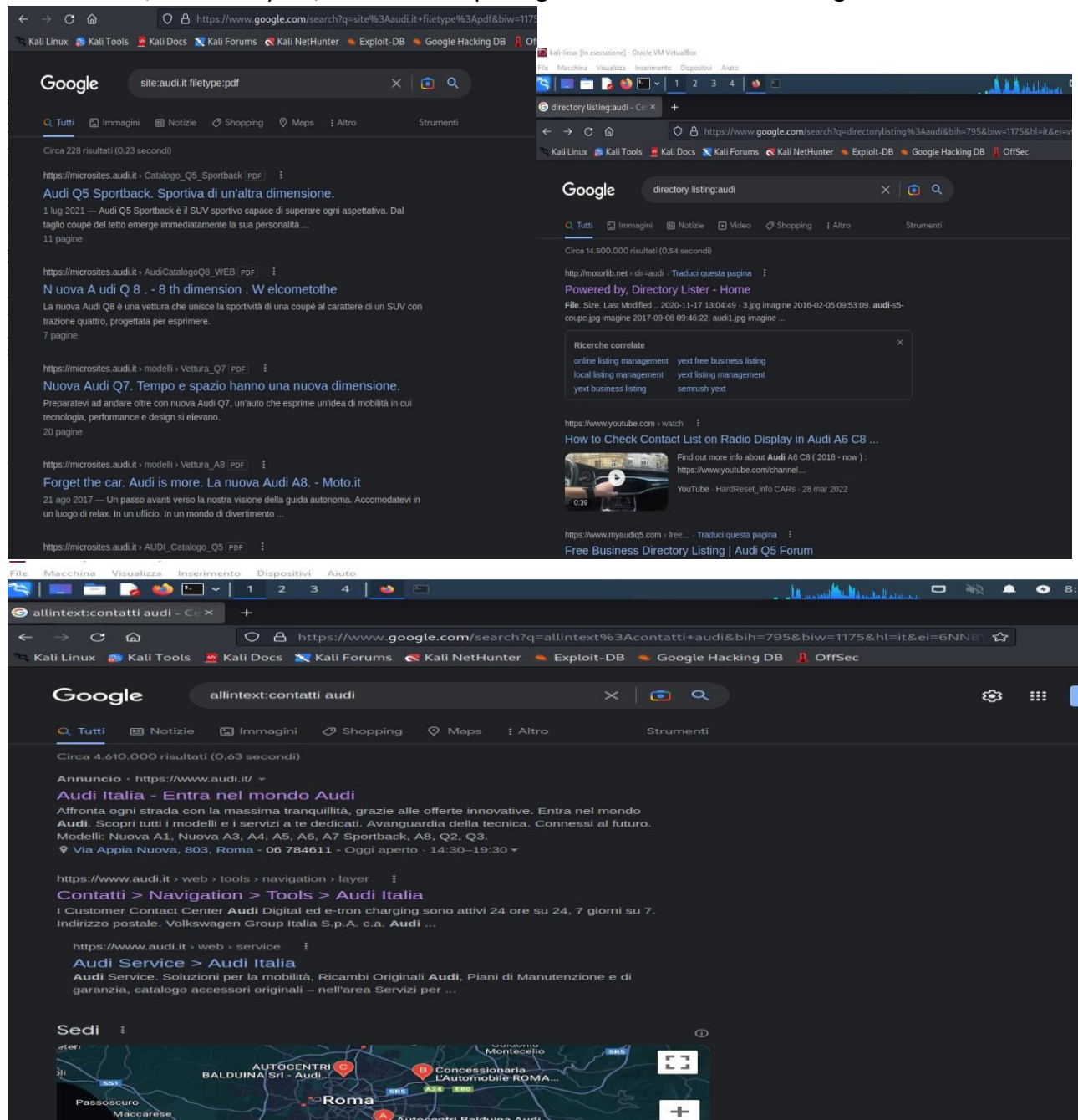


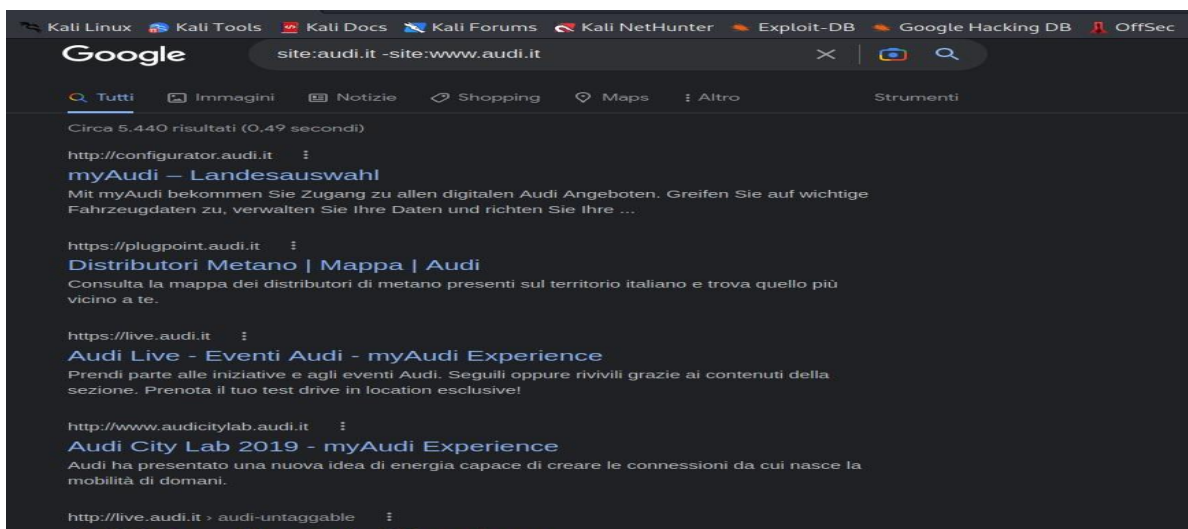
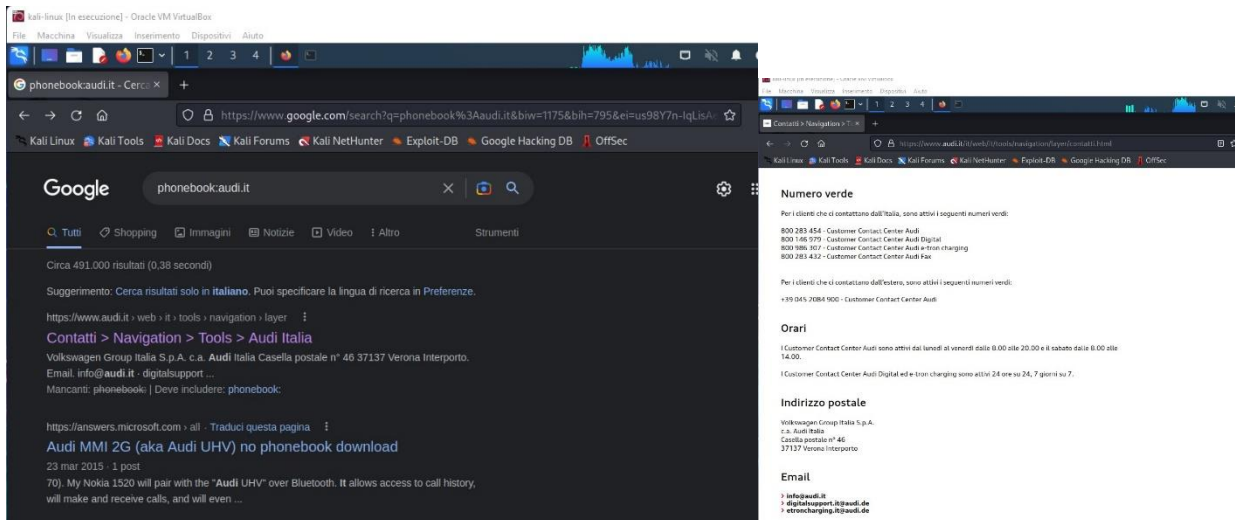
Claudio De cicco
22/11/2022

Report Raccolta informazioni Audi

1 tramite Google

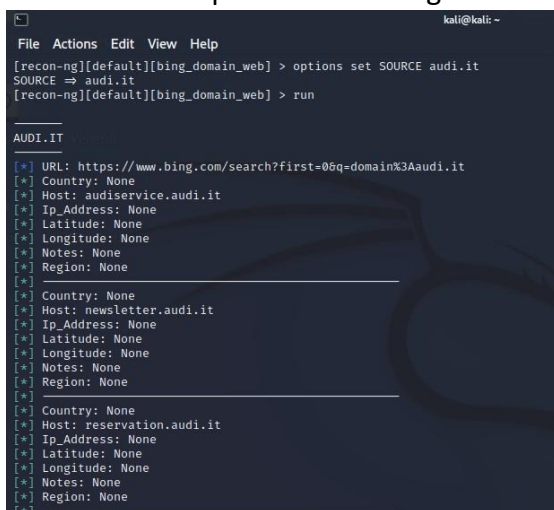
Sono andato a ricercare contatti, sia tramite “phonebook” che cercando tramite “allintext” i contatti audi, le directory list, eventuali file pdf legati ad audi.it e site crawling





2 tramite Recon-ng

Provando ad usare vari moduli sono riuscito ad attingere informazioni dal modulo "Bing serach". Andando a recuperare i nomi degli host.



```
kali@kali: ~  
File Actions Edit View Help  
| recon/hosts-ports/shodan_ip | 1.2 | installed | 2020-07-01 | * | + | +  
  
D = Has dependencies. See info for details.  
K = Requires keys. See info for details.  
  
recon-ng[default]] > modules load recon/domains-hosts/mx_spf_ip  
recon-ng[default]][mx_spf_ip] > info  
  
Name: Mail eXchange (MX) and Sender Policy Framework (SPF) Record Retriever  
Author: Jim Becher (@jimbacher, jbecher@korelogic.com)  
Version: 1.0  
  
Description:  
Retrieves the MX and SPF IPv4 records for a domain. Updates the 'hosts' and/or 'netblocks' tables  
with the results.  
  
Options:  
Name Current Value Required Description  
SOURCE default yes source of input (see 'info' for details)  
  
Source Options:  
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL  
<string> string representing a single input  
cpath path to a file containing a list of inputs  
query <sql> database query returning one column of inputs  
  
Comments:  
* This module reads domains from the domains table and retrieves the hostnames of the MX records  
associated with each domain. The hostnames are then stored in the hosts table. It also retrieves  
the IP addresses and/or netblocks of the SPF records associated with each domain. The addresses  
are then stored in the hosts and/or netblocks table.  
  
recon-ng[default]][mx_spf_ip] > options set SOURCE audi.it  
SOURCE => audi.it  
recon-ng[default]][mx_spf_ip] > run  
+ Retrieving MX records for audi.it.  
+ Country: None  
+ Host: mailrelay.volkswagen.de  
+ Ip Address: None  
+ Latitude: None  
+ Longitude: None  
+ Notes: None  
+ Region: None  
  
File Actions Edit View Help  
[x] Region: None  
[x]  
[x] Country: None  
[x] Host: mri.volkswagen.de  
[x] Ip Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x]  
[x] Country: None  
[x] Host: mr4.volkswagen.de  
[x] Ip Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x]  
[x] Retrieving SPF records for audi.it.  
[x] TXT record: "QuoVadis-d850a1c5-110f-4601-8038-8bb6bddcd44"  
[x] TXT record: "d79ljg6x583yfbbc4wyzttsjl70ymj"  
[x] TXT record: "vR39jbtb78azjgg8qkf8xfnplcj15p"  
[x] TXT record: "DFCA1330-6A38-41BA-BB8C-24QCAD478A_30.1e.2018"  
[x] TXT record: "SPF=audi.e36e2140-ac5b-4b86-a397-56beb91291bd"  
[x] TXT record: "vsfpfi mx include: spf.qualtrics.com ip4=80.74.184.0/26 ip4=77.246.3.160/27 ip4=77.246.3.160/27  
0 include: spf.salesforce.com -all"  
[x] Netblocks: 80.74.184.0/26  
[x] Notes: None  
[x]  
[x] Netblock: 77.246.3.160/27  
[x] Notes: None  
[x]  
[x] Netblock: 77.246.4.96/27  
[x] Notes: None  
[x]  
[x] Netblock: 91.198.139.128/26  
[x] Notes: None  
[x]  
[x] TXT record: "MS=ms87408668"
```

Tramite Maltego analizzando audi.it sono andato a reperire informazioni quali DNS, gli url collegati, i servizi di analytics presenti nel sito, come è costruito, e link.

