Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Fondamenti di Ethical Hacking
Parte 2

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- **I Dieci Comandamenti dell'Ethical Hacking**

I 10 Comandamenti dell' Ethical Hacking

1. **Stabilire gli Obiettivi**
   - Di quali informazioni potrebbero disporre gli hacker (criminali) per attaccare un determinato asset?
   - In che modo gli hacker (criminali) potrebbero sfruttare queste informazioni?
   - L'utente (o l'organizzazione) è a conoscenza di passati tentativi di violazione del proprio asset?

I 10 Comandamenti dell' Ethical Hacking

2. Pianificare Sempre in Anticipo

- La valutazione della sicurezza di un sistema è tipicamente soggetta a vincoli: tempo, risorse (soldi, manodopera), etc

- Il lavoro va quindi pianificato
  - Identificare quali componenti dell'asset devono essere valutate
  - Determinare gli intervalli dei testing
  - Definire in maniera chiara la procedura di testing
  - Creare un piano di testing da condividere con le parti interessate
  - Ottenere l'approvazione del piano

I 10 Comandamenti dell' Ethical Hacking

3. **Ottenere Sempre l'Autorizzazione** prima valutare la sicurezza di un sistema
   - **Si potrebbe incorrere in Rati Penali**
     - Assicurarsi che chi ha commissionato l'analisi di sicurezza (organizzazione, ente, singolo individuo) abbia concesso i necessari permessi tramite opportuni documenti scritti
     - I documenti dovrebbero stabilire che
       - È stata concessa l'approvazione per testare il sistema secondo un piano pre-approvato
       - Il committente supporterà l'hacker etico (pentester) in caso di eventuali spese legali

I 10 Comandamenti dell' Ethical Hacking

4. Essere Etico

- Un hacker etico è vincolato a rispettare requisiti di professionalità, riservatezza e coscienza

- È necessario
  - Rispettare sempre il piano precedentemente approvato ed evitare di aggiungere nuovi dettagli in corso d'opera
  - Non condividere i risultati dei test di sicurezza con persone non autorizzate
    - Sia all'interno che all'esterno dell'organizzazione che ha commissionato il test

I 10 Comandamenti dell' Ethical Hacking

5. **Tenere Traccia dell'Attività Svolta**, mediante documenti (*registri*) elettronici o cartacei per memorizzare di volta in volta le informazioni ottenute
   - Annotando tutte le attività eseguite
   - Annotando tutti i test eseguiti, comprese le date
   - Avendo sempre una copia di backup dei log
   - Memorizzando in maniera accurata i risultati ottenuti, anche se alcuni test o attività potrebbero non andare come pianificato

I 10 Comandamenti dell' Ethical Hacking

6. **<u>Proteggere le Informazioni Riservate:</u>** un hacker etico durante la propria attività potrebbe trovare molte informazioni, anche potenzialmente sensibili, in tal caso, esso dovrà
   - Rispettare la privacy delle persone e trattare ogni informazione con riservatezza
   - Proteggere e non usare le password ed altre informazioni sensibili trovate durante i test

I 10 Comandamenti dell' Ethical Hacking

7. **Non Causare Danni:** spesso vengono causati danni imprevisti. È necessario quindi
   - Avere sempre un piano ed attenersi ad esso
   - Evitare di causare (anche accidentalmente) interruzioni o di interferire con altre attività
   - Essere a conoscenza degli strumenti che si stanno utilizzando e delle loro implicazioni
     - Scegliere gli strumenti con consapevolezza e leggere sempre la relativa documentazione

I 10 Comandamenti dell' Ethical Hacking

8. Non Usare Strumenti a Caso

- Esistono numerosi strumenti per condurre attività di penetration testing / ethical hacking
- È facile essere tentati dal provarli tutti
  - La maggior parte di essi sono gratuiti e facilmente accessibili
- Meglio concentrarsi solo su alcuni strumenti
  - Di cui è nota l'efficacia e con cui si ha familiarità

I 10 Comandamenti dell' Ethical Hacking

9. **Il Processo di Penetration Testing deve essere Sempre Strutturato**
   - È necessario un processo caratterizzato da
     - Obiettivi quantificabili
     - Coerenza e ripetibilità
     - Permanenza dei risultati
   - Sono quindi necessarie **metodologie di testing**
     - Maggiori dettagli in seguito…

I 10 Comandamenti dell' Ethical Hacking

10. Segnalare e Memorizzare Tutte le Scoperte

- Se durante i test di sicurezza vengono individuate vulnerabilità o minacce nel sistema, queste devono essere immediatamente segnalate e memorizzate tramite l'opportuna documentazione

- Assicurarsi di non tralasciare alcun risultato, non importa quanto insignificante esso possa sembrare
- Tutti i risultati vanno sempre documentati
  - Non è necessario evidenziare nelle parti iniziali della documentazione (*Penetration Testing Report*) tutti i risultati ottenuti
  - È sempre necessario inserire tali risultati nelle descrizioni dettagliate presenti nella documentazione
  - *Maggiori dettagli in seguito…*

Bibliografia

- **Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security**. Gary Hall & Erin Watson. 2016
  - Capitoli 1, 2, 3 e 4