Utilizziamo gli operatori **intitle:**, **inurl:**, **intext**:, **numrange:**, **phonebook:**, **filetype:** e **site:**, anche concatenati tra loro (AND,OR, NOT), per una ricerca preliminare tramite **google dorks** sul nostro target.

L'operatore site: è particolarmente importante durante la fase di information gathering in quanto ci aiuta a capire il perimetro dell'esposizione sul web del nostro target poiché può essere utilizzato per restituire i **sottodomini** di un dato host, permettendoci di avere una visione più ampia della mappa di rete reale (**site crawling**).

In seguito si provano ad utilizzare query più specifiche utilizzando quelle del sito **https://www.exploit-db.com/google-hacking-database**; tramite esse si cercano per esempio file contenti informazioni di rilievo, server e/o directory vulnerabili, pagine di login (utilizzando come parole **chiave** script, log, dump, sql, php, …) relativi al target.

Eseguo anche una ricerca relativa al target specifico su **shodan**, un motore di ricerca specializzato in dispositivi connessi a Internet. A differenza dei normali motori di ricerca che indicizzano i contenuti delle pagine web, fornisce informazioni sulle porte e i servizi di dispositivi connessi, come server, router, stampanti, videocamere di sorveglianza e dispositivi IoT (Internet of Things); questo motore di ricerca consente di trovare dispositivi specifici in base a diversi parametri come il tipo di dispositivo, il sistema operativo, la località geografica e altro ancora.

Posso utilizzare anche **webmii** per ricerche specifiche su persone legate al target; esso è un motore di ricerca che raccoglie informazioni da varie fonti online per creare profili completi e aggiornati su individui specifici. Utilizza dati da social media, siti web personali, blog e altre fonti pubbliche per fornire una panoramica complessiva di un individuo in un'unica pagina; i profili webmii possono contenere informazioni come biografia, foto, link ai profili dei social media, risultati delle ricerche online e altro.

Utilizzo anche dei tool preinstallati su Kali Linux; **Whois** fornisce molte informazioni circa il dominio target, i name server, ed altro e **theHarvester** permette di trovare e-mail esistenti, e potenzialmente anche gli username che appartengono all' organizzazione. Le e-mail sono sicuramente una informazione preziosa in quanto rivelano i nomi degli impiegati della compagnia target per configurare attacchi di social engineering mirati.

Infine uno strumento molto potente utilizzato è **maltego**, che da definizione è una open source intelligence and forensics application; esso recupera le informazioni e le correla tra di loro sfruttando sorgenti pubbliche. Inoltre, mette a disposizione dell'utente una comoda interfaccia grafica, dove i dati possono essere rappresentati in diversi formati molto intuitivi. Utilizzandolo a partire dal sito web del target, tramite elaborazioni successive, otteniamo un grafico molto ricco di informazioni in cui si riescono graficamente a identificare le informazioni categorizzandole per **website**, **phrase**, **person** (si possono trovare profili di persone legate alla compagnia), **URL**, **company**, **location**.