EPICODE

Esercizio S5 – L2

TRACCIA

Nell’esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i tool principali della fase di information gathering, quali:  
● Google, per la raccolta delle info.  
● Maltego.

Alla fine dell’analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato:  
● Il target.  
● Le query utilizzate (dove applicabile).  
● I risultati ottenuti.

SVOLGIMENTO

Target: Mark Zuckerberg

L’analisi inizia con l’utilizzo di Maltego.

Immagine che contiene diagramma, schermata, linea, design

Descrizione generata automaticamente

Inserendo come “Person” il nome e facendo “All Transforms” si sono ottenuti 3 indirizzi mail. Si può subito notare come due mail su tre facciano riferimento ad una stessa azienda/organizzazione (l’altra mail porta ad un vicolo cieco). Si presuppone quindi che il soggetto faccia parte di suddetta azienda/organizzazione.  
Si procede dunque con l’analisi proprio con “All Transforms” su “facebook.com”.

Immagine che contiene testo, schermata, Parallelo, linea

Descrizione generata automaticamente

Immagine che contiene testo, schermata, diagramma, Carattere

Descrizione generata automaticamente

In queste immagini è possibile notare diverse informazioni molto interessanti da poter sfruttare:

* Il sito dell’azienda.
* L’azienda madre che controlla facebook.com (Meta Platforms Inc., utile per capire la grandezza dell’azienda e/o gli azionisti sui siti di finanza specializzati e scoprire conflitti di interesse e/o spionaggio industriale tra le persone e le società coinvolte).
* Diversi domini e server che aiutano a capire come è strutturata l’azienda.
* La sede dell’azienda.
* Nomi e cognomi di persone collegate alla società (potenzialmente da poter a loro volta analizzare).
* Mail dei dipendenti (per possibili furti d’identità o phishing).
* Numeri di telefono (per maggior credibilità in un attacco di ingegneria sociale).

segue

Immagine che contiene testo, mappa, schermata, atlante

Descrizione generata automaticamente

Grazie a Google Maps identifichiamo la sede aziendale.

Immagine che contiene testo, schermata, Carattere, Marchio

Descrizione generata automaticamente

Cercando su Google il sito si comprende immediatamente che si tratta di un social network.

Segue

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Grazie a Whois è possibile anche trovare gli indirizzi ip dei server.

Immagine che contiene testo, schermata, software, Sistema operativo

Descrizione generata automaticamente

Cercando l’azienda e il nostro target su Google si può comprendere il ruolo di CEO e Presidente che ricopre.