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 personal information from various social networking sites using Sherlock

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 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.

Here, we will use Sherlock to gather personal information about the target from the social networking sites.

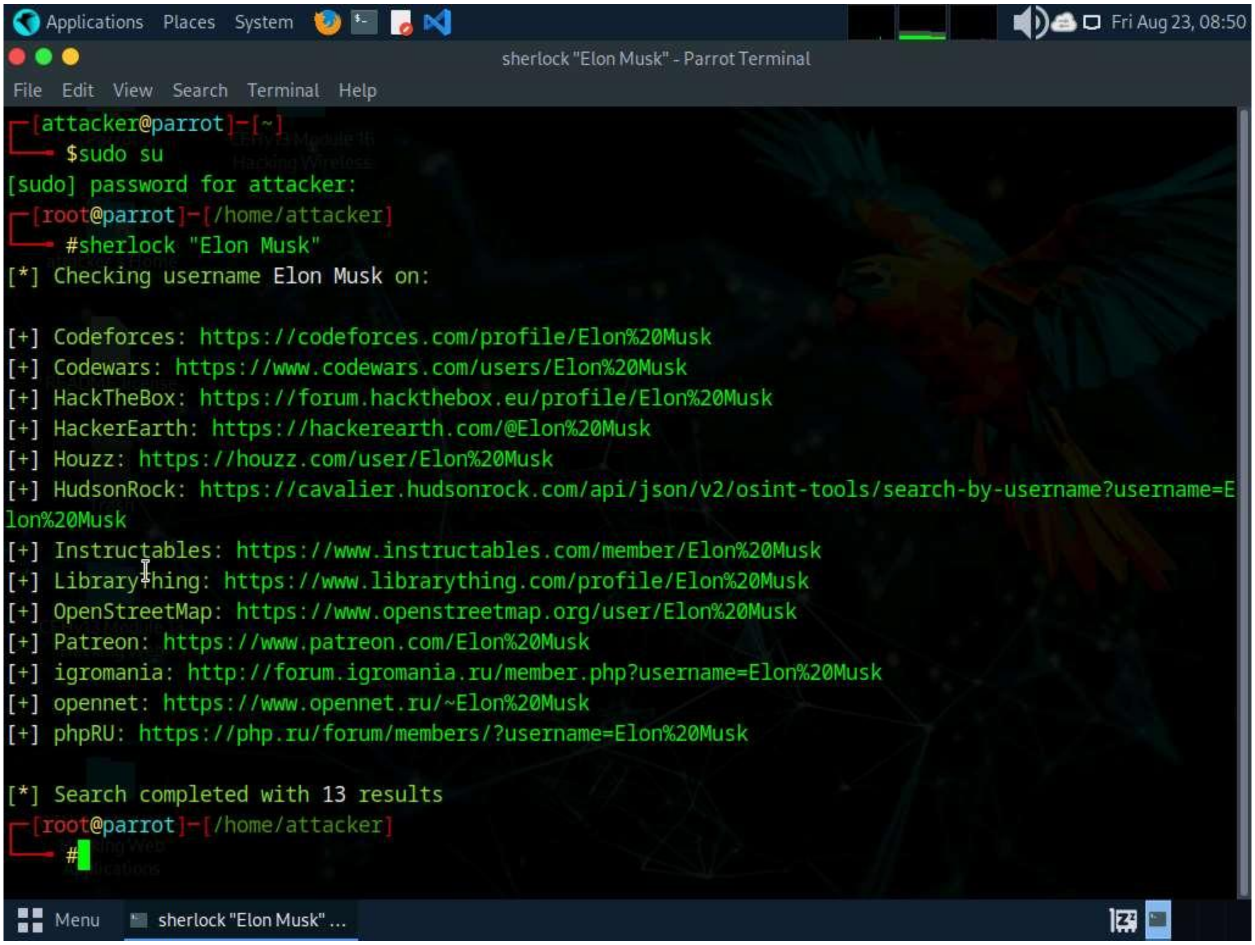
Here, we are gathering information about **Elon Musk**. However, you can select a target of your choice.

1. Turn on the Parrot Security virtual machine
2. Click Parrot Security to switch to **Parrot** machine, and login with attacker/toor. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

3. Run **sherlock "Elon Musk"** command and you will get all the URLs related to Elon Musk, as shown in the screenshot. Scroll-down to view all the results.

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



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #sherlock "Elon Musk"
[*] Checking username Elon Musk on:

[+] Codeforces: https://codeforces.com/profile/Elon%20Musk
[+] Codewars: https://www.codewars.com/users/Elon%20Musk
[+] HackTheBox: https://forum.hackthebox.eu/profile/Elon%20Musk
[+] HackerEarth: https://hackerearth.com/@Elon%20Musk
[+] Houzz: https://houzz.com/user/Elon%20Musk
[+] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=E
lon%20Musk
[+] Instructables: https://www.instructables.com/member/Elon%20Musk
[+] LibraryThing: https://www.librarything.com/profile/Elon%20Musk
[+] OpenStreetMap: https://www.openstreetmap.org/user/Elon%20Musk
[+] Patreon: https://www.patreon.com/Elon%20Musk
[+] igromania: http://forum.igromania.ru/member.php?username=Elon%20Musk
[+] opennet: https://www.opennet.ru/~Elon%20Musk
[+] phpRU: https://php.ru/forum/members/?username=Elon%20Musk

[*] Search completed with 13 results
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

4. The attackers can further use the gathered URLs to obtain sensitive information about the target such as DOB, employment status and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.

5. This concludes the demonstration of gathering personal information from various social networking sites using Sherlock.

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

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