

SIMULAZIONE DELLA FASE DI RACCOLTA INFORMAZIONI

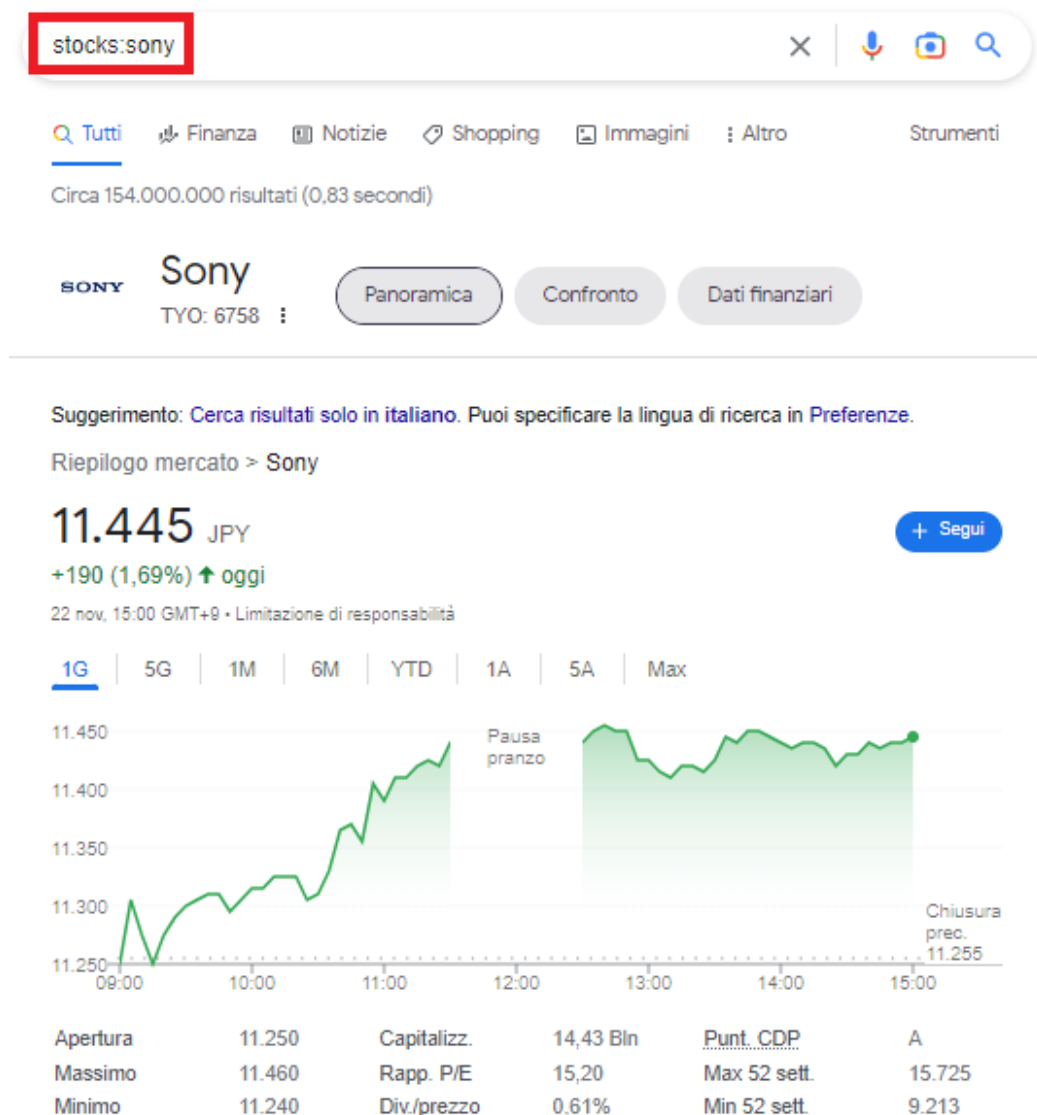
Target: **Sony.com**

Strumenti di information gathering utilizzati:

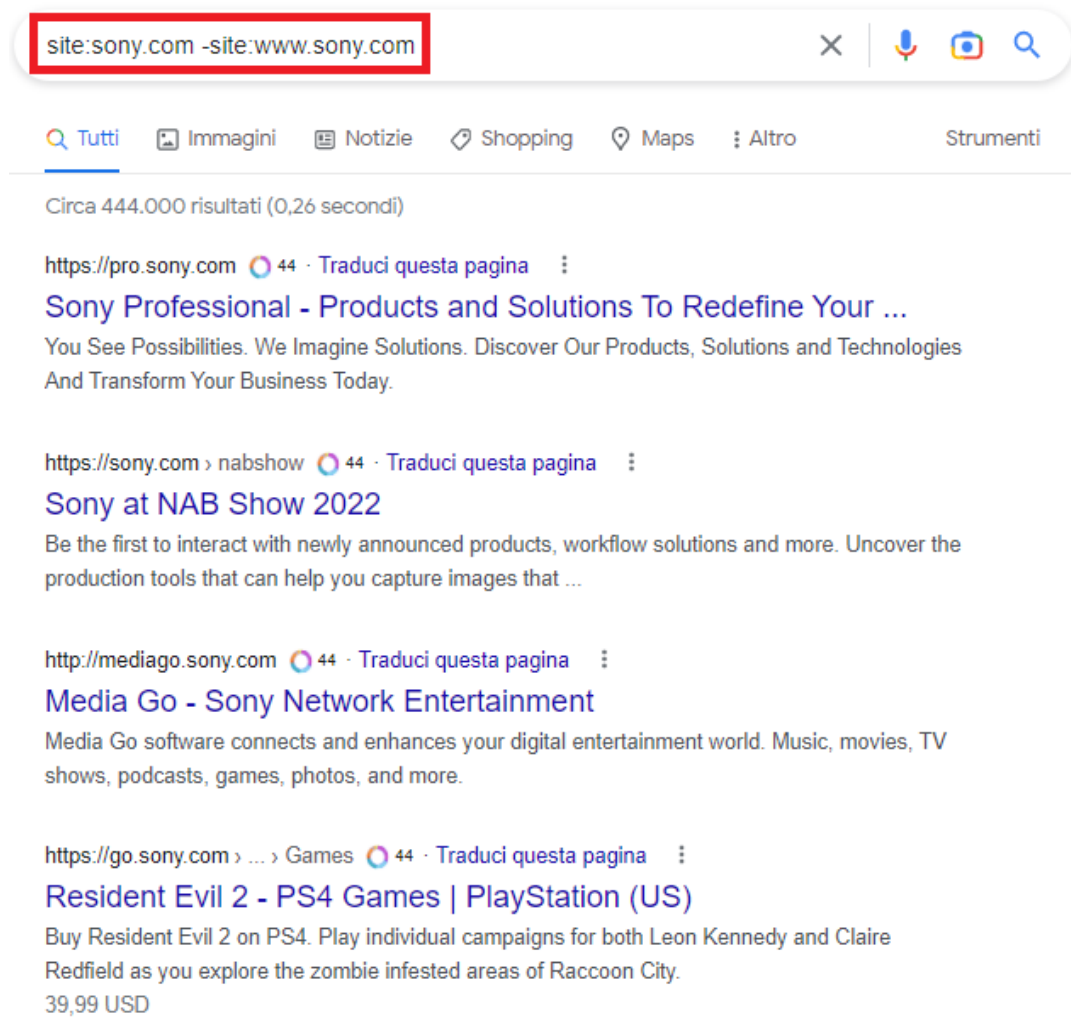
1. **Google Hacking**
2. **Recon-ng**
3. **Maltego**

1. Google Hacking

Utilizziamo la query **stocks:sony** per conoscere l'andamento in borsa dell'azienda target

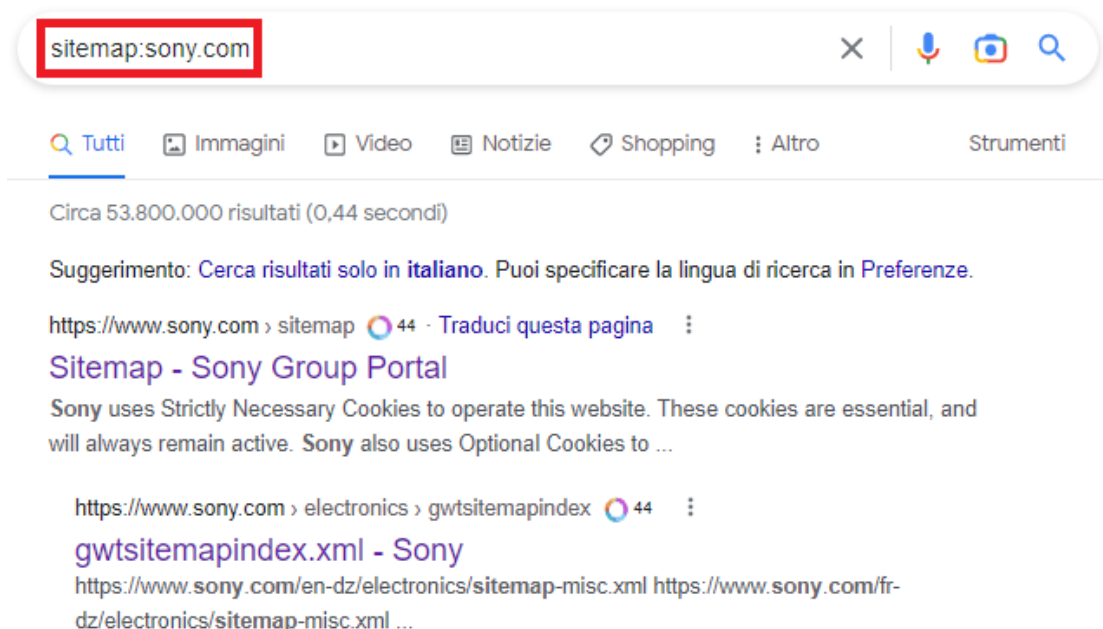


Utilizziamo la query **site** per identificare i sottodomini del sito (*site crawling*)



The screenshot shows a Google search interface. The search bar contains the query `site:sony.com -site:www.sony.com`, which is highlighted with a red rectangle. Below the search bar, there are tabs for 'Tutti', 'Immagini', 'Notizie', 'Shopping', 'Maps', 'Altro', and 'Strumenti'. The search results show 'Circa 444.000 risultati (0,26 secondi)'. The first result is from `https://pro.sony.com` with the title 'Sony Professional - Products and Solutions To Redefine Your ...'. The second result is from `https://sony.com` with the title 'Sony at NAB Show 2022'. The third result is from `http://mediago.sony.com` with the title 'Media Go - Sony Network Entertainment'. The fourth result is from `https://go.sony.com` with the title 'Resident Evil 2 - PS4 Games | PlayStation (US)'.

Utilizziamo la query **sitemap** per avere una panoramica della mappa del sito sony.com. Come possiamo vedere, è disponibile una sitemap anche in formato .xml



The screenshot shows a Google search interface. The search bar contains the query `sitemap:sony.com`, which is highlighted with a red rectangle. Below the search bar, there are tabs for 'Tutti', 'Immagini', 'Video', 'Notizie', 'Shopping', 'Altro', and 'Strumenti'. The search results show 'Circa 53.800.000 risultati (0,44 secondi)'. The first result is from `https://www.sony.com` with the title 'Sitemap - Sony Group Portal'. The second result is from `https://www.sony.com` with the title 'gwtsitemapindex.xml - Sony'.

Adesso, tramite la query **filetype**, andiamo alla ricerca di varie estensioni di file presenti all'interno del sito con URL sony.com (inurl:sony.com)

filetype:txt inurl:sony.com

Tutti Shopping Notizie Immagini Video Altro Strumenti

Circa 8 risultati (0,29 secondi)

https://www.sony.com > robots 44 · Traduci questa pagina

robots.txt - Sony

filetype:doc inurl:sony.com

Tutti Shopping Notizie Immagini Video Altro Strumenti

Circa 2 risultati (0,26 secondi)

https://www.sony.com.sg > Dec10 > quaysideform DOC

sony members

filetype:pdf inurl:sony.com

Tutti Shopping Notizie Immagini Video Altro Strumenti

Circa 78.300 risultati (0,34 secondi)

https://www.sony.com > support > res > manuals 44 PDF

Guida rapida - Sony

Prima di collegare il lettore al computer. Assicurarsi che il sistema operativo in uso sia Windows XP. (Service Pack 2 o successivi) oppure Windows Vista (...

https://www.sony.com > support > res > manuals 44 PDF

Guida rapida - Sony

Assicurarsi che il sistema operativo sia Windows XP (Service Pack 3 o versione successiva), Windows Vista*1 (Service Pack 1 o versione successiva) o Windows ...

Eseguiamo adesso un **reverse lookup** dell'hostname tramite la risorsa online Network Query Tool per risalire all'indirizzo IP del sito sony.com, e utilizziamo in seguito questa informazione per

eseguire una fast scan (switch **-F**) di **nmap online**. Lo scanning online si configura come particolarmente utile a preservare la nostra privacy.

Network Query Tool

Host Information	Host Connectivity
<input type="radio"/> Resolve/Reverse Lookup	<input type="radio"/> Check port: <input type="text" value="80"/>
<input type="radio"/> Get DNS Records	<input type="radio"/> Traceroute to host
<input type="radio"/> Whois (Web)	<input checked="" type="radio"/> Do it all
<input type="radio"/> Whois (IP owner)	
<input type="text" value="Enter host or IP"/> <input type="button" value="Do It"/>	

sony.com resolved to **52.54.18.9**

Scan report for "52.54.18.9"

Nmap Online > Scan report for "52.54.18.9"

\$ Membership level: Free member

Fast Scan (nmap -F 52.54.18.9)



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 01:19 EST
Nmap scan report for ec2-52-54-18-9.compute-1.amazonaws.com (52.54.18.9)
Host is up (0.0081s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
```

Come si può vedere, le uniche due porte risultate aperte sono la **80** (http) e la **443** (https).

2. Recon-ng

Una volta avviato il tool Recon-ng, utilizzo il modulo **whois_pocs** per raccogliere informazioni di contatto sui dipendenti di Sony:

```
SONY.COM
[*] URL: http://whois.arin.net/rest/pocs;domain=sony.com
[*] URL: http://whois.arin.net/rest/poc/AS277-ARIN
[*] Country: United States
[*] Email: ali@sony.com
[*] First_Name: Alison
[*] Last_Name: Shuman
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Jose, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/IA77-ARIN
[*] Country: United States
[*] Email: asaf_rapoport@spe.sony.com
[*] First_Name: None
[*] Last_Name: IP Admin
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: New York City, NY
[*] Title: Whois contact
[*]
[*] Country: United States
[*] Email: ip-admin@sony.com
[*] First_Name: None
[*] Last_Name: IP Admin
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: New York City, NY
[*] Title: Whois contact
[*]
SUMMARY
[*] 19 total (16 new) contacts found.
[recon-ng][default][whois_pocs] >
```

Come si può vedere, il tool ha recuperato 19 contatti totali comprensivi di nome, cognome ed indirizzo e-mail.

3. Maltego

Utilizzo il tool Maltego per raccogliere informazioni circa il sito web aziendale, dati di whois, tipi di Server in uso, dati di geolocalizzazione dell'indirizzo IP associato all'hostname, domini utilizzati, informazioni di contatto.



Source Entity	Target Entity
104.90.64.228	+1 617 274 7134
104.90.64.228	+1 617 444 0017
104.90.64.228	+1 617 444 2535
104.90.64.228	Abuse velocity: low
104.90.64.228	abuse@akamai.com
104.90.64.228	Akamai Technologies
104.90.64.228	Akamai Technologies, Inc.
104.90.64.228	Cambridge
104.90.64.228	ip-admin@akamai.com
104.90.64.228	OrgTechName
104.90.64.228	Philadelphia, Pennsylvania (United States)
104.90.64.228	Proxy
104.90.64.228	Steven Jay
104.90.64.228	US
104.90.64.228	Vpn
Benjamin Feld	benjamin.feld@sony.com
Benjamin Feld	benwfeld@gmail.com
Don Kossman	don.kossman@sony.com
Don Kossman	jacob.kossman@gmail.com

