Roll Number:- 2105048
Name:-Manav Jain
Date:- 02/08/2023

Lab Assignment No:-6

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 :- LO3

Theory:-

What is the critical information that attackers seek when using the whois command, and what attacks can be carried out using this information?

The whois command is a powerful tool that can be used **to gather information about domain names, IP addresses, and network devices.** This information can be valuable to attackers, who can use it to perform a **variety of attacks,** including:

Attackers can exploit the registrant information obtained from a whois lookup to target individuals or organizations with social engineering attacks. They might, for example, send phishing emails or phone calls appearing to be from the registrant in order to deceive the victim into disclosing sensitive information.
DNS assaults: DNS attacks, such as DNS spoofing and DNS cache poisoning, can be carried out using the name servers listed in a whois lookup. These attacks can cause traffic to be redirected to malicious websites or servers, as well as interrupt legitimate websites and services. Attackers can track the physical location of a domain or website by using the IP

addresses listed in a whois lookup. This information can be used to launch targeted attacks, or to gather intelligence about a target organization.

Fraudulent domain registration: Attackers can use the whois command to register domains that are similar to the names of legitimate businesses or organizations. This can be used to trick users into visiting malicious websites or to impersonate the legitimate business or organization.

How does the traceroute command operate to trace the route of a specified host?

The traceroute command communicates with the destination host by delivering Internet Control Message Protocol (ICMP) packets with the Time to Live (TTL) field set to a low value. The TTL field specifies how long a packet can stay in a network before being discarded.

When a router receives an ICMP packet with a TTL of 1, it decrements the TTL value by one before forwarding the message to the next hop in the route to the target host. If the TTL value hits 0 before the packet arrives at the destination host, the router will return an ICMP "Time Exceeded" message to the source host.

The traceroute command delivers a sequence of ICMP packets with progressively longer TTL values. The traceroute command will record the IP address of the router that sent the "Time Exceeded" message for each packet. This data is used to generate a list of the hops the packet took to reach the destination host.

Traceroute can also be used to calculate the round-trip time (RTT) for each hop. The RTT is the amount of time it takes for a packet to go from the source to the destination and back. The RTT can be used to identify possible network bottlenecks.

Explain dig command with various options.

The dig command is used to search for Domain Name System (DNS) servers. It can be used to seek for a domain name's IP address, the hostname of an IP address, and other DNS records.

The dig command has a number of options that can be used to customize the query. Some of the most common options include:

-t: The type of DNS record to query. The most common types are A (IP address), MX (mail exchange), NS (name server), and SOA (start of authority).
-c: The class of DNS record to query. The most common class is IN (Internet).
-q: The domain name or IP address to query.
-x: The hexadecimal value of the query type. This option is used to query for non-standard DNS record types.
-p: The port number of the DNS server to query. The default port number is 53.
-v: Verbose output. This option will print additional information about the query, such as the time it took to complete and the name servers that were queried.

example of how the dig command can be used to lookup the IP address of the Google homepage:

dig google.com

This command will **query the DNS server for the IP address of the Google homepage. The output of the command will show the IP address of the Google homepage, along with other information about the query, such as the time it took to complete and the name servers that were queried.**

Explain any two vulnerabilities discovered for the website you scanned with nikto. What types of attacks are conceivable if these flaws are exploited?

vulnerabilities that can be detected for a website using Nikto:

Directory indexing: It is a security flaw that allows unauthorized users to read the contents of a directory on a web server. Attackers can use this to find sensitive files such as configuration files or source code.

Outdated software: Outdated software is a security weakness that allows attackers to exploit known software vulnerabilities. Because many firms do not keep their software up to date, this is a prevalent vulnerability.

If these vulnerabilities are exploited, attackers can perform a **variety of attacks,** including:

File disclosure: Attackers can use directory indexing to view the contents of a directory on a web server, including sensitive files such as configuration files or source code. This information can be used to launch other attacks, such as gaining access to the web server or stealing sensitive data.
Remote code execution: In order to run arbitrary code on a web server, attackers can use outdated software. This gives attackers complete control of the web server, allowing them to steal data, install malware, or launch denial-of-service assaults.
Cross-site scripting (XSS): Attackers can insert harmful code into a web page by using obsolete software. Unsuspecting users may be fooled into supplying sensitive information or clicking on malicious sites if this code is executed.

Write commands for email harvesting and subdomain harvesting.

theHarvester is a neat information-gathering tool used by both ethical and non-ethical hackers to scrape up emails, subdomains, hosts, employee names, open ports, and banners from different public sources like popular search engines, PGP key servers, and the Shodan database.

Eg:**theharvester -d microsoft.com -b pgp**, searches for e-mail accounts for the
domain
microsoft.com in a PGP server

theharvester -d theguardian.com -b pgp.
This command will tell theHarvester to search for email accounts with the domain name “theguardian.com” in a pgp server, which is used for encrypting emails.

Other options in theharvestor command are :options:
-h, --help show this help
message and exit
-d DOMAIN, --domain DOMAIN
Company name or domain to search.
-l LIMIT, --limit LIMIT
Limit the number of search results, default=500.
-S START, --start START
Start with result number X, default=0.

-p, --proxies
Use proxies for requests, enter proxies in
proxies.yaml.
-s, --shodan
Use Shodan to query discovered hosts.
--screenshot SCREENSHOT
Take screenshots of resolved domains specify output
directory: --screenshot output_directory
-v, --virtual-host
Verify host name via DNS resolution and search for
virtual hosts.
-e DNS_SERVER, --dns-server DNS_SERVER
DNS server to use for lookup.
-t, --take-over
Check for takeovers.
-r [DNS_RESOLVE], --dns-resolve [DNS_RESOLVE]
Perform DNS resolution on subdomains with a resolver
list or passed in resolvers, default False.
-n, --dns-lookup
Enable DNS server lookup, default False.
-c, --dns-brute
Perform a DNS brute force on the domain.
-f FILENAME, --filename FILENAME
Save the results to an XML and JSON file.
-b SOURCE, --source SOURCE
anubis, baidu, bevigil, binaryedge, bing, bingapi,
bufferoverun, brave, censys, certspotter, criminalip,
crtsh, dnsdumpster, duckduckgo, fullhunt, github-code,
hackertarget, hunter, hunterhow, intelx, otx,
pentesttools, projectdiscovery, rapiddns, rocketreach,
securityTrails, sitedossier, subdomainfinderc99,
threatminer, urlscan, virustotal, yahoo, zoomeye

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

In Linux, the dmitry command is a command-line tool for gathering information about a computer's hardware. It can be used to determine the computer's make and model, CPU type, memory capacity, hard drive size, and other details.

The dmitry command is a helpful tool for troubleshooting hardware issues. For example, if your computer's memory is acting up, you can use dmitry to determine the type of memory it is using. This information can then be utilized to locate and purchase the appropriate new memory.

Whois lookup :dmitry -i example.txt example.com

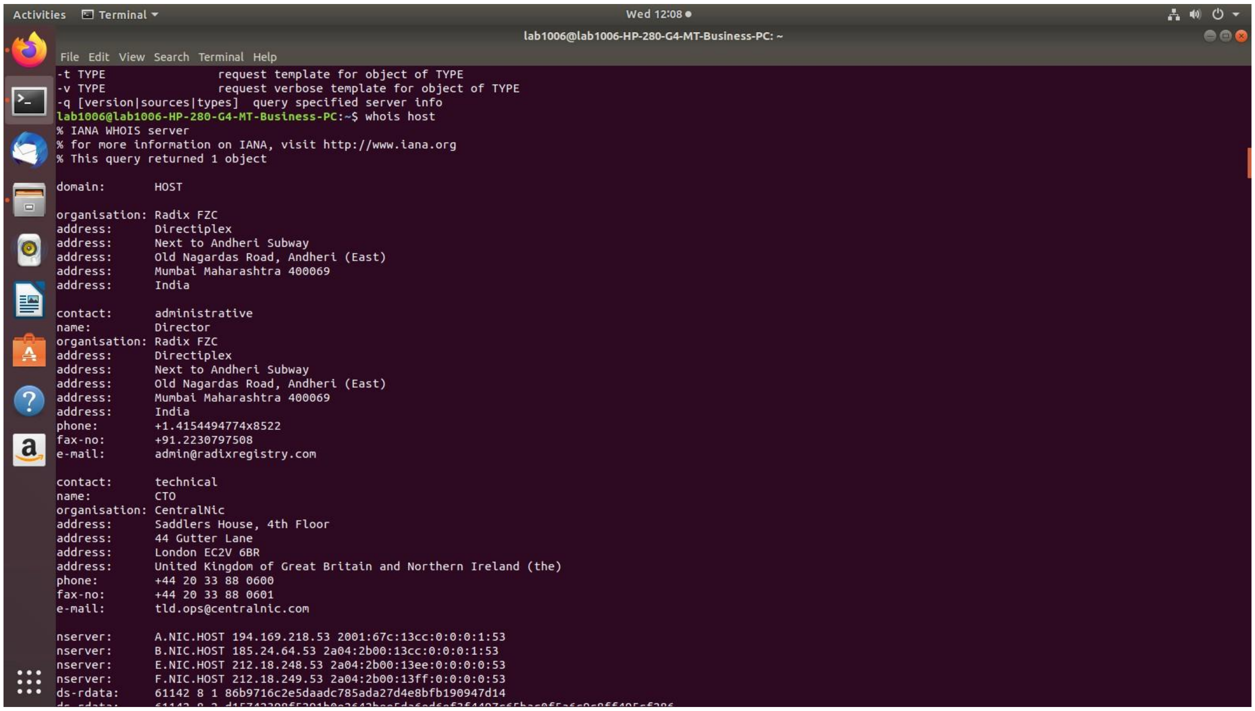
Retrieve netcraft info :dmitry -n example.txt example.com

Search for subdomain :dmitry -s example.txt example.com

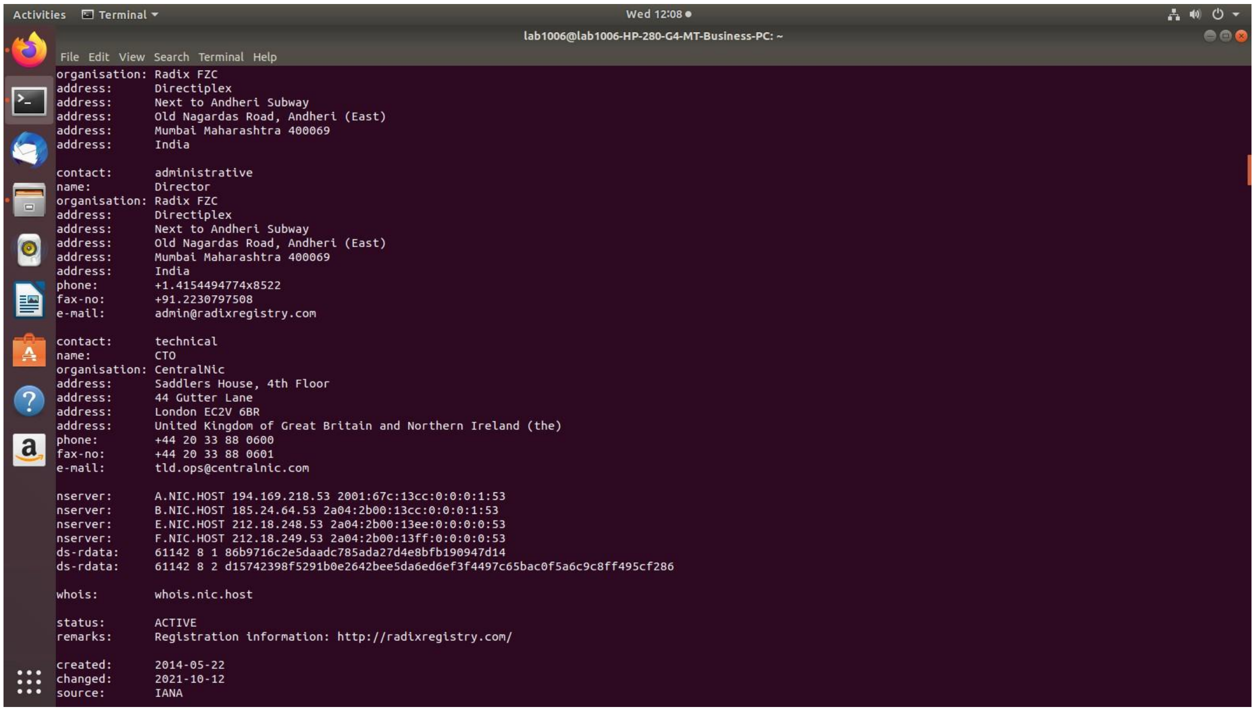
Search for email addresses :dmitry -e example.txt example.com

Do a TCP port scan :dmitry -p example.txt example.com

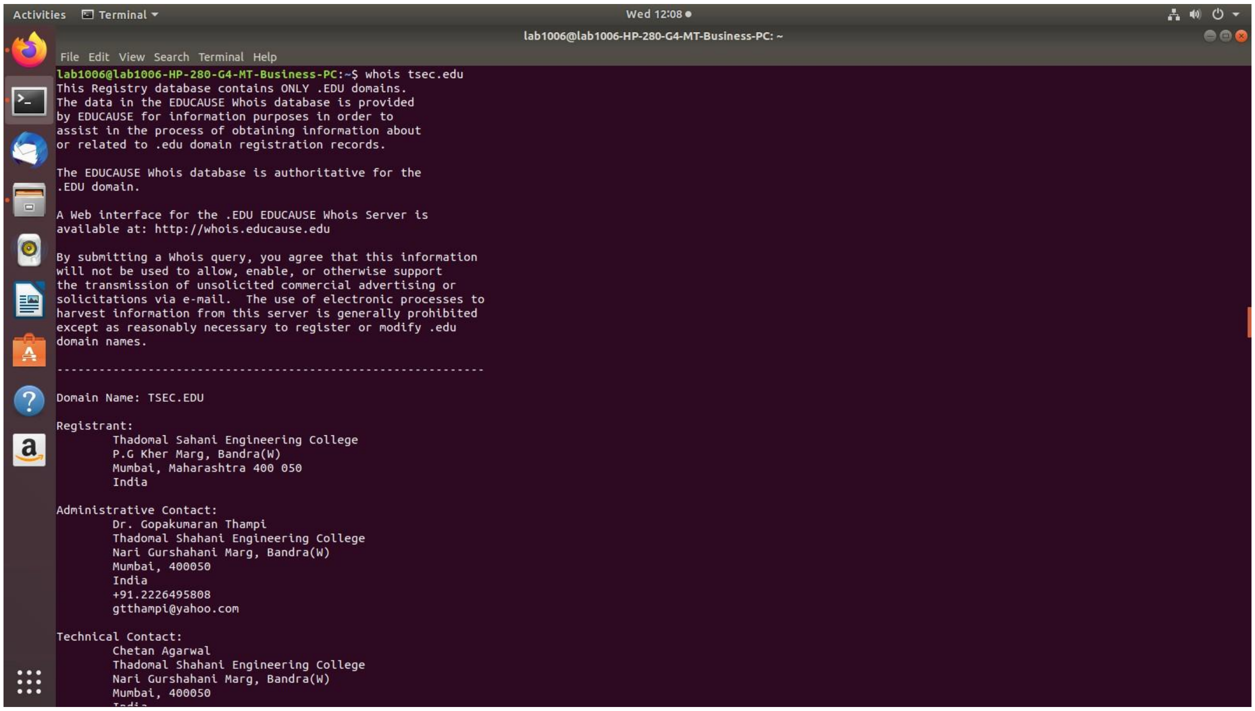
Output Screenshot:-


Activities
Terminal
Wed 12:08
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

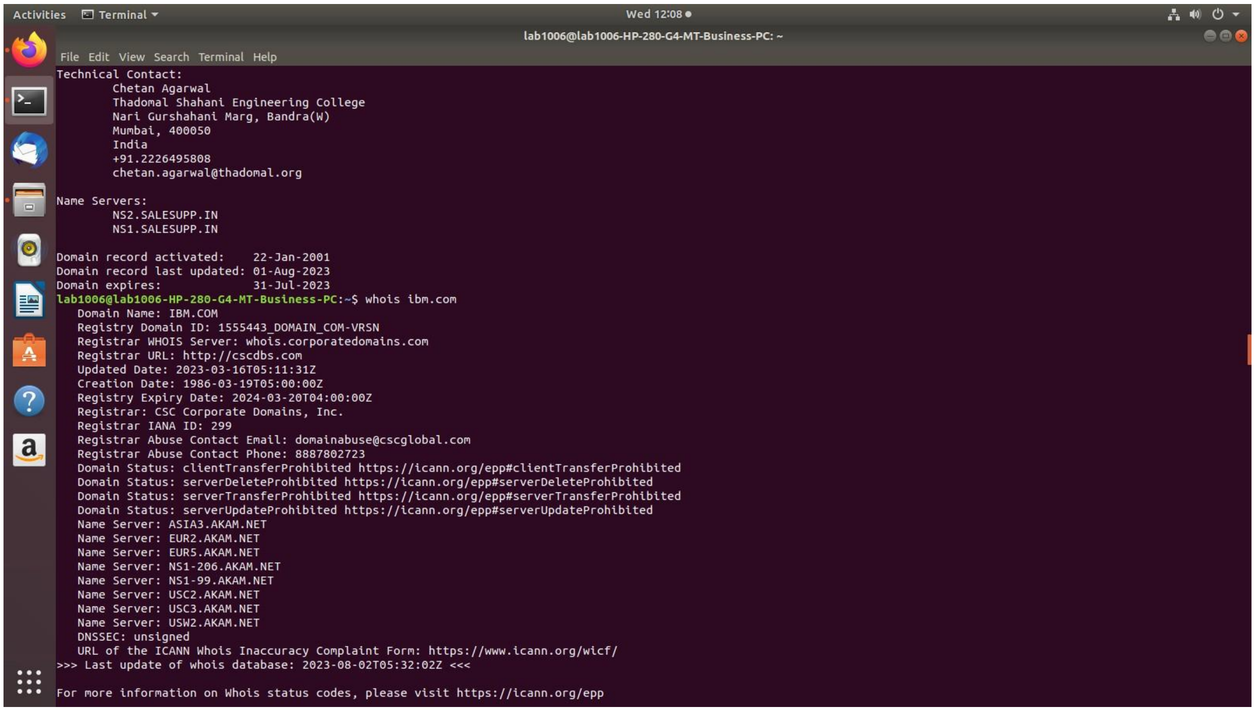
```
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ whois host
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       HOST

organisation: Radix FZC
address:      Directiplex
address:      Next to Andheri Subway
address:      Old Nagardas Road, Andheri (East)
address:      Mumbai Maharashtra 400069
address:      India

contact:      administrative
name:         Director
organisation: Radix FZC
address:      Directiplex
address:      Next to Andheri Subway
address:      Old Nagardas Road, Andheri (East)
address:      Mumbai Maharashtra 400069
address:      India
phone:        +1.4154494774x8522
fax-no:       +91.2230797508
e-mail:       admin@radixregistry.com

contact:      technical
name:         CTO
organisation: CentralNic
address:      Saddlers House, 4th Floor
address:      44 Gutter Lane
address:      London EC2V 6BR
address:      United Kingdom of Great Britain and Northern Ireland (the)
phone:        +44 20 33 88 0600
fax-no:       +44 20 33 88 0601
e-mail:       tld.ops@centralnic.com

nserver:      A.NIC.HOST 194.169.218.53 2001:67c:13cc:0:0:0:1:53
nserver:      B.NIC.HOST 185.24.64.53 2a04:2b00:13cc:0:0:0:1:53
nserver:      E.NIC.HOST 212.18.248.53 2a04:2b00:13ee:0:0:0:0:53
nserver:      F.NIC.HOST 212.18.249.53 2a04:2b00:13ff:0:0:0:0:53
ds-rdata:     61142 8 1 86b9716c2e5daadc785ada27d4e8bfb190947d14
ds-rdata:     61142 8 2 d15742398f5291b0e3643bee5da6ed6ef3f4497c65bac0f5a6c9c8ff405cf286
```



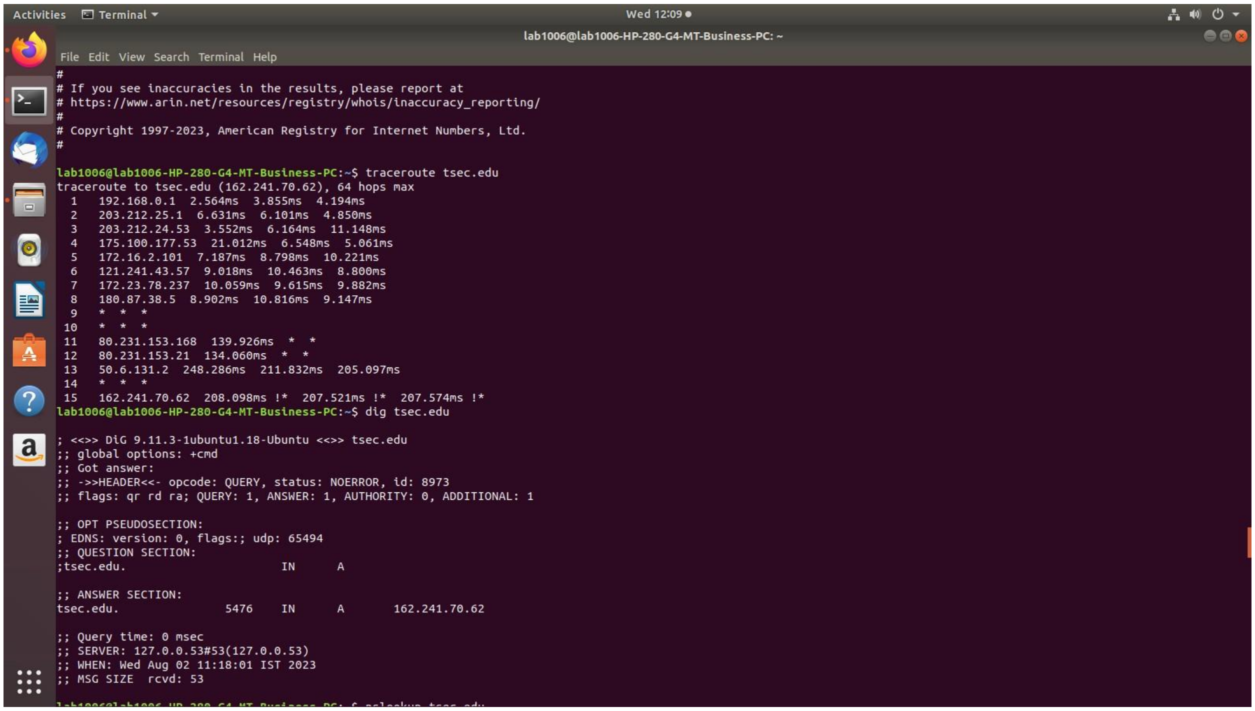
```
organisation: Radix FZC
address:      Directiplex
address:      Next to Andheri Subway
address:      Old Nagardas Road, Andheri (East)
address:      Mumbai Maharashtra 400069
address:      India

contact:      administrative
name:         Director
organisation: Radix FZC
address:      Directiplex
address:      Next to Andheri Subway
address:      Old Nagardas Road, Andheri (East)
address:      Mumbai Maharashtra 400069
address:      India
phone:        +1.4154494774x8522
fax-no:       +91.2230797508
e-mail:       admin@radixregistry.com

contact:      technical
name:         CTO
organisation: CentralNic
address:      Saddlers House, 4th Floor
address:      44 Gutter Lane
address:      London EC2V 6BR
address:      United Kingdom of Great Britain and Northern Ireland (the)
phone:        +44 20 33 88 0600
fax-no:       +44 20 33 88 0601
e-mail:       tld.ops@centralnic.com

nserver:      A.NIC.HOST 194.169.218.53 2001:67c:13cc:0:0:0:1:53
nserver:      B.NIC.HOST 185.24.64.53 2a04:2b00:13cc:0:0:0:1:53
nserver:      E.NIC.HOST 212.18.248.53 2a04:2b00:13ee:0:0:0:0:53
nserver:      F.NIC.HOST 212.18.249.53 2a04:2b00:13ff:0:0:0:0:53
ds-rdata:     61142 8 1 86b9716c2e5daadc785ada27d4e8bfb190947d14
ds-rdata:     61142 8 2 d15742398f5291b0e2642bee5da6ed6ef3f4497c65bac0f5a6c9c8ff495cf286

whois:        whois.nic.host

status:       ACTIVE
remarks:      Registration information: http://radixregistry.com/

created:      2014-05-22
changed:      2021-10-12
source:       IANA
```



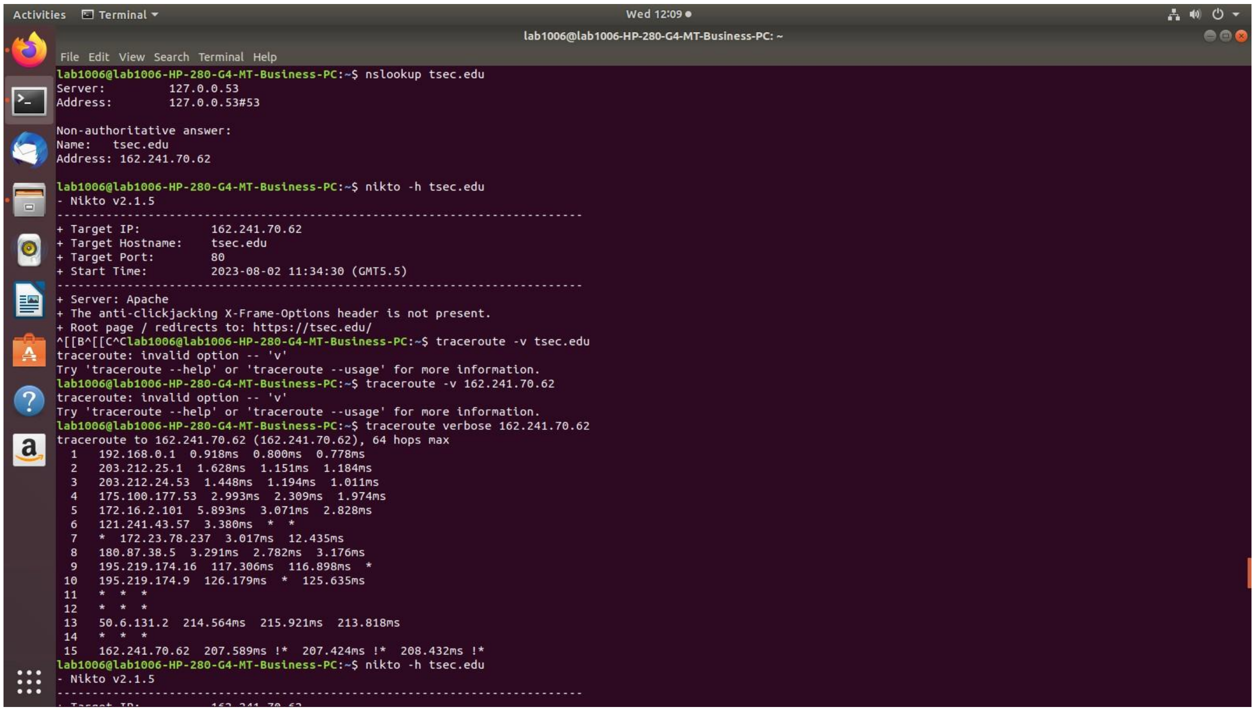
```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

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
```


Activities
Terminal
Wed 12:08
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

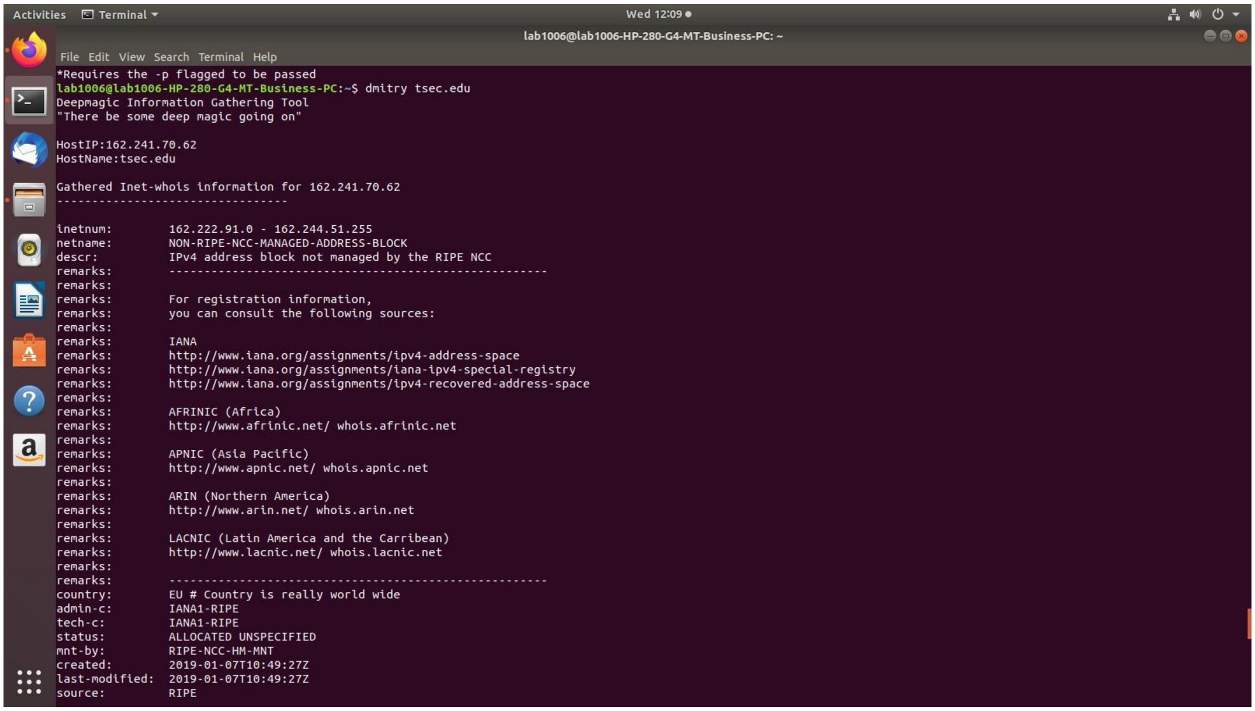
```
Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        chetan.agarwal@thadomal.org

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

Domain record activated:    22-Jan-2001
Domain record last updated: 01-Aug-2023
Domain expires:             31-Jul-2023
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ whois ibm.com
   Domain Name: IBM.COM
   Registry Domain ID: 1555443_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2023-03-16T05:11:31Z
   Creation Date: 1986-03-19T05:00:00Z
   Registry Expiry Date: 2024-03-20T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   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: ASIA3.AKAM.NET
   Name Server: EUR2.AKAM.NET
   Name Server: EUR5.AKAM.NET
   Name Server: NS1-206.AKAM.NET
   Name Server: NS1-99.AKAM.NET
   Name Server: USC2.AKAM.NET
   Name Server: USC3.AKAM.NET
   Name Server: USW2.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-02T05:32:02Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```


Activities
Terminal
Wed 12:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

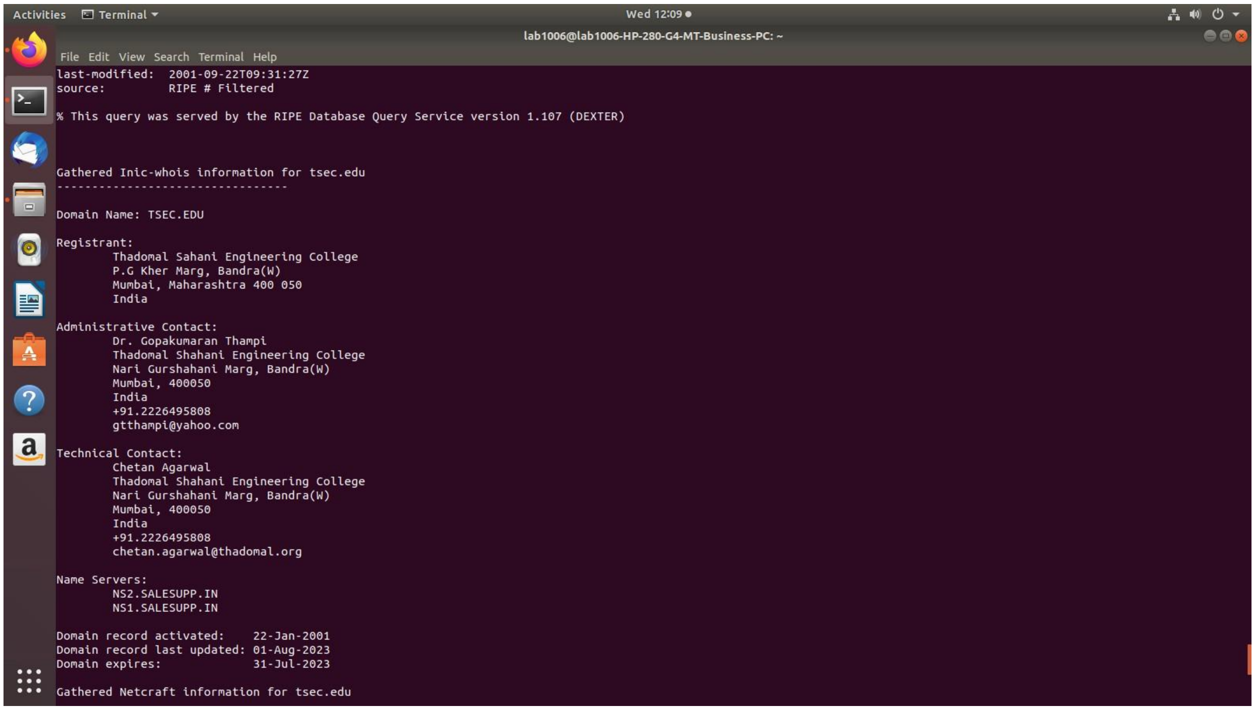
```
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute tsec.edu
traceroute to tsec.edu (162.241.70.62), 64 hops max
  1   192.168.0.1  2.564ms  3.855ms  4.194ms
  2   203.212.25.1  6.631ms  6.101ms  4.850ms
  3   203.212.24.53  3.552ms  6.164ms  11.148ms
  4   175.100.177.53  21.012ms  6.548ms  5.061ms
  5   172.16.2.101  7.187ms  8.798ms  10.221ms
  6   121.241.43.57  9.018ms  10.463ms  8.800ms
  7   172.23.78.237  10.059ms  9.615ms  9.882ms
  8   180.87.38.5  8.902ms  10.816ms  9.147ms
  9   *  *  *
 10   *  *  *
 11   80.231.153.168  139.926ms  *  *
 12   80.231.153.21  134.060ms  *  *
 13   50.6.131.2  248.286ms  211.832ms  205.097ms
 14   *  *  *
 15   162.241.70.62  208.098ms !*  207.521ms !*  207.574ms !*
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig tsec.edu

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> tsec.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8973
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;tsec.edu.                      IN      A

;; ANSWER SECTION:
tsec.edu.               5476    IN      A       162.241.70.62

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Aug 02 11:18:01 IST 2023
;; MSG SIZE  rcvd: 53

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup tsec.edu
```


Activities
Terminal
Wed 12:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

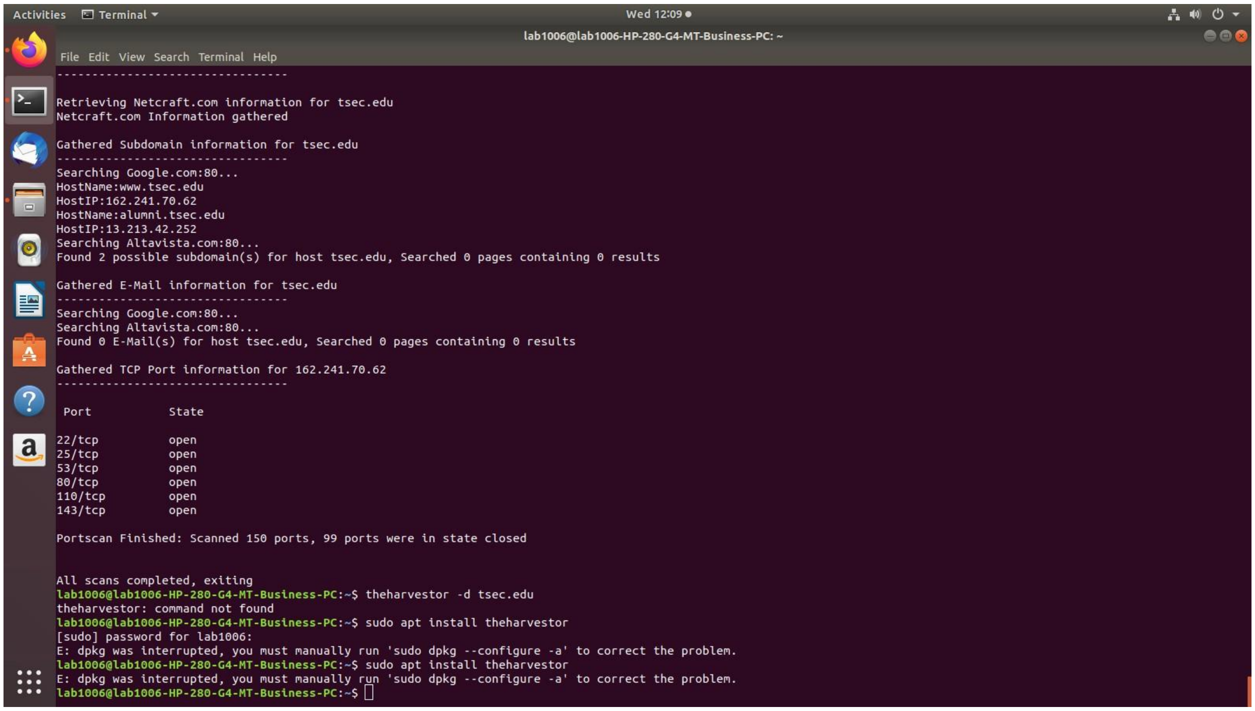
```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup tsec.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   tsec.edu
Address: 162.241.70.62

lab1006@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:         2023-08-02 11:34:30 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
^[[B^[[C^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute -v tsec.edu
traceroute: invalid option -- 'v'
Try 'traceroute --help' or 'traceroute --usage' for more information.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute -v 162.241.70.62
traceroute: invalid option -- 'v'
Try 'traceroute --help' or 'traceroute --usage' for more information.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute verbose 162.241.70.62
traceroute to 162.241.70.62 (162.241.70.62), 64 hops max
  1   192.168.0.1  0.918ms  0.800ms  0.778ms
  2   203.212.25.1  1.628ms  1.151ms  1.184ms
  3   203.212.24.53  1.448ms  1.194ms  1.011ms
  4   175.100.177.53  2.993ms  2.309ms  1.974ms
  5   172.16.2.101  5.893ms  3.071ms  2.828ms
  6   121.241.43.57  3.380ms  *  *
  7   *  172.23.78.237  3.017ms  12.435ms
  8   180.87.38.5  3.291ms  2.782ms  3.176ms
  9   195.219.174.16  117.306ms  116.898ms  *
 10   195.219.174.9  126.179ms  *  125.635ms
 11   *  *  *
 12   *  *  *
 13   50.6.131.2  214.564ms  215.921ms  213.818ms
 14   *  *  *
 15   162.241.70.62  207.589ms !*  207.424ms !*  208.432ms !*
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h tsec.edu
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          162.241.70.62
```


Activities
Terminal
Wed 12:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
*Requires the -p flagged to be passed
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dmitry tsec.edu
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:162.241.70.62
HostName:tsec.edu

Gathered Inet-whois information for 162.241.70.62
---------------------------------

inetnum:        162.222.91.0 - 162.244.51.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-01-07T10:49:27Z
last-modified:  2019-01-07T10:49:27Z
source:         RIPE
```


Activities
Terminal
Wed 12:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.107 (DEXTER)



Gathered Inic-whois information for tsec.edu
---------------------------------

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:
        NS2.SALESUPP.IN
        NS1.SALESUPP.IN

Domain record activated:    22-Jan-2001
Domain record last updated: 01-Aug-2023
Domain expires:             31-Jul-2023

Gathered Netcraft information for tsec.edu
```


Activities
Terminal
Wed 12:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
---------------------------------

Retrieving Netcraft.com information for tsec.edu
Netcraft.com Information gathered

Gathered Subdomain information for tsec.edu
---------------------------------
Searching Google.com:80...
HostName:www.tsec.edu
HostIP:162.241.70.62
HostName:alumni.tsec.edu
HostIP:13.213.42.252
Searching Altavista.com:80...
Found 2 possible subdomain(s) for host tsec.edu, Searched 0 pages containing 0 results

Gathered E-Mail information for tsec.edu
---------------------------------
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host tsec.edu, Searched 0 pages containing 0 results

Gathered TCP Port information for 162.241.70.62
---------------------------------

 Port           State

22/tcp          open
25/tcp          open
53/tcp          open
80/tcp          open
110/tcp         open
143/tcp         open

Portscan Finished: Scanned 150 ports, 99 ports were in state closed


All scans completed, exiting
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ theharvestor -d tsec.edu
theharvestor: command not found
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo apt install theharvestor
[sudo] password for lab1006:
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo apt install theharvestor
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 
```

Conclusion:-

Studied and investigated numerous network reconnaissance tools such as WHOIS, dig, traceroute, nslookup, nikto, dmitry, and obtained information and insights on network and domain registrars.