Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Documentazione e Reporting

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Documentazione e Verifica dei Risultati
- Tipi di Report
- Penetration Testing Report
- Preparazione della Presentazione
- Procedure di Post Testing

Outline

- **Documentazione e Verifica dei Risultati**
- Tipi di Report
- Penetration Testing Report
- Preparazione della Presentazione
- Procedure di Post Testing

Documentazione e Verifica dei Risultati

- Tracciamento e documentazione delle attività svolte rappresentano un aspetto fondamentale del processo di penetration testing
- Un pentester dovrebbe registrare tutte le azioni che ha svolto
- Tutti gli input e gli output degli strumenti utilizzati per il penetration testing dovrebbero essere memorizzati
  - Così da garantire, se necessario, che i risultati siano riproducibili da parte del committente
- Un committente potrebbe avere necessità di simulare i passi effettuati dal pentester
- Una parte importante del processo di penetration testing include la presentazione dei risultati ai committenti

Documentazione e Verifica dei Risultati

- La documentazione, la preparazione dei report e l'eventuale presentazione sono attività che devono essere affrontate in maniera strutturata e consistente con i risultati ottenuti
  - Anche un piccolo errore potrebbe portare a problemi legali
- L'obiettivo di queste attività dovrebbe essere quello di
  - Evidenziare tutte le potenziali debolezze riscontrate nell'asset
  - Fornire prove a supporto delle debolezze riscontrate
  - Indicare chiaramente
    - I possibili modus operandi dell'attaccante
    - Gli strumenti e le tecniche utilizzate
    - Le vulnerabilità scoperte e quelle sfruttate
    - I possibili rimedi per risolvere (o mitigare) le vulnerabilità

Documentazione e Verifica dei Risultati

- **Le seguenti operazioni possono essere utili per verificare e documentare i risultati del testing, prima di includerli nel report finale**
  - Prendere appunti dettagliati su ciascun passo effettuato durante il processo di penetration testing
  - Creare un template in cui possano essere inseriti i risultati prodotti da ogni singolo strumento utilizzato
    - Il template dovrebbe
      - Indicare l'obiettivo dello strumento, i parametri ed i profili di esecuzione utilizzati
      - Fornire spazio per memorizzare i risultati prodotti dallo strumento
    - Ad esempio, nel caso di Nmap si potrebbe
      - Definire: scopo di utilizzo, macchina/e target, opzioni di esecuzione e profili (rilevamento del servizio, tipo di Sistema Operativo, porte aperte, etc)
      - Documentare di conseguenza i risultati ottenuti

Documentazione e Verifica dei Risultati

- **Le seguenti operazioni possono essere utili per verificare e documentare i risultati del testing, prima di includerli nel report finale**
  - Per ciascuno strumento sarebbe opportuno ripetere il test per almeno tre volte prima di trarre conclusioni definitive
    - In questo modo si «certificherebbe» la bontà dei risultati ottenuti anche rispetto al verificarsi di eventuali condizioni anomale o impreviste

Documentazione e Verifica dei Risultati

- **Le seguenti operazioni possono essere utili per verificare e documentare i risultati del testing, prima di includerli nel report finale**
  - Non basarsi su un singolo strumento
    - Affidarsi ad un singolo strumento (ad esempio, per la raccolta di informazioni) potrebbe produrre risultati incompleti o non pienamente corretti
    - Una determinata attività del processo di penetration testing andrebbe ripetuta usando diversi strumenti realizzati per uno scopo simile
      - Ogni strumento ha le sue peculiarità per gestire situazioni specifiche
    - Ciò ridurrà i falsi positivi ed i falsi negativi
  - Se possibile, non affidarsi solo a strumenti automatici ma utilizzare anche
    - Tecniche manuali di penetration testing
    - Le proprie conoscenze ed esperienze per verificare tutti i risultati ottenuti

Outline

- Documentazione e Verifica dei Risultati
- Tipi di Report
- Penetration Testing Report
- **Preparazione della Presentazione**
- Procedure di Post Testing

Preparazione della Presentazione

- È spesso necessaria una presentazione per il committente
  - Che descriva brevemente il processo di penetration testing ed i risultati da esso prodotti
- Prima di realizzare una presentazione è fondamentale comprendere le conoscenze tecniche e gli obiettivi del committente
- È necessario modificare la presentazione in base al committente ed al suo livello di competenza
  - In caso contrario, si potrebbe avere una reazione negativa da parte del committente stesso
- Il compito principale del pentester dovrebbe essere quello di far capire al committente i potenziali fattori di rischio presenti nell'asset

Preparazione della Presentazione

- I manager di solito non hanno né il tempo né la preparazione adeguata per comprendere i dettagli tecnici alla base delle vulnerabilità

- Ma sono invece interessati a conoscere
  - Lo stato attuale della sicurezza dell'organizzazione che gestiscono
  - Le *misure di riparazione/mitigazione* che dovrebbero essere adottate per eliminare/mitigare eventuali vulnerabilità riscontrate

- La presentazione dovrebbe poter essere utile e comprensibile da un pubblico sia tecnico che non tecnico
  - Permettendo a ciascuno di adottare le misure più appropriate

Preparazione della Presentazione

- Le eventuali carenze di sicurezza rilevate dal processo di penetration testing dovrebbero essere descritte senza attaccamento emotivo, limitandosi ai fatti

- Il ruolo del pentester è quello di attenersi ai fatti ed alle scoperte
  - Dimostrandoli tecnicamente e consigliando le azioni correttive (*rimedi*) più opportune

- Un pentester dovrebbe prepararsi in anticipo a rispondere ad eventuali domande
  - Ad esempio, riguardanti i costi

Outline

- Documentazione e Verifica dei Risultati
- Tipi di Report
- Penetration Testing Report
- Preparazione della Presentazione
- **Procedure di Post Testing**

Procedure di Post Testing

- *Misure di Riparazione*, *Interventi Correttivi* e *Raccomandazioni* sono tutti termini che si riferiscono alle *procedure di Post Testing*

- Durante queste procedure, il pentester potrebbe agire come consulente a supporto del *Team di Riparazione* operante presso l'asset

- Al pentester potrebbe essere richiesto di interagire con varie figure tecniche, aventi background diversi, che siano in grado di supportarlo durante l'analisi di asset complessi
  - È improbabile che il pentester possegga tutte le competenze tecniche necessarie per rimediare ai problemi di sicurezza rilevati nell'asset

Procedure di Post Testing

- Per un pentester potrebbe essere impegnativo dover gestire e risolvere ogni singola vulnerabilità in maniera autonoma, senza alcun supporto da parte di esperti
  - Tale attività potrebbe inoltre richiedere tempi molto lunghi per poter essere portata a termine

- Esistono diverse linee guida che il pentester potrebbe seguire per fornire *Raccomandazioni* al proprio committente

- Tali raccomandazioni prendono anche il nome di *Raccomandazioni Critiche*

Procedure di Post Testing

Raccomandazioni Critiche – Esempi

- Rielaborare la progettazione della rete dell'*asset* e verificare la presenza di condizioni sfruttabili a causa delle vulnerabilità indicate nel report

- Utilizzare un approccio *Divide et Impera* per partizionare in livelli la rete dell'infrastruttura target
  - Separando le componenti critiche da quelle pubblicamente esposte

- Introdurre se necessario componenti quali IDS/IPS, Firewall, AntiVirus, Sistemi di Identity ed Access Management, etc
  - Ottimizzare il funzionamento di tali componenti, così che essi possano garantire sicurezza senza impattare sulle prestazioni di rete

Procedure di Post Testing

Raccomandazioni Critiche – Esempio

- Migliorare le competenze degli sviluppatori nella codifica di applicazioni utilizzate dall'asset
  - **N.B.** Valutare la sicurezza delle applicazioni ed eseguire verifiche sul codice potrebbe portare ad importanti benefici economici per l'organizzazione responsabile dell'asset

- Gli attacchi lato client o di social engineering sono estremamente difficili (se non impossibili) da fronteggiare
  - Ma potrebbero essere mitigati formando in maniera opportuna il personale

Procedure di Post Testing

Raccomandazioni Critiche – Esempio

- **N.B.** La mitigazione dei problemi di sicurezza dell'asset secondo le raccomandazioni fornite dal pentester potrebbe richiedere ulteriori indagini
  - Ad esempio, per garantire che qualsiasi modifica in un sistema non influenzi le sue caratteristiche funzionali

Procedure di Post Testing

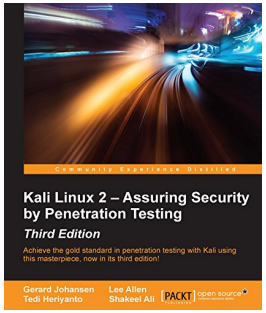
Raccomandazioni Critiche – Esempio

- Utilizzare contromisure per garantire la sicurezza fisica
  - Controllo degli accessi attraverso strumenti di tipo meccanico ed elettronico
  - Allarmi anti-intrusione
  - Monitoraggio tramite *Closed-Circuit Television (CCTV)*
  - Identificazione del personale (Biometria, smart surveillance, etc)

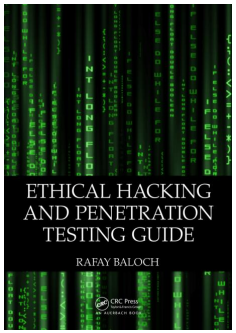
- Aggiornare regolarmente tutti i sistemi di sicurezza necessari per garantire la riservatezza, l'integrità e la disponibilità dell'*asset*

Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 14



- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 1
    - Da pagina 8 a pagina 17



Bibliografia

- **Offensive Security – Penetration Testing Report**
  - https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
- **SANS Institute - Writing a Penetration Testing Report**
  - https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343
- **PCI Security Report Guidance**
  - https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
- **Penetration Testing Reports Archive**
  - https://github.com/juliocesarfort/public-pentesting-reports