Disclaimer

Etica e responsabilità

- Commettere reali non è bello e non vi aiuta nella carriera
- Il nostro lavoro è portare alla luce i problemi di sicurezza, sensibilizzare le persone e dare loro i mezzi per combattere i crimini informatici
- Trattare le persone con rispetto.
- Agire sempre sotto l’autorizzazione di istituzioni, datori di lavoro e committenti
- Attenti a non oltrepassare i limiti e non addentrarvi troppo nella zona grigia
- Studiamo gli attaccanti per creare difese migliori

Tipologie di Social Engineer

- Ladri di identità
- Broker di informazioni
- Truffatori
- Headhunters
- Commerciali
- Governo (opinione pubblica)
- …
- Chiunque! In particolare i genitori!

Principali obiettivi del Social Engineer

- Guadagno economico
- Promuovere una causa
- Divertimento
- Guadagnare conoscenza (obfuscation)
- Sfida ed Ego
- Vendetta
- …
- **Difendersi da altri Social Engineer**

Perché utilizzare la Social Engineering?

Con il progredire delle tecnologie, sono necessari sempre tempo investito ed esperienza per violare un sistema informatico. Dall'altro lato, gli istinti primordiali dell'essere umano non si sono evoluti molto.

La Social Engineering sfrutta la tendenza degli esseri umani a fidarsi innatamente del prossimo, la sua emotività, l'inclinazione a conformarsi ad un gruppo di simili…

Potrete trovare molto affinità con il Marketing, con le Neuroscienze e, se preferite, con l'attività dei truffatori di strada.

Piano d’Attacco

Alcuni possibili attacchi

Servizio Clienti

Consegna Pacco

Supporto Tecnico

USB abbandonata

Commerciale

Pausa Sigaretta

Piano d’Attacco

Primo passo - Reconnaissance

La chiave di ogni attacco di Social Engineering sono le informazioni sul bersaglio.

Lo scopo è poter creare alla perfezione un personaggio da interpretare, e formulare in anticipo risposte a domande pericolose.

Piano d’Attacco

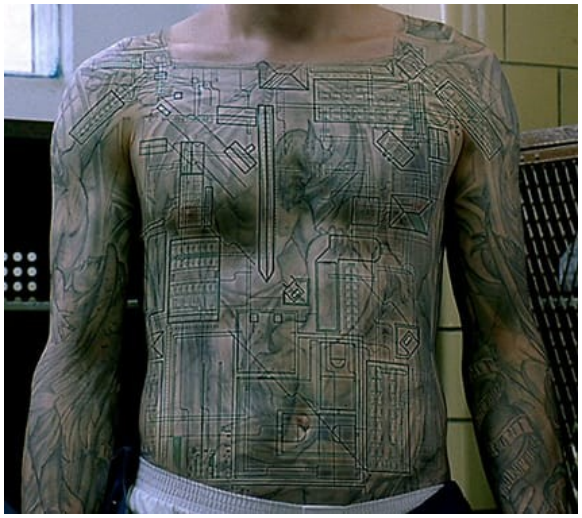
Primo passo - Reconnaissance

1) OSINT (open-source intelligence)
    - Google Maps
    - Social Networks (Facebook, LinkedIn)
    - TheHarvester
    - recon-ng

Piano d’Attacco

Primo passo - Reconnaissance

2) Osservazione ed appostamenti
   - Mappatura edificio, stanze ed entrate
   - Orari di lavoro
   - Convenzioni (vestiario, id card)
   - Fraternizzare con le persone
   - Terminologia specifica del settore



Piano d’Attacco

Primo passo - Reconnaissance

3) Dumpster Diving
   - “One man's trash is another man's treasure”
   - Documenti, strumentazione...

Piano d’Attacco

Secondo passo - Pretext

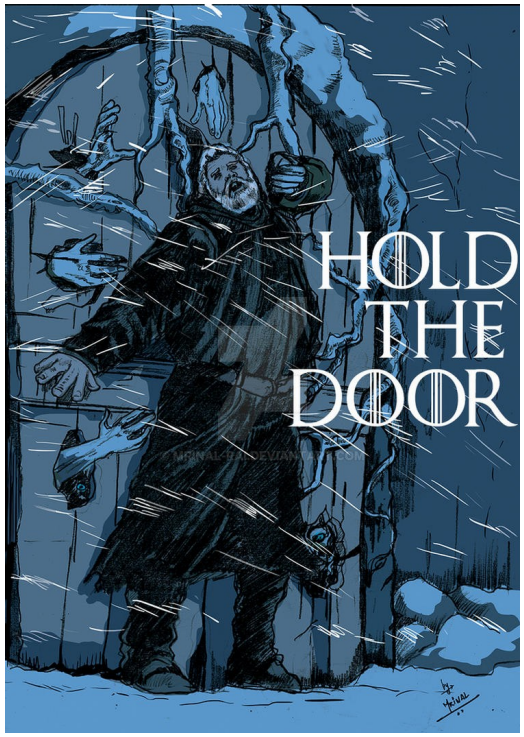
Il Pretext è la storia creata attorno alla propria nuova identità “inventata”. Il Social Engineer deve apparire genuino, portare motivazioni logiche ed essere sicuro di sé, così da ispirare fiducia negli altri. Se siete informatici, fingetevi informatici, o qualcosa di simile!

Il Pretext viene costruito dopo la Recon, sfruttando le informazioni raccolte. Importanti le apparenze, il linguaggio e gli strumenti collegati alla vostra storia.

Piano d’Attacco

Terzo passo - Accesso alla struttura

Come superare i controlli e le “gates”?
Guadagnare accesso a zone riservate semplicemente seguendo altri “colleghi”



Piano d’Attacco

Quarto passo - Azione

- Mantenere la calma (chiudersi in un bagno “Fuori Servizio”)
- Ricostruire la mappa della struttura
- Pensare a come uscire in seguito (gates)
- Ricordare il proprio obiettivo e pianificare le prossime mosse
- Non parlare in modo negativo “Non sono mica qui per hackerare il vostro network haha..”

Principi di Persuasione

Dr. Robert Cialdini - Principi di Persuasione

Principi con cui influenzare le persone. Potreste trovare diversi modi per identificarli e categorizzarli.

1. Reciprocity
2. Commitment and Consistency
3. Social Proof / Consensus
4. Authority
5. Liking
6. Scarcity
7. Unity

Principi di Persuasione

1) Reciprocity

Il ricambiare il modo in cui si viene trattati dalle altre persone.

E’ naturale che una persona ricambi con un regalo, un favore, un’informazione dopo aver ricevuto qualcosa. E’ ciò che permette agli esseri umani di cooperare nelle situazioni difficili.

Principi di Persuasione

1) Reciprocity

Esempi:

- Ricambiare un caffè / uno spritz offerto
- Scambiarsi i regali di Natale
- Scrivere il proprio indirizzo email per ricevere offerte promozionali
- Quid Pro Quo, “qualcosa per qualcosa”
- Advance Fee Scam, ereditare milioni ma dover pagare una piccola tassa per riceverli

Principi di Persuasione

2) Commitment and Consistency

Il desiderio di dimostrarsi coerenti nel proprio comportamento e di volersi mantenere consistenti con le proprie scelte.

Sfruttato chiedendo un piccolo “Commitment” iniziale, ed incrementandolo progressivamente, in una “Escalation of Commitment”.

2) Commitment and Consistency

Esempi:

- “Sunken Cost” o “Costo Sommerso”, continuare a pagare non per un guadagno, ma perché ormai si è speso troppo (videogiochi, investimenti, ricerca ed innovazione, aste online)
- Giustificare le proprie scelte passate, anche se errate

Principi di Persuasione

3) Social Proof / Consensus

L’attitudine a conformarsi con il comportamento degli altri, quando non si sa cosa fare, oppure di trovare conferma delle proprie azioni nel giudizio altrui.

Principi di Persuasione

3) Social Proof / Consensus

Esempi:

- Social Media, Influencer
- Identificarsi con un brand
- Situazioni di emergenza
- 90% delle persone appartenenti ad x consiglia y

4) Authority

Potere: possesso della capacità di controllare gli altri.
Autorità: diritto di esercitare il proprio controllo sugli altri.

Diversi tipi di Autorità:

- Legale
- Organizzativa (gerarchia e supervisione)
- Sociale

Principi di Persuasione

4) Authority

Esempi:

- Impersonare un superiore per richiedere informazioni, o direttamente denaro
- Forze di polizia
- Esperti di un settore (scienziati, tecnici, il Papa)

Principi di Persuasione

5) Liking

La tendenza a seguire e venire persuasi da chi e cosa ci piace.

Il concetto di piacere è molto ampio, ma è alla base dei rapporti interpersonali, e se un comportamento causa un rinforzo positivo da parte di chi ci piace, verremo influenzati a ripetere quel comportamento.

5) Liking

Esempi:

- Moda, design, arte
- Interagire con una persona famosa od importante
- Familiarità (ricetta della nonna)

Principi di Persuasione

6) Scarcity

La paura di perdere un’occasione perché limitata, oppure l’aumento del valore di qualcosa perché limitato.

La Scarcity scatena un senso di Urgenza, che può portare a decisioni irrazionali e sbagliate.

6) Scarcity

Esempi:

- Playstation 5
- Offerte “solo per le prime 5 chiamate”
- Mercato delle pietre preziose
- L’intero sistema economico

Principi di Persuasione

7) Unity

La condivisione di un’identità, dei nostri ideali, con altre persone. Si distingue dalla Social Proof per il suo significato più profondo e la necessità di essere genuina.

La famiglia è l’esempio di Unity più potente, ma ne fanno parte anche l’etnicità, il luogo e la co-creazione.

7) Unity

Esempio:

Cialdini ha chiesto di compilare un questionario a studenti e genitori. La percentuale di completamento degli studenti era molto alta, mentre dei genitori inferiore al 20%.

Allora Cialdini ha riproposto l'esperimento, offrendo 1 punto per il corso se i genitori avessero completato il questionario. Il 97% dei genitori lo ha completato, nonostante 1 punto fosse completamente irrilevante rispetto al punteggio finale del corso.

Principi di Persuasione

Framing

Porre una domanda, contestualizzandola in modo da predeterminare la risposta del soggetto.

Esempi:

- 75% Magro vs 25% Grasso
- Emissioni ridotte del 10% vs Emissioni di 95 g/km
- Trattamento A con 200 persone salvate su 600 vs Trattamento B con 33% di salvare tutti e 66% di non salvarne nessuno
- Trattamento C con 400 morti su 600 vs Trattamento B con 33% di salvare tutti e 66% di non salvare nessuno

Principi di Persuasione

Elicitation

L’atto di ottenere ed estrapolare informazioni in maniera indiretta.

Una corretta formulazione delle domande è fondamentale per l’Elicitation.

- Hai fame?
- Cosa vorresti mangiare?

Preloading: influenzare prima ancora della domanda.

- Non trovi che faccia caldo qui?
- Trailer “Un’esperienza videoludica di straordinaria bellezza” “Una trama avvincente” “Una gemma nascosta” “Una lacrima strappa-storie”

Difesa

Il valore nascosto dell’informazione

Le informazioni che circolano all’interno di un’azienda sembrano inutili e scontate ai lavoratori, ma sono di grande importanza per i Social Engineer.

Un attaccante che mostra padronanza di “come funzionano le cose” e possiede un linguaggio tecnico appropriato avrà un’alta probabilità di successo.

Come difendersi dalla Social Engineering