

INFO GATHERING  
OPEN SOURCE INTELLIGENCE  
#GOOGLE HACKING  
#DMITRY  
#RECON-NG  
#MALTEGO

FAMILIARIZZARE CON I TOOL PRINCIPALI DELLA FASE DI INFORMATION GATHERING E PRODURRE UN PICCOLO REPORT DOVE SI INDICA IL TOOL UTILIZZATO SU UN TARGET A SCELTA, LE QUERY (DOVE APPLICABILE), I MODULI UTILIZZATI (DOVE APPLICABILE), I RISULTATI OTTENUTI

MANTENGO SEMPRE LO STESSO TARGET - [www.bergamonews.it](http://www.bergamonews.it) E VEDO COME POSSO APPROFONDIRE LE RICERCHE CON QUALCHE QUERY PIÙ COMPLESSA E GRAZIE ALL'UTILIZZO DEI TOOL APPRESI DURANTE LA LEZIONE

#GOOGLE DORKING - QUERY "SITE" E "FILETYPE":

Kali burp [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

site:bergamonews.it at D x filetype:pdf site:bergamo x CURRICULUM VITAE - Ge x BergamoNews - Bergam x site:bergamone

https://duckduckgo.com/?q=filetype%3Apdf+site%3Abergamonews.it&t=h\_&ia=web

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

filetype:pdf site:bergamonews.it

Q All Images Videos News Maps Settings

https://www.bergamonews.it/wp-content/uploads/2023/10/PROGETTO-ANNIVERSARI-20...

PDF Promo BLACK FRIDAY

CHI SIAMO BergamoNews, nato a giugno 2008, è il primo giornale online della provincia di Bergamo (con una media di oltre 100.000 visitatori quotidiani, 1.600.000 visitatori unici al mese) e li ...

https://www.bergamonews.it/wp-content/uploads/2023/10/Promo-BLACK-FRIDAY-2023-p...

PDF Promo BLACK FRIDAY - bergamonews.it

Per la vostra comunicazione combina banner e social, da utilizzare dal 1 al 30 Novembre 2023 PREZZI scontati

https://www.bergamonews.it/presentazione/Comunicazione\_2024.pdf

PDF Ufficio Marketing

7 days ago · Comunicazione 2024, oltre 2.560.000, gli utenti unici medi mensili nel 2023, più di 5.300.000, di pagine viste al mese nel 2023, almeno 30.000, le impression al giorno garantite per i banner ...

https://www.bergamonews.it/wp-content/uploads/2016/05/COMMISSIONEAMMILITATO

↓

Kali burp [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

site:bergamonews.it at D x aprite-le-scuole.pdf x BergamoNews - Bergam x site:bergamonews.it - site: x +

https://www.ber-aprite-le-scuole.pdf ent/uploads/2021/01/aprite-le-scuole.pdf

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

3 of 18 Automatic Zoom

Recapito: [scuoleapertebg@gmail.com](mailto:scuoleapertebg@gmail.com)

Bergamo, 19 gennaio 2021

1	CENSURA	genitore I.C. Camozzi
2		docente secondaria di primo grado
3		insegnante scuola infanzia
4		genitore I.C. Mazzi
5		nonna I.C. Mazzi
6		genitore I.C. Lanfranchi, Sorisole
7		genitore I.C. Camozzi
8		pediatra
9		genitore Istituto Mazzi
10		insegnante
11		genitore scuola secondaria primo grado "Alessandro Manzoni" Alme'
12		genitore scuola secondaria primo grado I.C. Camozzi
13		genitore Secco Suardo e Sarpi
14		pensionata
15		educatrice asilo nido
16		insegnante scuola infanzia.



#RECON-NG:

È UN OSINT TOOL MODULARE DI KALI LINUX SCRITTO IN PYTHON DA TIM TONES. È MOLTO UTILE PER RACCOGLIERE INFORMAZIONI SUL TARGET PER TROVARNE LE VULNERABILITÀ DA SFRUTTARE IN SEGUITO. HA MODULI E PLUG-IN INDIPENDENTI, CHE SI POSSONO ESPLORARE COL COMANDO **show modules** E POI **marketplace search**, ALCUNI DI ESSI SONO A PAGAMENTO E NECESSITANO DI UNA API KEY, MENTRE ALTRI SONO FREE TO USE. I MODULI SONO DI 5 TIPOLOGIE: RECON/REPORTING/DISCOVERY/IMPORT/EXPLOIT.

I MODULI TESTATI DI SEGUITO SUL TARGET SONO:

- INTERESTING\_FILES
- HACKERTARGET
- VIEWDNS\_REVERSE\_WHOIS

```
[recon-ng][default][interesting_files] > options set SOURCE bergamoneWS.it
SOURCE => bergamoneWS.it
[recon-ng][default][interesting_files] > info

    Name: Interesting File Finder
    Author: Tim Tones (@lanmaster53), thraprt (thraprt@gmail.com), Jay Turla (@shipcod3), and Mark Jeffery
    Version: 1.2

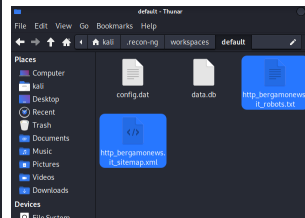
Description:
  Checks hosts for interesting files in predictable locations.

Options:
  Name      Current Value      Required  Description
  ---      -
  CSV_FILE  /home/kali/.recon-ng/data/interesting_files_verify.csv  yes       custom filename map
  DOWNLOAD  True                        yes       download discovered files
  PORT      80                         yes       request port
  PROTOCOL  http                       yes       request protocol
  SOURCE     bergamoneWS.it           yes       source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT host FROM hosts WHERE host IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

Comments:
  * Files: robots.txt, sitemap.xml, sitemap.xml.gz, crossdomain.xml, phpinfo.php, test.php, elmah.axd,
  server-status, jmx-console/, admin-console/, web-console/
  * CSV Default: /home/kali/.recon-ng/data/interesting_files_verify.csv
  * Google Dorks:
    - inurl:robots.txt ext:txt
    - inurl:elmah.axd ext:axd intitle:"Error log for"
    - inurl:server-status "Apache Status"
```

```
[recon-ng][default][interesting_files] > run
[*] http://bergamoneWS.it:80/robots.txt => 200. 'robots.txt' found!
[*] http://bergamoneWS.it:80/sitemap.xml => 200. 'sitemap.xml' found!
[*] http://bergamoneWS.it:80/sitemap.xml.gz => 404
[*] http://bergamoneWS.it:80/crossdomain.xml => 404
[*] http://bergamoneWS.it:80/phpinfo.php => 404
[*] http://bergamoneWS.it:80/test.php => 404
[*] http://bergamoneWS.it:80/elmah.axd => 404
[*] http://bergamoneWS.it:80/server-status => 404
[*] http://bergamoneWS.it:80/jmx-console/ => 404
[*] http://bergamoneWS.it:80/admin-console/ => 404
[*] http://bergamoneWS.it:80/web-console/ => 404
[*] 2 interesting files found.
[*] Files downloaded to '/home/kali/.recon-ng/workspaces/default/'
[recon-ng][default][interesting_files] > █
```



```
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set SOURCE bergamoneWS.it
SOURCE => bergamoneWS.it
[recon-ng][default][hackertarget] > run
```

```
BERGAMONEWS.IT

[*] Country: None
[*] Host: bergamoneWS.it
[*] Ip_Address: 5.135.123.73
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: elezioni2014.bergamoneWS.it
[*] Ip_Address: 212.97.33.201
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: sales.bergamoneWS.it
[*] Ip_Address: 45.77.55.108
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

**4 HOST+IP ADDRESS TROVATI:**

- **bergamoneWS.it / 5.135.123.73**
- **elezioni2014.bergamoneWS.it / 212.97.33.201**
- **live.bergamoneWS.it / 51.178.206.226**
- **sales.bergamoneWS.it / 45.77.55.108**

```
[recon-ng][Epicode_exercises][hackertarget] > show hosts

+-----+-----+-----+-----+-----+-----+-----+
| rowid | host                | ip_address | region | country | latitude | longitude | notes | module |
+-----+-----+-----+-----+-----+-----+-----+
| 1      | bergamoneWS.it      | 5.135.123.73 |        |          |           |           |       |         |
| 2      | elezioni2014.bergamoneWS.it | 212.97.33.201 |        |          |           |           |       |         |
| 3      | live.bergamoneWS.it | 51.178.206.226 |        |          |           |           |       |         |
| 4      | sales.bergamoneWS.it | 45.77.55.108 |        |          |           |           |       |         |
+-----+-----+-----+-----+-----+-----+-----+

[*] 4 rows returned
```

```
SUMMARY

[*] 4 total (4 new) hosts found.
[recon-ng][default][hackertarget] > █
```

```
[recon-ng][default][viewdns_reverse_whois] > options set SOURCE bergamoneWS.it
SOURCE => bergamoneWS.it
[recon-ng][default][viewdns_reverse_whois] > info

    Name: Viewdns Reverse Whois Domain Harvester
    Author: Gaetan Ferry (@_mabote_) from @synacktiv
    Version: 1.1

Description:
  Harvests domain names belonging to a company by using the viewdns.info free reverse whois tool.

Options:
  Name      Current Value      Required  Description
  ---      -
  SOURCE     bergamoneWS.it           yes       source of input (see 'info' for details)

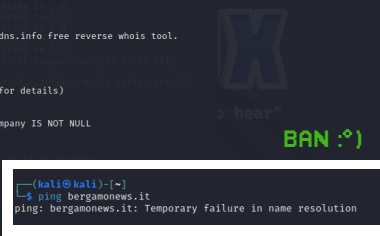
Source Options:
  default      SELECT DISTINCT company FROM companies WHERE company IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

Comments:
  * Does not support company names < 6 characters
```

```
[recon-ng][default][viewdns_reverse_whois] > run

BERGAMONEWS.IT

[!] HTTPSConnectionPool(host='viewdns.info', port=443): Max retries exceeded with url: /reversewhois/?q=bergamoneWS.it (Caused by New
ConnectionError(<quilllib.connection.HTTPSConnection object at 0x7fed4b3a4790>: Failed to establish a new connection: [Errno -3] Temp
rary failure in name resolution'))
[!] Something broken? See https://github.com/lanmaster53/recon-ng/wiki/Troubleshootingissue-reporting.
[recon-ng][default][viewdns_reverse_whois] > █
```



## #MALTEGO:

È UN OSINT TOOL GRAFICO SVILUPPATO DALLA SOCIETÀ "PATERVA" CHE PERMETTE DI RACCOGLIERE E RAGGRUPPARE DATI ACCESSIBILI PUBBLICAMENTE VISUALIZZANDOLI IN FORMATO GRAFICO. I DATI VENGONO RACCOLTI TRAMITE SITI WEB, SOCIAL NETWORK, BLOG, DATI PUBBLICI COME CONFERENZE STAMPA, RAPPORTI DEI GOVERNI E DATI DEMOGRAFICI, OSSERVAZIONI DIRETTE (DATI GEOLOCALIZZATI, CONVERSAZIONI RADIO, FOTO SATELLITARI...) E FONTI COME PROFESSIONISTI ED ACCADEMICI E LE LORO PUBBLICAZIONI.

PREVIA REGISTRAZIONE, PROVO AD UTILIZZARE SUL TARGET SCELTO L'OPZIONE SUGGERITA DALLE SLIDE DEL CORSO:

The screenshot displays the Maltego Community Edition 4.4.1 interface. The main window shows a graph with a central entity 'BergamoneWS' at the top, which is connected to several other entities below it. These entities include 'Giacomo Fornoni', 'Giovanni Fianza', 'Nicola Colombi', 'Elena Scarpellini', 'Alessandro Galeandro', 'Faisal Bangal', 'Melissa Saffa', 'Reserve team', 'Sofia Goggia', 'Boat of Saint Peter', 'Roberto Micheletti', and 'Alfonsofan'. Each entity is represented by a circular icon with a unique pattern. The interface includes a left sidebar with 'Entity Palette' and 'Run View' sections. The 'Run View' section shows a list of transforms applied to the data. The bottom of the interface features a 'Transform Output' section with a list of results. A cookie notice is visible at the very bottom of the browser window.

File Macchina Visualizza Inserimento Dispositivi Aiuto

Kali burp [In esecuzione] - Oracle VM VirtualBox

site:bergamoneWS... phonebook:site:ber... Recon-NG Tutorial... BergamoNews - Ber... site:bergamoneWS... eco di bergamo da Di... +

Maltego Community Edition 4.4.1

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Number of Results: 100 (0 50 100 150)

Privacy Mode: Normal

Quick Find Find in Files Entity Selection

Entity Palette

Search: phrase

Recently Used

Phrase Any text or part thereof

Personal

Phrase Any text or part thereof

Run View

Transforms

Machines

Company St...

This machine...

New Graph (1) \*

BergamoneWS

Giacomo Fornoni Giovanni Fianza Nicola Colombi Elena Scarpellini

Alessandro Galeandro Faisal Bangal Melissa Saffa Reserve team

Sofia Goggia Boat of Saint Peter Roberto Micheletti Alfonsofan

Overview

Detail View

Phrase maltego Phrase BergamoNews

Relationships

Property View Hub Transf...

Output - Transform Output

No results found (from entity "BergamoneWS")

Transform to URLs (within Properties) returned with 0 entities (from entity "BergamoneWS")

No results found (from entity "BergamoneWS")

Transform to DNSNames (within Properties) returned with 0 entities (from entity "BergamoneWS")

No results found (from entity "BergamoneWS")

Transform to URLs (within Properties) done (from entity "BergamoneWS")

Transform to Email Addresses (using Search Engine) done (from entity "BergamoneWS")

1 of 1 entity

We use cookies to ensure that we give you the best experience on our site. If you continue to use this site we assume that you accept this. [Ok](#)

## #CONCLUSIONI:

IN DEFINITIVA, I RISULTATI OTTENUTI NON SONO MOLTISSIMI AD ORA, MA ABBIAMO 4 IP ASSOCIABILI A 4 HOST DA TESTARE EVENTUALMENTE IN SEGUITO PER SCOVARE POTENZIALI VULNERABILITÀ (AD ESEMPIO L'HOST "ELEZIONI2014" FA PENSARE A QUALCOSA DI ALQUANTO VECCHIO E DIMENTICATO), ABBIAMO DELLE E-MAIL, UN DOCUMENTO PDF CON L'ELENCO DI TANTE PERSONE PER NOME COGNOME E RUOLO ALL'INTERNO DI UN ISTITUTO SCOLASTICO PASSIBILE DI EVENTUALE PHISHING, E DEI FILE DI INTERESSE DA ANALIZZARE.