

# Report S5/L1

## Penetration Testing

Nell'esercizio di oggi viene richiesto di simulare la fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i principali strumenti della fase di information gathering.

Gli strumenti principali che andremo a utilizzare saranno:

1. **GOOGLE**: Utilizzato per la raccolta iniziale di informazioni.
2. **MALTEGO(tool)**: Strumento per l'analisi e la visualizzazione di relazione tra persone, gruppi, organizzazioni, domini, siti web e altre entità.

Abbiamo prima di tutto effettuato le nostre ricerche tramite google utilizzando operatori booleani(**AND,OR,NOT**) e altri più speciali come **filetype**: per affinare i nostri risultati. Dopodiché abbiamo utilizzato **Maltego** per riportare le informazioni e le relazioni che abbiamo trovato per il nostro target scelto.

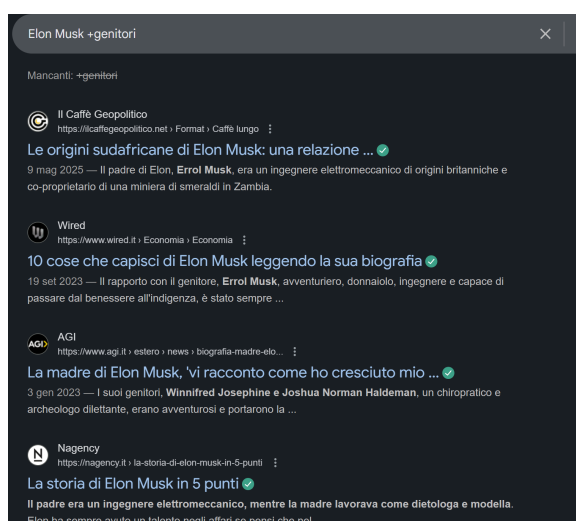
Target: **Elon Musk**

Prima Fase:

### Ricerca tramite Google

#### **Elon Musk +Genitori:**

Digitando **Elon Musk +Genitori** Google cercherà tutte le frasi che contengono le parole specificate. Pertanto il risultato che ci verrà restituito saranno tutte le informazioni su Elon Musk e i suoi genitori:



### **Elon Musk +Fratelli:**

Sempre utilizzando l'operatore “+” la ricerca effettuata su Google mi restituirà le parole che ho richiesto. In questo abbiamo chiesto se Elon Musk ha dei fratelli:



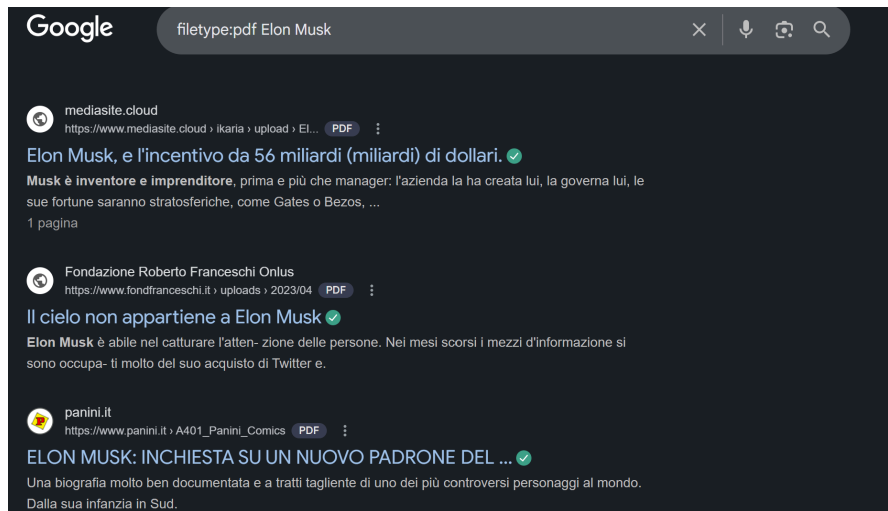
### **Elon Musk -Genitori:**

Questo operatore “ - “ (NOT) va ad escludere i risultati che vengono dopo l'operatore ” - “. In questo caso quindi la ricerca ci restituirà solo risultati in base a “Elon Musk”.



### Utilizzo termine speciale ***filetype***:

In questo caso abbiamo utilizzato la dicitura ***filetype:pdf Elon Musk*** Questo termine speciale ci permette di focalizzare la ricerca su file specifici (In questo caso **PDF**) che abbiano come argomento **Elon Musk**:

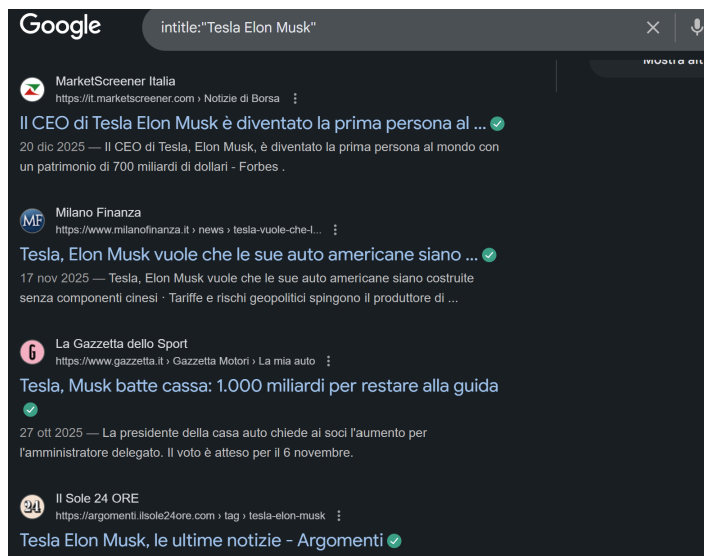


### Utilizzo termine ***Intitle***:

Per familiarizzare con l'utilizzo dei termini speciali abbiamo utilizzato anche Intitle

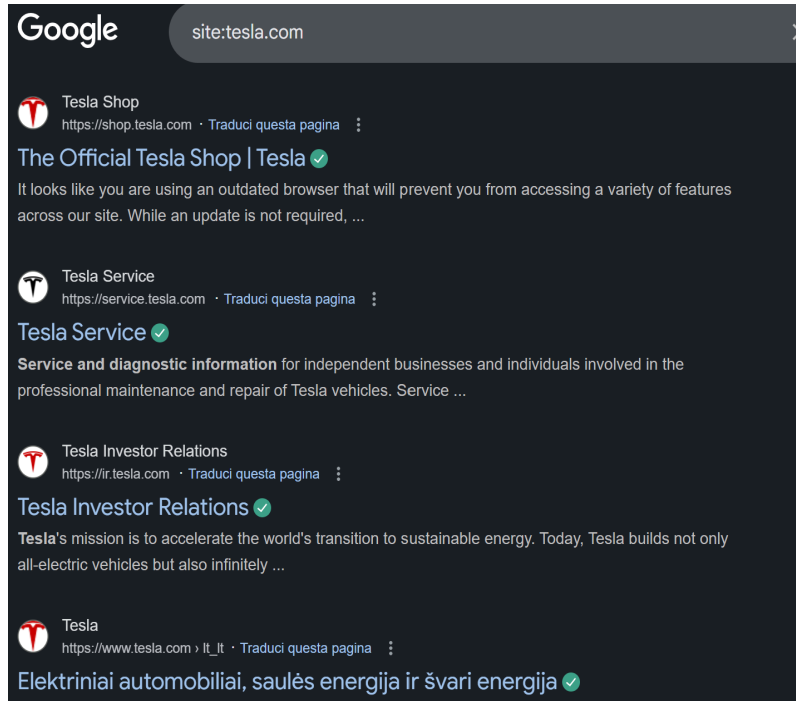
### ***intitle:"Tesla Elon Musk"***

In questo modo questo operatore speciale cerca parole specifiche nei titoli delle pagine web



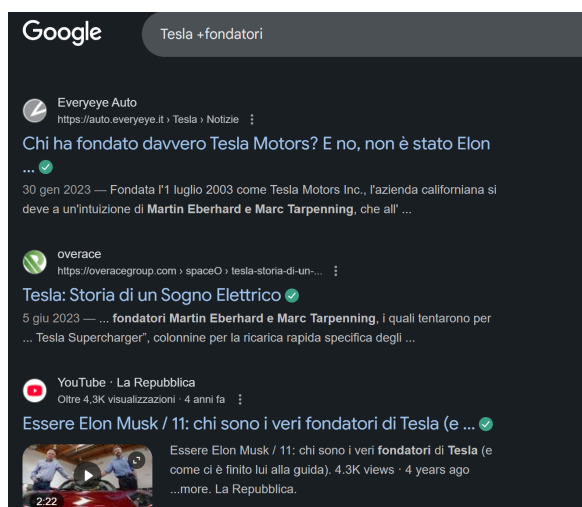
Utilizzo termine **site: tesla.com**

Così facendo abbiamo limitato la ricerca a un sito web specifico che richiama “**Tesla.com**”



### **Fondatori Tesla (Dettagli nascosti):**

Durante l'esercitazione abbiamo deciso di fare una ricerca più dettagliata dell'azienda **Tesla**. Quindi abbiamo cercato chi fossero i fondatori della Tesla e il risultato che ci ha restituito è il seguente: abbiamo scoperto che esistono **Martin Eberhard** e **Marc Tarpenning** che sono i fondatori della **Tesla**.



Seconda fase:

### Maltego

Dopo aver effettuato le nostre ricerche su Google andiamo a riportare le nostre ricerche su Maltego.

