Python Whois Tutorial

Contents

Time required: 60 minutes

Whois

WHOIS is a TCP-based query and response protocol that is commonly used to provide information services to Internet users. It returns information about the registered Domain Names, an IP address block, Name Servers and a much wider range of information services.

WHOIS allows you to look up the name and contact information of whoever operates any website's generic domain name. As part of the registration process, you must provide your registrar with accurate and reliable contact details and promptly correct and update these details as necessary.

Using whois is part of the fingerprinting process. The more you know about your target, the easier it is to hack.

Kali Linux

Kali Linux has a built in **whois** command.

1. Start a terminal session.

2. The syntax is: whois <domainname>

3. Example **whois wncc.net**

4. Attach a screenshot to the assignment of the top part of the information.

Python Whois

https://pypi.org/project/python-whois/

Python whois is a simple importable Python module which will produce parsed WHOIS data for a given domain. It can extract data for all the popular TLDs (com, org, net, …)

Tutorial 1: Whois Hardcoded

A good way to develop a program is to build it a little at a time. Hard coding means we type in a specific value to test the program.

We will use Geany in Kali Linux to create this Python program.

In Kali Linux, create a Python program named **whois_cli_1.py**

```python
"""
    Name: whois_cli_1.py
    Author:
    Created:
    Purpose: Lookup whois info about web site
"""

# https://pypi.org/project/python-whois/
# pip install python-whois
import whois

# Get whois attributes about hard coded domain
domain_info = whois.whois("www.billthecomputerguy.com")
# Print dictionary of whois attributes
print(domain_info)
```

Example run:

```
{
  "domain_name": [
    "BILLTHECOMPUTERGUY.COM",
    "billthecomputerguy.com"
  ],
  "registrar": "GoDaddy.com, LLC",
  "whois_server": "whois.godaddy.com",
  "referral_url": null,
  "updated_date": [
    "2022-09-01 01:02:05",
    "2022-08-31 19:58:48"
  ],
  "creation_date": [
    "1998-08-04 04:00:00",
    "1998-08-03 23:00:00"
  ],
  "expiration_date": [
    "2023-08-03 04:00:00",
    "2023-08-02 23:00:00"
  ],
  "name_servers": [
    "NS17.DOMAINCONTROL.COM",
    "NS18.DOMAINCONTROL.COM"
  ],
```

Pick a different domain for your example run.

Tutorial 2: Whois Input

We know the program works. Let's add input and better formatting.

```python
1  """
2      Name: whois_cli_2.py
3      Author:
4      Created:
5      Purpose: Lookup whois info about web site
6      This program can also be used as a module in another program
7  """
8
9  # https://pypi.org/project/python-whois/
10 # pip install python-whois
11 import whois
12
13
14 def main():
15     print(" +-----------------------------------------+")
16     print(" |   -----   Domain Whois Information   -----   |")
17     print(" +-----------------------------------------+")
18     while True:
19         domain_name = input(" Enter a domain name: ")
20         get_who_is(domain_name)
21         menu = input("Enter another domain? (y) ")
22         if menu.lower() != "y":
23             break
24
25
26 #---------------- GET WHO IS ----------------------------------#
27 def get_who_is(domain_name):
28     """
29         Get and display whois info from domain_name parameter
30     """
31     # Get domain whois information
32     d = whois.whois(domain_name)
33
34     print(f"\n -----   {domain_name} Whois Information   -----\n")
35     print(f"    Expiration Date: {d.expiration_date}")
36     print(f"       Creation Date: {d.creation_date}")
37     print(f"        Updated Date: {d.updated_date}")
38     print(f"              Email: {d.emails}")
39     print(f"          Nameserver: {d.name_servers}")
40     print(f"        Whois Server: {d.whois_server}")
41     print(f"    Registrant Name: {d.name}")
42     print(f"      Registrant Org: {d.org}")
43     print(f"   Registrant State: {d.state}")
44     print(f"  Registrant Street: {d.address}")
45     print(f"      Registrant Zip: {d.city}")
46     print(f" Registrant Country: {d.country}")
47
48
49 # If a standalone program, call the main function
50 # Else, use as a module
51 if __name__ == "__main__":
52     main()
```

Example run:

```
+---------------------------------------------+
|    -----    Domain Whois Information    -----    |
+---------------------------------------------+
Enter a domain name: godaddy.com

-----    godaddy.com Whois Information    -----

    Expiration Date: [datetime.datetime(2023, 11, 1, 11, 59, 59),
(2023, 11, 1, 6, 59, 59)]
      Creation Date: [datetime.datetime(1999, 3, 2, 5, 0), dateti
3, 2, 0, 0)]
       Updated Date: [datetime.datetime(2021, 9, 30, 19, 45, 51),
(2021, 9, 30, 14, 22, 7)]
              Email: abuse@godaddy.com
         Nameserver: ['A1-245.AKAM.NET', 'A11-64.AKAM.NET', 'A20-
-66.AKAM.NET', 'A8-67.AKAM.NET', 'A9-67.AKAM.NET', 'CNS1.GODADDY.
DY.COM']
       Whois Server: whois.godaddy.com
    Registrant Name: Registration Private
     Registrant Org: Domains By Proxy, LLC
   Registrant State: Arizona
  Registrant Street: ['DomainsByProxy.com', '2155 E Warner Rd']
      Registrant Zip: Tempe
 Registrant Country: US
```

Tutorial 3: Rich Formatting

We are going to add some colorful formatting to our program.

In Kali Linux, save your current Python program as **whois_cli_rich.py**

```python
"""
    Name: whois_cli_rich.py
    Author:
    Created:
    Purpose: Lookup whois info about web site
    This program can also be used as a module in another program
"""

# https://pypi.org/project/python-whois/
# pip install python-whois
import whois

# pip install rich
# Import Console for console printing
from rich.console import Console
# Import Panel for title displays
from rich.panel import Panel

# Initialize rich.console
console = Console()


def main():
    console.print(
        Panel.fit(
            "\n           Domain Whois Information           \n",
            style="bold blue"
        )
    )
    while True:
        domain_name = input(" Enter a domain name: ")
        get_who_is(domain_name)
        menu = input("Enter another domain? (y) ")
        if menu.lower() != "y":
            break
```

```python
#---------------- GET WHO IS ------------------------------------#
def get_who_is(domain_name):
    """
        Get and display whois info from domain_name parameter
    """
    # Get domain whois information
    d = whois.whois(domain_name)
    print()
    console.print(
        Panel.fit(f"  ---   {domain_name} Whois Information   --- "),
        style="bold blue"
    )
    print(f"  Expiration Date: {d.expiration_date}")
    print(f"    Creation Date: {d.creation_date}")
    print(f"     Updated Date: {d.updated_date}")
    console.print(f"            Email: [yellow bold]{d.emails}")
    console.print(f"       Nameserver: [yellow bold]{d.name_servers}")
    console.print(f"     Whois Server: [yellow bold]{d.whois_server}")
    console.print(f"  Registrant Name: [yellow bold]{d.name}")
    console.print(f"   Registrant Org: [yellow bold]{d.org}")
    console.print(f" Registrant State: [yellow bold]{d.state}")
    console.print(f"Registrant Street: [yellow bold]{d.address}")
    console.print(f"   Registrant Zip: [yellow bold]{d.city}")
    console.print(f" Registrant Country: [yellow bold]{d.country}")


# If a standalone program, call the main function
# Else, use as a module
if __name__ == "__main__":
    main()
```

Example run:

```
          Domain Whois Information

Enter a domain name: lab.wncc.net

   ---      lab.wncc.net Whois Information     ---

    Expiration Date: 2025-11-18 05:00:00
      Creation Date: 1998-11-19 05:00:00
       Updated Date: [datetime.datetime(2020, 9, 19, 6, 11, 27), datetime.datetime(2020, 9, 19, 6, 11, 56)]
              Email: ['abuse@web.com', 'wnccit@wncc.edu', 'domains@wncc.edu', 'domain.operations@web.com']
         Nameserver: ['NS0.WNCC.EDU', 'NS1.WNCC.EDU', 'NS2.WNCC.EDU', 'NS3.WNCC.EDU', 'NS4.WNCC.EDU']
       Whois Server: whois.networksolutions.com
    Registrant Name: Western Nebraska Community College
     Registrant Org: Western Nebraska Community College
   Registrant State: NE
  Registrant Street: 1601 E 27TH ST
     Registrant Zip: SCOTTSBLUFF
 Registrant Country: US
Enter another domain? (y) _
```

Assignment Submission

1. Attach all program files.

2. Attach a screenshot of each successful program run.

3. Submit the assignment in Blackboard.