

# Lab 9: Perform Footprinting using AI

## Lab Scenario

In this lab, you will use AI to analyze and map digital footprints from social media data. The AI will identify patterns and highlight privacy risks. By comparing AI-generated insights with manual analysis, students will understand the power and limitations of AI in cybersecurity.

## Lab Objectives

- Footprinting a target using ShellGPT

## Overview of Footprinting using AI

Footprinting using AI accelerates the reconnaissance process by automating data collection and analysis, allowing security professionals to uncover vulnerabilities more efficiently. AI-powered footprinting enhances threat intelligence by identifying patterns and anomalies in vast amounts of data, providing deeper insights into potential risks. As an ethical hacker you should look for as much information as possible about the target using AI.

### Task 1: Footprinting a Target using ShellGPT

Footprinting with ShellGPT involves leveraging shell scripting capabilities along with GPT's language processing prowess. By crafting tailored scripts, ShellGPT automates data gathering from various sources, including WHOIS databases and online forums. It parses and extracts relevant information such as domain registrations, IP addresses, and network configurations. ShellGPT streamlines the reconnaissance process, enabling efficient analysis and identification of potential security vulnerabilities. Its integration enhances the footprinting phase with automation and intelligent data processing.

Here, we will use ShellGPT to perform footprinting on a target.

The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

1. Before starting this lab, click [Parrot Security](#) to switch to the **Parrot Security** machine and incorporate ShellGPT by following steps provided in [Integrate ShellGPT in Parrot Security Machine.pdf](#).

Alternatively, you can follow the steps to integrate ShellGPT provided in **Module 00: Integrate ShellGPT in Parrot Security Machine**.

2. After incorporating the ShellGPT API in **Parrot Security** machine, we will use ShellGPT for harvesting emails pertaining to a target organization. To do so, run `sgpt --chat footprint --shell "Use theHarvester to gather email accounts associated with 'microsoft.com', limiting results to 200, and leveraging 'baidu' as a data source"` command.

In the prompt type **E** and press **Enter** to execute the command.

3. ShellGPT will harvest the emails using theHarvester tool and displays the email and host list.

```
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] Emails found: 3 3 MB (13 MB selected) File space: 58.9 GB
```

The screenshot shows a Linux desktop environment with a terminal window open. The terminal output is as follows:

```
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] Emails found: 3
a-yuwa@microsoft.com
contactopencode@microsoft.com
emailopencode@microsoft.com
[*] Hosts found: 22
.windowsupdate.microsoft.com
2Fdevblogs.microsoft.com
account.microsoft.com
azure.microsoft.com
clarity.microsoft.com
devblogs.microsoft.com
docs.microsoft.com
go.microsoft.com
learn.microsoft.com
learning.microsoft.com
login.microsoft.com _Key_CEHT3.txt selected (56 bytes), Free space: 58.9 GB
```

4. We will perform footprinting through social networking sites using ShellGPT, to do so run **sgpt --chat footprint --shell "Use Sherlock to gather personal information about 'Sundar Pichai' and save the result in recon2.txt"** command.

In the prompt type **E** and press **Enter** to execute the command.

```
[root@parrot]~[/home/attacker]
#sgpt --chat footprint --shell "Use Sherlock to gather personal information about 'Sundar Pichai' and save the result in recon2.txt" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --chat footprint --shell "Use Sherlock to gather personal information about 'Sundar Pichai' and save the result in recon2.txt"
sherlock SundarPichai --output recon2.txt
[E]xecute, [D]escribe, [A]bort: E
Update Available! CEHv13 Module 13 CEHv13 Module 14 CEHv13 Module 16 Kali Linux CTF VM README License
You are running version 0.14.3. Version 0.14.4 is available at https://github.com/sherlock-project/sherlock
[*] Checking username SundarPichai on:
[+] About.me: https://about.me/SundarPichai
[+] Academia.edu: https://independent.academia.edu/SundarPichai
[+] Behance: https://www.behance.net/SundarPichai
[+] Blogger: https://SundarPichai.blogspot.com
[+] Codecademy: https://www.codecademy.com/profiles/SundarPichai
[+] Codeforces: https://codeforces.com/profile/SundarPichai
[+] Disqus: https://disqus.com/SundarPichai
[+] Duolingo: https://www.duolingo.com/profile/SundarPichai
[+] Fiverr: https://www.fiverr.com/SundarPichai
[+] Freelancer: https://www.freelancer.com/u/SundarPichai
[+] Giphy: https://giphy.com/SundarPichai
[+] GitHub: https://www.github.com/SundarPichai
[+] HackerEarth: https://hackerearth.com/@SundarPichai
[+] HackerOne: https://hackerone.com/SundarPichai
[+] HackerRank: https://hackerrank.com/SundarPichai
[+] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=SundarPichai
```

- After the execution of the command, in the terminal run **ls** command to view the contents in the present working directory.

The screenshot shows a terminal window titled "ls --color=auto - Parrot Terminal". The command run was "#sgpt --chat footprint --shell "Use Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"" followed by "sherlock Sundar Pichai --print-found > recon2.txt". The output shows a file named "recon2.txt" created in the current directory. The terminal also displays a file browser interface with various tools like AndroRAT, BloodHound, ClickjackPoc, etc., and a file named "New\_Key\_CEHV13.txt" is selected.

```
[root@parrot]~[/home/attacker]
└─#sgpt --chat footprint --shell "Use Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"
sherlock Sundar Pichai --print-found > recon2.txt
[E]xecute, [D]escribe, [A]bort: E
[root@parrot]~[/home/attacker]
└─#ls
AndroRAT          jwt_tool      reverse-shell-generator
BloodHound-win32-x64.zip lazys3-master roguehostapd
ClickjackPoc       Maltego.v4.6.0.deb RPCScan
create_ap          microsoft_emails.json Rustscan
Desktop           microsoft_emails.xml S3Scanner
dirsearch          Music        SharpHound-v1.1.1.zip
dnsrecon          ntlm_theft  Sniper
Documents          passwords.txt spiderfoot
Downloads         PhoneSploit-Pro Sundar.txt
DSSS              Photon       SuperEnum
ghauri             Pictures     sx-Tool
ghost_eye          PowerTools-master Templates
GRecon            Public       Videos
Havoc              PwnXSS      wifiphisher
holehe             Pichai.txt  Wmi-Persistence-master
jdk-8u202-linux-x64.tar.gz recon2.txt
[root@parrot]~[/home/attacker]
└─#
```

6. We can see that recon2.txt file is created by previous command. In the terminal window, run **pluma recon2.txt** command to view its contents. Close the text editor window.

The screenshot shows a terminal window with a text editor titled "recon2.txt". The file contains a list of 15 URLs related to Sundar Pichai:

```
1 https://about.me/SundarPichai
2 https://independent.academia.edu/SundarPichai
3 https://www.behance.net/SundarPichai
4 https://SundarPichai.blogspot.com
5 https://www.codecademy.com/profiles/SundarPichai
6 https://codeforces.com/profile/SundarPichai
7 https://disqus.com/SundarPichai
8 https://www.duolingo.com/profile/SundarPichai
9 https://www.fiverr.com/SundarPichai
10 https://www.freelancer.com/u/SundarPichai
11 https://giphy.com/SundarPichai
12 https://www.github.com/SundarPichai
13 https://hackerearth.com/@SundarPichai
14 https://hackerone.com/SundarPichai
15 https://hackerrank.com/SundarPichai
```

The terminal also displays the command used to run the tool:

```
# pluma recon2.txt
```

7. We will perform DNS lookup using ShellGPT, to do so, run **sgpt --chat footprint --shell “Install and use DNSRecon to perform DNS enumeration on the target domain www.certifiedhacker.com” command.**

In the prompt type **E** and press **Enter** to execute the command.

[root@parrot]~[/home/attacker]

```
#sgpt --chat footprint --shell "Install and use DNSRecon to perform DNS enumeration on the target domain www.certifiedhacker.com" - Parrot
```

```
sudo apt-get install dnsrecon && dnsrecon -d www.certifiedhacker.com
```

```
[E]xecute, [D]escribe, [A]bort: E
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
dnsrecon is already the newest version (1.1.3-2).
```

```
The following packages were automatically installed and are no longer required:
```

```
ccze hcxdumptool hcxtools hostapd isc-dhcp-server libubl1 lua-lpeg macchanger
```

```
oracle-instantclient-basic policycoreutils postgresql rfkill selinux-utils tmux upx-ucl
```

```
Use 'sudo apt autoremove' to remove them.
```

```
0 upgraded, 0 newly installed, 0 to remove and 179 not upgraded.
```

```
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
```

```
[+] DNSSEC is not configured for www.certifiedhacker.com
```

```
[*] SOA ns1.bluehost.com 162.159.24.80
```

```
[*] NS ns1.bluehost.com 162.159.24.80
```

```
[*] NS ns2.bluehost.com 162.159.25.175
```

```
[*] Bind Version for 162.159.25.175 "2024.5.2"
```

```
[*] MX mail.certifiedhacker.com 162.241.216.11
```

```
[*] CNAME www.certifiedhacker.com certifiedhacker.com
```

```
[*] A certifiedhacker.com 162.241.216.11
```

```
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
```

```
[*] Enumerating SRV Records
```

```
[+] 0 Records Found
```

8. In the terminal run **sgpt --chat footprint --shell** “Perform network tracerouting to discover the routers on the path to a target host [www.certifiedhacker.com](http://www.certifiedhacker.com)” command to perform Traceroute to a target.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title bar reads "sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com" - P". The terminal content displays a traceroute command being run against the target host "www.certifiedhacker.com". The output shows the path through various routers and switches, with hop numbers 1 through 13 listed, along with their respective IP addresses and round-trip times (RTTs) in milliseconds. The terminal prompt "[root@parrot]~[/home/attacker]" is visible at the bottom.

```
[root@parrot]~[/home/attacker]
└─# sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"
traceroute www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  0.808 ms  0.754 ms  1.418 ms
 2  172.18.0.1 (172.18.0.1)  3.062 ms  3.033 ms  3.008 ms
 3  192.168.0.1 (192.168.0.1)  2.996 ms  2.970 ms  2.893 ms
 4  185.254.56.25 (185.254.56.25)  1.627 ms  1.600 ms  2.123 ms
 5  * * port-channel4.switch2.lon3.he.net (216.66.95.117)  3.096 ms
 6  * * *
 7  port-channel18.core2.lon2.he.net (184.104.197.217)  34.378 ms  34.353 ms  16.650 ms
 8  ae-23.edge7.London1.Level3.net (4.68.127.237)  34.296 ms  34.270 ms  34.245 ms
 9  ae1.37.bar4.SaltLakeCity1.level3.net (4.69.219.58)  128.244 ms  142.395 ms  142.369 ms
10  4.53.7.174 (4.53.7.174)  159.655 ms  153.902 ms  159.438 ms
11  69-195-64-111.unifiedlayer.com (69.195.64.111)  160.043 ms  159.995 ms  147.701 ms
12  po97.prv-leaf1a.net.unifiedlayer.com (162.144.240.123)  143.202 ms po99.prv-leaf1b.net.unifiedlayer.com (162.144.240.131)  147.570 ms
13  box5331.bluehost.com (162.241.216.11)  150.722 ms  149.059 ms  147.165 ms
[root@parrot]~[/home/attacker]
└─#
```

9. Now run **sgpt --chat footprint --shell “Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain”** command to run a python script to automate footprinting tasks.

In the prompt type **E** and press **Enter** to execute the command.

It might take some time develop and run the script.

Applications Places System Fri May 17, 00:44

sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain"

[root@parrot]~[/home/attacker]

```
#sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain"
cat > footprint_script.py << 'EOF'
import subprocess

def footprint(domain):
    # Perform DNS lookup
    subprocess.run(['dig', domain, '+short'])

    # Retrieve WHOIS records
    subprocess.run(['whois', domain])

    # Enumerate emails using theHarvester (assuming theHarvester is installed and in PATH)
    subprocess.run(['theHarvester', '-d', domain, '-b', 'all', '-l', '100'])

    # Add more footprinting commands as needed

if __name__ == "__main__":
    domain = 'microsoft.com'
    footprint(domain)
EOF
```

Hacking Web Servers

python3 footprint\_script.py  
[E]xecute, [D]escribe, [A]bort: E

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window has a dark background and displays the output of the command `sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website..."`. The output includes a list of IP addresses and detailed WHOIS information for the domain `MICROSOFT.COM`, including registrar details, status, and name servers.

```
[E]xecute, [D]escribe, [A]bort: E
20.112.250.133
20.231.239.246
20.76.201.171
20.70.246.20
20.236.44.162
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2025-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
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: NS1-39.AZURE-DNS.COM
Name Server: NS2-39.AZURE-DNS.NET
Name Server: NS3-39.AZURE-DNS.ORG
```

10. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct footprinting on the target.
11. This concludes the demonstration of performing footprinting using the ShellGPT.
12. Close all open windows and document all the acquired information.