S5L1, BENVENUTI LUIGI

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.

Si andrà ad effettuare information gathering utilizzando:

1. Google Dorks
2. Maltego

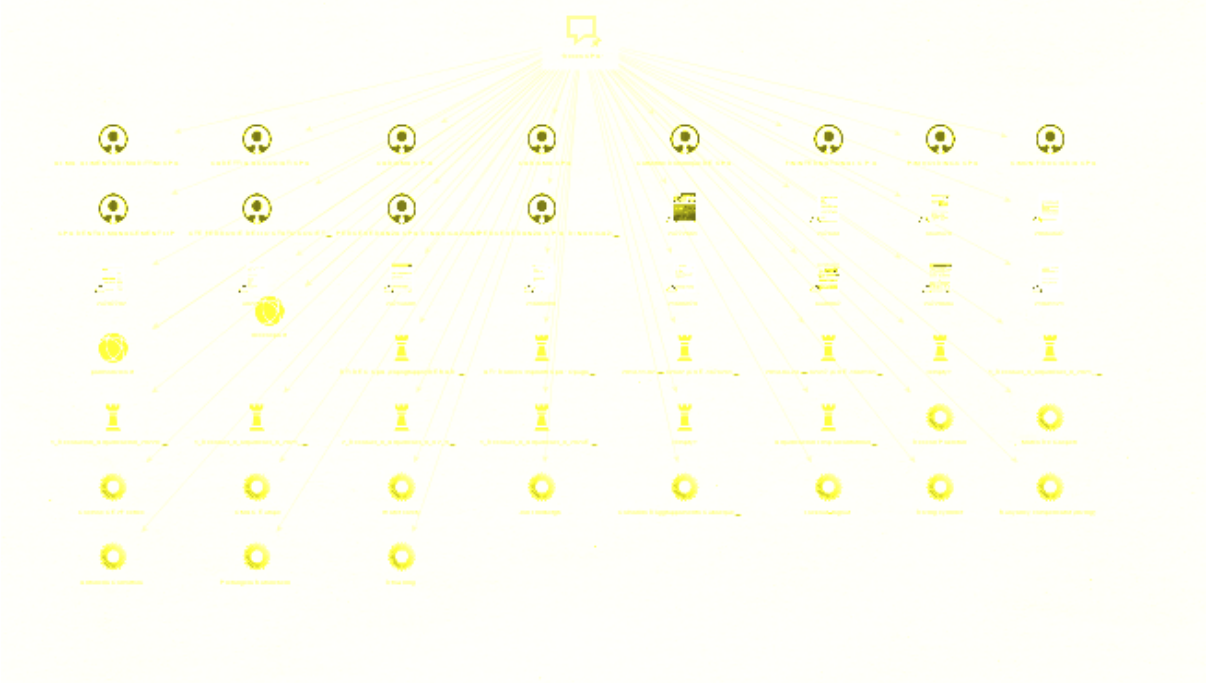
1.
Google Dorks è un set di strumenti di ricerca avanzata che, grazie all'utilizzo di speciali operatori, permette di raffinare la ricerca ricevendo così risultati sempre più specifici.
Nel nostro caso, cercheremo di sfruttare al meglio le potenzialità OSINT di questo strumento.
Utilizzeremo le dorks "AND", "site:" "intext" e "map".

2. Maltego è un link analysis software, usato per OSINT, analisi forensi ed investigazioni. Esso offre in tempo reale servizi data-mining ed information gathering.

Esercizio:
Il nostro target sarà un'azienda operativa nel campo agro-alimentare. Andremo a sviluppare un'analisi sul perimetro aziendale, sui dati sensibili esposti pubblicamente e sulle identità direttamente collegate all'azienda stessa.

Fase 1: Raccolta informazioni tramite Maltego

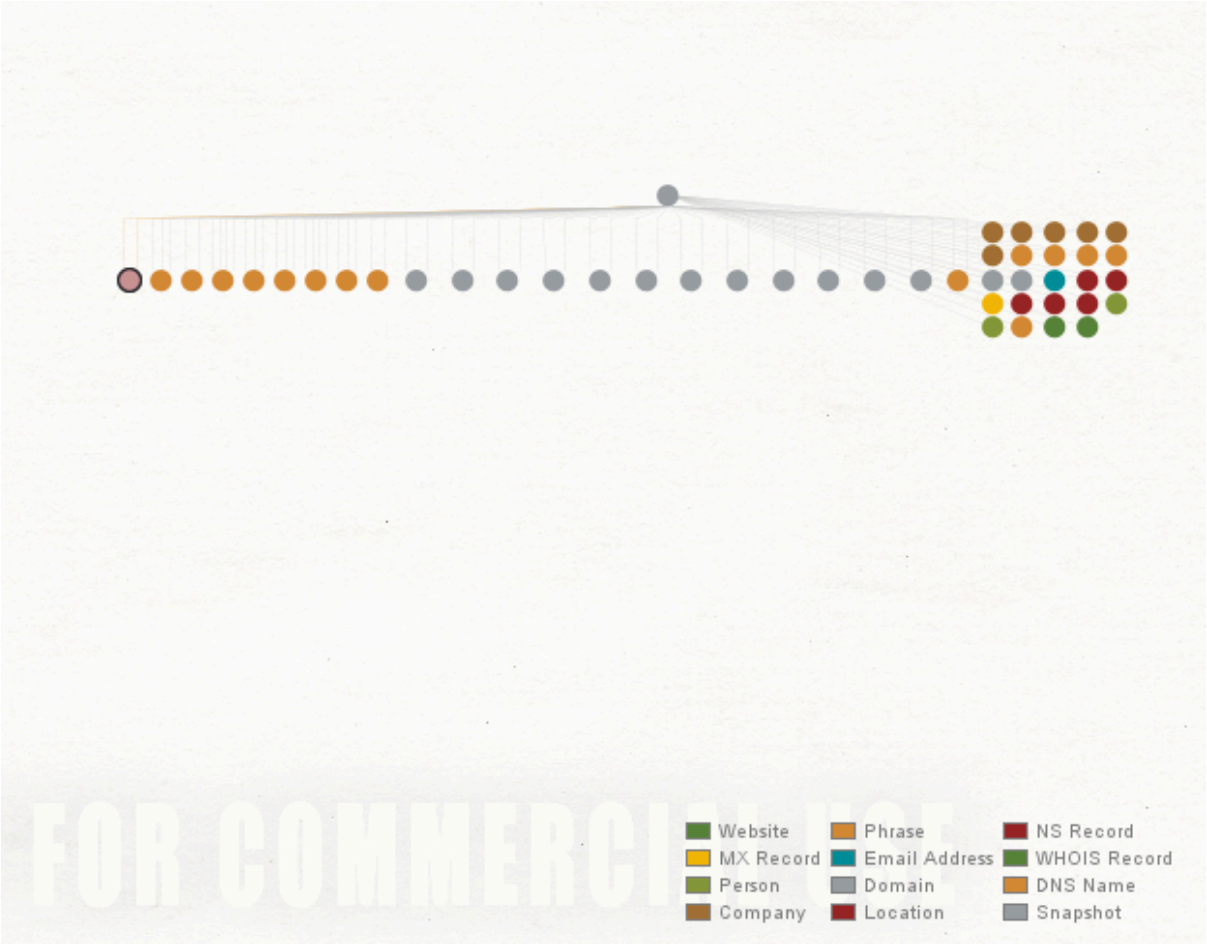
1a. Phrase browsing
Partendo da nessuna informazione disponibile se non il nome dell'azienda, andiamo ad inserire lo stesso come nodo cruciale di un grafo in Maltego.
Per fare ciò, inseriamo una entity Phrase con contenuto "nome azienda".
Azioniamo i vari transform; di seguito una versione censurata dei risultati ottenuti:



Notiamo come siano presenti molti dati relativi all’azienda. Ci concentreremo in particolare su 1 aspetto: il sito web, descritto univocamente in chiaro.

1b. Site Browsing

Andiamo a creare, per facilitare la comprensione, un nuovo grafo, il cui nodo primario sarà il sito web precedentemente trovato. Applicando i transform, vediamo i risultati trovati:

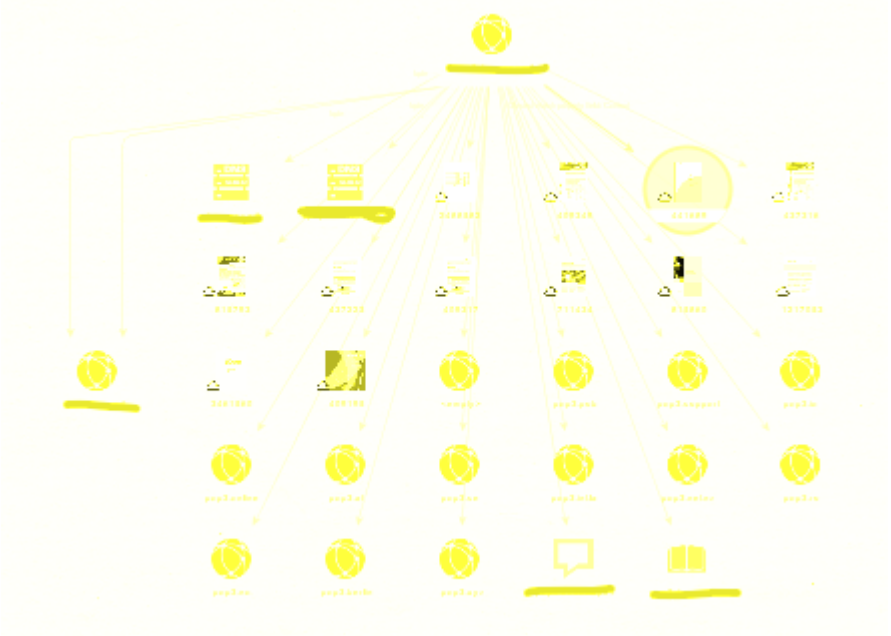


La quantità di risultati direttamente collegati a quel sito è pressoché infinita, ed espone ad internet una serie di informazioni sensibili. Vengono mostrate diverse edizioni precedenti del sito web e la versione più recente (nonostante il sito sia attualmente in manutenzione).
Ci concentreremo in particolare su 3 di queste: esplorazione di server, locazione dell'azienda e profilo dell'amministratore.

1c: Esplorazione server esterni che forniscono servizi all'azienda
Di seguito, un grafo riguardante dispositivi e registri associabili ad un server DNS gestito da un provider esterno collegato al sito preso in esame:

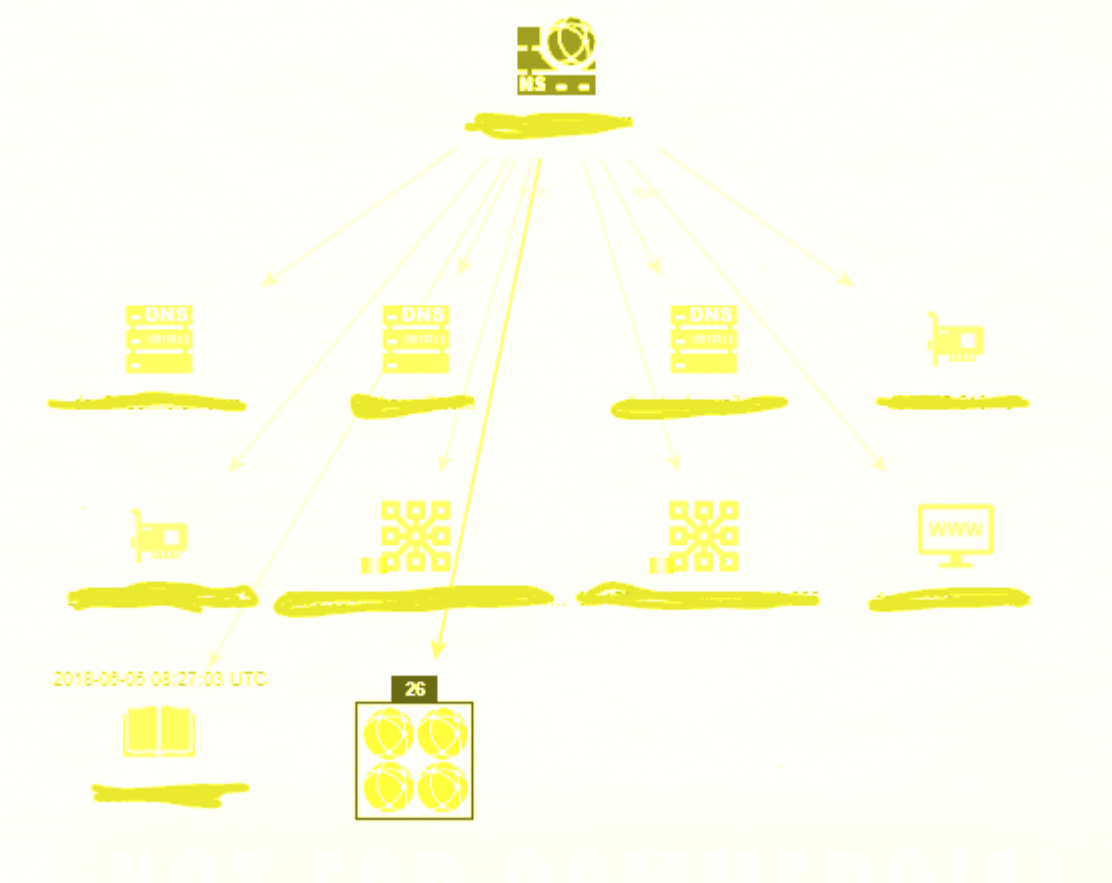
Vediamo in chiaro indirizzi IP, indirizzi MAC, registri WHOIS e domini.

1d: Esplorazione di servizi interni all'azienda
Andiamo adesso a ripetere il procedimento sul server che hosta il sito web.
Ecco i risultati nel dettaglio:



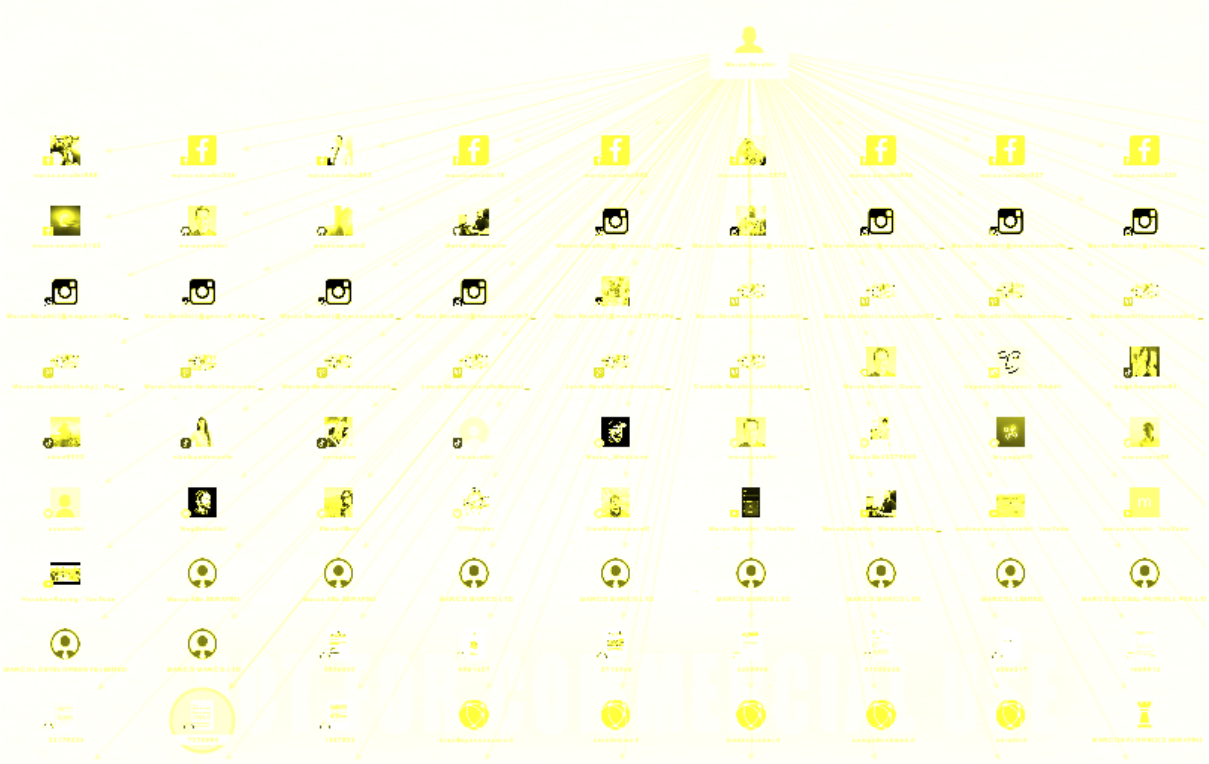
Alcuni elementi raffigurano documentazione tecnica in PDF riconducibile ad impianti di produzione.

1e. esplorazioni NS relativi al server DNS precedente:
Vediamo un registro di domini del precedente web server.



Al suo interno, troviamo 26 domini web in chiaro, oltre ad altri elementi riguardanti il provider di hosting.

1f. Ricerca amministratore
A questo punto, eseguiamo i transform sull'amministratore, per vederne attività passate e social network.



Oltre ai social network, troviamo articoli che riguardano incarichi politici e sindacali ricoperti al di fuori dell'azienda.

A questo punto, sfruttiamo le Google Dorks per affinare ulteriormente alcuni risultati ottenuti. Prima di tutto, cerchiamo conferma che l'indirizzo fisico dell'azienda ottenuto tramite Maltego sia quello attuale.
La ricerca da effettuare sarà:

- **map:location**

  Permette di visualizzare direttamente la mappa relativa al luogo richiesto;

Ottenuta conferma, passiamo al confronto del contenuto del sito.

- **site:URL**

  Visualizza tutti i risultati e le pagine del sito inserito;

Ed infine, cerchiamo conferma sui dati relativi all'amministratore. Nello specifico:

- **intext:nomeamministratore** Cercherà nei file online il nome amministratore;

Otteniamo risultati troppo generici. Affiniamo la ricerca con la Google Dork **"AND"**, aggiungendo il nome dell'azienda.

- **intext:nomeamministatore AND intext:nomeazienda** Cercherà nei file online il nome amministratore ed il nome dell'azienda;

La ricerca adesso è estremamente pertinente e combacia con i dati forniti da Maltego in precedenza.