Information Gathering

Questa fase ha l'obiettivo di raccogliere quante più informazioni possibili sul target, al fine di ricavare dati preziosi da poter sfruttare nel corso del pentest.

Strumenti usati

Google dorks: query di ricerca che ci permettono di avere delle informazioni specifiche e che normalmente non apparirebbero nei motori di ricerca.

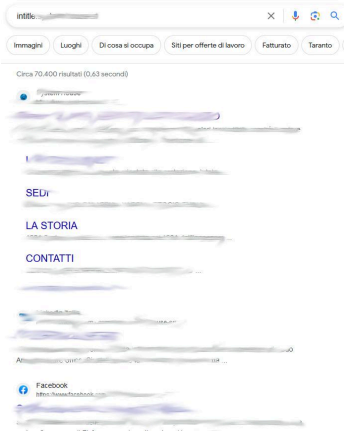
Shodan: un motore di ricerca che consente di individuare tutti gli asset connessi ad Internet in modo da analizzare in modo completo l'infrastruttura IT di un'organizzazione.

IntelX: un motore di ricerca che mostra alcuni dati presenti nel dark web, permette di trovare informazioni che sono state sottratte e poi condivise.

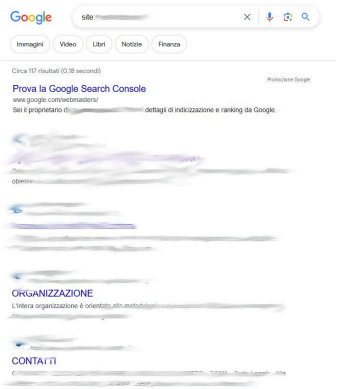
Azienda Target

Risultati ottenuti

Attraverso l'operatore intitle troviamo tutti risultati che hanno nel campo TITLE dell'HTML il valore o l'espressione ricercati.



L'operatore SITE è particolarmente importante durante la fase di information gathering di un pentest perché ci aiuta a capire il perimetro di esposizione sul web del nostro target:



Info in ufficio camerale:

- **Partita IVA:** [redacted] **- Codice Fiscale:** [redacted]
- **Rag. Sociale:** [redacted]
- **Indirizzo:** [redacted]
- **Fatturato**: € 56.848.507,00
- **Dipendenti :** 2453 (2024)

Servizi offerti dall'azienda target:

- **Customer service**
- **Credit management**
- **Help Desk**
- **Back Office**
- **Riscossione tributi**
- **Soluzioni ICT**

Info:

- PEC: [redacted]
- **Resolver name:** [redacted]

Attraverso Maltego - e poi andando a verificare le informazioni trovate - è possibile individuare:

- *amministratore* unico, Ing.[redacted].
- individuare i vari domani usati dell'azienda
- I sistemi di comunicazione interni all'azienda
- La location di alcune sedi, compreso di strada e civico in chiaro

Grazie ad IntelX è stato possibile trovare alcune collezioni di password e mail trafugate in passato [2019 (Collection 1/Collection #1_NEW combo semi private_Private combos.tar.gz)]**:**

Questa è stata solo una piccola analisi preliminare che potrebbe però essere ampiamente approfondita.