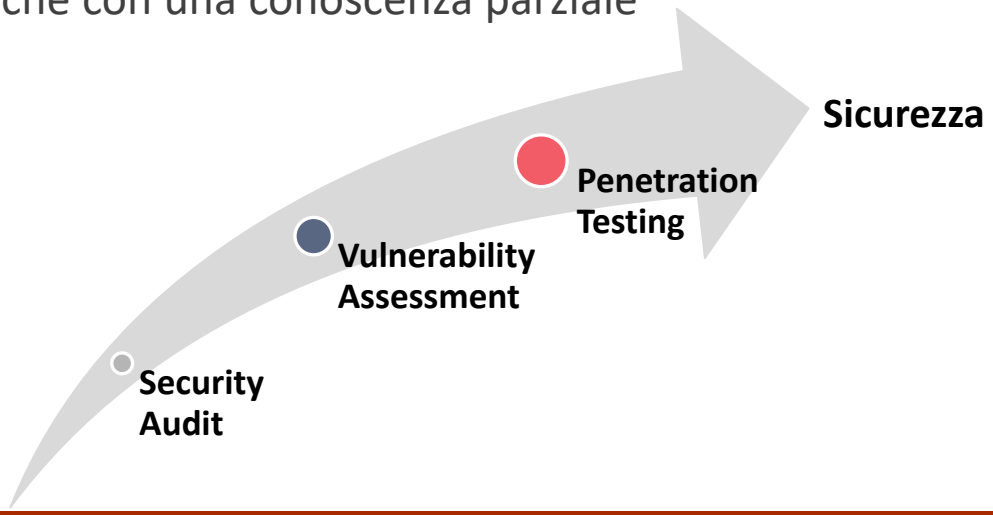
- Il Penetration Testing potrebbe essere eseguito
  - **Indipendentemente**, come processo stand-alone, oppure
  - **Durante un processo di gestione dei rischi**, incorporato nel normale ciclo di vita dello sviluppo software
    - Ad es., *Microsoft Security Development Lifecycle (SDL)*

Tipologie di Test di Sicurezza
Penetration Testing

- **Osservazione:** La sicurezza di un asset non dipende solo da fattori tecnologici ma anche da altri
  - Controllo degli accessi fisici
  - Sorveglianza degli ambienti
  - Definizione ed implementazione di adeguate politiche di sicurezza
  - Analisi dei comportamenti del personale
  - Formazione del personale
  - Etc

Tipologie di Test di Sicurezza
Penetration Testing

- Il **penetration testing** è considerato come la **più «aggressiva» forma di valutazione della sicurezza**
  - Deve essere condotto da professionisti qualificati
- Può essere condotto con o senza la conoscenza preliminare dell'asset da analizzare
  - Talvolta anche con una conoscenza parziale



Tipologie di Test di Sicurezza
Penetration Testing

- Il penetration testing è tipicamente usato per valutare tutte le componenti di un asset
  - Applicazioni
  - Dispositivi di Rete
  - Sistemi Operativi
  - Mezzi di Comunicazione
  - Sicurezza Fisica
  - Psicologia Umana
  - Etc

Vulnerability Assessment vs. Penetration Testing

- **Vulnerability Assessment**
  - Fornisce una visione esaustiva dei difetti dell'asset in esame
    - Non misura l'impatto dei difetti sull'asset
  - Identifica e quantifica in modo non invasivo tutte le vulnerabilità (tipicamente, note) dell'asset
- **Penetration Testing**
  - Va oltre l'identificazione delle vulnerabilità
    - Include le fasi di **Exploitation** e **Post-Exploitation**
  - Notevolmente più intrusivo del Vulnerability Assessment
    - Utilizza tutte le metodologie e gli strumenti usati da un attaccante reale (i.e., *Black Hat Hacker*)

Outline

- Terminologia
- Tipologie di Test di Sicurezza
- **Tipi di Penetration Testing**
- Metodologie di Testing
- Framework Generale per il Penetration Testing
- 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

Tipi di Penetration Testing
Come Scegliere il Tipo di Test?

- In generale, un'organizzazione
  - 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
- Penetration Testing Report

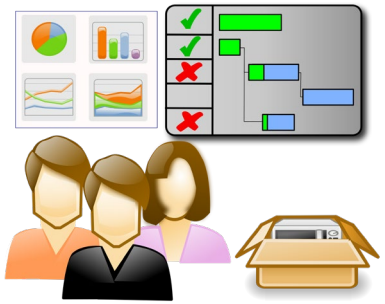
Metodologie di Testing
Motivazioni

- 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

- Alcune metodologie si concentrano su aspetti tecnici, altre su criteri manageriali
  - Pochissime su entrambi



Metodologie di Testing
Come Scegliere quella Migliore?

- 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
  - 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
  - **O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual (**OSSTMM**)
  - **I**nformation **S**ystems **S**ecurity **A**ssessment **F**ramework (**ISSAF**)
  - **O**pen **W**eb **A**pplication **S**ecurity **P**roject (**OWASP**)
  - **W**eb **A**pplication **S**ecurity **C**onsortium **T**hreat **C**lassification (**WASC-TC**)
  - **P**enetration **T**esting **E**xecution **S**tandard (**PTES**)
  - **NIST S**pecial **P**ublication (**SP**) **800-115**

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

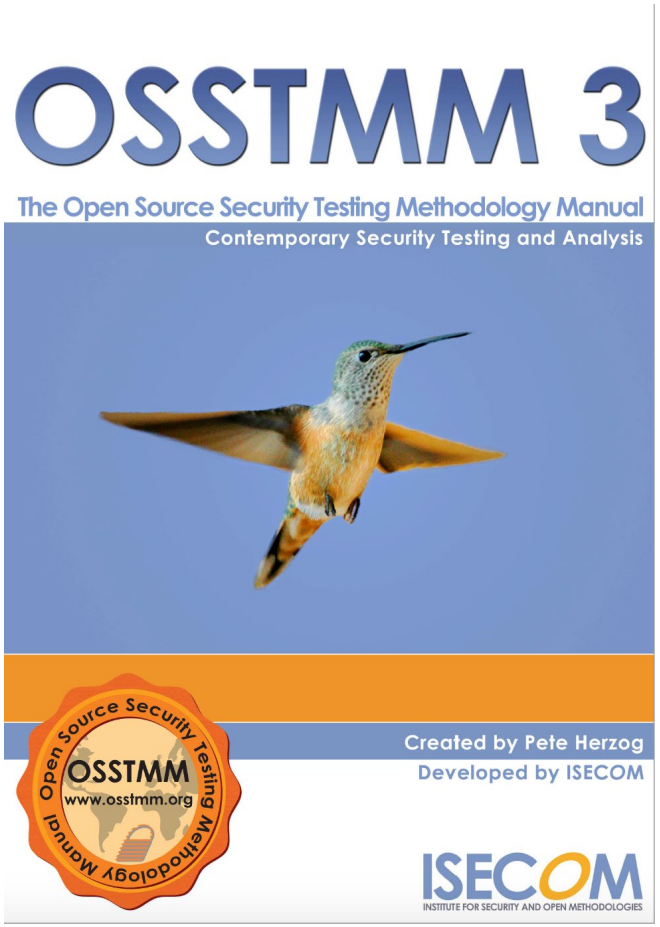
Metodologie di Testing

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)



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 olistica 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*
    - ***R**isk **A**ssessment **V**alue* (***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 diversi punti in cui un utente malintenzionato può tentare di inserire o estrarre 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 ed altre risorse

- 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*» all'interno dell'**Ambito di Valutazione** e 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 all'esterno, dall'esterno all'interno, dall'interno all'interno, dalla risorsa A alla risorsa B, etc
   - Tali interazioni sono chiamate **Vettori**
   - Ciascun vettore dovrebbe essere valutato da un test separato, così da mantenere breve la durata di ciascun test prima che possano verificarsi cambiamenti significativi nell'ambiente operativo

Metodologie di Testing

OSSTMM – Definizione di un Test di Sicurezza

- Un test di sicurezza secondo OSSTMM prevede 7 passi

5. Identificare quali attrezzature saranno necessarie 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**
6. Determinare le informazioni che si vogliono acquisire dal test
   - Ad es., se verranno valutate solo le interazioni con gli asset (i.e., valutazione di ciascun **Canale** per ciascun **Vettore**) o anche le misure di sicurezza poste a protezione dell'asset (*firewall*, *IDS*, etc)
   - La metodologia OSSTMM definisce sei **Tipi di Test** comuni: *Blind*, *Double Blind*, *Grey Box*, *Double Grey Box*, *Tandem* e *Reversal*
     - Maggiori dettagli in seguito…

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 che sono stati definiti siano conformi alle **Regole di Ingaggio**
   - Linee guida per garantire che il processo di valutazione della sicurezza sia adeguato, e non crei incomprensioni, idee sbagliate o false aspettative

- Il risultato finale di un 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** rispetto ad un determinato **Vettore**