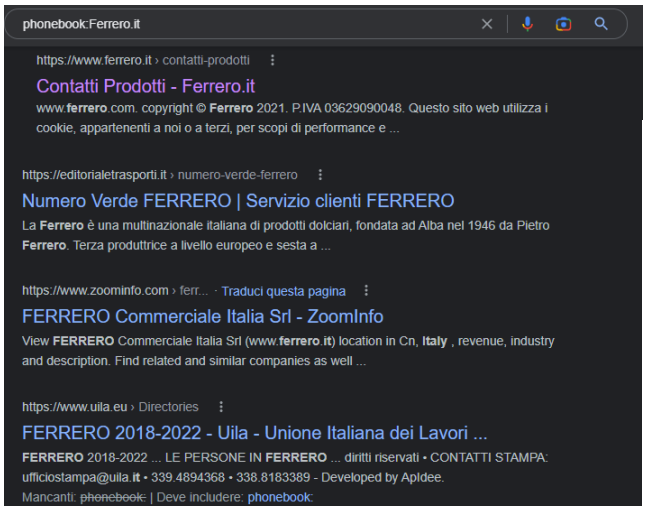
Gabriele Di giampietro **Data 22/11/2022**

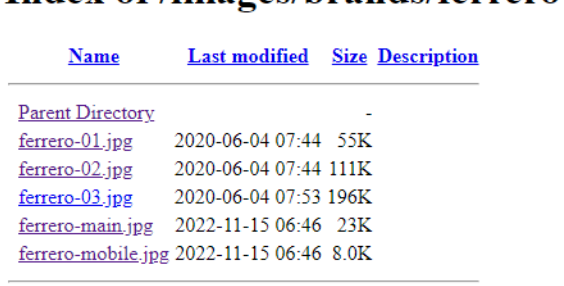
Obbiettivo: simulazione di raccolta informazioni di un target a scelta, utilizzando Google hacking; Recon –ng; Maltego.

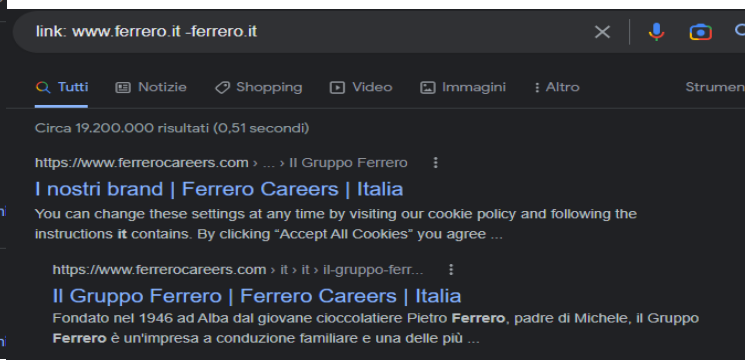
Prima fase Google Hacking Target: Ferrero.it

Nella prima fase di raccolta dati, andiamo a fare una ricerca passiva utilizzando google hacking verso l'azienda Ferrero.it. Per fare ciò ho utilizzato le seguenti query: phonebook:Ferreo.it ed ho trovato il numero di telefono dell'azienda e altri contatti; allintext: ferrero sede italia ed ho trovato la sede fisica dell'azienda in Italia; Intitle: index.of inurl: Ferrero.it ed ho trovato delle sottocartelle con varie immagini brand utilizzati per il sito principale; link: www.ferrero.it – ferrero.it ed ho trovato tutti gli altri siti che citano il link ferrero.

I risultati nelle imagini seguenti:



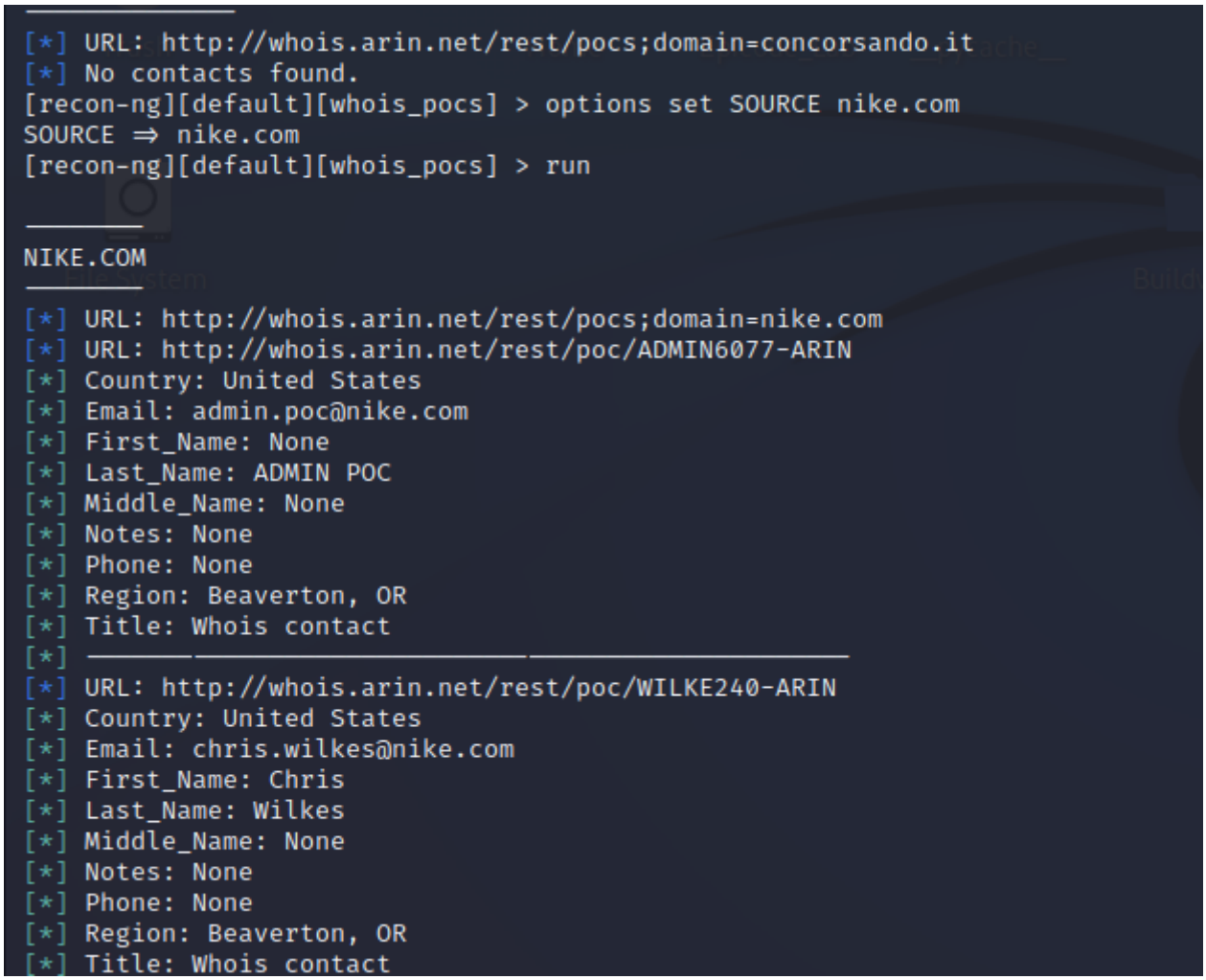




Seconda fase Recon-ng **Target: nike.com**

Nella seconda ricerca di informazioni utiliziamo da Kali recon-ng, andimo ad utilizzare il modulo domains-contacts/whois_pocs cosi da trovare le email e le informazioni dei dipendeti contenute sul sito.

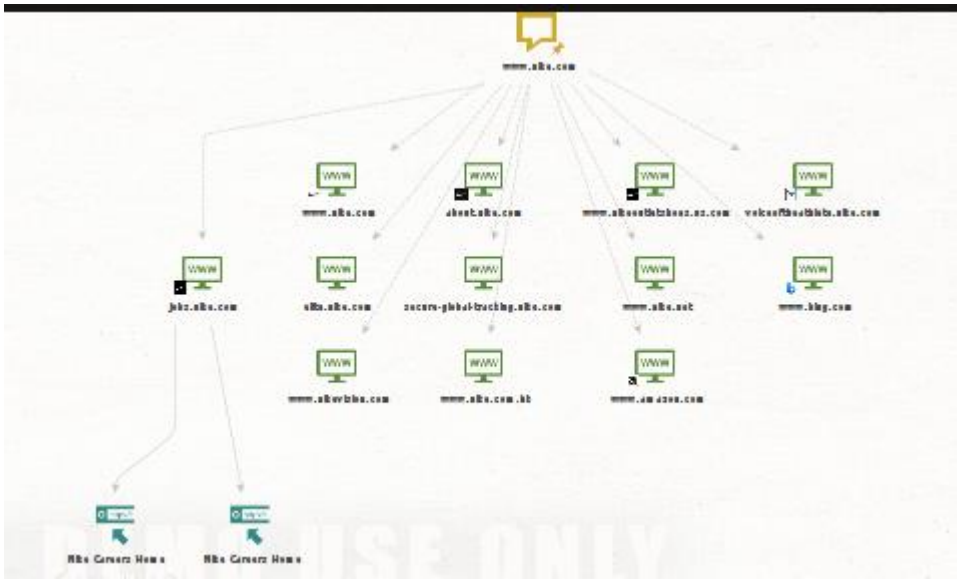
Vediamo i risultati nell'imaggine seguente:



Terza fase Maltego **Target:nike.com**

Inquesta ultima fase invece abbiamo utilizzato Maltego che attraverso la sue funzione che viene chiamata trasformazione possiamo ricavare ancora molte più informazione dal sito principale, arrivando ad altri su altri url di origine fino ad informazioni sul personale dipendente come numeri di telefono, email e indirizzi ip di origine.

Vediamo i risultati nella figura seguente:



Dopo gli url abbiamo ottenuto anche come dicevamo sopra informazioni sul personale dipendente collegato per non incorrere nella pubblicazioni di informazioni private, possiamo vedere un immagine che rappresenta lo schema sintetizzato di tutta la nostra ricerca su maltego: