Dopo aver effettuato ricerche specifiche da google (vedi pdf “google hacking”), andiamo a vedere quali informazioni ricaviamo dai programmi online e quelli installati su kali.

Query tool

www.zanichelli.it resolved to 52.19.238.178

DNS Query Results:

```
; <<>> DiG 9.2.4 <<>> any www.zanichelli.it
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7554
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.zanichelli.it. IN ANY

;; ANSWER SECTION:
www.zanichelli.it. 300 IN CNAME zan-prod-elb-518790956.eu-west-1.elb.amazonaws.com.
zan-prod-elb-518790956.eu-west-1.elb.amazonaws.com. 60 IN A 52.19.238.178
zan-prod-elb-518790956.eu-west-1.elb.amazonaws.com. 60 IN A 54.216.103.134

;; Query time: 31 msec
;; SERVER: 66.11.0.58#53(66.11.0.58)
;; WHEN: Tue Nov 22 10:02:39 2022
;; MSG SIZE rcvd: 131
```

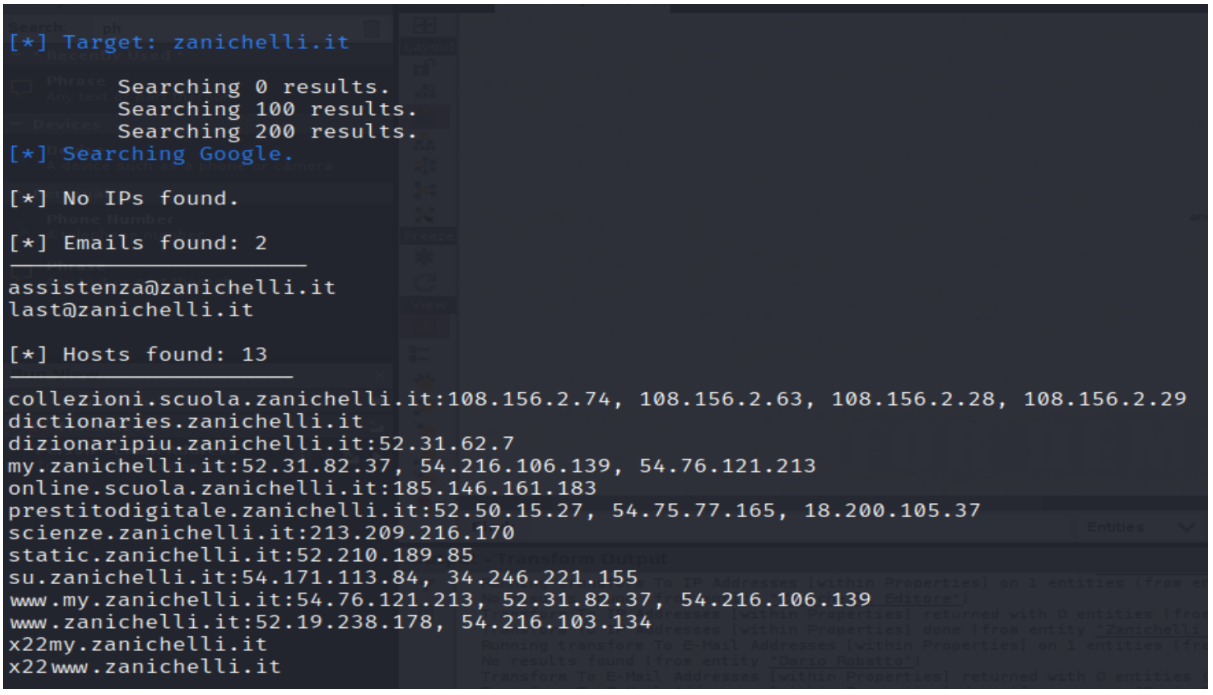
Utilizzando questo tool online possiamo eseguire una scan molto approfondita ottenendo informazioni circa il dominio e i proprietari e molte altre.

The Harvest

Lanciamo il comando dal terminale Linux:

theHarvester -d zanichelli.it -l 200 -b google

Si noti che tale comando eseguirà una scansione su dominio scelto (-d) con ricerca limitata a 200 risultati (-l) utilizzando come risorsa della scansione google (-b).



Come possiamo vedere il programma ci restituisce il numero di ricerche che spuntano nel motore di ricerca google, gli indirizzi e-mail contenuti nel sito e tutti gli hots legati ad esso.

Recon-ng

```
[recon-ng][default][whois_pocs] > options set SOURCE zanichelli.it
SOURCE ⇒ zanichelli.it
[recon-ng][default][whois_pocs] > run

ZANICHELLI.IT
[*] URL: http://whois.arin.net/rest/pocs;domain=zanichelli.it
[*] No contacts found.
```

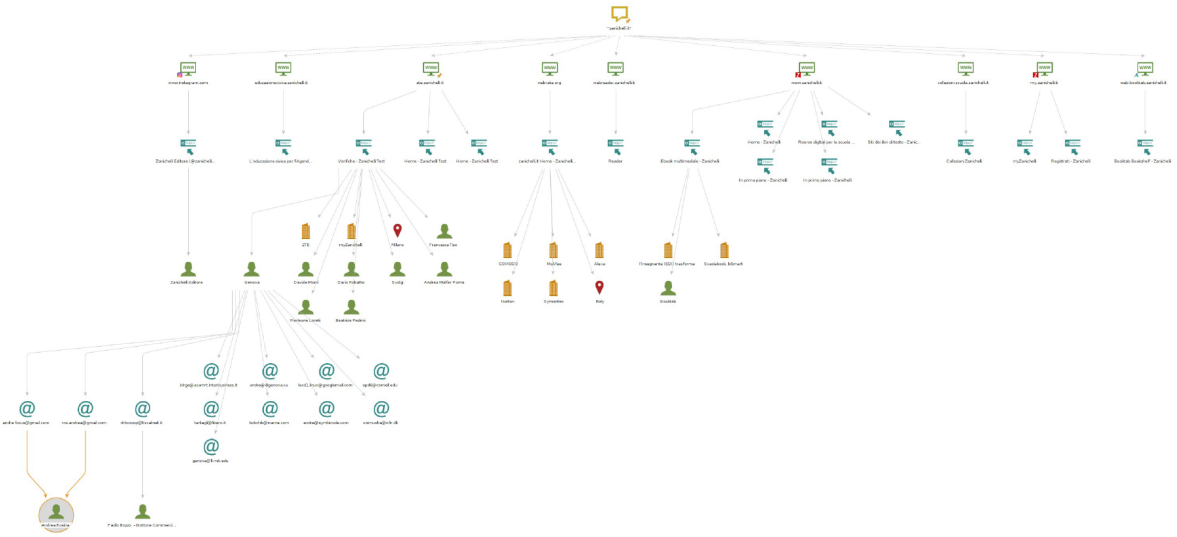
Utilizzando la libreria *whois_pocs* e settando il dominio desiderato il programma dovrebbe restituirci le informazioni di contatto che riesce a trovare.

Whois

```
┌──(kali㉿kali)-[~]
└─$ whois zanichelli.it

*******************************************************************
* Please note that the following result could be a subgroup of    *
* the data contained in the database.                             *
*                                                                 *
* Additional information can be visualized at:                    *
* http://web-whois.nic.it                                         *
*******************************************************************

Domain:                 zanichelli.it
Status:                 ok
Signed:                 no
Created:                1996-01-29 00:00:00
Last Update:            2021-12-28 00:52:22
Expire Date:            2022-12-12

Registrant
  Organization:         ZANICHELLI EDITORE SPA
  Address:              VIA IRNERIO, 34
                        BOLOGNA
                        40126
                        BO
                        IT
  Created:              2019-12-09 16:36:48
  Last Update:          2019-12-09 16:36:48

Admin Contact
  Name:                 FERRANTE ENRIQUES ZANICHELLI ED
  Organization:         ZANICHELLI EDITORE SPA
  Address:              VIA IRNERIO, 34
                        BOLOGNA
                        40126
                        BO
                        IT
  Created:              2019-12-09 16:36:48
```

Con il comando whois otteniamo notevolmente più informazioni (molte di più di quelle nell'immagine)

Maltego



Maltego è sicuramente il programma più completo tra quelli visti ora, dopo aver impostato una ***phrase*** è sufficiente utilizzare i ***Trasforms*** (ovvero query pronte a essere utilizzate) già presenti nel programma per compiere azioni tali al fine di ricavare informazioni di ogni tipo sul target. L'immagine qui sopra è volutamente a bassa definizione dato che sono riuscito a risalire addirittura all'identità del personale (presente e passato), i loro contatti e-mail, numeri di telefono e addirittura 1 indirizzo postale.