Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

LAB ASSIGNMENT NO:06

Aim: Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup, nikto, dmitry to gather information about networks and domain registrars.

Lab Outcome Attained: Explore the different network reconnaissance tools to gather information about networks.

Theory:

1. What is the important information that attackers look for using whois command and what attacks can be performed using this information?

Attackers can gather valuable information using the "whois" command, which retrieves domain registration and ownership details. The information obtained from a "whois" query includes domain names, registrant names, email addresses, phone numbers, registration dates, and more. While the "whois" command serves legitimate purposes, attackers can exploit the information it provides for various malicious activities:

1. Social Engineering: Attackers can use contact information obtained from "whois" to craft convincing phishing emails or phone calls, pretending to be domain registrants or administrators to gain trust and extract sensitive information.

2. Domain Hijacking: Attackers can identify domains nearing expiration, impersonate the registrant, and fraudulently renew the domain. They could then redirect traffic to malicious sites or demand a ransom to release control.

3. Identity Theft: Attackers can use publicly available contact information from "whois" to gather data for identity theft or fraud, including impersonating registrants or exploiting their personal information.

4. Exploiting Vulnerabilities: Attackers can analyze domain registration dates and other information to identify recently registered domains and then search for known vulnerabilities in the websites associated with those domains.

5. Reconnaissance: Attackers can gather information about an organization's infrastructure, contact information, and technology stack from "whois" results, aiding in subsequent attacks like network intrusion.

6. Blacklisting: Attackers can discover details about IP addresses associated with a domain, enabling them to check if those IPs are blacklisted due to malicious activities.

7. Social Media Targeting: Attackers can use "whois" details to search for the domain registrant's presence on social media platforms, gathering more information for crafting convincing social engineering attacks.

2. <u>How traceroute command works in order to trace the route of given host?</u>

The traceroute command is a network diagnostic tool that allows you to trace the route that packets take from your computer to a target host (server or IP address).
The traceroute command works as follows:

1. TTL (Time to Live) Field: When a packet is sent, it includes a TTL field in its IP header. The TTL value is initially set to a certain number, often starting at 1.
2. Sending Packets: The traceroute command sends packets with incrementing TTL values. The first packet has a TTL of 1, the second packet has a TTL of 2, and so on.
3. Router Behavior: As packets travel through routers, each router decrements the TTL value by 1. When the TTL reaches 0, the router discards the packet and sends an ICMP "Time Exceeded" message back to the sender.
4. ICMP Responses: When the sender receives an "Time Exceeded" message, it knows that the packet has reached the router with the current TTL value. This helps determine the IP address of that router.
5. Packet Round-Trip: The traceroute command measures the time taken for the packet to travel to the router and back. This provides an estimate of the delay (latency) experienced on that route.
6. Hops and Routes: By sending multiple packets with increasing TTL values, traceroute gathers information about each router along the path to the target host. Each router is known as a "hop."
7. Output: The traceroute command displays the list of routers (hops) along with their IP addresses, domain names (if available), and round-trip times. This output helps identify the route and the potential network delays.
8. Completion: The traceroute command completes when packets successfully reach the target host (or a specified maximum number of hops is reached) or when an error occurs due to network congestion or filtering.
9. Interpreting Results: By analyzing the output, you can identify the route taken by packets and any potential bottlenecks or delays. Longer round-trip times or high latencies may indicate network congestion or issues.

Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

3. Explain dig command with various options.
   The dig command is a powerful network administration tool used to query DNS (Domain Name System) servers to retrieve information about domain names, IP addresses, and DNS records. It's commonly used for troubleshooting network connectivity, diagnosing DNS issues, and retrieving DNS-related information.
   - Basic Query: dig example.com
   - Query a Specific DNS Server: dig example.com @8.8.8.8
   - Query a Specific DNS Server and Record Type: dig example.com MX @8.8.8.8
   - Reverse DNS Lookup: dig -x 8.8.8.8
   - Query Authoritative Nameservers: dig example.com NS

4. Explain any two vulnerabilities detected for the website that you have scanned using nikto. Which attacks are possible if these vulnerabilities are exploited?
   1. Cross-Site Scripting (XSS):
      - Vulnerability: XSS occurs when a web application allows untrusted data to be executed by a user's browser. Attackers inject malicious scripts into a website, which are then executed when other users visit the page.
      - Potential Attacks: Attackers can steal user session cookies, redirect users to malicious websites, deface websites, or perform phishing attacks by displaying fake login forms.
   2. SQL Injection:
      - Vulnerability: SQL injection occurs when an application fails to validate or sanitize user inputs before passing them to a SQL database. Attackers inject malicious SQL queries that can manipulate or extract data from the database.
      - Potential Attacks: Attackers can gain unauthorized access to sensitive information, modify or delete data in the database, and even execute administrative commands on the database server.

   These vulnerabilities highlight the importance of secure coding practices and ongoing security assessments. Regularly scanning websites using tools like Nikto can help identify and mitigate potential vulnerabilities before they can be exploited by attackers.

Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

5. Write commands for email harvesting and subdomain harvesting.

- Email Harvesting: `theharvester -d example.com -l 100 -b google`
- Subdomain Harvesting: `sublist3r -d example.com`

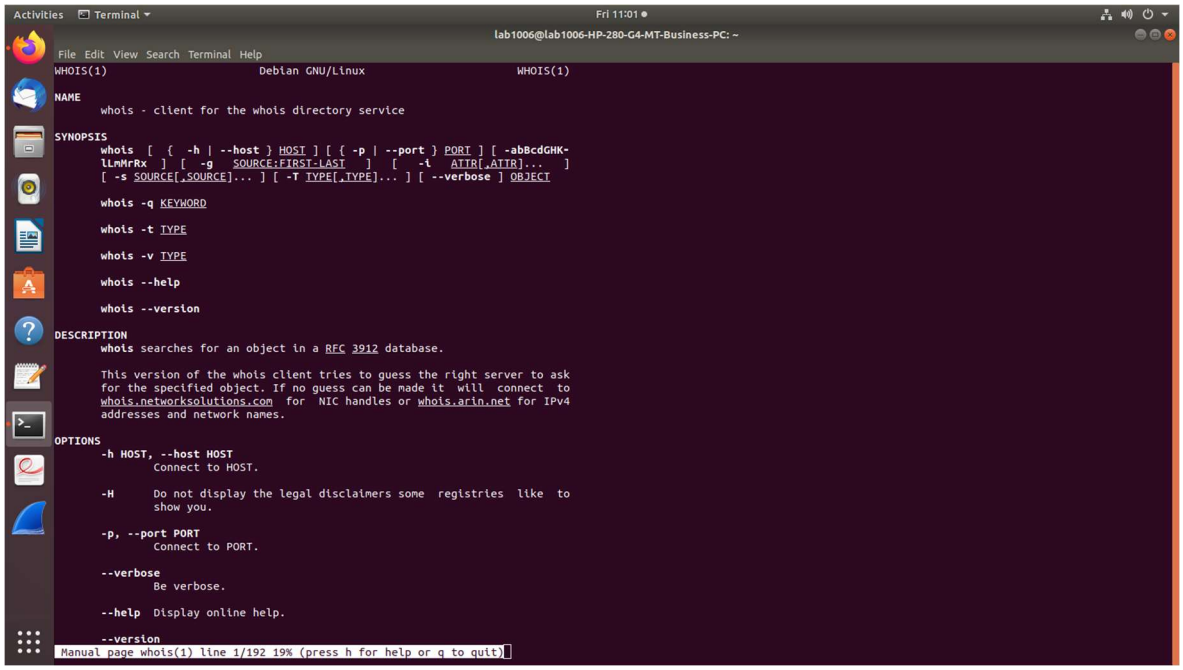
6. What are different functionalities provided by dimtry. Write Dmitry command for whois lookup, an IP whois lookup, retrieve Netcraft info, search for subdomains, search for email addresses, do a TCP port scan, and save the output to example.txt for the domain example.com

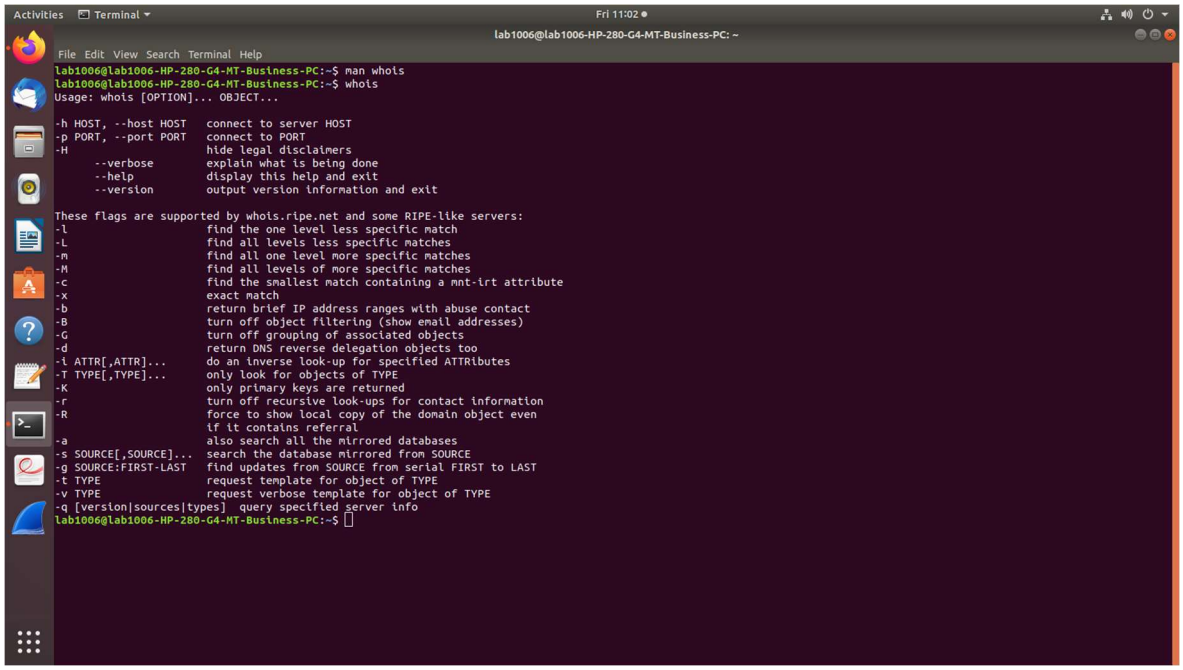
   Dmitry is a command-line tool for gathering information about a target domain. Here are some examples:

   - WHOIS Lookup: `dmitry -wn example.com`
   - IP WHOIS Lookup: `dmitry -wi 8.8.8.8`
   - Retrieve Netcraft Info: `dmitry -wne example.com`
   - Search for Subdomains: `dmitry -ws example.com`
   - Search for Email Addresses: `dmitry -we example.com`
   - TCP Port Scan: `dmitry -p example.com`
   - Save Output to File: `dmitry -o example.txt example.com`

Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

Output Screenshots:





Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

```
Activities  Terminal                    Fri 11:06
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...       do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.132
Name:   www.google.com
Address: 2404:6800:4009:82b::2004

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man traceroute
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tracerout www.google.com

Command 'tracerout' not found, did you mean:

  command 'traceroute' from deb inetutils-traceroute
  command 'traceroute' from deb traceroute

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute www.google.com
traceroute to www.google.com (142.250.192.132), 64 hops max
  1   192.168.0.1  0.689ms  0.555ms  0.573ms
  2   203.212.25.1  4.765ms  2.702ms  1.825ms
  3   203.212.24.53  2.952ms  1.908ms  1.047ms
  4   *
```

```
Activities  Terminal                    Fri 11:03
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
-R                     force to show local copy of the domain object even
                       if it contains referral
-a                     also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.132
Name:   www.google.com
Address: 2404:6800:4009:82b::2004

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

```
Activities  Terminal                    Fri 11:06
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...       do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.132
Name:   www.google.com
Address: 2404:6800:4009:82b::2004

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man traceroute
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tracerout www.google.com

Command 'tracerout' not found, did you mean:

  command 'traceroute' from deb inetutils-traceroute
  command 'traceroute' from deb traceroute

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute www.google.com
traceroute to www.google.com (142.250.192.132), 64 hops max
  1   192.168.0.1  0.689ms  0.555ms  0.573ms
  2   203.212.25.1  4.765ms  2.702ms  1.825ms
  3   203.212.24.53  2.952ms  1.908ms  1.047ms
  4   *  *  *
  5   72.14.196.213  2.900ms  2.900ms  2.481ms
  6   108.170.248.161  2.730ms  2.338ms  2.451ms
  7   142.250.238.81  2.346ms  1.970ms  2.057ms
  8   142.250.192.132  2.612ms  2.370ms  2.433ms
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

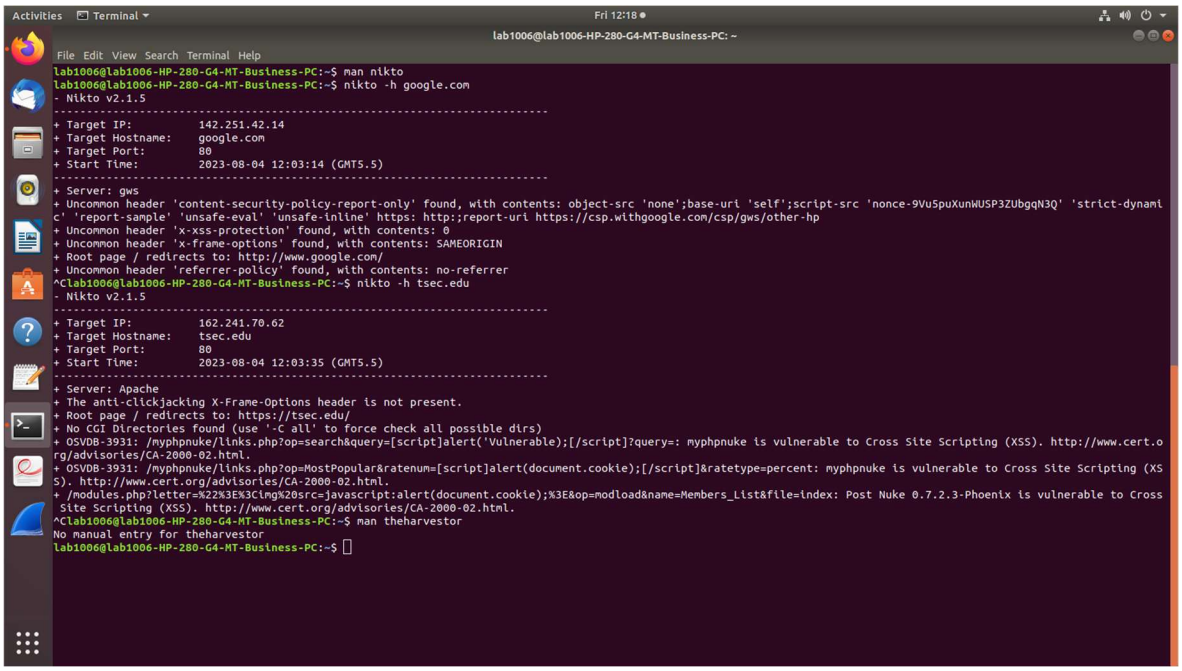
```
Activities  Terminal                    Fri 11:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-----------------------------------------------------------

Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        gtthampi@yahoo.com

Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        chetan.agarwal@thadomal.org

Name Servers:
        NS1.SALESUPP.IN
        NS2.SALESUPP.IN

Domain record activated:    22-Jan-2001
Domain record last updated: 03-Aug-2023
Domain expires:             31-Jul-2023
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023

```
Activities  Terminal                    Fri 11:20
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        gtthampi@yahoo.com

Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        chetan.agarwal@thadomal.org

Name Servers:
        NS1.SALESUPP.IN
        NS2.SALESUPP.IN

Domain record activated:    22-Jan-2001
Domain record last updated: 03-Aug-2023
Domain expires:             31-Jul-2023
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.132
Name:   www.google.com
Address: 2404:6800:4009:82b::2004

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute www.google.com
traceroute to www.google.com (142.250.192.132), 64 hops max
  1   192.168.0.1  0.648ms  0.543ms  1.108ms
  2   203.212.25.1  1.372ms  0.787ms  0.792ms
  3   203.212.24.53  1.247ms  1.331ms  0.889ms
  4   *  *  *
  5   72.14.196.213  2.618ms  2.224ms  2.105ms
  6   108.170.248.177  3.207ms  2.993ms  2.853ms
  7   172.253.50.147  2.692ms  2.394ms  1.907ms
  8   142.250.192.132  2.798ms  2.267ms  2.132ms
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
Activities  Terminal                    Fri 12:07
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man nikto
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h google.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          142.251.42.14
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2023-08-04 12:03:14 (GMT5.5)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'content-security-policy-report-only' found, with contents: object-src 'none';base-uri 'self';script-src 'nonce-9Vu5puXunWUSP3ZUbgqN3Q' 'strict-dynami
c' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Root page / redirects to: http://www.google.com/
+ Uncommon header 'referrer-policy' found, with contents: no-referrer
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h tsec.edu
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          162.241.70.62
+ Target Hostname:    tsec.edu
+ Target Port:        80
+ Start Time:         2023-08-04 12:03:35 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Roll No: 09
Name: Shreya Bagade
Date: 04/08/2023



```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man nikto
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h google.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          142.251.42.14
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2023-08-04 12:03:14 (GMT5.5)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'content-security-policy-report-only' found, with contents: object-src 'none';base-uri 'self';script-src 'nonce-9Vu5puXunWUSP3ZUbgqN3Q' 'strict-dynami
c' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Root page / redirects to: http://www.google.com/
+ Uncommon header 'referrer-policy' found, with contents: no-referrer
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h tsec.edu
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          162.241.70.62
+ Target Hostname:    tsec.edu
+ Target Port:        80
+ Start Time:         2023-08-04 12:03:35 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3931: /myphpnuke/links.php?op=search&query=[script]alert('Vulnerable');[/script]?query=: myphpnuke is vulnerable to Cross Site Scripting (XSS). http://www.cert.o
rg/advisories/CA-2000-02.html.
+ OSVDB-3931: /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XS
S). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross
 Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man theharvestor
No manual entry for theharvestor
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Conclusion: The experiment focused on network reconnaissance tools provided valuable insights into the methods and techniques used by attackers to gather information about potential targets. The experiment underscored the importance of network administrators and security professionals being vigilant and proactive in safeguarding their systems. By using similar tools in a controlled and ethical environment, participants gained a deeper understanding of the vulnerabilities and potential attack vectors that malicious actors may exploit.