

Esercizio S5L2

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 più che altro familiarizzare con i tool principali della fase di information gathering, quali:

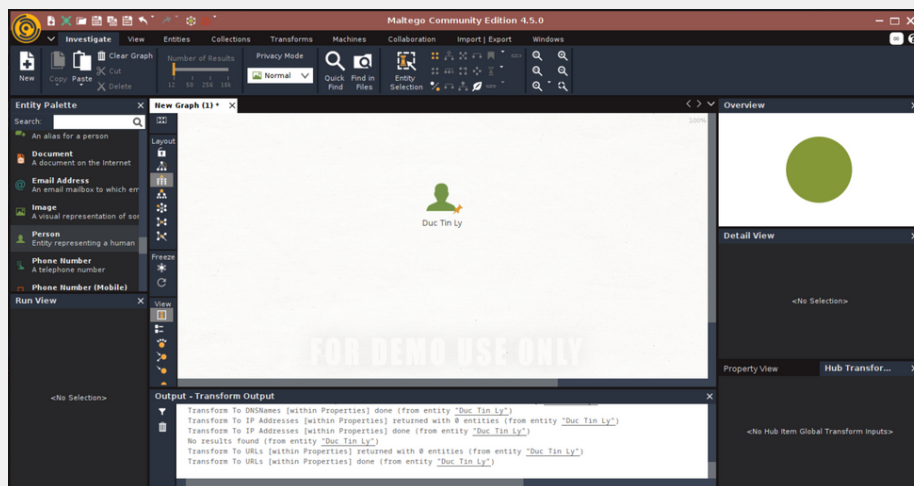
- Google, per la raccolta passiva delle info
- Maltego

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

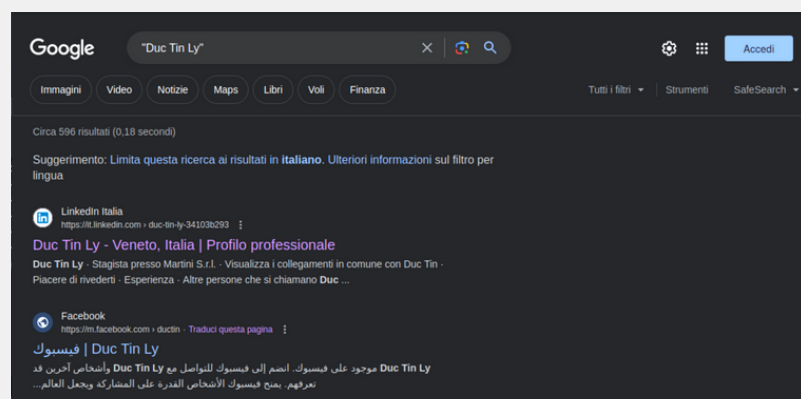
L'esercizio chiedeva di raccogliere dell'informazioni su di me(1) e sul dominio di Epicode(2) ,grazie a degli strumenti(Google e Maltego) e come risultati mostrati qui sotto:

Maltego 1



Per quanto riguarda la ricerca su me non vi è nessun risultato su Maltego come mostrato la figura a sinistra.

Google 1



Invece su Google vi è soltanto un risultato.

Maltego 2



Per quanto riguarda Epicode come mostrato nell'immagini a sinistra si può vedere che vi sono dei sottodomini e dei server DNS collegati al dominio di Epicode.



Andando sul sottodominio Epcode si può vedere le sedi, dei server DNS, numero di cellulare di un utente, dei e-mail server, dei altri sottodomini, dell'e-mail e dei siti di wayback machine che mostrano i vari anni del dominio.

Google 2

Su Google vi sono molti risultati dei siti di Epicode anche in altri siti dove Epicode si è registrato.

