









Eseguiamo l'information gathering sul sito del Politecnico di Milano.

Metodo 1: Google

Eseguendo il comando **intitle:index.of inurl:polimi** si trovano diverse informazioni sensibili come mail di professori e studenti, curriculum, voti degli esami universitari e i relativi nomi degli studenti, in diversi anni accademici.

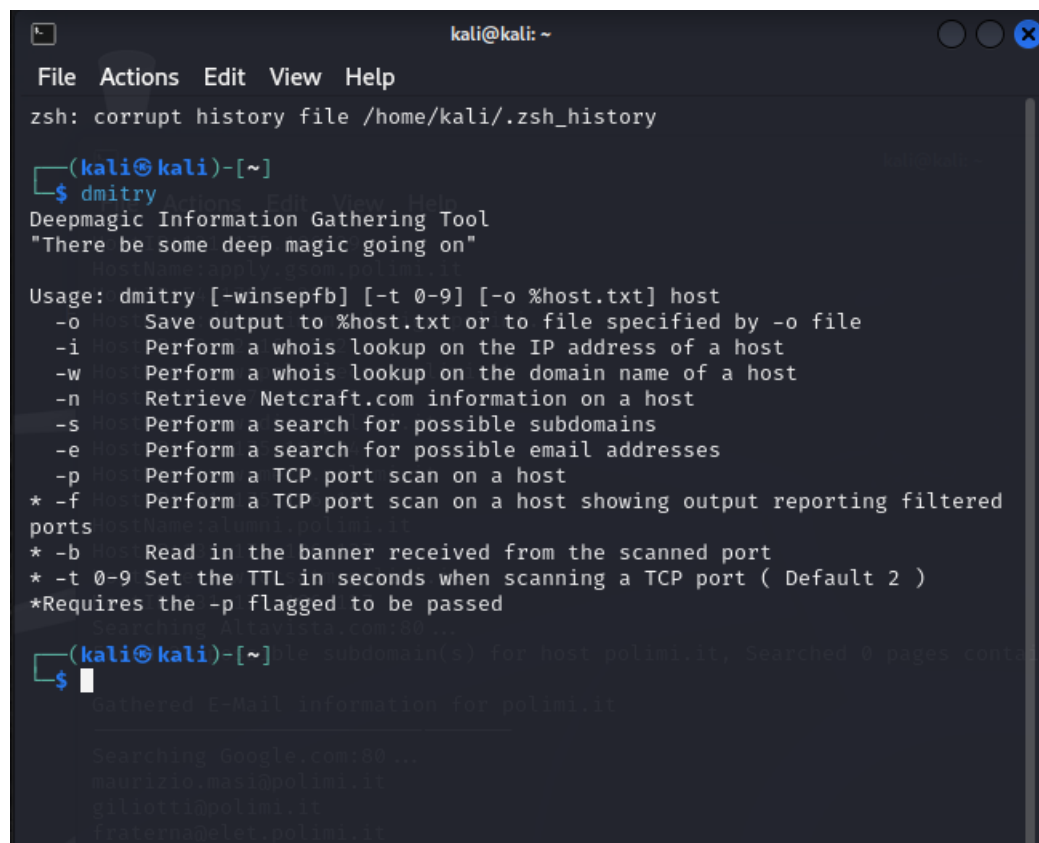
Index of /wp-content/uploads

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 2014/	2014-12-01 00:06	-	
 2015/	2015-12-01 00:04	-	
 2016/	2016-12-01 00:06	-	
 2017/	2017-12-01 00:00	-	
 2018/	2018-12-01 00:02	-	
 2019/	2019-12-01 00:08	-	
 2020/	2020-12-01 00:00	-	
 2021/	2021-12-01 00:23	-	
 2022/	2022-12-01 00:13	-	
 2023/	2023-12-01 00:13	-	
 2024/	2024-04-01 00:13	-	

Apache/2.4.7 (Ubuntu) Server at pselab.chem.polimi.it Port 443

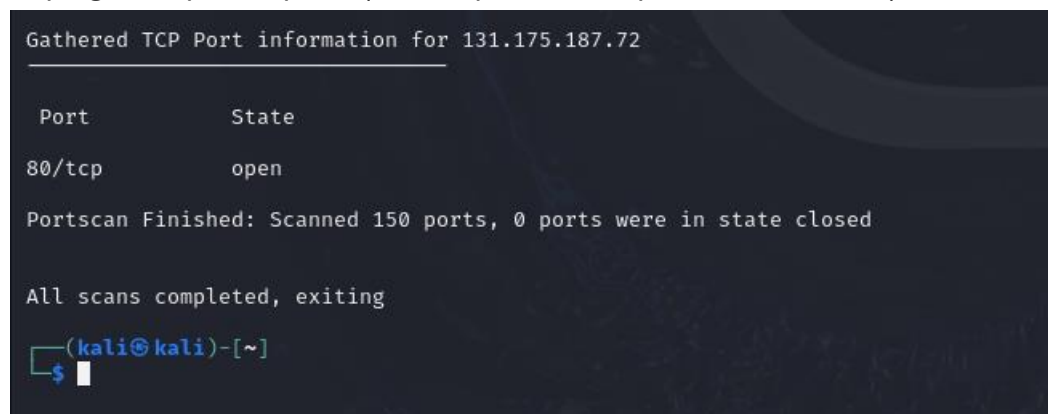
Metodo 2: Dmitry

Utilizzando il comando `dmitry polimi.it`, senza specificare nessuna flag, viene eseguita una scansione di tutte le flag proposte dall'help del comando:



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
  
(kali@kali)-[~]  
$ dmitry  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
HostName: polimi.it  
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host  
-o Host Save output to %host.txt or to file specified by -o file  
-i Host Perform a whois lookup on the IP address of a host  
-w Host Perform a whois lookup on the domain name of a host  
-n Host Retrieve Netcraft.com information on a host  
-s Host Perform a search for possible subdomains  
-e Host Perform a search for possible email addresses  
-p Host Perform a TCP port scan on a host  
* -f Host Perform a TCP port scan on a host showing output reporting filtered  
ports  
* -b Host Read in the banner received from the scanned port  
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )  
* Requires the -p flagged to be passed  
Searching Alienvault.com...  
(kali@kali)-[~]  
$  
Gathered E-Mail information for polimi.it  
  
Searching Google.com...  
maurizio.masi@polimi.it  
gillotti@polimi.it  
fratern@polimi.it
```

I risultati che ne escono fuori includono una scansione porte, i sottodomini del sito `polimi.it` e i relativi indirizzi IP, l'indirizzo dell'università, mail e numeri di telefono degli impiegati, le porte aperte (erano aperte tutte quelle scansionate).



```
Gathered TCP Port information for 131.175.187.72  
  
Port      State  
80/tcp    open  
  
Portscan Finished: Scanned 150 ports, 0 ports were in state closed  
  
All scans completed, exiting  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
HostName:www.software.polimi.it  
HostIP:131.175.186.70  
HostName:www.deib.polimi.it  
HostIP:131.175.187.208  
HostName:www.energia.polimi.it  
HostIP:131.175.186.12  
HostName:www.biblio.polimi.it  
HostIP:131.175.186.29  
HostName:apply.gsom.polimi.it  
HostIP:52.51.147.72  
HostName:dipartimentodesign.polimi.it  
HostIP:54.247.69.169  
HostName:www.polo-lecco.polimi.it  
HostIP:131.175.186.29  
HostName:www.dica.polimi.it  
HostIP:131.175.186.84  
HostName:www.mecc.polimi.it  
HostIP:131.175.186.109  
HostName:alumni.polimi.it  
HostIP:131.175.186.137  
Searching Altavista.com:80 ...  
Found 26 possible subdomain(s) for host polimi.it, Searched 0 pages containin  
g 0 results  
  
Gathered E-Mail information for polimi.it  
  
Searching Google.com:80 ...  
maurizio.masi@polimi.it  
giliotti@polimi.it  
fraterna@elet.polimi.it  
siwa@polimi.it  
barbara.pernici@polimi.it  
pierluigi.plebani@polimi.it  
emanuele.dellavalle@polimi.it  
xuefei.lu@polimi.it  
francesco.frontini@polimi.it  
alessio.frassoldati@polimi.it  
marco.derudi@polimi.it  
greta.chiaravalli@polimi.it  
francesco.casella@polimi.it  
paola.bertola@polimi.it  
arianna.seghezzi@polimi.it  
federicopaolo.zasa@polimi.it  
fraternali@polimi.it  
Searching Altavista.com:80 ...  
Found 17 E-Mail(s) for host polimi.it, Searched 0 pages containing 0 results  
  
Gathered TCP Port information for 131.175.187.72
```

```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ dmitry polimi.it  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
HostIP:131.175.187.72  
HostName:polimi.it  
  
Gathered Inet-whois information for 131.175.187.72  
-----  
inetnum:          131.175.0.0 - 131.175.255.255  
netname:          CILEA-NET  
descr:            CINECA Consorzio Interuniversitario  
org:              ORG-CCI2-RIPE  
country:          IT  
admin-c:          AN1337-RIPE  
tech-c:           GB2654-RIPE  
tech-c:           SI4194-RIPE  
status:           LEGACY  
remarks:          This prefix is statically assigned  
remarks:          To notify abuse mailto: cert@garr.it  
remarks:          GARR - Italian academic and research network  
mnt-by:           RIPE-NCC-LEGACY-MNT  
-GARR-CERT  
mnt-by:           GARR-LIR  
mnt-by:           CINECA-MNT  
mnt-routes:       CINECA-MNT  
abuse-c:          AG16225-RIPE  
created:          1970-01-01T00:00:00Z  
last-modified:    2020-08-26T10:15:50Z  
source:           RIPE  
  
organisation:     ORG-CCI2-RIPE  
org-name:         CINECA CONSORZIO INTERUNIVERSITARIO  
country:          IT  
org-type:         LIR  
address:          Via Magnanelli 6/3  
address:          40033  
address:          Casalecchio di Reno (Bologna)  
address:          ITALY  
phone:            +390516171411  
+390512130217  
admin-c:          AN1337-RIPE  
abuse-c:          TC4375-RIPE  
mnt-ref:          RIPE-NCC-HM-MNT  
mnt-ref:          INROMA-MNT  
mnt-by:           RIPE-NCC-HM-MNT  
mnt-by:           INROMA-MNT  
created:          2012-08-16T14:39:13Z  
last-modified:    2020-12-16T13:31:35Z  
source:           RIPE # Filtered  
  
person:           Angelo Neri  
address:          Via Magnanelli 6/3  
address:          Casalecchio di Reno  
address:          Bologna  
address:          Italy  
phone:            +39 051 6171411
```

Metodo 3: Recon-ng

I risultati ottenuti sono essenzialmente gli stessi, con un procedimento più macchinoso rispetto a Dmitry ma che fornisce informazioni più dettagliate.

```
kali@kali: ~  
File Actions Edit View Help  
| recon/companies-domains/censys_subdomains | 2.0 | disabled | 2021-05-10 | * | * |  
| recon/domains-hosts/binaryedge | 1.2 | installed | 2020-06-18 | | * |  
| recon/domains-hosts/censys_domain | 2.0 | disabled | 2021-05-10 | * | * |  
| recon/domains-hosts/spyse_subdomains | 1.1 | installed | 2021-08-24 | | * |  
| recon/domains-hosts/threatcrowd | 1.0 | installed | 2019-06-24 | | |  
| recon/domains-hosts/threatminer | 1.0 | installed | 2019-06-24 | | |  
+-----+  
D = Has dependencies. See info for details.  
K = Requires keys. See info for details.  
[recon-ng][default] > marketplace info recon/domains-hosts/binaryedge  
+-----+  
| path | recon/domains-hosts/binaryedge |  
| name | BinaryEdge.io DNS lookup |  
| author | Ryan Hays |  
| version | 1.2 |  
| last_updated | 2020-06-18 |  
| description | Uses the BinaryEdge API to discover subdomains. |  
| required_keys | ['binaryedge_api'] |  
| dependencies | [] |  
| files | [] |  
| status | installed |  
+-----+  
[recon-ng][default] > modules load recon/domains-hosts/binaryedge  
[recon-ng][default][binaryedge] > options set SOURCE polimi.it  
SOURCE => polimi.it  
[recon-ng][default][binaryedge] > run  
POLIMI.IT  
^C  
[recon-ng][default][binaryedge] >  
[recon-ng][default] > marketplace search who  
[*] Searching module index for 'who' ...  
+-----+  
| Path | Version | Status | Updated | D | K |  
+-----+  
| recon/companies-domains/viewdns_reverse_whois | 1.1 | installed | 2021-08-24 | | |  
| recon/companies-domains/whoxy_dns | 1.1 | installed | 2020-06-17 | | * |  
| recon/companies-multi/whois_miner | 1.1 | installed | 2019-10-15 | | |  
| recon/domains-companies/whoxy_whois | 1.1 | installed | 2020-06-24 | | * |  
| recon/domains-contacts/whois_pocs | 1.0 | installed | 2019-06-24 | | |  
| recon/netblocks-companies/whois_orgs | 1.0 | installed | 2019-06-24 | | |  
+-----+  
D = Has dependencies. See info for details.  
K = Requires keys. See info for details.
```

Metodo 4: Maltego

Risultati ottenuti essenzialmente gli stessi. L'interfaccia grafica è molto comoda per avere un quadro generale dell'information gathering e da quale "nodo" deriva un'informazione, come fossero delle cartelle e sottocartelle. (Sito/Impiegato/E-mail)

Home New Graph (1) * X Overview X Machines

Layout

Freeze

View

100%

polimi.it

File Macchina Visualizza Inserimento Dispositivi Aiuto

Maltego Community Edition 4.4.1

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

New Copy Paste Cut Clear Graph Number of Results Privacy Mode Quick Find Find in Files Entity Selection

Entity Palette

Search:

Recently Used *

Domain

An internet domain

Cryptocurrency

Bitcoin Cash Add An address in a Bit

Bitcoin Cash Blo A generic block in e

BitcoinCash Bloc The incremental bl

Bitcoin Cash Trai A transaction in a E

Bitcoin Address An address in a Bit

Bitcoin Block A generic block in e

Bitcoin Block Hei The incremental bl

Bitcoin Transacti A transaction in a E

Cryptocurrency A Cryptocurrency Add

Cryptocurrency B Cryptocurrency Blo

Cryptocurrency B The incremental bl

Cryptocurrency C Owner of a Cryptoc

20%

Website Email Address File Snapshot Company IPv4 Address MX Record Domain Snapshot NS Record DNS Name Person Document Snapshot

Output - Transform Output

Transform To Email Addresses [PGP] returned with 0 entities (from entity "polimi.it")

Transform To Email Addresses [PGP] done (from entity "polimi.it")

Running transform To Email Addresses [PGP] on 1 entities (from entity "Michele Fa

Transform To Email Addresses [PGP] returned with 0 entities (from entity "Michele

Transform To Email Addresses [PGP] done (from entity "Michele Fachin")

Running transform To Email Addresses [PGP] on 1 entities (from entity "Luca Magro

Transform To Email Addresses [PGP] returned with 5 entities (from entity "Luca Ma

Transform To Email Addresses [PGP] done (from entity "Luca Magrone")

1 of 124 entities