De La Salle University
College of Computer Studies

Ethical Hacking

Module No. 2 – Footprinting

Name : Daniel Gavrie Y. Clemente

1.0 Objective

- To familiarize the student on the footprinting technique.
- To familiarize the student with tools that can be used for footprinting, which are: whois, traceroute, nslookup

2.0 Procedure

2.1. Initial Setup

1. Set-up a machine/s (whether physical or virtual) with the following specifications :

Machine	Operating System	IP Address Settings
Hacker – Linux	Kali Linux	Set to DHCP

2.2. whois – gathering domain information

2. Open a web browser and go to the URL https://viewdns.info/

3. Type in the domain name “www.google.com” in the WHOIS Lookup textbox and press Lookup.

4. Determine the Name Servers used by the domain name:

Name Servers
ns2.google.com
ns1.google.com
ns4.google.com
ns3.google.com

5. Determine the contact information of the domain:

Contact Information
https://domains.markmonitor.com/whois/google.com

6. Determine the creation date of the domain:

Creation Date
Creation Date: 1997-09-15T07:00:00+0000

7. Type in the domain name “www.google.com” in the DNS Record Lookup textbox and press Lookup.

8. Determine the IPv4 Address used by the domain

IP Address
142.250.72.36

Type in the URL http://<IP Address>

Can you see its webpage? Yes

2.3. nslookup -

9. Open a Terminal application in Kali Linux and type in the command “nslookup”.

10. Type in the domain name “www.dlsu.edu.ph” and then press Enter.

What type of information is displayed?	different types of IP addresses

Displayed information
Server: 192.168.19.2 Address: 192.168.19.2#53 Non-authoritative answer:

Name: www.dlsu.edu.ph
Address: 104.22.36.142
Name: www.dlsu.edu.ph
Address: 172.67.14.223
Name: www.dlsu.edu.ph
Address: 104.22.37.142
Name: www.dlsu.edu.ph
Address: 2606:4700:10::6816:248e
Name: www.dlsu.edu.ph
Address: 2606:4700:10::ac43:edf
Name: www.dlsu.edu.ph
Address: 2606:4700:10::6816:258e

11. Open a web browser and go to the URL https://ipinfo.io/ . On the text box, type one of the IP Address Displayed in Item no. 10.

To what company does the IP Address is registered?	Cloudflare, Inc.
What does this mean?	The IP address is owned and managed by Cloudflare

12. On the nslookup command prompt, type in the command “set type=mx”

13. Type in the domain name “dlsu.edu.ph”. What is the possible mail exchanger used for the domain? What does this imply?

The possible mail exchanger used for the domain are the following:
dlsu.edu.ph mail exchanger = 5 alt1.aspmx.l.google.com.
dlsu.edu.ph mail exchanger = 5 alt2.aspmx.l.google.com.
dlsu.edu.ph mail exchanger = 1 aspmx.l.google.com.
dlsu.edu.ph mail exchanger = 10 aspmx2.googlemail.com.
dlsu.edu.ph mail exchanger = 10 aspmx3.googlemail.com.

This implies that any of the mail exchanger is used, it get rerouted through the googlemail domain.

14. On the nslookup command prompt, type in the command “set type=cname”

15. Type in the domain name www.fb.com. What is the result? What does this imply?

The result is a non-authoritative answer that gives us the canonical name of www.facebook.com. This implies that the URL will redirect to www.facebook.com.

16. Open a web browser and go to the URL www.fb.com. What happened when you browsed the website? Does this prove your answer in Item no. 15?

It redirected to www.facebook.com and its login page. Yes, this proved my answer in item no. 15.

2.4. traceroute – route information of a host

17. Open a command prompt on your host machine.

18. At the command prompt, type the command "tracert <IP Address of www.dlsu.edu.ph>" or "tracert "www.dlsu.edu.ph". Do you see where your traffic passes through before arriving to your destination? Post the results of your traceroute in the textbox below.

```
C:\Users\gavri>tracert www.dlsu.edu.ph

Tracing route to www.dlsu.edu.ph [104.22.37.142]
over a maximum of 30 hops:

  1    22 ms    19 ms     9 ms  192.168.68.1
  2   194 ms    89 ms    19 ms  192.168.254.254
  3     *      315 ms   257 ms  10.205.252.18
  4   307 ms   294 ms   273 ms  10.205.252.50
  5   277 ms   248 ms     *     112.198.189.1
  6     *        *        *     Request timed out.
  7    88 ms    53 ms    34 ms  cloudflare.sgix.sg [103.16.102.93]
  8   314 ms   585 ms     *     162.158.160.137
  9   337 ms   311 ms   336 ms  104.22.37.142

Trace complete.
```

2.5. Google Hacking

19. Open a web browser and go to the URL https://www.google.com/

20. In the search bar, input **DLSU,** then press the search button. Scroll down a bit to familiarize yourself with the results. Do another search, this time with **"DLSU"**. Do the results differ? Why or why not?

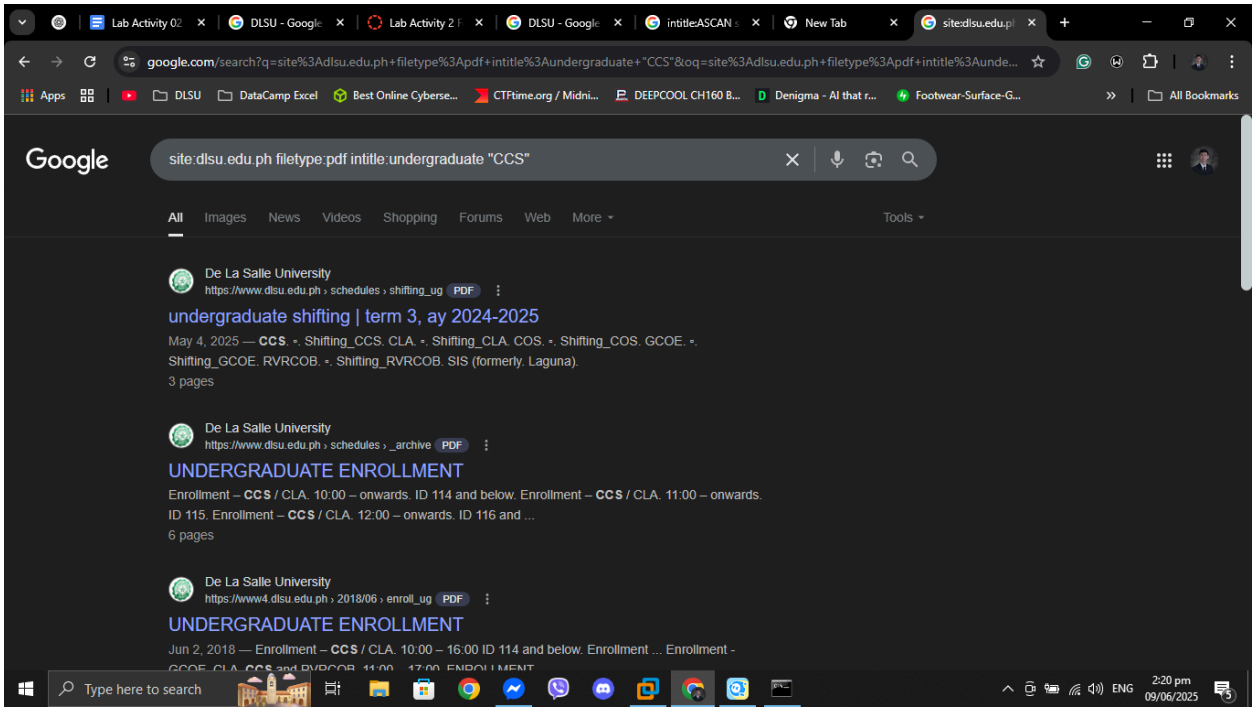
The results differ in some areas, such as social media platforms, which appeared in the second instance when DLSU was entered in the search bar. However, the only thing that remained consistent was DLSU's webpage. This occurs because the query triggers dynamic search engine behavior based on factors such as

user location, search history, personalization settings, or real-time indexing of content. As a result, while the core site (dlsu.edu.ph) remains stable, surrounding results may change.

21. Do another search using **intitle:ASCAN site:www.dlsu.edu.ph**. How many results do you see? Please describe the result webpage.

Only one result came up, which was a link to Ascan, Adrian Giovanni, a lecturer in the Department of Computer Technology.

22. If you were to query **pdf** documents within **dlsu.edu.ph** that contains **undergraduate** on its title that has exact string match of **CCS.** What would be your query? Please attach or insert the screenshot of your answers in the text box below.



3.0 Guide Questions

1. What information does the “viewdns.info” website show?
   The “viewdns.info” website offers various DNS and domain-related tools that display information such as IP address ownership, DNS records, and domain registration details.
2. What does the nslookup application do? What information does it show?
   The nslookup application queries DNS servers to obtain mapping information between domain names and IP addresses.
3. What does the traceroute application do? What information does it show?
   The traceroute application tracks the path packets take to reach a destination, showing each hop and the time it takes.
4. Are there any other tools that you can use to obtain the information in the activity?
   Yes, tools like WHOIS, dig, Ping, and Nmap can also be used to gather similar information.
5. What can you do with the information gathered when footprinting?
   The information gathered during footprinting helps identify potential vulnerabilities, map network structure, and prepare for penetration testing or cybersecurity assessments.

https://www.kali.org/get-kali/#kali-virtual-machines