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.

Target scelto

Un'azienda di formazione.

Primo step, normale ricerca su Google

Da una semplice ricerca su Google, è possibile individuare l'indirizzo fisico della sede principale, associato ad un numero di telefono. Inoltre, entrando sul sito, si possono vedere i profili di Instagram, Facebook, Linkedin e YouTube.

Secondo step, ricerca con le Google Dorks

- Ricerca dei sotto-domini tramite la dork: "Site:dominio.com –site:www.dominio.com". Non è stato trovato alcun risultato.
- Ricerca dei file pdf collegati al target tramite la dork: "Site:dominio.com filetype: pdf". Sono state trovate alcune brochure sui corsi offerti dall'azienda, da cui si possono ricavare diversi indirizzi email aziendali.

Terzo step, ricerca con Maltego

Per prima cosa è stato cercato il nome dell'azienda, da qui, l'unica informazione utile ricavata è il nome del dominio. La ricerca è poi stata continuata proprio su di esso. Sono stati trovati diversi snapshots e il nome del sito. Proseguendo la ricerca dal sito sono stati trovati diversi indirizzi IP. Inoltre, si può vedere che il sito utilizza le tecnologie HTML5, JavaScript, jQuery ed alcune API di Google.