Lab

3

Perform Footprinting Through Social Networking Sites

Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker, during information gathering, you need to gather personal information about employees working in critical positions in the target organization; for example, the Chief Information Security Officer, Security Architect, or Network Administrator. By footprinting through social networking sites, you can extract personal information such as name, position, organization name, current location, and educational qualifications. Further, you can find professional information such as company or business, current location, phone number, email ID, photos, videos, etc. The information gathered can be useful to perform social engineering and other types of advanced attacks.

Lab Objectives

- Gather employees' information from LinkedIn using theHarvester
- Gather personal information from various social networking sites using Sherlock
- Gather information using Followerwonk

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites to provide basic information about themselves and to help make and maintain connections with others; the profile generally contains information such as name, contact information (cellphone number, email address), friends' information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Thus, social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc.

Lab Tasks

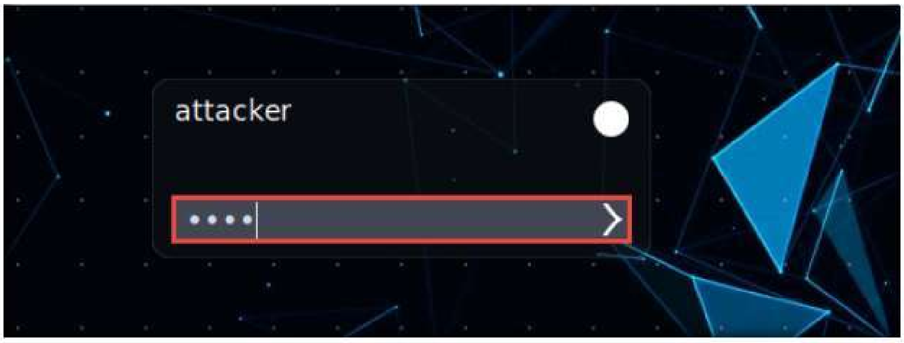
TASK 1

Gather Employees' Information from LinkedIn using theHarvester

LinkedIn is a social networking website for industry professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, etc.

Here, we will gather information about the employees (name and job title) of a target organization that is available on LinkedIn using theHarvester tool.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



attacker

••••

Figure 3.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

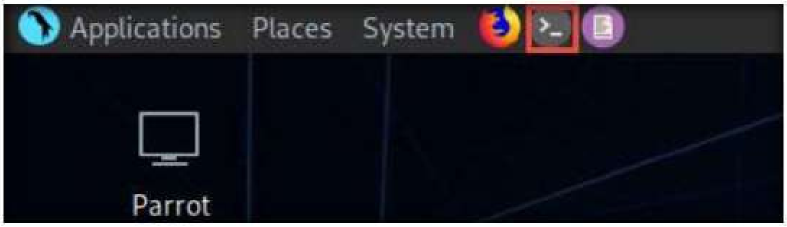


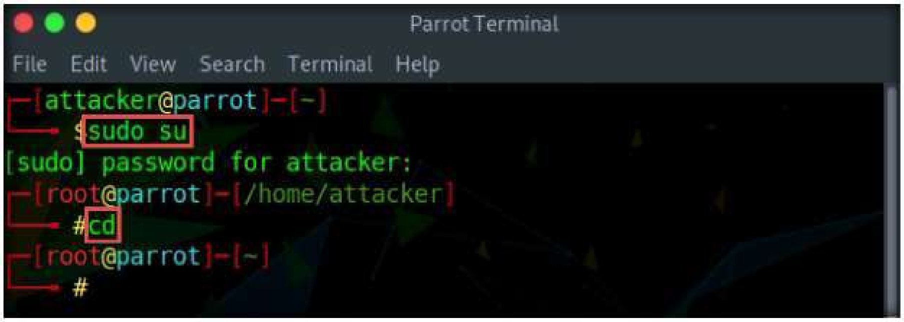
Figure 3.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

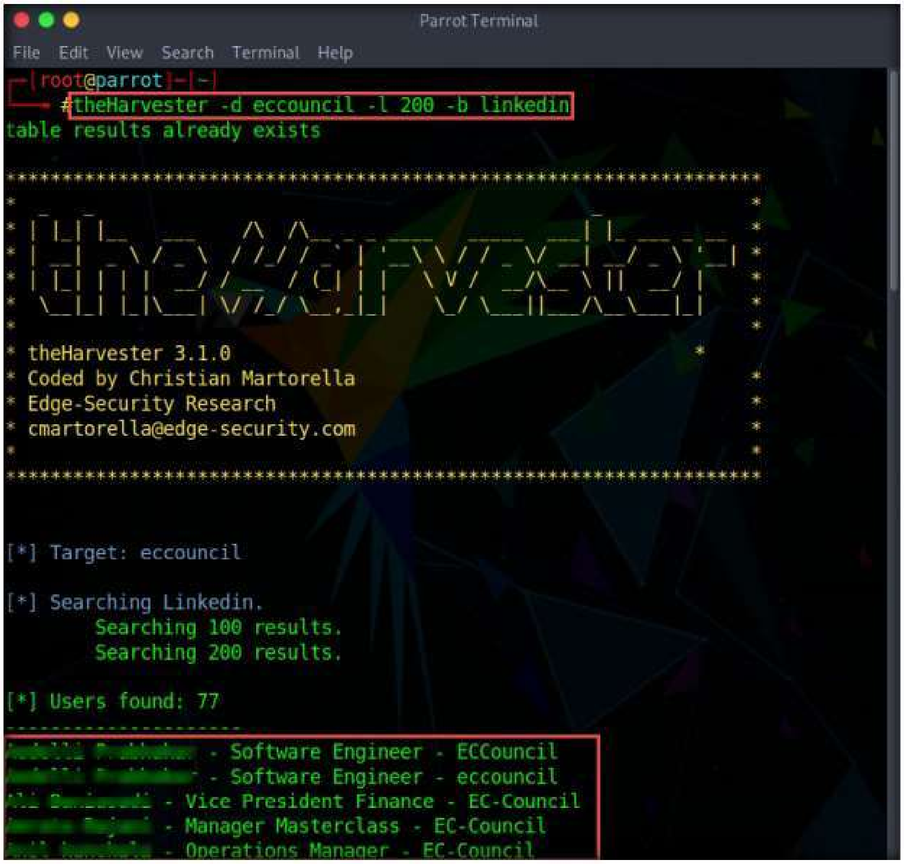


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

Figure 3.1.3: Running the programs as a root user

7. In the terminal window, type **theHarvester -d eccouncil -l 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source. Scroll down to view all the 200 results of the employees of the EC-Council.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.



```
┌─[root@parrot]─[~]
└──╼ #theHarvester -d eccouncil -l 200 -b linkedin
table results already exists

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0                                            *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: eccouncil

[*] Searching Linkedin.
        Searching 100 results.
        Searching 200 results.

[*] Users found: 77
---------------------
[redacted] - Software Engineer - ECCouncil
[redacted] - Software Engineer - eccouncil
[redacted] - Vice President Finance - EC-Council
[redacted] - Manager Masterclass - EC-Council
[redacted] - Operations Manager - EC-Council
```

Figure 3.1.4: theHarvester result

8. This concludes the demonstration of gathering employees' information from LinkedIn using theHarvester.

9. Close all open windows and document all the acquired information.

TASK 2

Gather Personal Information from Various Social Networking Sites using Sherlock

Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

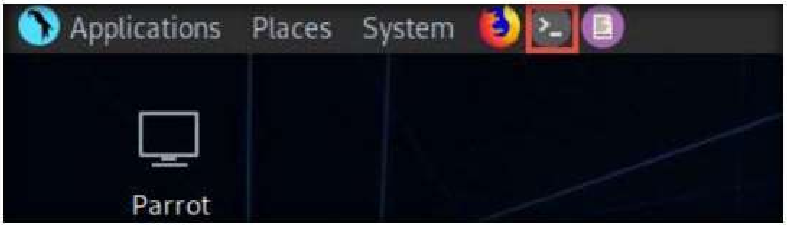


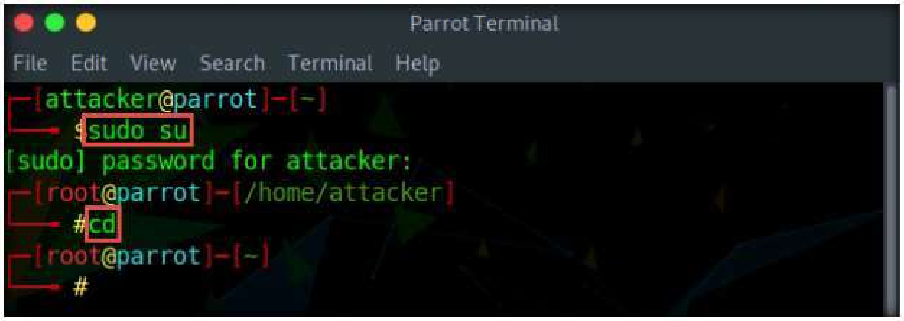
Figure 3.2.1: MATE Terminal Icon

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

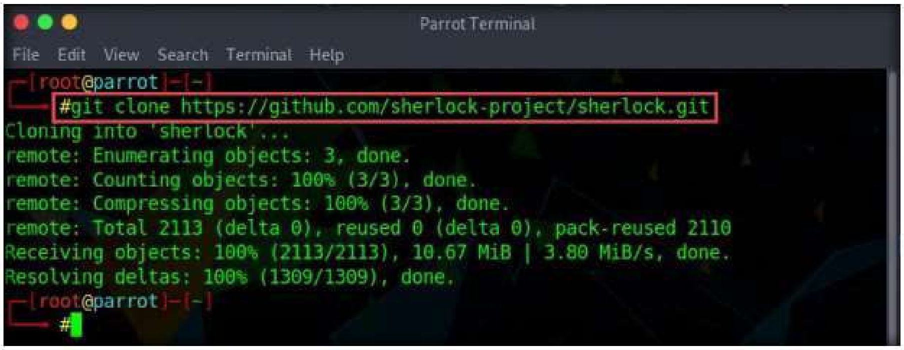
4. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

Figure 3.2.2: Running the programs as a root user

5. In the **Parrot Terminal** window, type **git clone https://github.com/sherlock-project/sherlock.git** and press **Enter**.

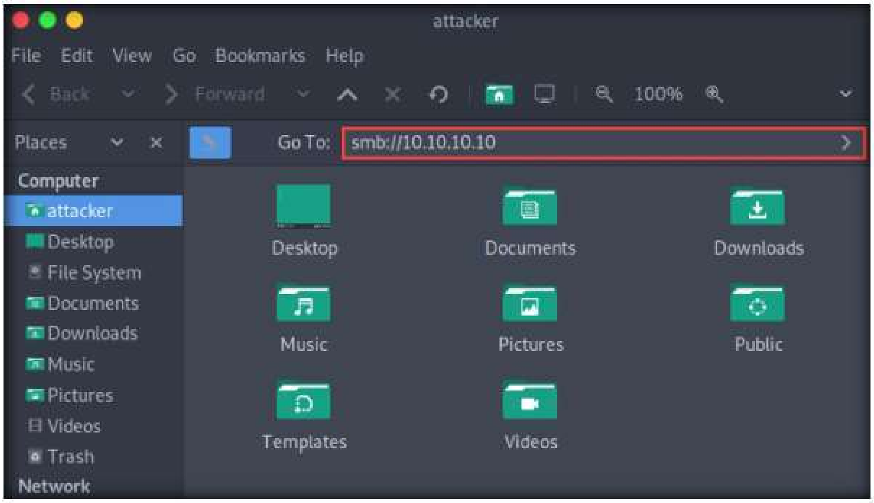


```
┌─[root@parrot]─[~]
└──╼ #git clone https://github.com/sherlock-project/sherlock.git
Cloning into 'sherlock'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 2113 (delta 0), reused 0 (delta 0), pack-reused 2110
Receiving objects: 100% (2113/2113), 10.67 MiB | 3.80 MiB/s, done.
Resolving deltas: 100% (1309/1309), done.
┌─[root@parrot]─[~]
└──╼ #
```

Figure 3.2.3: Cloning Sherlock tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

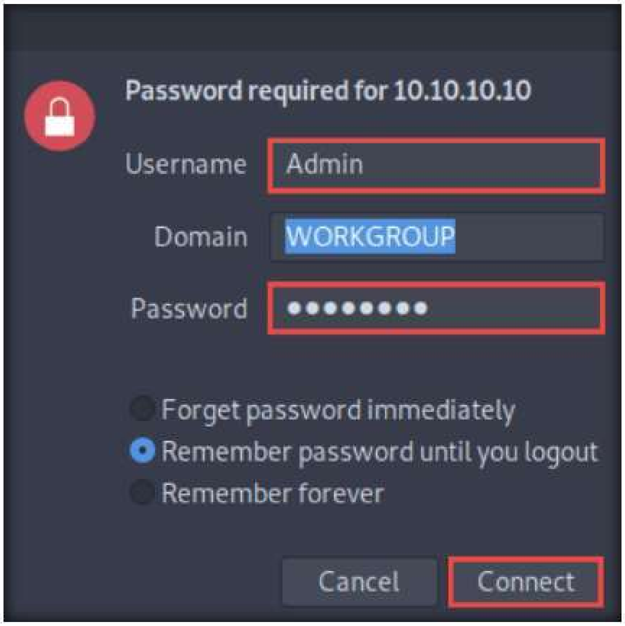
- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.



Go To: smb://10.10.10.10

Figure 3.2.4: Accessing Windows 10 shared folder

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.



Password required for 10.10.10.10

Username: Admin

Domain: WORKGROUP

Password: ●●●●●●●●

○ Forget password immediately

● Remember password until you logout

○ Remember forever

Figure 3.2.5: Security pop-up

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **sherlock** folder.

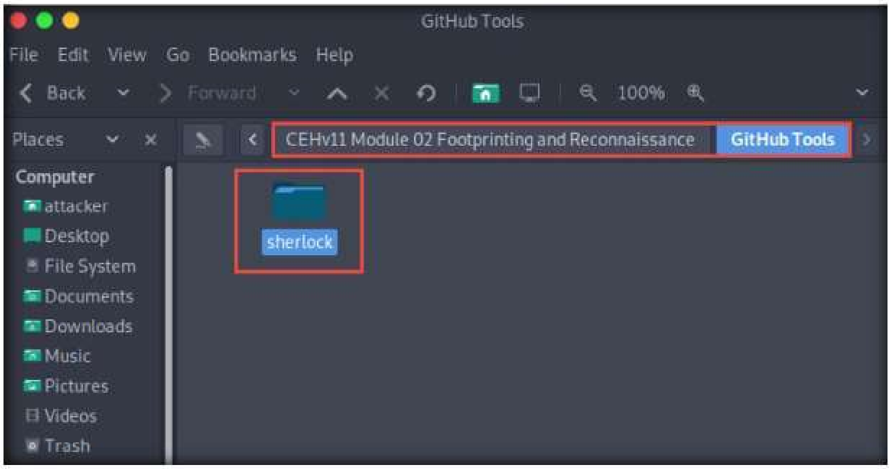


Figure 3.2.6: Copy sherlock folder

- Paste the copied **sherlock** folder on the location **/home/attacker/.**

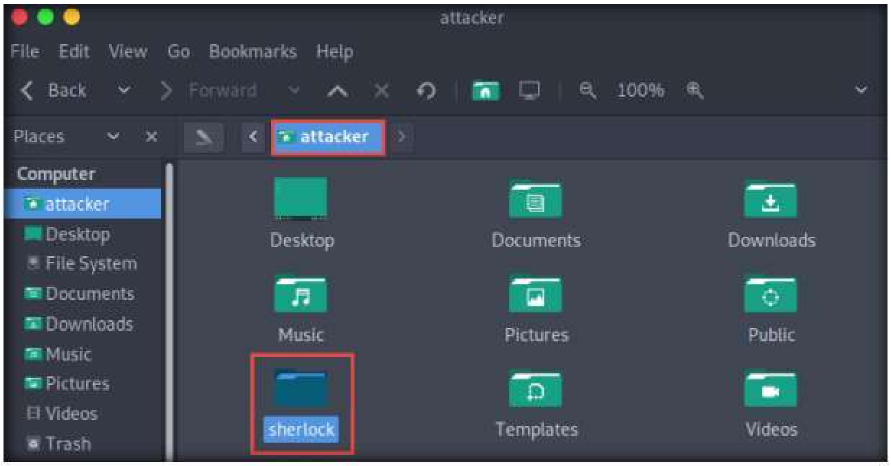
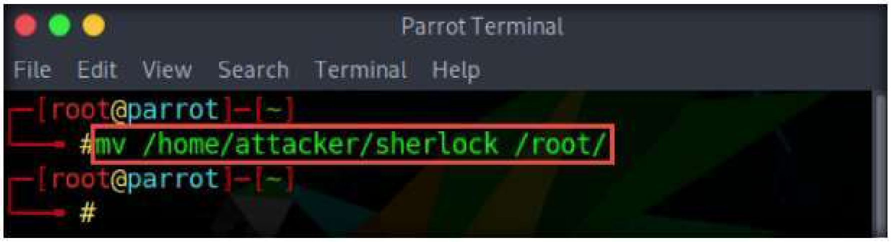


Figure 3.2.7: Paste the directory

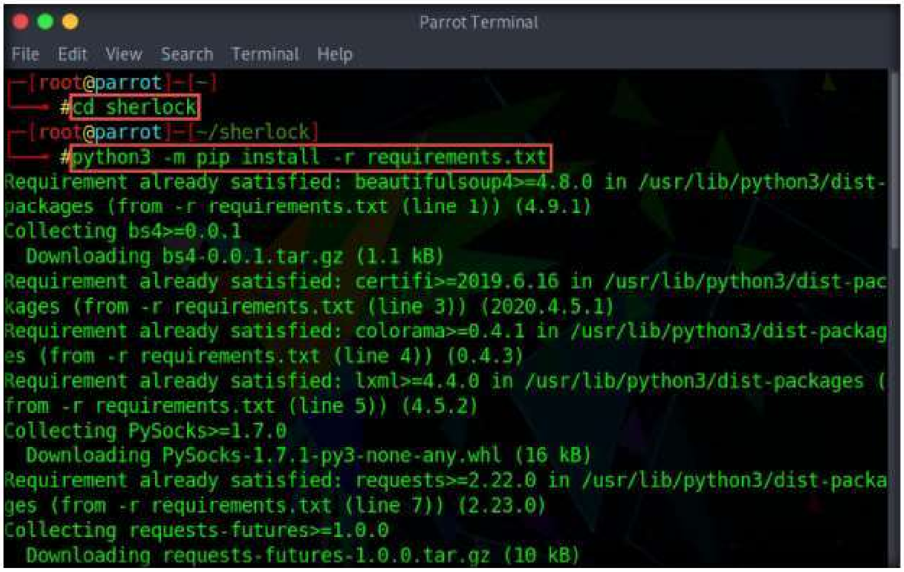
- In the terminal window, type **mv /home/attacker/sherlock /root/**.



```
┌─[root@parrot]─[~]
└──╼ #mv /home/attacker/sherlock /root/
┌─[root@parrot]─[~]
└──╼ #
```

Figure 3.2.8: Move the directory to root folder

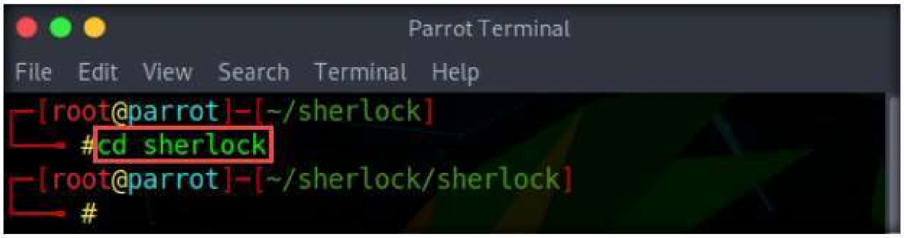
6. Type **cd sherlock** and press **Enter** to navigate to the **sherlock** folder. To install the python-pip requirements, type **python3 -m pip install -r requirements.txt** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #cd sherlock
┌─[root@parrot]─[~/sherlock]
└──╼ #python3 -m pip install -r requirements.txt
Requirement already satisfied: beautifulsoup4>=4.8.0 in /usr/lib/python3/dist-
packages (from -r requirements.txt (line 1)) (4.9.1)
Collecting bs4>=0.0.1
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
Requirement already satisfied: certifi>=2019.6.16 in /usr/lib/python3/dist-pac
kages (from -r requirements.txt (line 3)) (2020.4.5.1)
Requirement already satisfied: colorama>=0.4.1 in /usr/lib/python3/dist-packag
es (from -r requirements.txt (line 4)) (0.4.3)
Requirement already satisfied: lxml>=4.4.0 in /usr/lib/python3/dist-packages (
from -r requirements.txt (line 5)) (4.5.2)
Collecting PySocks>=1.7.0
  Downloading PySocks-1.7.1-py3-none-any.whl (16 kB)
Requirement already satisfied: requests>=2.22.0 in /usr/lib/python3/dist-packa
ges (from -r requirements.txt (line 7)) (2.23.0)
Collecting requests-futures>=1.0.0
  Downloading requests-futures-1.0.0.tar.gz (10 kB)
```

Figure 3.2.9: requirements.txt installation

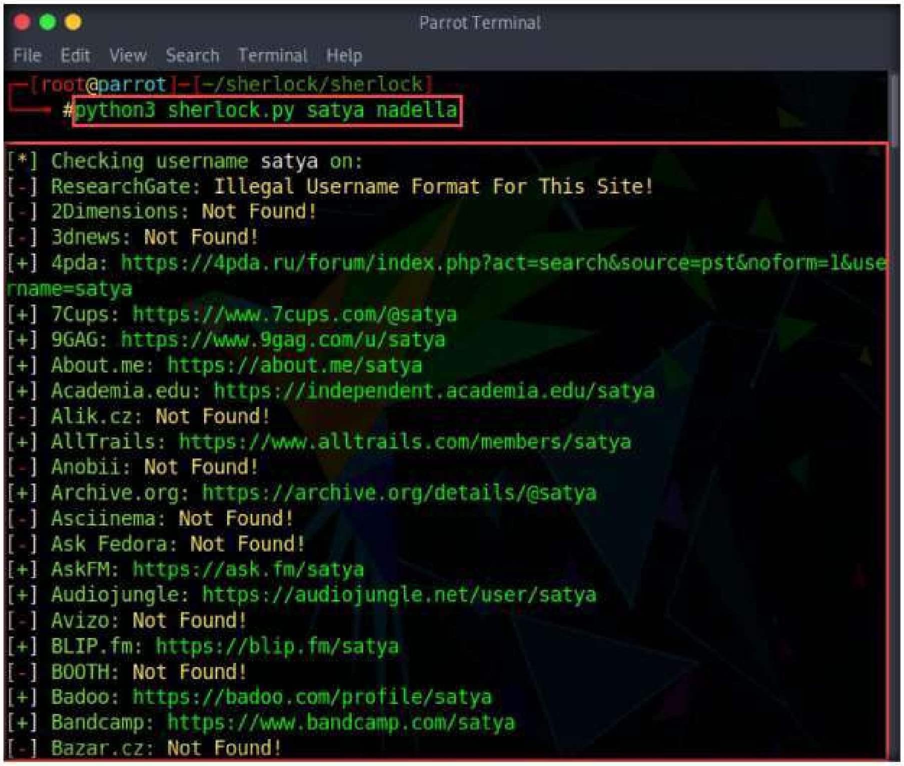
7. Once the installation is complete, type **cd sherlock** and press **Enter**.



```
┌─[root@parrot]─[~/sherlock]
└──╼ #cd sherlock
┌─[root@parrot]─[~/sherlock/sherlock]
└──╼ #
```

Figure 3.2.10: Navigate to the sherlock folder

8. Now, type **python3 sherlock.py satya nadella** and press **Enter**. You will get all the URLs related to Satya Nadella, as shown in the screenshot. Scroll down to view all the results.



```
┌─[root@parrot]─[~/sherlock/sherlock]
└──╼ #python3 sherlock.py satya nadella

[*] Checking username satya on:
[-] ResearchGate: Illegal Username Format For This Site!
[-] 2Dimensions: Not Found!
[-] 3dnews: Not Found!
[+] 4pda: https://4pda.ru/forum/index.php?act=search&source=pst&noform=1&use
rname=satya
[+] 7Cups: https://www.7cups.com/@satya
[+] 9GAG: https://www.9gag.com/u/satya
[+] About.me: https://about.me/satya
[+] Academia.edu: https://independent.academia.edu/satya
[-] Alik.cz: Not Found!
[+] AllTrails: https://www.alltrails.com/members/satya
[-] Anobii: Not Found!
[+] Archive.org: https://archive.org/details/@satya
[-] Asciinema: Not Found!
[-] Ask Fedora: Not Found!
[+] AskFM: https://ask.fm/satya
[+] Audiojungle: https://audiojungle.net/user/satya
[-] Avizo: Not Found!
[+] BLIP.fm: https://blip.fm/satya
[-] BOOTH: Not Found!
[+] Badoo: https://badoo.com/profile/satya
[+] Bandcamp: https://www.bandcamp.com/satya
[-] Bazar.cz: Not Found!
```

Figure 3.2.11: sherlock search result

You can also use tools such as **Social Searcher** (https://www.social-searcher.com), **UserRecon** (https://github.com), etc. to gather additional information related to the target company and its employees from social networking sites.

9. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.

10. Close all open windows and document all the acquired information.

11. Turn off the **Parrot Security** virtual machine.

TASK 3

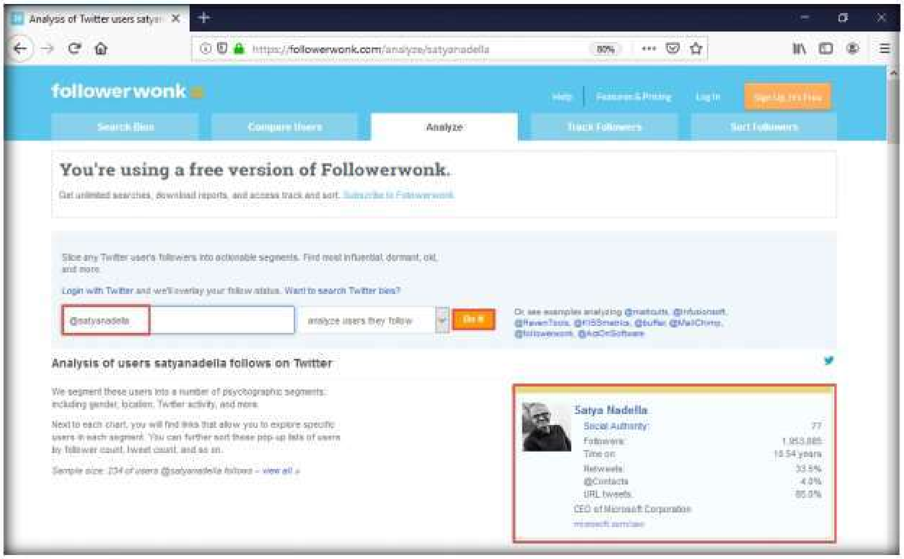
Gather Information using Followerwonk

Followerwonk is an online tool that helps you explore and grow your social graph, digging deeper into Twitter analytics; for example, Who are your followers? Where are they located? When do they tweet? This can be used to gather Twitter information about any target organization or individual.

1. Turn on the **Windows 10** virtual machine.

2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://followerwonk.com/analyze**. In the **screen name** search bar, type your target individual's twitter tag (here, **@satyanadella**) and click the **Do it** button to analyze the users whom the target person follows.



Analysis of Twitter users satya

https://followerwonk.com/analyze/satyanadella

You're using a free version of Followerwonk.

Get unlimited searches, download reports, and access track and sort. Subscribe to Followerwonk

Slice any Twitter user's followers into actionable segments. Find most influential, dormant, old, and more.

Login with Twitter and we'll overlay your follow status. Want to search Twitter bios?

@satyanadella | analyze users they follow | Do it

Or see examples analyzing @mattcutts, @infusionsoft, @RavenTools, @KISSmetrics, @buffer, @MailChimp, @followerwonk, @AddOnSoftware

Analysis of users satyanadella follows on Twitter

We segment these users into a number of psychographic segments: including gender, location, Twitter activity, and more.

Next to each chart, you will find links that allow you to explore specific users in each segment. You can further sort these pop-up lists of users by follower count, tweet count, and so on.

Sample size: 234 of users @satyanadella follows – view all »

Satya Nadella

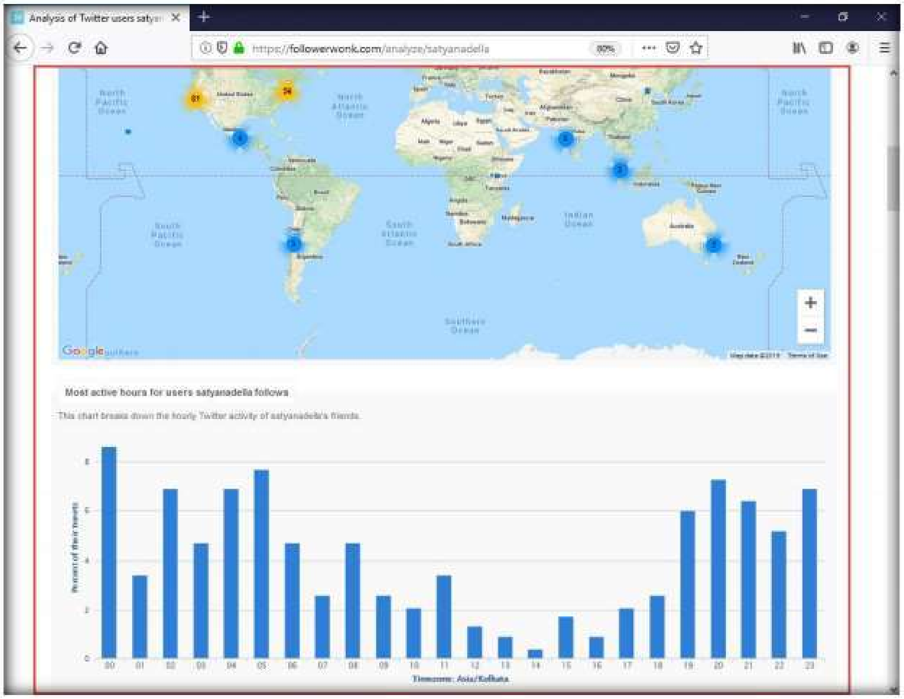
Social Authority:	77
Followers:	1,953,885
Time on:	10.54 years
Retweets:	33.5%
@Contacts:	4.0%
URL tweets:	85.0%

CEO of Microsoft Corporation

microsoft.com/ceo

Figure 3.3.1: Followerwonk search result

4. Scroll down to view the detailed analysis, as shown in the screenshot.



Analysis of Twitter users satya

https://followerwonk.com/analyze/satyanadella

Most active hours for users satyanadella follows

This chart breaks down the hourly Twitter activity of satyanadella's friends.

Figure 3.3.2: Followerwonk detailed search result

You can also use **Hootsuite** (https://hootsuite.com), **Sysomos** (https://www.sysomos.com), etc. to gather additional information related to the target company and its employees from social networking sites

5. This concludes the demonstration of gathering information using Followerwonk.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	□ No
Platform Supported	
☑ Classroom	☑ iLabs