Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

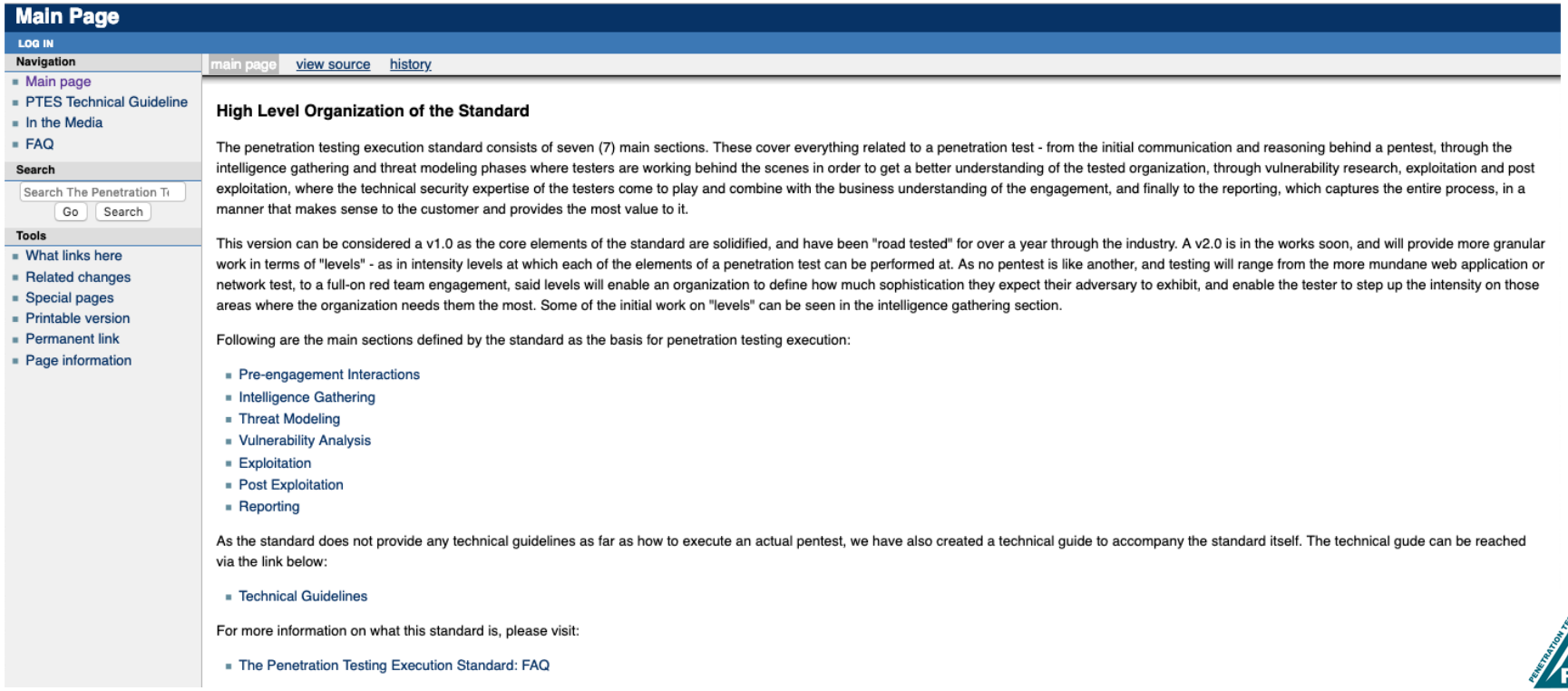
Tipi e Metodologie di Testing
Parte 4

Arcangelo Castiglione
arcastiglione@unisa.it

Metodologie di Testing

Penetration Testing Execution Standard (PTES)

- **P**enetration **T**esting **E**xecution **S**tandard (**PTES**)
  - http://www.pentest-standard.org/index.php/Main_Page



Main Page

LOG IN

Navigation
- Main page
- PTES Technical Guideline
- In the Media
- FAQ

Search

Search The Penetration Te

Go Search

Tools
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

main page | view source | history

High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "road tested" for over a year through the industry. A v2.0 is in the works soon, and will provide more granular work in terms of "levels" - as in intensity levels at which each of the elements of a penetration test can be performed at. As no pentest is like another, and testing will range from the more mundane web application or network test, to a full-on red team engagement, said levels will enable an organization to define how much sophistication they expect their adversary to exhibit, and enable the tester to step up the intensity on those areas where the organization needs them the most. Some of the initial work on "levels" can be seen in the intelligence gathering section.

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we have also created a technical guide to accompany the standard itself. The technical gude can be reached via the link below:

- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

Metodologie di Testing
Penetration Testing Execution Standard (PTES)

- Sviluppato da un gruppo di esperti di sicurezza per fornire una metodologia di penetration testing ripetibile e coerente
- Può essere utilizzato per eseguire un processo di penetration testing in un qualsiasi dominio applicativo
- Definisce l'intero processo di penetration testing in maniera organizzata e completa
  - Il penetration testing è composto da sette fasi
  - Fasi descritte in maniera dettagliata
    - Mediante mappe concettuali che esplicitano le azioni da compiere in ciascuna di esse
- Aiuta a garantire la coerenza tra le varie fasi del processo e tra tutte le interazioni che possono avvenire all'interno di esso
- Si tratta della metodologia generale di penetration testing più simile a quella che sarà studiata nel prosieguo del corso

Metodologie di Testing
Penetration Testing Execution Standard (PTES)

- Nel PTES il processo di penetration testing è composto da 7 fasi
  1. *Pre-Engagement*: Stabilisce le regole di ingaggio, l'ambito di valutazione, i meccanismi di comunicazione tra le parti e gli accordi legali
  2. *Intelligence Gathering*: Identifica e caratterizza la presenza online dell'asset, raccogliendo informazioni su nomi di dominio, blocchi di indirizzi IP, nomi/e-mail dei dipendenti e le tecnologie utilizzate
  3. *Threat Modeling*: Crea modelli per caratterizzare come gli aggressori potrebbero violare l'asset e causare danni ad esso. Utilizzato come linea guida per i test
  4. *Vulnerability Analysis*: Scopre ed analizza le vulnerabilità tecniche, come i punti deboli del sistema operativo, della rete e delle applicazioni, e ne valuta la gravità
  5. *Exploitation*: Tenta di accedere all'asset o di comprometterne il regolare funzionamento
  6. *Post-Exploitation*: Esfiltra dati dall'asset, mantiene l'accesso persistente all'asset, aumenta i privilegi all'interno dell'asset, passa ad altri sistemi (*pivoting*)
  7. *Reporting*: Documenta le vulnerabilità rilevate e quelle sfruttate, fornendo un'analisi dei risultati ottenuti e consigliando opportune strategie di mitigazione

Metodologie di Testing

PTES – Principali Vantaggi

- Framework molto accurato che copre sia aspetti tecnici che gestionali di un processo di penetration testing
- Fornisce istruzioni dettagliate su come eseguire molte delle attività necessarie per valutare accuratamente la sicurezza di un asset
- Creato da penetration tester che svolgono queste attività quotidianamente
- Riguarda sia le tecnologie più comunemente utilizzate che quelle non molto comuni
  - Anche se non copre quelle più recenti
- È facile da comprendere e può essere adattato a varie esigenze e contesti di testing

Metodologie di Testing

ISSAF – Caratteristiche

- **I**nformation **S**ystems **S**ecurity **A**ssessment **F**ramework (**ISSAF**)
  - Framework Open Source
  - Suddiviso in diversi **domini**, che permettono di affrontare la valutazione della sicurezza secondo un preciso ordine logico
    - Ciascuno dominio valuta una parte dell'asset da analizzare

Metodologie di Testing

ISSAF – Caratteristiche

- Il framework si focalizza su due aspetti del testing
  - **Tecnico**
    - Stabilisce l'insieme di regole e procedure da seguire
    - Crea un processo di valutazione della sicurezza adeguato
  - **Manageriale**
    - Definisce le migliori pratiche che dovrebbero essere seguite durante la gestione del processo di penetration testing

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

Metodologie di Testing

ISSAF – Caratteristiche

- Contiene numerosi criteri di valutazione tecnica per testare numerose tecnologie e processi
- Può essere integrato nel ciclo di vita dell'organizzazione per soddisfare i suoi requisiti di sicurezza
- Affronta diversi aspetti della sicurezza
  - Valutazione dei rischi
  - Gestione delle risorse aziendali
  - Valutazione dei controlli di sicurezza
  - Sviluppo delle politiche di sicurezza
  - Best Practice

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

Metodologie di Testing

ISSAF – Caratteristiche

- Il framework può focalizzarsi su specifiche tecnologie
  - Router / Switch
  - Firewall
  - Intrusion Detection / Prevention System
  - Virtual Private Network
  - Sistemi Operativi
  - Web Application Server
  - Database
  - Etc

- **Problema:** mantenere aggiornato il framework rispetto all'introduzione di nuove tecnologie e processi

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

Metodologie di Testing

ISSAF – Principali Vantaggi

- Cerca di colmare il divario tra la visione tecnica e gestionale dei test di sicurezza
  - Implementando i controlli necessari per gestire entrambi gli aspetti

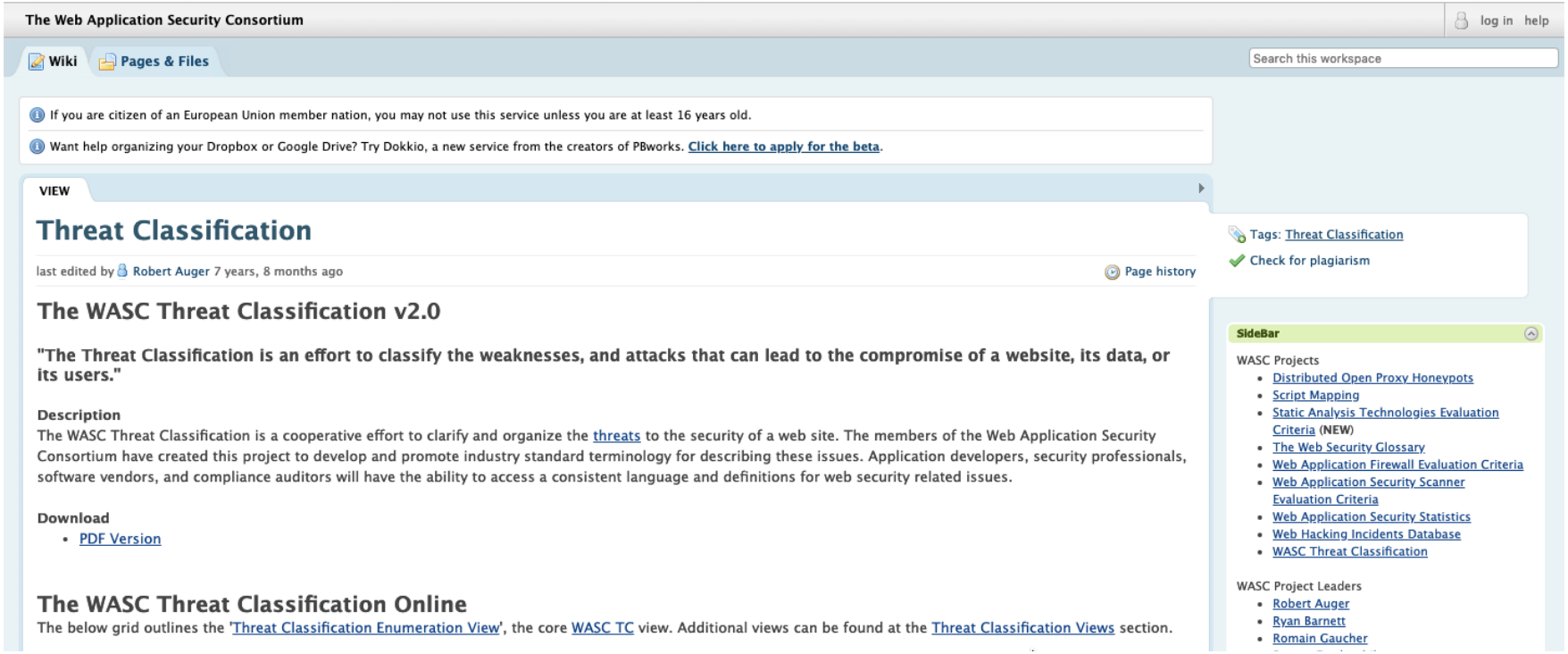
- Permette di
  - Esaminare la sicurezza di un asset
  - Proteggere l'asset valutando i controlli di sicurezza esistenti rispetto a vulnerabilità critiche
  - Comprendere i rischi esistenti in un asset e ridurli in modo proattivo
    - Identificando le vulnerabilità che possono influire sulla sicurezza dell'asset

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

Metodologie di Testing

Web Application Security Consortium: Threat Classification (WASC-TC)

- **W**eb **A**pplication **S**ecurity **C**onsortium: **T**hreat **C**lassification (WASC-TC)
  - http://www.webappsec.org/projects/threat/



Metodologie di Testing

Web Application Security Consortium: Threat Classification (WASC-TC)

- Standard Open Source per valutare la sicurezza delle Web App

- Simile allo standard OWASP
  - Classifica una serie di attacchi e vulnerabilità, ma li affronta in modo più approfondito

Web Application Security Consortium

Metodologie di Testing

Web Application Security Consortium: Threat Classification (WASC-TC)

- Lo standard definisce tre diverse **«view»**, che permettono di valutare da diverse «prospettive» le principali minacce di sicurezza per le Web App
  - *Enumeration View*
  - *Development View*
  - *Taxonomy Cross-reference View*

Web Application Security Consortium

Metodologie di Testing

WASC-TC – Enumeration View

- Fornisce una lista (enumerazione) delle principali «debolezze» e dei principali attacchi per le Web App

- Debolezze ed attacchi sono discussi individualmente (non a livello di macro-aree), fornendo per ciascuno di essi
  - Definizione concisa
  - Tipologia
  - Esempi su varie piattaforme di programmazione

Web Application Security Consortium

Metodologie di Testing

WASC-TC – Development View

- Fornisce allo sviluppatore una visione più completa sulla sicurezza di un determinato asset

- Definisce le vulnerabilità a partire da un insieme di debolezze ed attacchi che possono verificarsi in una delle seguenti fasi del ciclo di vita di una Web App
  1. Progettazione
  2. Sviluppo
  3. Distribuzione

Web Application Security Consortium

Metodologie di Testing

WASC-TC – Development View

- **Vulnerabilità di Progettazione:** introdotte quando le problematiche di sicurezza della Web App non sono state tenute in considerazione durante la fase di raccolta dei requisiti

- **Vulnerabilità di Implementazione:** si verificano a causa di regole e pratiche di programmazione sbagliate o non sicure

- **Vulnerabilità di Distribuzione:** causate dell'errata configurazione della Web App, del Web server o di altri sistemi ad essi relati

Web Application Security Consortium

Metodologie di Testing

WASC-TC – Taxonomy Cross-reference View

- Permette di «mappare» la terminologia usata da uno standard in quella usata da un altro standard
  - Talvolta per avere la conformità rispetto a più standard
  - Ciascuno standard definisce i propri criteri per valutare le Web App sotto diversi punti di vista e misura i rischi associati alle vulnerabilità

- Permette di valutare in maniera approfondita le Web App rispetto alle debolezze ed agli attacchi più comuni

- WASC-TC è accettato a livello industriale ed è utilizzato in molte soluzioni sia Open Source che commerciali

Web Application Security Consortium

Outline

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

Framework Generale per il Penetration Testing (FGPT)

- Kali Linux fornisce numerosi strumenti per condurre varie tipologie di test di sicurezza su un determinato asset

- L'uso di questi strumenti richiede un approccio strutturato
  - Framework secondo il quale tali strumenti possono operare

- Formalizzare il processo di penetration testing attraverso un approccio strutturato è estremamente importante
  - Sia dal punto di vista tecnico che gestionale

KALI
BY OFFENSIVE SECURITY

Framework Generale per il Penetration Testing (FGPT)

- Il framework definisce i passi da seguire durante un processo di penetration testing per valutare la sicurezza di un asset in modo efficace
  - Fornisce una panoramica delle tipiche fasi che un pentester dovrebbe condurre

- Include sia le tecnologie più comunemente utilizzate che quelle meno note

KALI
BY OFFENSIVE SECURITY

Framework Generale per il Penetration Testing (FGPT)

- È di facile apprendimento e può essere adattato a varie esigenze di testing
- Permette di realizzare sia approcci di tipo Black Box che White Box
- Ciascuno di questi approcci può essere «specializzato» in base all'asset da valutare
- Approccio generale che può essere
  - Combinato con una qualsiasi delle metodologie esistenti
  - Usato come linea guida tecnica ed operativa

KALI
BY OFFENSIVE SECURITY

Framework Generale per il Penetration Testing (FGPT)

- Il FGPT è costituito dalle seguenti fasi, tipicamente sequenziali

1. *Target Scoping*
2. *Information Gathering*
3. *Target Discovery*
4. *Enumerating Target*
5. *Vulnerability Mapping*
6. *Social Engineering*
7. *Target Exploitation*
8. *Privilege Escalation*
9. *Maintaining Access*

Target Post-Exploitation

10. *Documentation and Reporting*

KALI
BY OFFENSIVE SECURITY

Framework Generale per il Penetration Testing (FGPT)

- Un «qualsiasi sottoinsieme» di queste fasi può essere utilizzato sia in approcci di tipo Black Box che White Box

- Il pentester deve scegliere il migliore percorso di testing in base
  - Alle richieste del committente
  - Alla tipologia ed alla complessità dell'asset
  - Alle informazioni disponibili sull'asset prima dell'inizio del processo di penetration testing
  - Alle risorse che ha a disposizione (budget, tempo, personale, etc)

KALI
BY OFFENSIVE SECURITY

FGPT

Target Scoping

- Si occupa di comprendere l'ambito ed i «confini» del penetration testing

- Durante questa fase vengono tipicamente prese le seguenti decisioni
  - Cosa deve essere analizzato?
  - Come deve essere analizzato?
  - Quali condizioni devono essere applicate durante il processo di test?
  - Cosa limiterà l'esecuzione del processo di test?
  - Quanto in termini di risorse e tempo ci vorrà per completare il test?
  - Quali obiettivi tecnici/aziendali saranno raggiunti?

KALI
BY OFFENSIVE SECURITY

FGPT

Target Scoping

- Per condurre efficacemente un processo di penetration testing il pentester dovrebbe conoscere i seguenti fattori
  - Tecnologia che sta valutando
  - Funzionalità di base di tale tecnologia
  - Interazione di tale tecnologia con l'ambiente esterno

- La competenza e l'esperienza del pentester contribuiscono in maniera significativa al successo di un qualsiasi tipo di valutazione della sicurezza

KALI
BY OFFENSIVE SECURITY

FGPT

Information Gathering

- Il pentester per «conoscere meglio» il suo obiettivo (asset) consulta una serie di risorse pubblicamente disponibili
  - Forum
  - Bacheche
  - Albi
  - Articoli
  - Blog
  - Social Network
  - Siti Web
  - Etc

KALI
BY OFFENSIVE SECURITY

FGPT

Information Gathering

- Informazioni possono anche essere raccolte attraverso motori di ricerca
  - Google, Yahoo!, Microsoft Bing, Baidu, Yandex Search, etc

- Un pentester può utilizzare gli strumenti forniti da Kali Linux per raccogliere quante più informazioni possibili su un determinato asset
  - Informazioni di rete, Whois, Informazioni sul DNS e sugli spazi di indirizzamento
  - Indirizzi e-mail e numeri di telefono
  - Informazioni personali
  - Account utente
  - Etc

KALI
BY OFFENSIVE SECURITY

FGPT

Information Gathering

- Man mano che vengono raccolte ulteriori informazioni aumenta la probabilità di condurre con successo il processo di penetration testing

- Altra importante fonte di informazioni è il **Dark Web**
  - Tipicamente accessibile tramite TOR Browser
  - Contiene molte informazioni utili su vulnerabilità, exploit, etc
  - La ricerca nel Dark Web può fornire una visione più esaustiva sulle vulnerabilità e le minacce per un determinato asset

KALI
BY OFFENSIVE SECURITY

FGPT

Target Discovery

- Permette di
  - Determinare gli host attivi all'interno dell'asset ed i sistemi operativi in esecuzione su tali host
  - Caratterizzare ciascun host in base al proprio ruolo all'interno dell'architettura di rete
- Fornisce una visione completa delle tecnologie e dei dispositivi interconnessi in un determinato asset
- Gli strumenti per il target discovery generalmente implementano tecniche di rilevamento attivo e passivo

KALI
BY OFFENSIVE SECURITY

FGPT

Enumerating Target

- Utilizza numerose tecniche per la scansione delle porte
- Rileva le «porte aperte» sui sistemi analizzati
  - Le porte rilevate come «aperte» possono essere enumerate in base ai servizi che esse erogano
- Utile per valutare la «visibilità» delle porte anche se l'host è protetto da firewall o *Intrusion Detection System* (*IDS*)

KALI
BY OFFENSIVE SECURITY

FGPT

Enumerating Target

- I servizi associati alle porte aperte verranno ulteriormente analizzati per rilevare le vulnerabilità dell'asset

- Questa fase rappresenta il primo passo per la ricerca delle vulnerabilità nelle componenti dell'asset analizzato

KALI
BY OFFENSIVE SECURITY

FGPT

Vulnerability Mapping

- Identifica ed analizza le vulnerabilità in base alle porte aperte ed ai servizi erogati dall'asset

- Fase che può essere condotta tramite due approcci
  - Strumenti automatici
  - Manualmente

- La combinazione dei due approcci permette al pentester di esaminare sia vulnerabilità note che sconosciute (*0-day*)

KALI
BY OFFENSIVE SECURITY

FGPT

Social Engineering

- Praticare l'«arte dell'inganno» può essere «molto utile» quando non vengono rilevati punti di accesso (vulnerabilità sfruttabili) nell'asset analizzato

- Il social engineering rappresenta un'ulteriore opportunità da sfruttare per tentare di «violare» l'asset analizzato
  - Ingannando un utente attraverso l'esecuzione di codice dannoso che potrebbe consentire l'accesso all'asset stesso

KALI
BY OFFENSIVE SECURITY

FGPT

Social Engineering

- Il social engineering può essere attuato in varie forme, non solo digitali
  - Ad esempio, imitando il personale per entrare in un luogo fisico

- Ampia casistica di possibilità che potrebbero essere messe in atto per raggiungere l'obiettivo richiesto

KALI
BY OFFENSIVE SECURITY

FGPT

Social Engineering

- Condurre un attacco efficace potrebbe richiedere tempo
  - Necessario per comprendere la psicologia dell'obiettivo ed applicare la forma di inganno più adatta nei suoi confronti

- Fondamentale comprendere appieno le leggi nazionali ed internazionali in materia di social engineering prima di intraprendere questa fase
  - Che dovrebbe essere espressamente richiesta ed autorizzata dal committente

KALI
BY OFFENSIVE SECURITY

FGPT

Target Exploitation

- Dopo aver esaminato le vulnerabilità esistenti in un asset si cerca di «violarle» attraverso la rete sfruttando opportuni vettori di attacco (*exploit remoti*)

- Un pentester potrebbe anche utilizzare *exploit client-side* per assumere il controllo di un determinato asset
  - Veicolati alla vittima tramite tecniche di ingegneria sociale

- Potrebbero essere necessarie ulteriori ricerche o modifiche agli exploit esistenti per farli funzionare correttamente

KALI
BY OFFENSIVE SECURITY

FGPT

Target Exploitation

- Questa fase
  - Si concentra principalmente sul processo di «acquisizione» dell'asset analizzato
    - Per assumerne il controllo o per causare malfunzionamenti ad esso
  - È strettamente relata alle attività di *Post-Exploitation*
    - *Privilege Escalation*
    - *Maintaining Access*

KALI
BY OFFENSIVE SECURITY

FGPT

Privilege Escalation

- Una volta «acquisito» l'asset, un pentester potrebbe «operare» all'interno di esso
  - In base a determinati privilegi di accesso

- I privilegi potrebbero anche essere «aumentati» utilizzando opportuni strumenti
  - Che ad esempio permettono di ottenere i permessi di *super-user (root)* o di *amministratore* di sistema

KALI
BY OFFENSIVE SECURITY

FGPT

Privilege Escalation

- Lo scopo dell'attività di Privilege Escalation è quello di ottenere l'accesso all'asset disponendo dei massimi permessi possibili

- Questa attività può essere di portata *limitata* o *non limitata*, a seconda dello scopo del testing

KALI
BY OFFENSIVE SECURITY

FGPT

Privilege Escalation

- Dopo aver ottenuto l'accesso ad alcune componenti dell'asset, un pentester potrebbe
  - Acquisire ulteriori informazioni/permessi/visibilità sull'asset
    - Utilizzando *exploit locali*
    - Analizzando il traffico di rete (*Sniffing*)
    - Effettuando il «cracking» delle password di alcuni servizi
    - Sfruttando errate o improprie configurazioni dell'asset
    - Etc
  - Condurre ulteriori attacchi verso altre componenti dell'asset
    - *Pivoting*

KALI
BY OFFENSIVE SECURITY

FGPT

Maintaining Access

- Potrebbe essere necessario mantenere l'accesso all'asset per un determinato periodo di tempo (*persistenza*)
  - Ad esempio, per dimostrare l'accesso «non autorizzato» all'asset senza eseguire nuovamente l'intero processo di penetration testing

- Ciò consente di risparmiare tempo, costi e risorse per dimostrare l'accesso all'asset

KALI
BY OFFENSIVE SECURITY

FGPT

Maintaining Access

- Tipicamente l'accesso all'asset è mantenuto mediante software chiamati *backdoor*

- Questo tipo di accesso fornisce una visione chiara di come un attaccante potrebbe mantenere la propria persistenza all'interno dell'asset
  - Spesso, senza che ciò venga rilevato

KALI
BY OFFENSIVE SECURITY

FGPT

Documentation and Reporting

- Documentare, riportare e presentare le vulnerabilità rilevate e sfruttate
  - Penetration Testing Report
  - Rapporto di Scansione Dettagliato
  - Presentazione Digitale

- Fondamentale sia dal punto di vista etico che professionale
  - L'analisi delle vulnerabilità può permettere di risolverle o mitigarle

KALI
BY OFFENSIVE SECURITY

FGPT

Documentation and Reporting

- I report creati possono essere di diverso tipo
  - A seconda di chi dovrà utilizzarli per comprendere ed analizzare i punti deboli presenti nell'asset

- I report permettono anche di stabilire e confrontare la sicurezza dell'asset analizzato, prima e dopo il processo di penetration testing

KALI
BY OFFENSIVE SECURITY

Outline

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

Penetration Testing Report

Struttura – Cover Page

- Dovrebbe includere dettagli quali
  - Eventuali loghi delle entità (aziende, organizzazioni, etc) coinvolte nel processo di penetration testing
  - Titolo
  - Breve descrizione del processo effettuato

Penetration Test Report

MegaCorp One

August 10th, 2013

Penetration Testing Report

Struttura – Table of Contents

- Indice che permette di leggere anche solo determinate parti del penetration testing report

Table of Contents

Penetration Testing Report

Struttura – Executive Summary

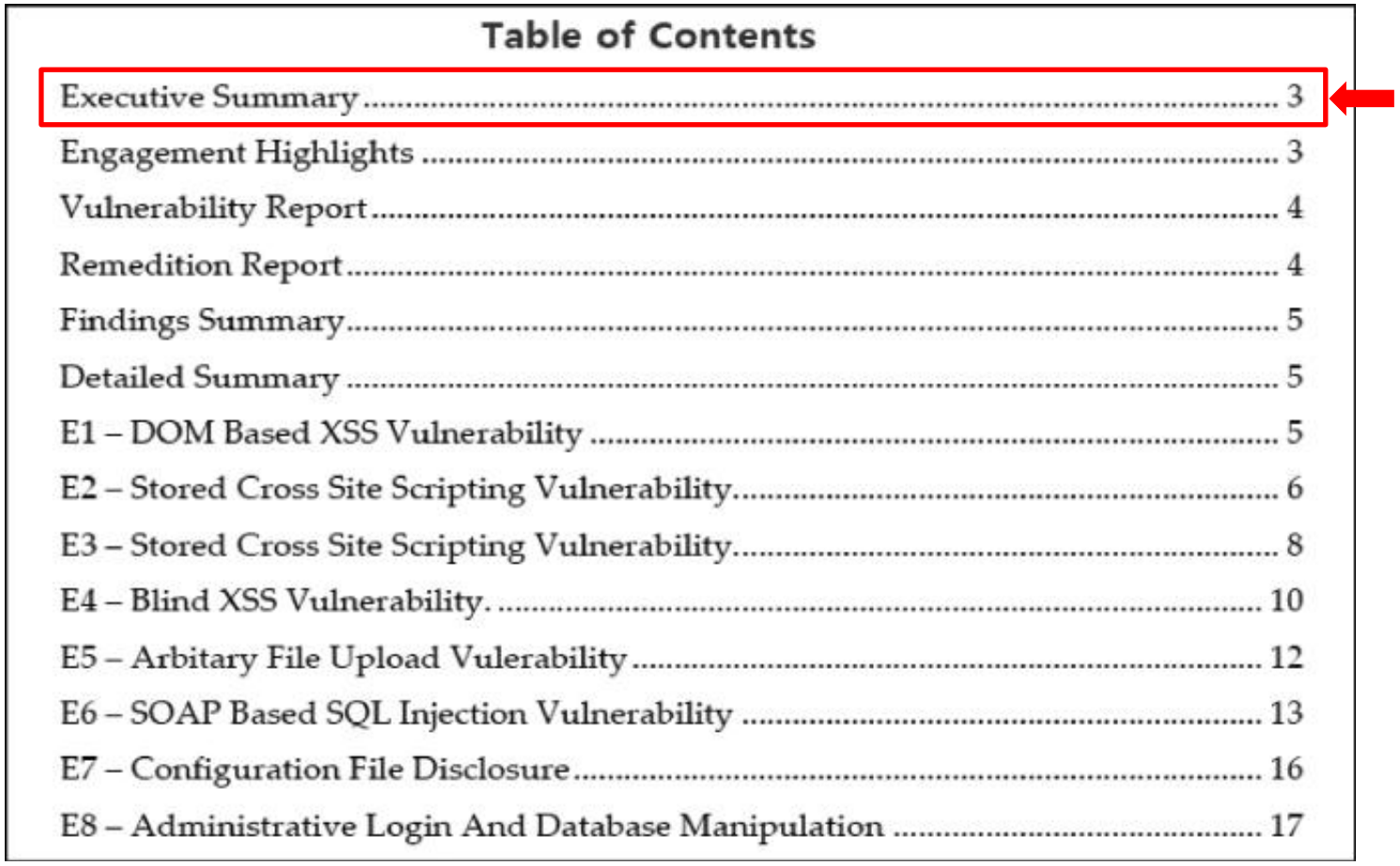


Table of Contents

Penetration Testing Report

Struttura – Executive Summary

- Parte più importante del penetration testing report
- Rivolto alla parte gestionale dell'ente (o organizzazione) che ha commissionato il processo di penetration testing
- Scritto per rivolgersi ad un pubblico non tecnico
  - Deve essere facilmente comprensibile da esso

Penetration Testing Report

Struttura – Executive Summary

- Tipicamente la parte gestionale di un ente ha poco tempo a disposizione per leggere i report e non ha competenze tecniche
  - L'Executive Summary deve essere preciso e conciso

- L'Executive Summary dovrebbe iniziare con la definizione dello Scopo/Ambito del processo di penetration testing e del modo in cui tale processo è stato condotto
  - Lo Scopo (o ambito) deve essere definito in modo molto preciso

Penetration Testing Report

Struttura – Executive Summary

- In questa sezione andrebbero
  - Spiegati i risultati ottenuti dal processo di penetration testing e le eventuali scoperte
  - Discusse, in generale, le problematiche di sicurezza rilevate, le relative cause ed eventuali contromisure

Penetration Testing Report

Struttura – Executive Summary

- Andrebbe poi inserita la parte di analisi, che dovrebbe evidenziare
  - Rischio complessivo per l'asset, determinato in base ai risultati ottenuti dal processo di penetration testing
  - Diminuzione del rischio dopo aver affrontato le problematiche di sicurezza ed implementato le opportune contromisure

Penetration Testing Report

Struttura – Executive Summary – Esempio

EXECUTIVE SUMMARY

RHAinfoSec conducted a full webapplication penetration test on **foonetworks**, the goal was to analyze the security posture of the Webapplications and suggest countermeasures for all the findings requiring remediation.

The Application Penetration test was conducted on foonetworks from January 2013 onwards. The target subdomains were also included in the scope of penetration test, which were not provided by default since it was a full black box penetration test.

As a result of the engagement we managed to find lots of high risk vulnerabilities which confirmed that the security posture of the application is very low and proper security countermeasures have not been implemented inside the environment.

This report contains detailed analysis about the vulnerabilities that we found during the engagement along with the report also contains a remediation report which would help you improve the overall security posture of your application. The report also contains a detailed explanation about every vulnerability found along with the detailed countermeasures to fix the vulnerability.

The overall risk of compromise was analyzed to be 70%. Addressing the security issues that present inside the report would significantly increase the overall risk of compromise.

Penetration Testing Report

Struttura – Executive Summary – Esempio

EXECUTIVE SUMMARY

RHAinfoSec conducted a full webapplication penetration test on **foonetworks**, the goal was to analyze the security posture of the Webapplications and suggest countermeasures for all the findings requiring remediation.

The Application Penetration test was conducted on foonetworks from January 2013 onwards. The target subdomains were also included in the scope of penetration test, which were not provided by default since it was a full black box penetration test.

As a result of the engagement we managed to find lots of high risk vulnerabilities which confirmed that the security posture of the application is very poor and proper security countermeasures have not been implemented inside the enviro

This report contains detailed analysis about the vulnerabilities engagement along with the report also contains a remediation improve the overall security posture of your application. The re explanation about every vulnerability found along with the deta vulnerability.

The overall risk of compromise was analyzed to be 70%. Addressing the security issues that present inside the report would significantly increase the overall risk of compromise.

Definizione dello scopo/ambito del testing e del modo in cui è stato realizzato

Penetration Testing Report

Struttura – Executive Summary – Esempio

EXECUTIVE SUMMARY

RHAinfoSec conducted a full webapplication penetration test on **foonetworks**, the goal was to analyze the security posture of the Webapplications and suggest countermeasures for all the findings requiring remediation.

The Application Penetration test was conducted on foonetworks from January 2013 onwards. The target subdomains were also included in the scope of penetration test, which were not provided by default since it was a full black box penetration test.

As a result of the engagement we managed to find lots of high risk vulnerabilities which confirmed that the security posture of the application is very low and proper security countermeasures have not been implemented inside the environment.

This report contains detailed analysis about the vulnerabi[illegible] that we found during the engagement along with the report also contains a remediation re[illegible]ich would help you improve the overall security posture of your application. The repor[illegible] detailed explanation about every vulnerability found along with the det[illegible] vulnerability.

The overall risk of compromise was analyzed to be 70%. Add[illegible] present inside the report would significantly increase the overall risk of compromise.

Descrizione generale dei risultati del penetration testing e delle problematiche rilevate

Penetration Testing Report

Struttura – Executive Summary – Esempio

EXECUTIVE SUMMARY

RHAinfoSec conducted a full
analyze the security posture o
findings requiring remediation

The Application Penetration tes
The target subdomains were also included
provided by default since it was a full bla

As a result of the engagement we mar
confirmed that the security posture
countermeasures have not been i

This report contains detailed analysis about the vulnerabilities that we found during the engagement along with the report also contains a remediation report which would help you improve the overall security posture of your application. The report also contains a detailed explanation about every vulnerability found along with the detailed countermeasures to fix the vulnerability.

The overall risk of compromise was analyzed to be 70%. Addressing the security issues that present inside the report would significantly increase the overall risk of compromise.

- **Parte di analisi**
  - **Descrizione dei rischi in base ai risultati del testing**
  - **In che modo il rischio diminuirà dopo aver implementato le appropriate contromisure**

Penetration Testing Report

Struttura – Engagement Highlights

Table of Contents

Penetration Testing Report

Struttura – Engagement Highlights

- **Pre-Ingaggio**
  - Vengono discusse tra le parti coinvolte i requisiti legali e le «Regole di Ingaggio»

- Le **Regole di Ingaggio** definiscono
  - Come deve essere condotto il processo di penetration testing
  - Quale metodologia deve essere utilizzata
  - Le date di inizio e fine del processo
  - Gli obiettivi del processo
  - Gli obblighi e le responsabilità delle parti coinvolte nel processo
  - Etc

Penetration Testing Report

Struttura – Engagement Highlights

- Tutte le **Regole di Ingaggio** devono essere **concordate** tra le parti **prima dell'inizio** del processo di **penetration testing**

- Le **Regole di Ingaggio** dovrebbero definire almeno i seguenti aspetti
  - Accordo di «Non Divulgazione» (*Non-Disclosure Agreement - NDA*)
  - Portata del processo di penetration testing
    - Parti dell'asset che devono essere valutate e come devono esserlo
  - Tecniche consentite e non consentite
  - Strumenti consentiti e non consentiti

Penetration Testing Report

Struttura – Vulnerability Report

Table of Contents

Penetration Testing Report

Struttura – Vulnerability Report

- Descrizione generale (non tecnica) delle vulnerabilità

- Descrizione del come tali vulnerabilità vanno ad impattare sulla sicurezza dell'asset

Penetration Testing Report

Struttura – Remediation Report

Table of Contents

Penetration Testing Report

Struttura – Remediation Report

- Raccomandazioni generali da implementare per migliorare la sicurezza dell'asset

- Rivolto a chi si occupa di stabilire dal punto di vista manageriale le politiche di sicurezza dell'asset
  - Deve essere molto preciso e di facile comprensione

Penetration Testing Report

Struttura – Remediation Report – Esempio

REMEDIATION

The security control environment for foonetworks was found very poor, as a result of which there are certain security countermeasures we would like to suggest. With the goal of protecting the Web application's infrastructure, we would recommend you to perform the following actions.

- A perfect plan for fixing the Critical, High, Medium, low risk vulnerabilities should designed and implemented. The vulnerabilities should be fixed in the descending order of priority.
- Secure development life cycle (SDLC) for developing web applications shall be implemented.
- A Web Application Firewall shall be implemented to detect, filter and block all the malicious packets.
- Security Audits shall be performed on the regular basis.
- Early security checks should be performed in the development process.