

EPISODE

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.

Google Hacking

Con l'ausilio del motore di ricerca google avviamo una ricerca delle informazioni, ovvero utilizzando fonti di pubblico dominio. Con una banale ricerca su google risaliamo immediatamente: a cosa fa l'azienda, alle varie sedi, il numero di dipendenti, i vari profili social e i recapiti.

Da qui cominciamo a muoverci per studiare la sua infrastruttura, partendo dal dominio del target ricerchiamo i vari sottodomini utilizzando la query: site:nome_target.com



- Il target verrà coperto per privacy

Google Hacking

Google

intitle:(facebook + [REDACTED].it)

- **INTITLE**, l'operatore intitle, da un punto di vista tecnico, restituisce tutti quei risultati che hanno nel campo TITLE dell'HTML il valore o l'espressione ricercati.

- Qui abbiamo trovato un profilo facebook con nome e cognome che potrebbe essere collegato al target. Questo risultato si vedrà anche con Maltego.



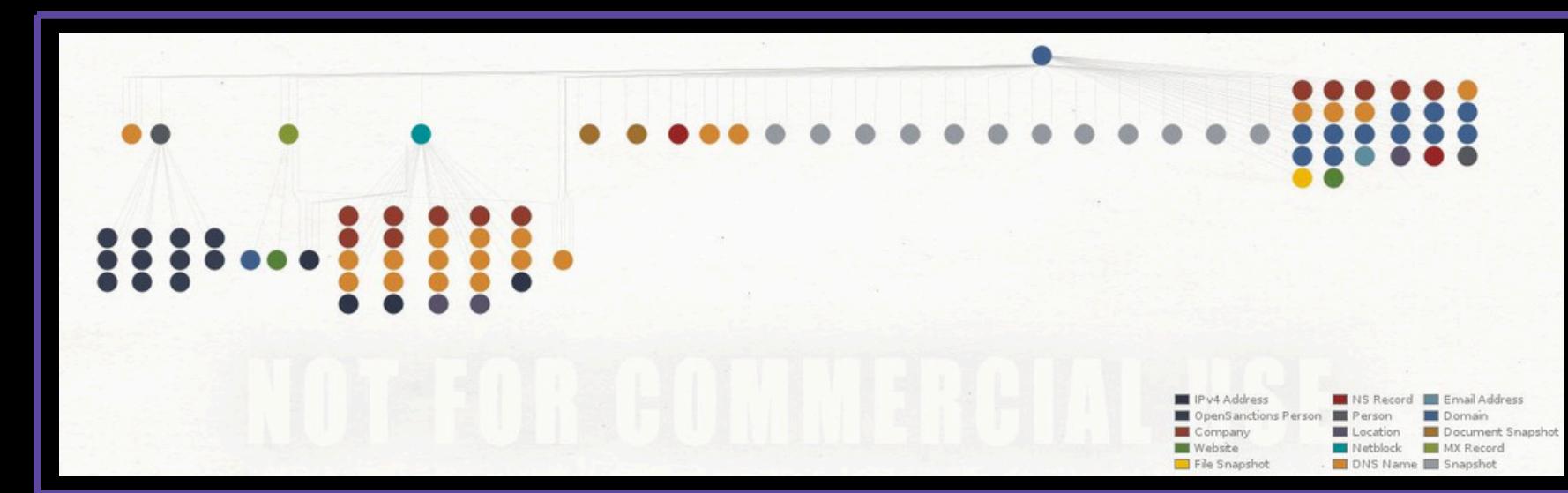
Facebook

<https://m.facebook.com> > public >

M [REDACTED] R [REDACTED] Profiles

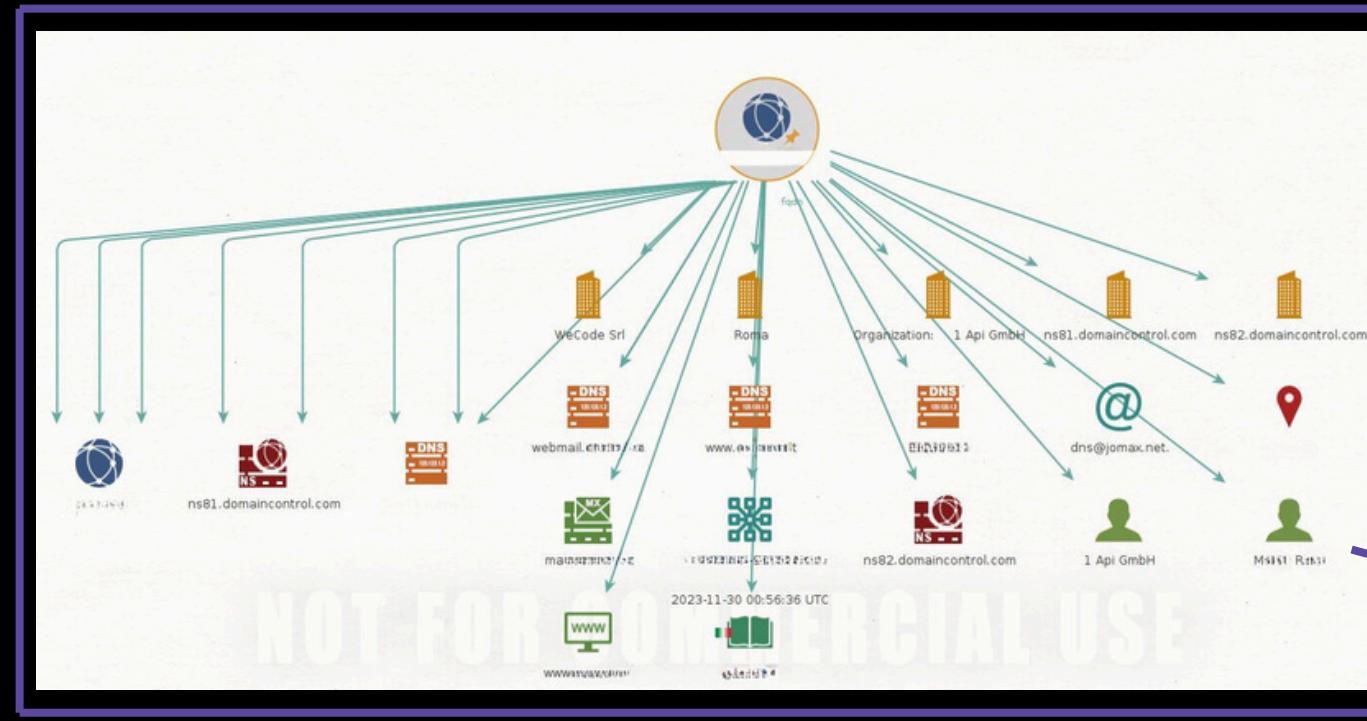
Maltego

Ci spostiamo adesso su [Maltego](#), dove avviamo l'operazione partendo da una frase, nel nostro caso "[Nome target](#)".



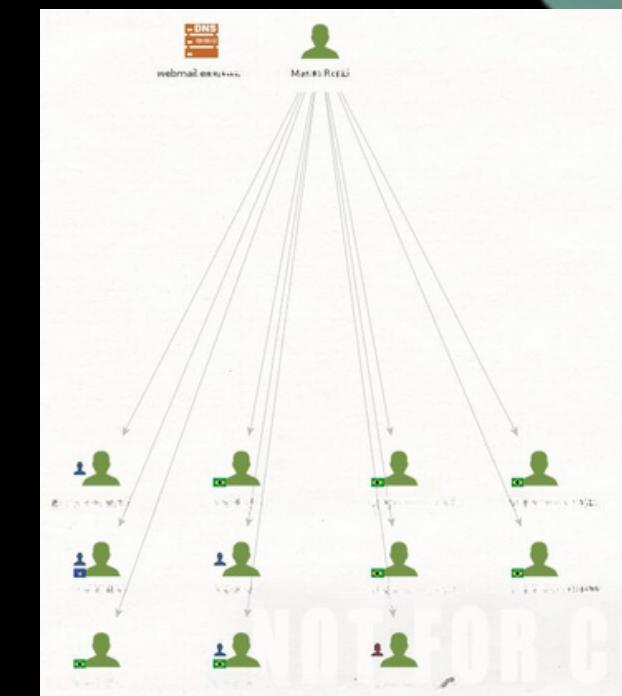
Questa è la mappa generale con i vari nodi partendo dal nodo "[O](#)", ovvero il target.

Maltego



Nel primo nodo si è trovato un CAP, dei server mail, sito web ed un profilo con nome e cognome, la stessa persona trovata in precedenza nella ricerca di google dork.

Facendo una ricerca anche sul nome trovato, verranno fuori altri nomi simili e in caso anche pagine Facebook, instagram e di altri social collegati magari a quella persona.



Maltego

In conclusione possiamo dire che Google Dorking è un metodo fondamentale per eseguire ricerche avanzate su Google utilizzando operatori speciali per trovare informazioni specifiche. Questo permette di effettuare una prima e importante raccolta delle informazioni con semplici e veloci comandi. Tuttavia, per ottenere una visione più dettagliata e strutturata di un dominio o di un servizio web, è possibile utilizzare strumenti più specializzati come Maltego.

Maltego è un potente strumento analisi che consente di ottenere una panoramica dettagliata delle interconnessioni e delle informazioni pubbliche associate a un dominio o a un servizio web.

È importante sottolineare che tutte queste ricerche dovrebbero essere condotte in modo etico e legale, e solo a scopo educativo e informativo.

Qui possiamo vedere altri nodi del target, come la mail e web mail service.

