**A close-up of a logo

Description automatically generated**

**Course: CYB302**

**Ethical Hacking  
(Canadian Context)**

**Lab 3: Information Gathering**

**Coordinator and Instructor:**

**Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

**Activity 1:**

**Manual OSINT Gathering**

Identify a domain belonging to a company or organization that you are familiar with. You can  
use www.afrinic.net for this activity. use the Dig command to review information about the  
domain and record your results as required.  
• In your Kali Linux VM, Open up a terminal and type in the following command:  
o dig a www.afrinic.net.  
In the above command, the dig tool is looking for the A resource record for the web  
server named www, in the afrinic second-level domain, in the .net TLD.  
a) What is the IP address returned in the Answer Section in response of the command  
you typed above? Answer = **192.168.229.2**

**A screenshot of a computer

AI-generated content may be incorrect.**

Now query with the +dnssec switch. The response includes the A  
resource record as before, but now there is a resource record signature  
(RRSIG) resource record as well. The RRSIG resource record is a hash of all  
the A resource records of www.afrinic.net that are returned, encrypted with the  
private key of afrinic.net. In this case, there is only one A resource record, but if  
there were more, they all would be hashed together. Type the following command:  
o dig +dnssec a www.afrinic.net.  
b) Do you notice the hash in the Answer section? To answer this question, Take the  
screenshot of the complete output received after the above-mentioned command is  
executed

A screenshot of a computer screen

AI-generated content may be incorrect.

To decrypt this encrypted hash, the RIT DNS server would request the  
public key of afrinic.net at this point, on behalf of a DNS client. To do that  
manually, enter the following command:

o dig +dnssec dnskey afrinic.net.

d) Check the output of above-mentioned command and determine how many DS  
records were return in the answer section. To answer this question, Take the  
screenshot of the complete output received after the above-mentioned command is  
executed and place the screenshot as answer of this question.  
• Now the RIT DNS server would request that the .net zone send its DNSKEY resource records.  
To do that manually, enter the following command:  
o dig +dnssec dnskey net.  
Check the output of above-mentioned command and determine the following:  
e) How many ZSKs are send by .net? Answer = 257  
f) How many KSKs are send by .net? Answer = 257

To do that, enter the following command:  
o dig +trace www.afrinic.net.  
g) What is the output of the above-mentioned command? Take the screenshot of the  
complete output received after the above-mentioned command is executed and  
place it under answer of this question

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Now try an external zone transfer. The @ symbol means we are going to ask the serverfol lowing the symbol the query. In this case, we are going to ask one of the authoritative DNS  
servers for the afrinic.net zone for an AXFR of the entire zone. Enter the following command:  
o dig axfr @ns1.afrinic.net afrinic.net.  
• Of course, afrinic.net has allowed only authorized internal zone transfers from its DNS  
servers, so you will see the message “Transfer failed,

A screenshot of a computer

AI-generated content may be incorrect.

**Activity 2: WHOIS tool**  
• Use the appropriate WHOIS engine to look up the domain and identify contacts and other  
interesting information. Type the following command in terminal at Kali Linux:  
o whois 104.19.177.99 (Take the screen shot)  
h) What is the organization name? Answer = **Cloudflare inc**  
i) What is the organization address along with city, country, state/province and postal  
code?

Answer = **Address: 101 Townsend Street**

**City: San Francisco**

**StateProv: CA**

**PostalCode: 94107**

**Country: US**  
j) What is organizon’s phone and email address? Answer = **abuse@cloudflare.com**

A screenshot of a computer

AI-generated content may be incorrect.

**Activity 3: Traceroute tool**  
• Perform a traceroute for the domain. Record your findings and any interesting data about the route.  
Hint: If traceroute is not installed then first type these commands:  
♣ sudo apt update  
♣ sudo apt install traceroute  
• Type the following command in terminal at Kali Linux:  
o sudo traceroute -I [www.cira.caA screenshot of a computer

AI-generated content may be incorrect.](http://www.cira.ca)

NOTE: The -I option instructs traceroute to use ICMP ECHO packets, which are blocked less frequently, and can usually give you faster results.  
Based on traceroute output:  
k) identify that who is the company’s ISP? Dyn.295.ca  
l) What is the geographic location of the company? Canada

**Activity 4: theHarvester tool**  
• Kali users only—use theHarvester to gather search engine information, including emails for  
the domain.  
o theHarvester -d microsoft.com -b google  
m) Take the screen shot and explain what information is publicly exposed?  
NOTE: -d: Domain to search or company name.  
-b: Data source: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus,  
google-profiles, linkedin, pgp, twitter, vhost, yahoo, al

A screenshot of a computer screen

AI-generated content may be incorrect.

Activity 5: Exploring Shodan  
In this lab, you will use the Shodan and Censyssys search engines to gather information about an organization. Pick an organization that you are familiar with for this exercise.  
• Visit www.shodan.io and search for the main domain for the organization you have selected.

You may use facebook.com for this activity.  
a) Review the results and identify how many unique results you have.  
b) Record the URL or IP address for one or more interesting hosts. If you do not find anything  
interesting, select another domain to test.  
• Using the URLs or IP addresses that you identified, visit censys.io and search for them.  
c) Identify what differences you see between the two search engines. How would this influence  
your use of each?

**Shodan** finds exposed servers, ports, and vulnerabilities.

**Censys** searches for in-depth SSL/TLS certificate and domain analysis.

How could the information be useful as part of an OSINT gathering  
exercise?

Answers: Used to reveal open ports and subdomains.  
d) Return to Shodan and click Explore. Select one of the top voted or featured categories, and explore systems listed there. What types of issues can you identify from these listings?

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.