



DMITRY

(Deepmagic Information Gathering Tool)

FATMA KAYGISIZ

RUTGERS UNIVERSITY/CYBERSECURITY

BOOTCON PRESENTATION



WHAT IS DMITRY ?

- A CLI-based tool for passive information gathering.
- Collects essential details about a target domain.
- Useful for reconnaissance in penetration testing and vulnerability assessment.

WHY USE DMITRY ?

- Open-source and lightweight.
- Easy to integrate into cybersecurity workflows.
- Efficient for reconnaissance while adhering to legal and ethical guidelines.

KEY FEATURES OF DMITRY

- **SUBDOMAIN ENUMERATION** : Identifies subdomains of a target.
- **WHOIS LOOKUP** : Retrieves domain ownership details.
- **PORT SCANNING** : Checks open ports on a domain (if allowed).
- **EMAIL HARVESTING** : Extracts email addresses from a domain.
- **BANNER GRABBING** : Collects service information from open ports.





WHY DID WE CHOOSE DMITRY ?

- **Simple and Efficient to Us**

1- DMitry has an easy-to-use command-line interface, making it accessible even for beginners in cybersecurity.

2- Its clear syntax and modular flags allow you to target specific types of data (e.g., subdomains, email addresses, or WHOIS information).

- **Ethical and Legal Use Cases**
- **Versatility in Data Collection**
- **Practical for Demonstration**



HOW DID WE FIND “DMITRY” ?


I found the **DMitry tool** by exploring the comprehensive **Kali Linux Tools list**, which is available on the official Kali Linux website: <https://www.kali.org/tools/dmitry/>.

INSTALLING DMITRY (KALI LINUX)

- `sudo apt update`
- `sudo apt install dmitry`
- `dmitry -h`
- `git clone https://github.com/jaygreig86/DMitry.git`
- `cd DMitry`
- `make`
- `./dmitry -h`

```
(kali㉿kali)-[~/dmitry]
$ dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting filtered ports
* -b      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
```



GOAL : Focusing on using Dmitry to gather information about “**twitter.com**” and “**rumble.com**”.

The basic syntax for using dmitry is : **dmitry [options] target**

- w** : Perform whois lookup on domain name
- i** : Perform whois lookup on IP address
- n** : Retrieve Netcraft information
- s** : Search for subdomains
- e** : Search for email addresses
- p** : Perform TCP port scan
- o** : Save output to a file



A BRIEF SUMMARY

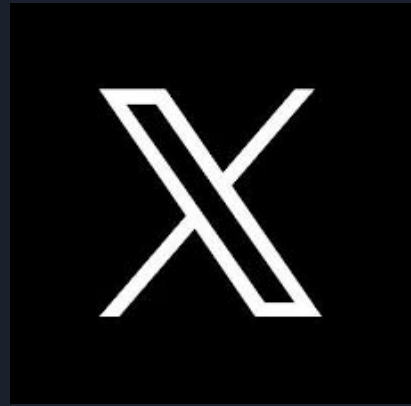
I successfully installed Kali Linux on my Mac to enhance my cybersecurity learning environment. As part of my setup, I installed the **Dmitry tool** (Deepmagic Information Gathering Tool), which is a versatile CLI-based tool used for reconnaissance. Dmitry allows users to gather various types of information about a target, such as subdomains, email addresses, open ports, and WHOIS data, making it ideal for network analysis and reconnaissance tasks.

Using Dmitry, I conducted information gathering on **twitter.com** and **rumble.com**, exploring their publicly accessible data. Throughout the process, I utilized multiple command-line options and techniques to extract and analyze the information effectively, enhancing my hands-on experience with Linux-based tools and commands.



DEMONSTRATION





“TWITTER.COM”



(kali㉿kali)-[~/dmitry]

\$ dmitry -w twitter.com

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:104.244.42.193

HostName:twitter.com

Gathered Inic-whois information for twitter.com

Domain Name: TWITTER.COM

Registry Domain ID: 18195971_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.corporatedomains.com

Registrar URL: <http://cscdbs.com>

Updated Date: 2024-01-17T06:10:05Z

Creation Date: 2000-01-21T16:28:17Z

Registry Expiry Date: 2025-01-21T16:28:17Z

Registrar: CSC Corporate Domains, Inc.

Registrar IANA ID: 299

Registrar Abuse Contact Email: domainabuse@cscglobal.com

Registrar Abuse Contact Phone: 8887802723

nsferProhibited <https://icann.org/epp#clientTransferProhibited>

Domain Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>

Domain Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>

Domain Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>

Name Server: A.R06.TWTRDNS.NET

Name Server: A.U06.TWTRDNS.NET

Name Server: B.R06.TWTRDNS.NET

Name Server: B.U06.TWTRDNS.NET

ET

Name Server: C.U06.TWTRDNS.NET

Name Server: D.R06.TWTRDNS.NET

Name Server: D.U06.TWTRDNS.NET

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>

>>> Last update of whois database: 2024-11-16T01:08:27Z <<<

```
└─$ dmitry -i twitter.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"
```

```
HostIP:104.244.42.193
HostName:twitter.com
```

Gathered Inet-whois information for 104.244.42.193

```
inetnum:      104.244.12.0 - 104.245.87.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
ce
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
ca and the Carribean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
```

```
mnt-by:      RIPE-NCC-HM-MNT
created:      2024-01-04T15:01:32Z
last-modified: 2024-01-04T15:01:32Z
source:       RIPE
```

```
role:         Internet Assigned Numbers Authority
http://www.iana.org.
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
nic-hdl:      IANA1-RIPE
remarks:      For more information on IANA services
remarks:      go to IANA web site at http://www.iana.org.
mnt-by:       RIPE-NCC-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:       RIPE # Filtered
```

% This query was served by the RIPE Database Query Service version 1.114 (SHETLAND)

All scans completed, exiting



```
(kali㉿kali)-[~/dmitry]
```

```
$ dmitry -s twitter.com
```

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:104.244.42.193

HostName:twitter.com

Gathered Subdomain information for twitter.com

Searching Google.com:80 ...

HostName:www.twitter.com

HostIP:104.244.42.1

HostName:mobile.twitter.com

HostIP:104.244.42.70

HostName:cards-dev.twitter.com

HostIP:104.244.42.195

HostName:pro.twitter.com

HostIP:104.244.42.132

HostName:developer.twitter.com

HostIP:104.244.42.67


HostName:publish.twitter.com

HostIP:104.244.42.67

Searching Altavista.com:80 ...

Found 6 possible subdomain(s) for host twitter.com, Searched 0 pages containing 0 results

All scans completed, exiting



```
(kali®kali)-[~/dmitry]
```

```
$ dmitry -n twitter.com
```

```
Deepmagic Information Gathering Tool
```

```
"There be some deep magic going on"
```

```
HostIP:104.244.42.1
```


```
HostName:twitter.com
```

```
Gathered Netcraft information for twitter.com
```

```
Retrieving Netcraft.com information for twitter.com
```

```
Netcraft.com Information gathered
```

```
All scans completed, exiting
```



```
(kali@kali)-[~/dmitry]
```

```
$ dmitry -e twitter.com
```

```
Deepmagic Information Gathering Tool
```

```
"There be some deep magic going on"
```

```
HostIP:104.244.42.1
```

```
HostName:twitter.com
```

```
Gathered E-Mail information for twitter.com
```

```
Searching Google.com:80 ...
```

```
tprintezis@twitter.com
```

```
Searching Altavista.com:80 ...
```

```
Found 1 E-Mail(s) for host twitter.com, Searched 0 pages containing 0 results
```

```
All scans completed, exiting
```





SUMMARY

The domain “[twitter.com](#)” is registered with [CSC Corporate Domains](#) and secured with restrictions to prevent unauthorized changes. The IP address [104.244.42.129](#) belongs to a global address range managed by [IANA](#), likely hosted on cloud services like AWS or Google Cloud. Six subdomains were found, including [mobile.twitter.com](#), [developer.twitter.com](#), and [publish.twitter.com](#), supporting various platform features. The email tprintezis@twitter.com was also discovered, likely an internal contact. Overall, twitter.com has secure domain management, a global infrastructure, and multiple subdomains for its service.



“RUMBLE.COM”





```
(kali@kali)-[~/dmitry]
```

```
$ dmitry -w rumble.com
```

```
Deepmagic Information Gathering Tool
```

```
"There be some deep magic going on"
```

```
HostIP:205.220.231.24
```

```
HostName:rumble.com
```

```
Gathered Inic-whois information for rumble.com
```

```
Domain Name: RUMBLE.COM
```

```
Registry Domain ID: 2670227_DOMAIN_COM-VRSN
```

```
Registrar WHOIS Server: whois.tucows.com
```

```
Registrar URL: http://www.tucows.com
```

```
Updated Date: 2021-05-11T22:57:45Z
```

```
Creation Date: 1998-12-07T05:00:00Z
```

```
Registry Expiry Date: 2030-12-06T05:00:00Z
```

```
Registrar: Tucows Domains Inc.
```

```
Registrar IANA ID: 69
```

```
Registrar Abuse Contact Email: domainabuse@tucows.com
```

```
Registrar Abuse Contact Phone: +1.4165350123
```

```
https://icann.org/epp#clientTransferProhibited
```

```
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
```

```
Name Server: NS-1404.AWSDNS-47.ORG
```

```
Name Server: NS-1594.AWSDNS-07.CO.UK
```

```
Name Server: NS-479.AWSDNS-59.COM
```

```
Name Server: NS-640.AWSDNS-16.NET
```

```
DNSSEC: unsigned
```

```
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

```
>>> Last update of whois database: 2024-11-16T02:23:45Z <<<
```

(kali@kali)-[~/dmitry]

\$ dmitry -i rumble.com

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:205.220.231.24

HostName:rumble.com

Gathered Inet-whois information for 205.220.231.24

```
inetnum:      205.220.218.0 - 205.238.63.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
ration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
ic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
```

```
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED

created:      2021-11-15T13:31:02Z
last-modified: 2021-11-15T13:31:02Z
source:       RIPE
```

```
role:         Internet Assigned Numbers Authority
address:       see http://www.iana.org.
admin-c:       IANA1-RIPE
tech-c:        IANA1-RIPE
nic-hdl:       IANA1-RIPE
remarks:       For more information on IANA services
remarks:       go to IANA web site at http://www.iana.org.
mnt-by:        RIPE-NCC-MNT
created:       1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
RIPE # Filtered
```

% This query was served by the RIPE Database Query Service version 1.114 (ABERDEEN)

All scans completed, exiting



```
(kali@kali)-[~/dmitry]
```

```
$ dmitry -n rumble.com
```

```
Deepmagic Information Gathering Tool
```

```
"There be some deep magic going on"
```

```
HostIP:205.220.231.24
```


```
HostName:rumble.com
```

```
Gathered Netcraft information for rumble.com
```

```
Retrieving Netcraft.com information for rumble.com
```

```
Netcraft.com Information gathered
```

```
All scans completed, exiting
```



```
(kali㉿kali)-[~/dmitry]
$ dmitry -s rumble.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"
```

```
HostIP:205.220.231.24
HostName:rumble.com
```

```
Gathered Subdomain information for rumble.com
```

```
Searching Google.com:80 ...
HostName:corp.rumble.com
HostIP:172.98.56.149
HostName:studio.rumble.com
HostIP:76.76.21.22
HostName:investors.rumble.com
HostIP:172.98.58.31
HostName:rb.rumble.com
HostIP:172.98.59.28
HostName:www.rumble.com
HostIP:205.220.231.24
Searching Altavista.com:80 ...
Found 5 possible subdomain(s) for host rumble.com, Searched 0 pages containing 0 results
```

```
All scans completed, exiting
```



```
(kali㉿kali)-[~/dmitry]
```

```
$ dmitry -e rumble.com
```

```
Deepmagic Information Gathering Tool
```

```
"There be some deep magic going on"
```

```
HostIP:205.220.231.24
```

```
HostName:rumble.com
```

```
Gathered E-Mail information for rumble.com
```

```
Searching Google.com:80 ...
```

```
swilliamson@rumble.com
```

```
Searching Altavista.com:80 ...
```

```
Found 1 E-Mail(s) for host rumble.com, Searched 0 pages containing 0 results
```

```
All scans completed, exiting
```



SUMMARY

The domain rumble.com has been active since 1998 and is registered with [Tucows](#), set to expire in 2030. It's hosted on AWS has a [clientUpdateProhibited](#) status, preventing unauthorized changes. The associated IP address, [205.220.231.24](#), belongs to a globally allocated IP block. Several subdomains were found, including [corp.rumble.com](#), [studio.rumble.com](#), and [investors.rumble.com](#), each with unique IPs. No detailed insights were found from Netcraft scans. The email swilliamson@rumble.com is linked to the domain, likely belonging to a Rumble contact.