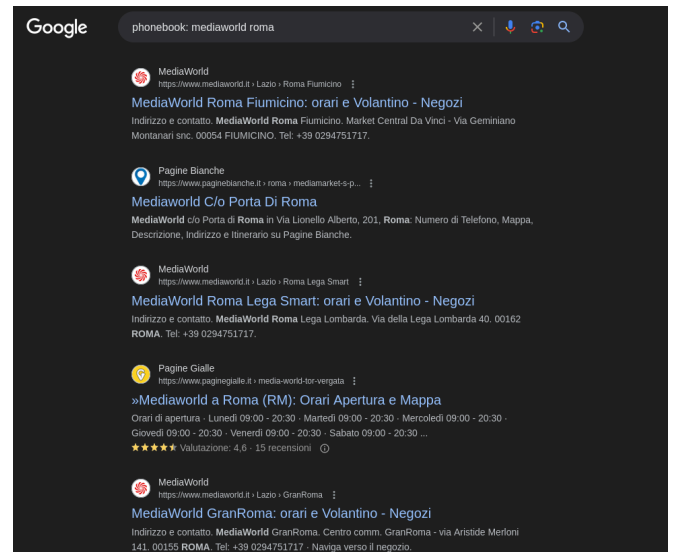
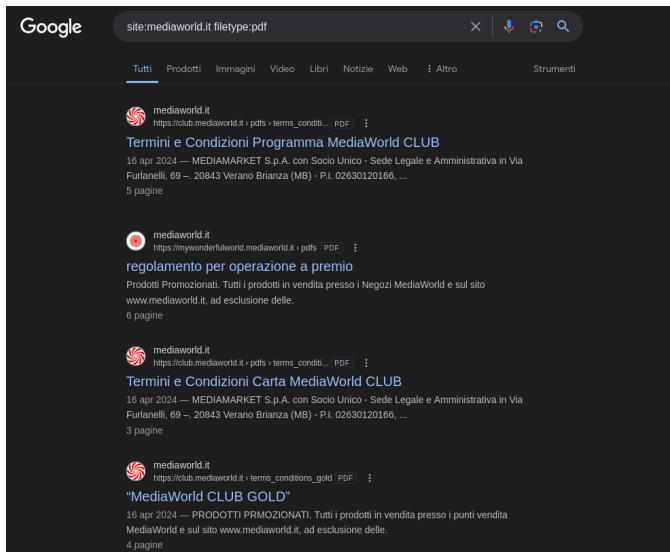


## Consegna S5\_L2



Con Google Hacking, ho cercato delle informazioni riguardanti il target Mediaworld. Tramite FileType:pdf ho trovato informazioni come: la sede legale, partita iva; Con PhoneBook ho trovato il numero di telefono della Mediaworld di Roma.

```
(kali@kali)-[~] Edit View Help
$ nslookup www.mediaworld.it
Server:          192.168.1.254
Address:         192.168.1.254#53

Non-authoritative answer:
www.mediaworld.it canonical name = www.mediaworld.it.cdn.cloudflare.net.
Name:   www.mediaworld.it.cdn.cloudflare.net
Address: 172.65.227.140
Name:   www.mediaworld.it.cdn.cloudflare.net
Address: 2606:4700:90:0:a97c:389b:e45:3a74
```

Con nslookup verso il target [www.mediaworld.it](http://www.mediaworld.it) ho scoperto l'indirizzo ip del sito ufficiale

Con il tool theHarvester, sempre sul target [www.mediaworld.com](http://www.mediaworld.com), sono arrivato a conoscenza di molti altri ip collegati al sito ufficiale, trovando anche un email e diversi Host

```

[*] LinkedIn Links found: 0

[*] IPs found: 138
104.17.225.68
104.18.4.173
104.18.41.189
104.18.5.173
104.40.146.227
129.35.110.102
129.35.122.12
129.35.122.20
13.224.29.100
13.224.29.125
13.224.29.31
13.224.29.98
13.80.3.94
137.117.231.26
138.1.46.118
142.250.217.115
142.250.217.83
142.250.69.211
142.251.33.115
142.251.33.83
147.154.132.7
148.253.228.139
151.139.128.10
151.139.240.1
151.99.151.12
151.99.151.13
151.99.151.14
151.99.151.28
151.99.151.9
157.185.151.69
160.8.84.212
168.63.97.26
172.217.14.211
172.217.14.243
172.64.146.67
172.65.227.140
174.35.12.116
174.35.2.109
174.35.21.198
174.35.21.28
174.35.21.29
174.35.21.32
174.35.21.7
174.35.21.70

```

```

[*] Emails found: 1
servizioclientemediaworld@mediaworld.it

[*] Hosts found: 313
*.mediaworld.it
100mediaworld.it
admin.mediaworld.it
admin.mediaworld.it:35.214.224.70
amer.mediaworld.it
antbl2.mediaworld.it
antbl2.mediaworld.it:dnsdelegation.io
antbl2.mediaworld.it:dnsdelegation.io
antbl2.mediaworld.it:ipm-dsl.vip.prod.criteo.com
app.mediaworld.it
app.mediaworld.it:81.88.46.78
app.mediaworld.it:ms-ssc-firebase-mit-p-3000.web.app
apps.mediaworld.it
apps.mediaworld.it:81.31.150.87
assets.mediaworld.it:129.35.122.20
attesa.mediaworld.it
attesa.mediaworld.it:mediamarketitaly.queue-it.net
attesa.mediaworld.it:mediamarketitaly.queue-it.net
auth-dev.mediaworld.it
auth-test.mediaworld.it
auth-test.mediaworld.it:35.190.90.85
auth-test.mediaworld.it:auth-int.mediamarkt.de
auth.mediaworld.it
auth.mediaworld.it:35.186.247.132
auth.mediaworld.it:auth.mediamarkt.de
autodiscover.mediaworld.it:autod.ms-acdc-autod.office.com
autodiscover.mediaworld.it:autodiscover.outlook.com
autodiscover.mediaworld.it:autodiscover.outlook.com
award.mediaworld.it
award.mediaworld.it:212.78.4.76
award.mediaworld.it:81.31.150.82
blackfriday.mediaworld.it
blackfriday.mediaworld.it:blackfriday.mediaworld.it.cdnga.net
blackfriday.mediaworld.it:blackfriday.mediaworld.it.cdnga.net
bozen.mediaworld.it
cdn.mediaworld.it
cdn.mediaworld.it:81.31.150.80
cdnfpm.mediaworld.it:gb01.ecn.nohup.it
cdnfpm.mediaworld.it:mediaworldatcn.nohup.it
cdnfpm.mediaworld.it:mediaworldatcn.nohup.it
changefirst.mediaworld.it

```

Infine con la query whois, sul target mediaworld.it, ho scoperto i nameserver e la registrazione del sito

```

(kali@kali)-[~]
$ whois mediaworld.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:                mediaworld.it
Status:                ok
Signed:                no
Created:               1998-06-10 00:00:00
Last Update:          2024-06-12 01:12:02
Expire Date:           2025-06-12

Registrant
  Organization:        MMS Intangibles GmbH & Co. KG
  Address:              Media-Saturn-Str. 1
                       Ingolstadt
                       85053
                       DE
  Created:              2023-12-07 11:04:40
  Last Update:          2024-05-08 14:31:52

Admin Contact
  Name:                hidden
  Organization:         hidden

Technical Contacts
  Name:                hidden
  Organization:         hidden

Registrar
  Organization:         InterNetX GmbH
  Name:                 INTERNETXGMBH-REG
  Web:                  http://www.internetx.com/
  DNSSEC:               no

Nameservers
  a5-66.akam.net
  a4-65.akam.net
  a18-64.akam.net
  a10-67.akam.net
  a9-67.akam.net
  a1-250.akam.net

```