Lab 3: Perform Footprinting Through Social Networking Sites

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

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.

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. ☐ Click Parrot Security to switch to the **Parrot Security** machine.
2. ☐ Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.

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

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

The password that you type will not be visible.

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

6.   A **Parrot Terminal** window appears. 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.

In this command, **-d** specifies the domain or company name to search (here, **eccouncil**), **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.
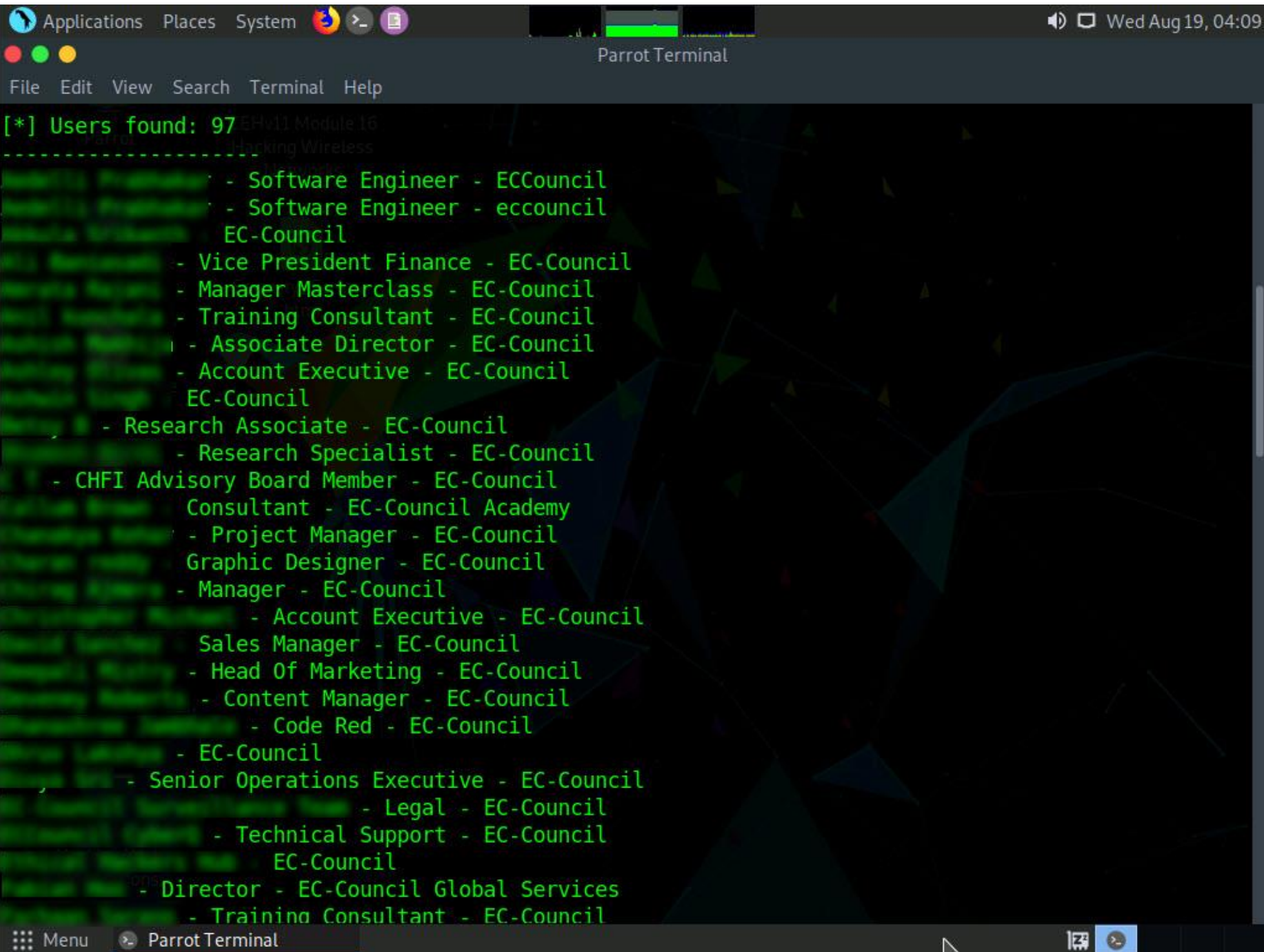
The complete eccouncil domain is **eccouncil.org**.

Parrot Terminal

File   Edit   View   Search   Terminal   Help

```
[attacker@parrot]-[~]
  $sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
  #cd
[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.
```

7. ☐ Scroll down to view the list of employees of the EC-Council.

Parrot Terminal

File   Edit   View   Search   Terminal   Help

```
[*] Users found: 97
---------------------
                      - Software Engineer - ECCouncil
                      - Software Engineer - eccouncil
              EC-Council
         - Vice President Finance - EC-Council
         - Manager Masterclass - EC-Council
         - Training Consultant - EC-Council
         - Associate Director - EC-Council
         - Account Executive - EC-Council
           EC-Council
       - Research Associate - EC-Council
           - Research Specialist - EC-Council
    - CHFI Advisory Board Member - EC-Council
              Consultant - EC-Council Academy
              - Project Manager - EC-Council
           Graphic Designer - EC-Council
           - Manager - EC-Council
                   - Account Executive - EC-Council
           Sales Manager - EC-Council
           - Head Of Marketing - EC-Council
             - Content Manager - EC-Council
                    - Code Red - EC-Council
         - EC-Council
       - Senior Operations Executive - EC-Council
                         - Legal - EC-Council
             - Technical Support - EC-Council
                 EC-Council
        - Director - EC-Council Global Services
             - Training Consultant - EC-Council
```

Menu   Parrot Terminal

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** machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.

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**.

The password that you type will not be visible.

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

5. ☐ Type **cd sherlock/sherlock/** and press **Enter** to navigate to the sherlock folder.

Parrot Terminal

File Edit View Search Terminal Help

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

Menu   Parrot Terminal

6. ☐ 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.

The results might differ when you perform the lab. If you receive any error messages in between ignore them.

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└─ #sudo su
┌─[root@parrot]─[~]
└─ #cd
┌─[root@parrot]─[~]
└─ #cd sherlock/sherlock/
┌─[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&username=satya
[+] 500px: https://500px.com/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!
[+] Aptoide: https://satya.en.aptoide.com/
[+] 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
```

Menu   💻 Parrot Terminal

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

8. ☐ 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. ☐ Close all open windows and document all the acquired information.

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. ☐ Click Windows 10 to switch to the **Windows 10** machine.

2. ☐ Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, click https://followerwonk.com/analyze and press **Enter**.

3. ☐ **Followerwonk** website appears, as shown in the screenshot.

followerwonk »

Help | Features & Pricing | Log In | Sign Up, It's Free

| Search Bios | Compare Users | Analyze | Track Followers | Sort Followers |

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 find your top followers?

| Screen Name... | analyze users they follow ▾ | Do it |

Or, see examples analyzing @AlysonMurphy, @mattcutts, @Demandbase, @simplymeasured, @avinash, @sengineland, @EmmaWatson, @anildash

©2020 @followerwonk – Terms & Privacy Policy

Privacy - Terms

Type here to search   O 🗐 e 🖿 🦊   ∧ 및 ◁ₓ 1:26 AM 5/20/2020 🖷₂

4. ☐ 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.

5. ☐ The results regarding the target appears, as shown in the screenshot.

https://followerwonk.com/analyze/satyanadella

followerwonk »

Search Bios | Compare Users | **Analyze** | Track Followers | Sort Followers

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?

| Screen Name... | analyze users they follow | Do it |

Or, see examples analyzing @SarahKSilverman, @EmmaWatson, @HubSpot, @sengineland, @SproutSocial, @Benioff, @ValaAfshar, @buffer

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: 236 of users @satyanadella follows – view all »

Satya Nadella

Social Authority:	77
Followers:	2,144,498
Time on:	11.27 years
Retweets:	31.0%
@Contacts	3.5%
URL tweets:	67.0%

CEO of Microsoft Corporation

microsoft.com/ceo

Mapped locations of users satyanadella follows

Using the location field in Twitter accounts, we try to approximate the geographic location of up

6. ☐ Scroll down to view the detailed analysis.

7. ☐ This concludes the demonstration of gathering information using Followerwonk.

8. ☐ 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.

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