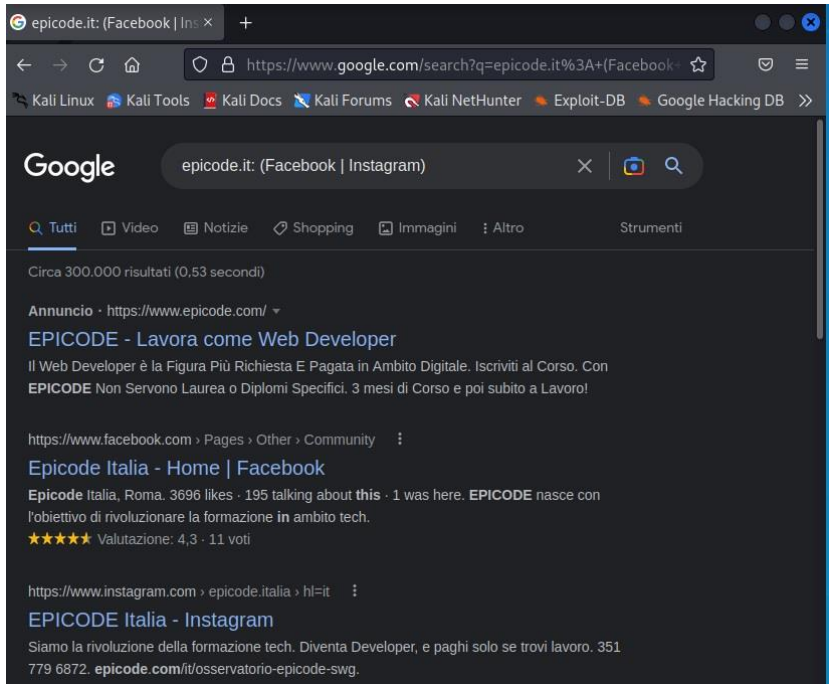
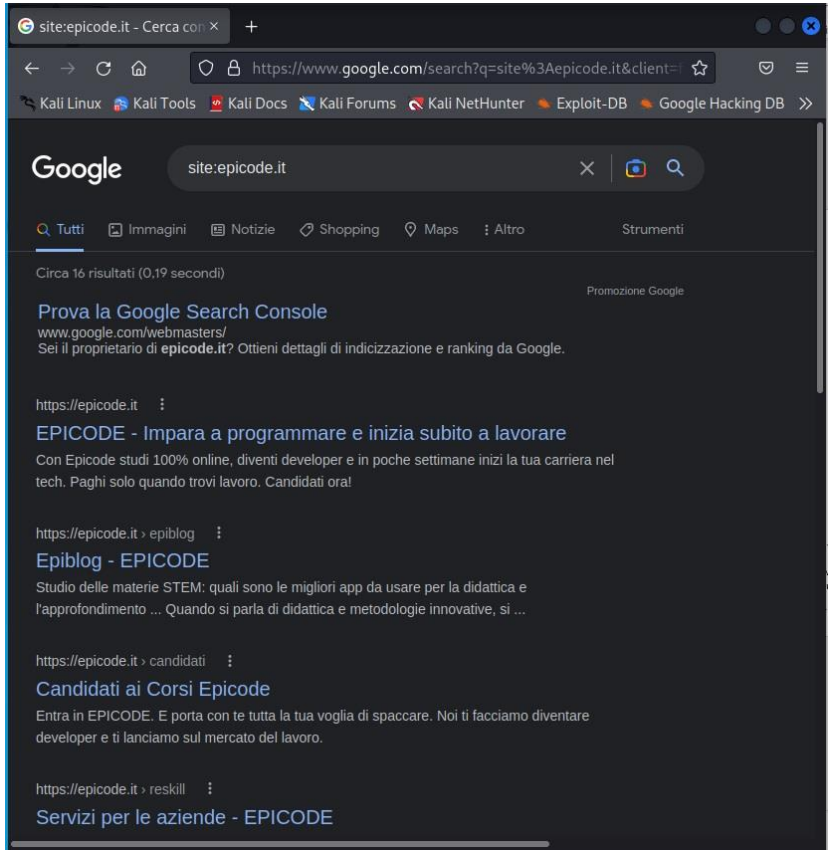
Raccolta informazioni attraverso:
Google (raccolta passiva)
Recon-ng
Maltego
del target: *www.epicode.it*

Orlando Tangari



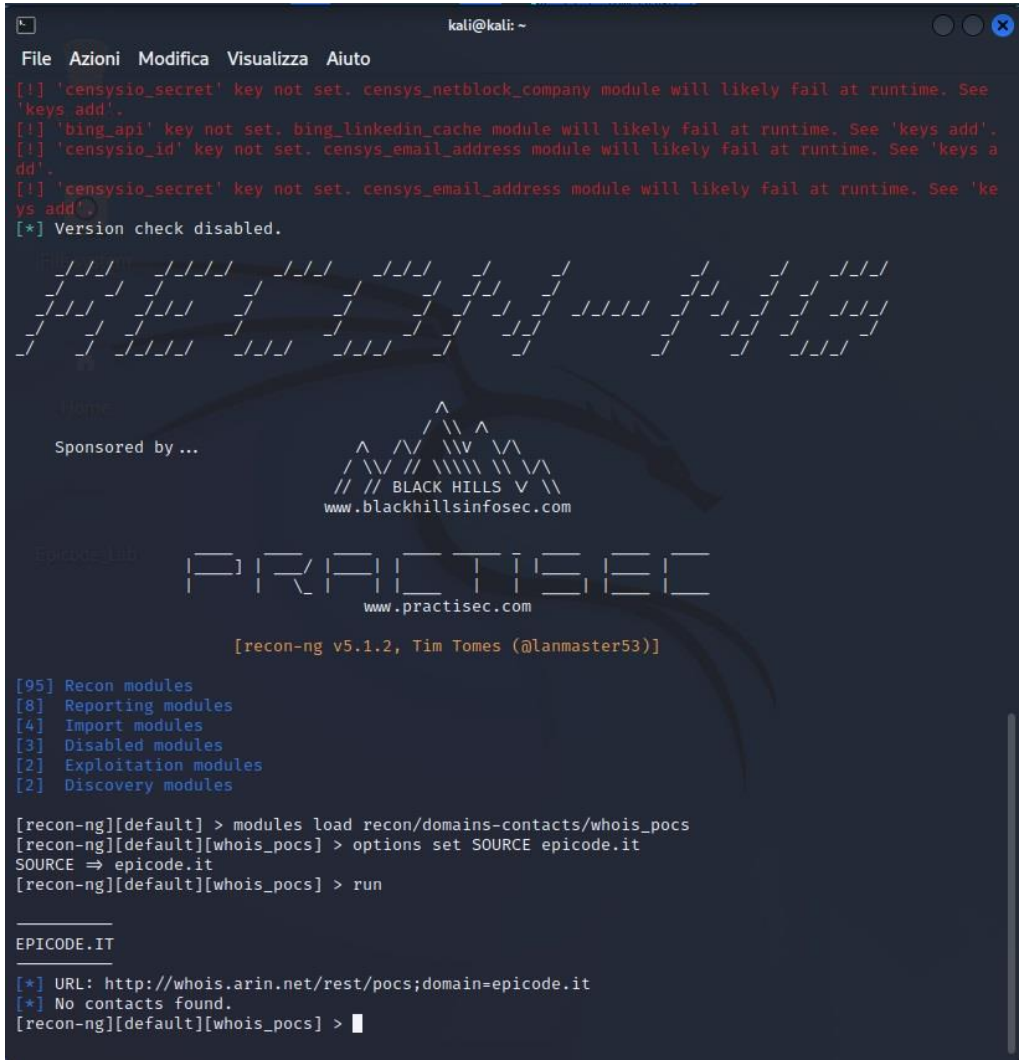


Fase di raccolta informazioni con Google (raccolta passiva)

Si utilizza Google per ricercare informazioni sul target di riferimento*: epicode.it*, in maniera molto più avanzata.

Attraverso la query combinata: *epicode.it: (Facebook| Instagram)*, come mostrato nell'immagine in alto a sinistra, vengono restituiti all'utente solamente la pagine che hanno Facebook e Instagram nel titolo.

L'operatore SITE, come mostrato nell'immagine centrale; è importante, in quanto aiuta a capire il perimetro dell'esposizione sul web del target di riferimento e, inoltre, restituisce i sottodomini di un dato host in base alla popolarità delle ricerche, capendo quale sottodominio è potenzialmente più esposto a rischi.



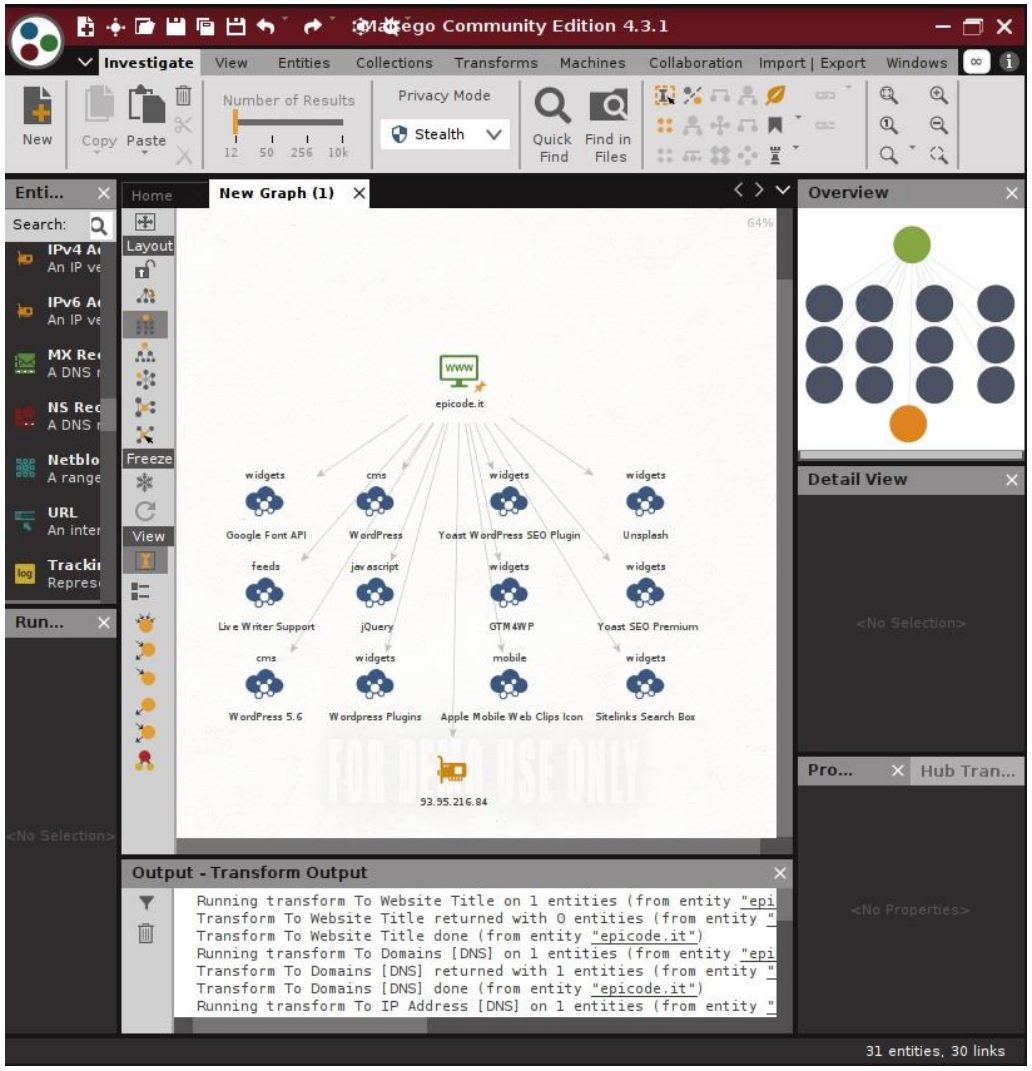
Fase raccolta informazioni con Recon-ng

Recon- ng è un tool utilizzato per la raccolta di informazioni composto in moduli, utilizzati per essere utilizzati per diversi scopi, come il recupero delle email degli impiegati, come mostrato nell'immagine, facendo riferimento al target: *epicode.it*.

Il primo comando da eseguire, nell'interfaccia a riga di comando, è: *modules load recon/domains-contacts/whois_poc*, per scegliere il modulo da eseguire.

Il secondo comando da eseguire, per settarlo con il target di riferimento è: *options SOURCE epicode.it* .

Infine, si esegue il playload con il comando *run*, elencando, se presenti, le email degli impiegati.



Fase raccolta informazioni con Maltego

Maltego è un tool che recupera informazioni e le correla tra di loro, sottoforma di grafici, sfruttando sorgenti pubbliche.

Attraverso il menu a sinistra, si seleziona il cosiddetto: *nodo 0*, punto di partenza per recuperare le informazioni disponibili nel tool.

Come mostrato nell'immagine, si è partiti dal sito internet del target di riferimento: *epicode.it* e gli output in basso al *nodo 0* si scelgono tramite il click del tasto destro su di esso. In questo caso: IP del sito e servizi usati.