Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Social Engineering
Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Modellare la Psicologia Umana
- Processo di Attacco
- Metodi di Attacco
- Social Engineering Toolkit (SET)

Outline

- **Concetti Preliminari**
- Modellare la Psicologia Umana
- Processo di Attacco
- Metodi di Attacco
- Social Engineering Toolkit (SET)

Concetti Preliminari

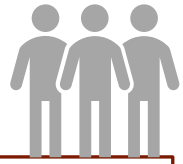
- L'Ingegneria Sociale (o *Social Engineering*) sfrutta le «debolezze umane» per apprendere ed ottenere informazioni talvolta preziose

> **È l'arte dell'inganno**

Vitale per un pentester quando non ci sono vulnerabilità che potrebbero essere sfruttate sulla macchina target

Concetti Preliminari

- Le **persone** (componente umana) rappresentano l'**anello più debole** nella difesa della sicurezza di un qualsiasi asset



Livello più <u>vulnerabile</u> dell'infrastruttura di sicurezza

- L'essere umano è per sua natura una creatura sociale e questo potrebbe diventare una «vulnerabilità sfruttabile»
  - I pentester (o gli ingegneri sociali) potrebbero sfruttare questa «vulnerabilità» per ottenere informazioni riservate o per accedere ad aree/risorse riservate

Concetti Preliminari

- L'ingegneria sociale prevede **diversi vettori di attacco**

- Ciascuno attacco è di solito
  - Limitato solo dall'immaginazione di chi lo conduce (pentester o attaccante) e
  - Personalizzato in base alla «vittima» da attaccare

Concetti Preliminari

- Dal punto di vista della sicurezza, l'ingegneria sociale rappresenta un'**arma potente**
  - Utilizzata per **manipolare le persone** e raggiungere l'obiettivo desiderato

- In molte organizzazioni questa pratica potrebbe essere utilizzata per
  - Valutare la sicurezza e l'affidabilità dei dipendenti
  - Investigare le debolezze (umane) del personale

- L'**utilizzo** di tecniche di **ingegneria sociale** deve essere **esplicitamente richiesto** in fase di *Target Scoping* ed **approvato** da **tutte le parti** coinvolte nel processo di penetration testing

Concetti Preliminari

- L'ingegneria sociale è una pratica molto diffusa, adottata da varie figure totalmente eterogenee tra loro
  - **Penetration tester**
  - Truffatori, ladri d'identità o spie
  - Partner commerciali
  - Reclutatori di lavoro o dipendenti scontenti
  - Addetti alle vendite
  - Etc

- Il fattore di differenziazione tra queste figure è la **motivazione** alla base delle loro azioni