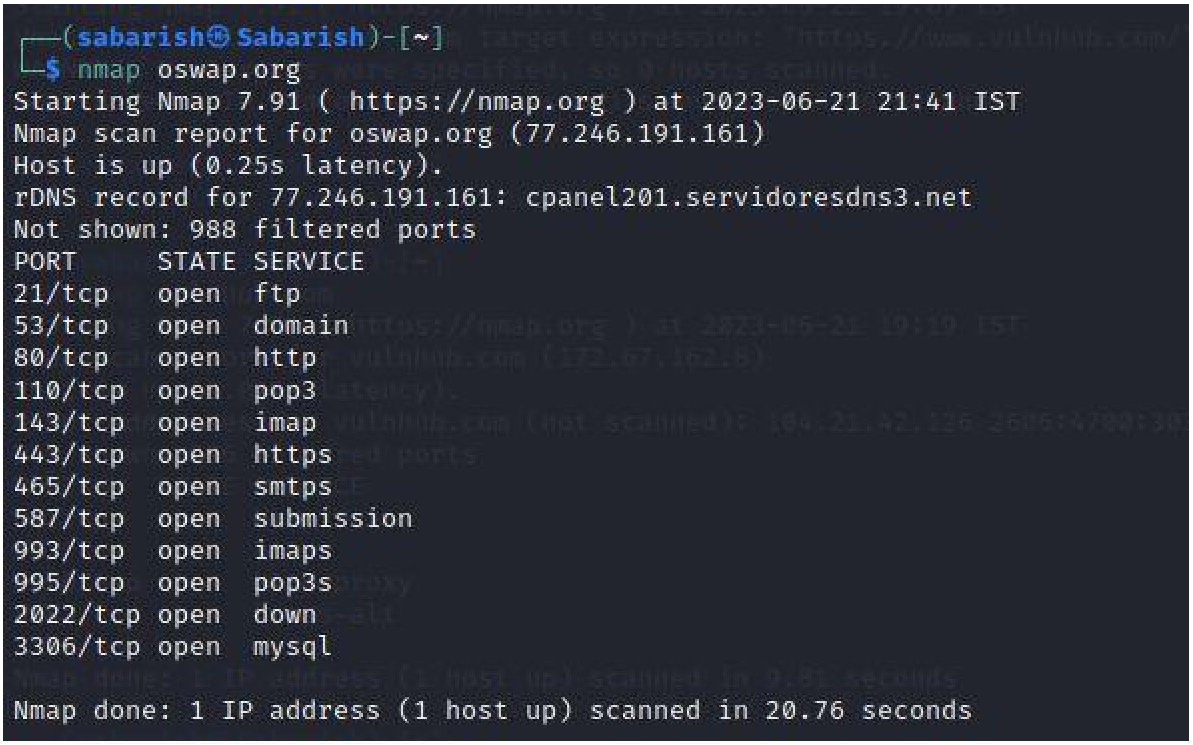
Team no : 2.13

Date:26-06-23

Team members:

Yerramsetty Sai Naga Sabarish-20BCE2370
Jayasree N -20MIS0370
Satya Harika- 20BKT0131
Nikitha AR-20MIA1025

TARGET WEBSITE: Owasp.org



```
┌──(sabarish㉿Sabarish)-[~]
└─$ nmap oswap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-21 21:41 IST
Nmap scan report for oswap.org (77.246.191.161)
Host is up (0.25s latency).
rDNS record for 77.246.191.161: cpanel201.servidoresdns3.net
Not shown: 988 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2022/tcp open  down
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 20.76 seconds
```

OPEN PORTS:

1. **FTP:** FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and a server on a computer network. By default, FTP uses two ports:
    - port 21 for control and port 20 for data transfer. Here are the details of these two ports:Port 21 (Control Port): This port is used for sending commands and receiving responses between the FTP client and server. It handles the control flow of the FTP session, including authentication, file listing, and commands for file transfer.

- Port 20 (Data Transfer Port): This port is used for the actual transfer of data files between the FTP client and server. When a file transfer request is made, the data channel is established on port 20 to transfer the file content.

2. **HTTP** (Hypertext Transfer Protocol) is the primary protocol used for transmitting data over the World Wide Web. It operates over TCP (Transmission Control Protocol) and typically uses port 80 for communication. Here are the details of an open HTTP port:

   - Port 80 (Default HTTP Port): This port is the default port for serving HTTP traffic. When a client makes an HTTP request to a server, it establishes a connection on port 80 to send the request and receive the response. The server listens on this port for incoming HTTP connections.

3. **Pop3** (Post office protocol version 3),which is a widely used Internet protocol that email clients utilise to get email from a mail server. Users can download their email from the server to local devices using this TCP/IP-based system.

   - Port 110 (Default Pop3 port): This is associated with the Post Office Protocol version 3 (POP3), used for email retrieval from a mail server. It operates over TCP/IP and listens for incoming POP3 requests. While considered an older email protocol, it may still be used by some mail servers and clients for accessing email messages.

4. **IMAPS** (Internet Message Access Protocol over SSL) is a secure protocol used for retrieving email messages from a remote mail server. It operates over TCP and typically uses port 993 for communication. Here are the details of an open IMAPS port:

   - Port 993 (Default IMAPS Port): This port is the default port for establishing a secure IMAP connection using SSL/TLS encryption. When a client connects to an email server over IMAPS, it establishes a connection on port 993 to securely retrieve email messages.

5. **SMTPS** (Simple Mail Transfer Protocol Secure) is a secure version of the SMTP protocol used for sending email messages. It operates over TCP and typically uses port 465 for communication. Here are the details of an open SMTPS port:

   - Port 465 (Default SMTPS Port): This port is the default port for establishing a secure SMTP connection using SSL/TLS encryption. When a client wants to send an email using SMTPS, it establishes a connection on port 465 to securely communicate with the mail server.SMTPS provides enhanced security by encrypting the communication between the email client and the mail server, protecting the integrity and confidentiality of the email content, as well as any sensitive information, such as usernames and passwords.

6. **Submission port** is an alternative SMTP (Simple Mail Transfer Protocol) port used for email submission by mail clients. It is primarily designed for email clients to send outgoing mail to mail servers.

    - Port 587 is commonly used with encryption and authentication mechanisms, ensuring secure transmission of email messages. It helps prevent issues related to ISP blocking of port 25, the default SMTP port.

7. **Pop3s** (Post Office Protocol version 3 Secure) is an extension of POP3 that adds encryption and security features to the protocol. It operates over a secure SSL/TLS connection.

    - Port 995: It is commonly used for retrieving email messages securely from a mail server. By default, POP3 over port 995 ensures that data transmitted between the mail client and server is encrypted, adding an extra layer of security.

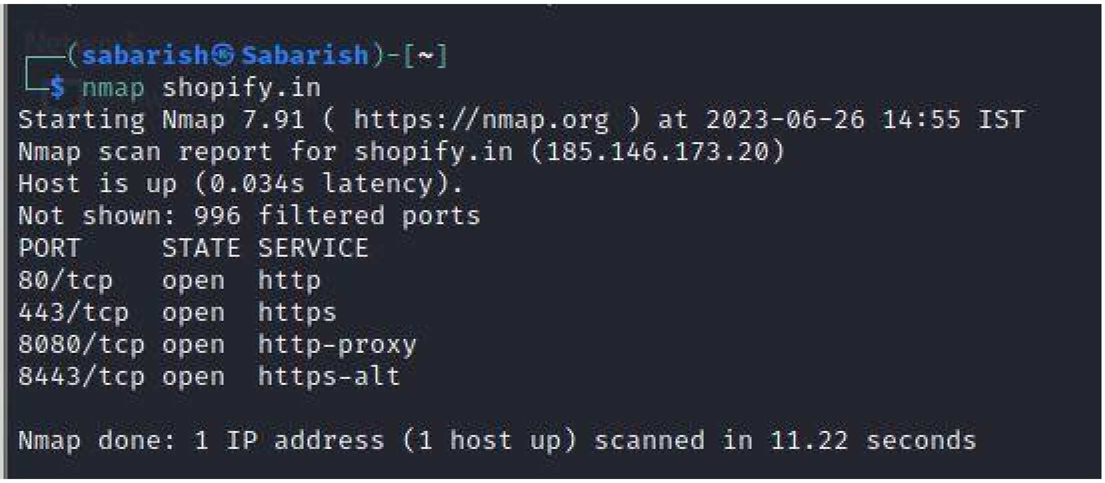
8. **Down :** When a port is reported as "down," it means that there is no service actively listening on that port.

    - Port 2022: An open port status on port 2022 may indicate that there is no service running or listening on that specific port. This could be intentional, as the port might be unused or reserved for future use, or it could be due to a misconfiguration or firewall blocking the port.

9. **Mysql: It** is typically associated with the MySQL database management system. It allows communication between clients and the MySQL server for database operations. It's crucial to secure this port by implementing proper authentication mechanisms and firewall rules to protect against unauthorized access and potential vulnerabilities. Regular security updates and best practices should be followed to ensure the integrity and confidentiality of the MySQL database.

    - Port 3306 is commonly used for MySQL, a popular open-source database management system.It's important to secure this port to prevent unauthorized access and protect the confidentiality and integrity of the database.

MAIN WEBSITE : shopify.in



```
┌──(sabarish㉿Sabarish)-[~]
└─$ nmap shopify.in
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-26 14:55 IST
Nmap scan report for shopify.in (185.146.173.20)
Host is up (0.034s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
```

1. OPEN PORTS:

1. **HTTP** (Hypertext Transfer Protocol) is the primary protocol used for transmitting data over the World Wide Web. It operates over TCP (Transmission Control Protocol) and typically uses port 80 for communication. Here are the details of an open HTTP port:

- Port 80 (Default HTTP Port): This port is the default port for serving HTTP traffic. When a client makes an HTTP request to a server, it establishes a connection on port 80 to send the request and receive the response. The server listens on this port for incoming HTTP connections.

2. **HTTPS** (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol used for secure communication over the internet. It operates over TCP and typically uses port 443 for communication. Here are the details of an open HTTPS port:

- Port 443 (Default HTTPS Port): This port is the default port for establishing secure HTTP connections. When a client wants to access a website or web application securely using HTTPS, it establishes a connection on port 443 to communicate with the server.

3. **HTTP** proxy is a type of proxy server that acts as an intermediary between a client and a web server. It allows clients to make HTTP requests to the proxy server, which then forwards those requests to the appropriate web server. Here are the details of an open HTTP proxy port:

- Port 8080 (Common HTTP Proxy Port): Port 8080 is a commonly used port for HTTP proxy servers. However, it's important to note that HTTP proxies can be configured to listen on various ports, depending on the server's configuration.

4. The port number 443 is typically associated with **HTTPS** (HTTP Secure), which is the secure version of the HTTP protocol. However, the term "https-alt" refers to an alternative port that can be used for HTTPS communication. The "https-alt" port number commonly used is 8443. Here are the details of an open "https-alt" port:

- Port 8443 (HTTPS-ALT): This port is an alternative port for secure HTTP communication. It is often used when the default HTTPS port 443 is already in use or when running multiple HTTPS services on the same server.

2. WHOIS COMMANDS

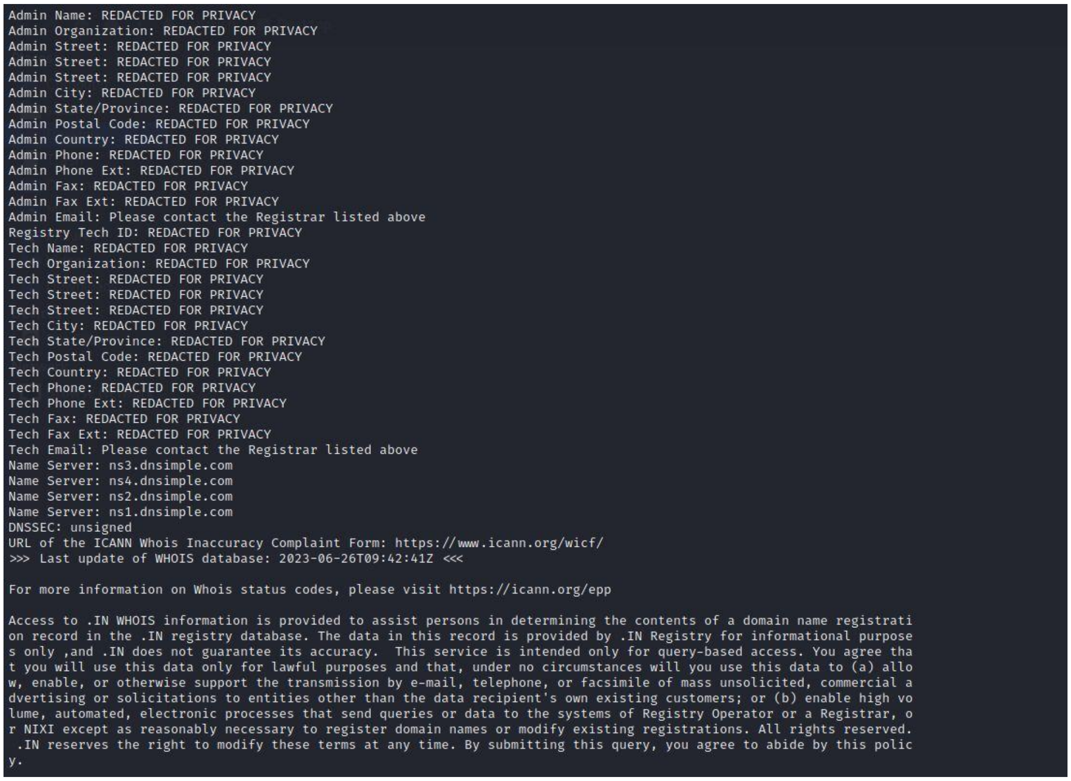
The WHOIS command is a widely used network utility that allows you to retrieve information about domain names, IP addresses, and various network resources. While WHOIS queries can be performed using various methods and tools, including online WHOIS lookup services or dedicated WHOIS command-line tools, here are some common WHOIS commands you can use in a terminal:

1. **Basic WHOIS Lookup:** whois domainname
   Replace "domainname" with the actual domain name you want to retrieve WHOIS information for. This command will display details such as the registrar, registration date, expiration date, and name servers associated with the domain.

2. **WHOIS for IP Address:** whois ipaddress
   Replace "ipaddress" with the IP address you want to look up. This command will provide information about the IP address range, allocation details, and contact information of the organization that owns the IP address.

3. **Verbose WHOIS Output:**whois -v domainname
   This command provides more detailed and comprehensive WHOIS information for the specified domain name, including administrative and technical contacts, DNS records, and more.

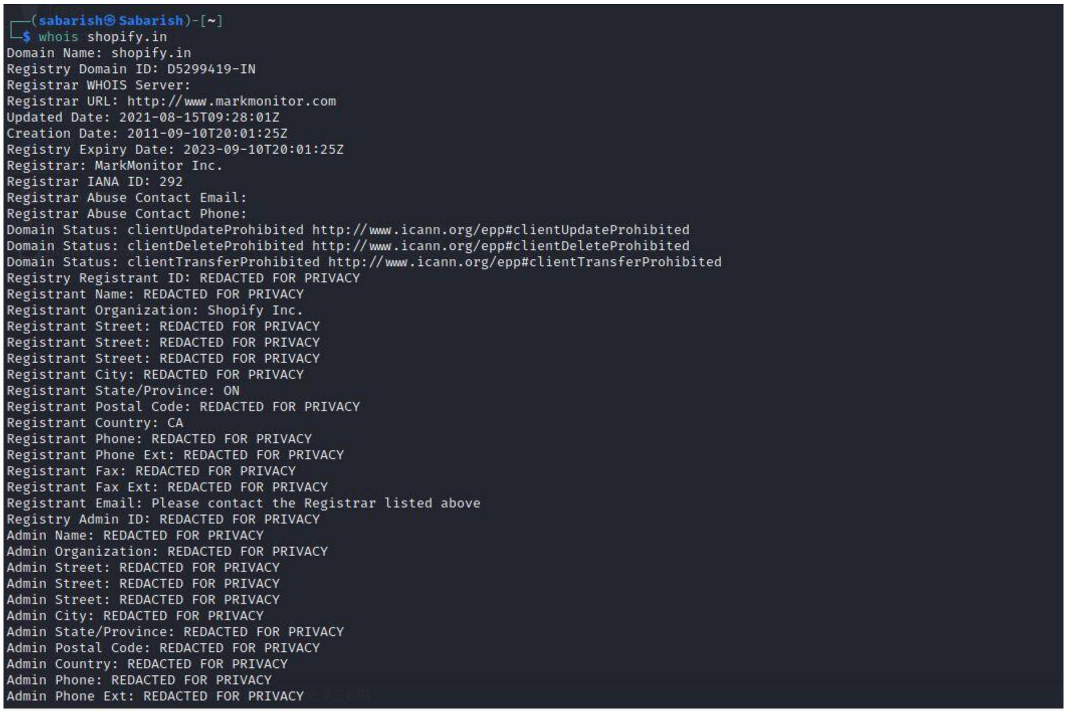
4. **WHOIS Server Override:**whois -h whois.example.com domainname
   Use this command to specify a specific WHOIS server to query instead of the default WHOIS server. Replace "whois.example.com" with the desired WHOIS server and "domainname" with the domain you want to look up.



```
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns3.dnsimple.com
Name Server: ns4.dnsimple.com
Name Server: ns2.dnsimple.com
Name Server: ns1.dnsimple.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-06-26T09:42:41Z <<<

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

Access to .IN WHOIS information is provided to assist persons in determining the contents of a domain name registrati
on record in the .IN registry database. The data in this record is provided by .IN Registry for informational purpose
s only ,and .IN does not guarantee its accuracy.  This service is intended only for query-based access. You agree tha
t you will use this data only for lawful purposes and that, under no circumstances will you use this data to (a) allo
w, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial a
dvertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high vo
lume, automated, electronic processes that send queries or data to the systems of Registry Operator or a Registrar, o
r NIXI except as reasonably necessary to register domain names or modify existing registrations. All rights reserved.
 .IN reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this polic
y.
```



```
┌──(sabarish㉿Sabarish)-[~]
└─$ whois shopify.in
Domain Name: shopify.in
Registry Domain ID: D5299419-IN
Registrar WHOIS Server:
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-08-15T09:28:01Z
Creation Date: 2011-09-10T20:01:25Z
Registry Expiry Date: 2023-09-10T20:01:25Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Shopify Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: ON
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CA
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
```

OUTPUT :

Name: shopify.in
Registry Domain ID: D5299419-IN
Registrar WHOIS Server:
Registrar URL: http://www.markmonitor.com

Important dates :
Updated Date: 2021-08-15T09:28:01Z
Creation Date: 2011-09-10T20:01:25Z
Registry Expiry Date: 2023-09-10T20:01:25Z

Registrar details:
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:

Domain status :
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited

Registrant details :
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Shopify Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: ON
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CA
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY

Admin details :
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY

Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above

Tech details:
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above

Name server details :
Name Server: ns3.dnsimple.com
Name Server: ns4.dnsimple.com
Name Server: ns2.dnsimple.com
Name Server: ns1.dnsimple.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-06-26T10:39:32Z <<<

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

SUMMARY:
Domain: shopify.in
- Creation Date: September 10, 2011
- Registrar: MarkMonitor Inc.
- Registrant: Shopify Inc. (based in Canada)

- Updated Date: August 15, 2021
- Domain Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
- Name Servers: ns1.dnsimple.com, ns2.dnsimple.com, ns3.dnsimple.com, ns4.dnsimple.com
-specific contact details have been redacted for privacy reasons. The domain is associated with Shopify Inc., a company that offers e-commerce solutions.

3. NSLOOKUP

The NSLOOKUP command is a network utility used to query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and related DNS records. It is available in most operating systems, including Windows, macOS, and Linux. Here are some common uses of the NSLOOKUP command:

1. **Basic DNS Lookup:** nslookup domainname
   Replace "domainname" with the actual domain name you want to look up. This command will display the corresponding IP address(es) associated with the domain.

2. **Reverse DNS Lookup** :nslookup IPaddress

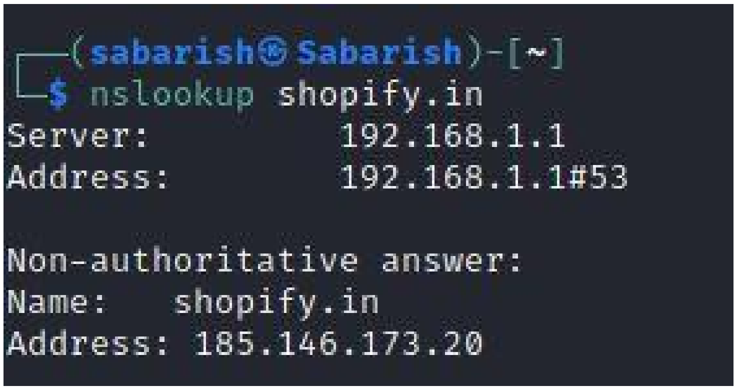
   Replace "IPaddress" with the IP address you want to perform a reverse DNS lookup on. This command will return the domain name associated with the given IP address.

3**. DNS Server Lookup:** nslookup

   Running the nslookup command without any arguments will open the interactive mode. From there, you can specify the DNS server you want to use for lookups by typing:
   server DNSserverIP

   Replace "DNSserverIP" with the IP address of the DNS server you want to use. Once set, subsequent queries will be directed to that DNS server.

4. **Query Specific DNS Record Types:** nslookup -type=recordtype domainname
   Replace "recordtype" with the specific DNS record type you want to query, such as A, MX, CNAME, TXT, etc. This command will return the records of the specified type associated with the domain.



```
┌──(sabarish㉿Sabarish)-[~]
└─$ nslookup shopify.in
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   shopify.in
Address: 185.146.173.20
```

OUTPUT :

```
nslookup shopify.in
Server:         192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   shopify.in
Address: 185.146.173.20
```

the command queried the DNS server at IP address 192.168.1.1 for the domain "shopify.in". The non-authoritative answer states that the corresponding IP address for "shopify.in" is 185.146.173.20.

5. DIG COMMAND :

The DIG command is a versatile DNS (Domain Name System) troubleshooting tool used to query DNS servers and retrieve DNS-related information. It is commonly used in command-line interfaces and is available on various operating systems, including Linux, macOS, and Windows (through third-party installations). Here are some common uses of the DIG command:

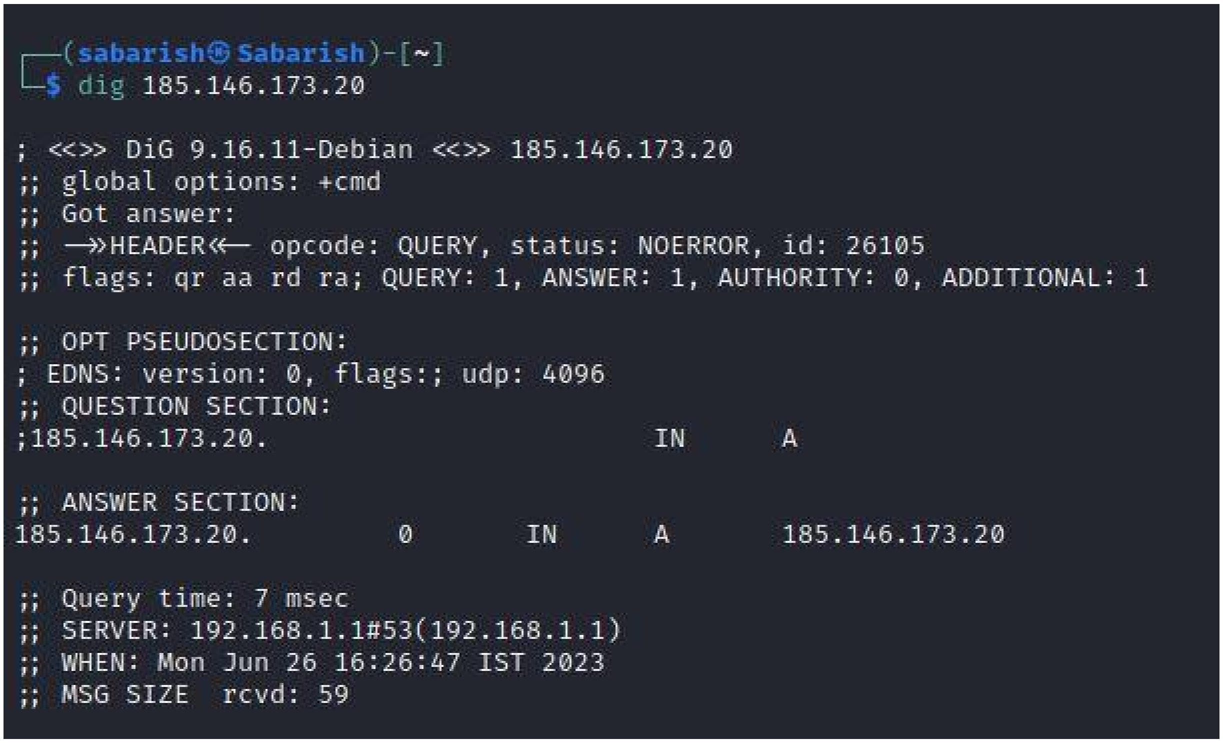
1. **Basic DNS Query:** dig domainname
Replace "domainname" with the actual domain name you want to query. This command will provide you with information such as the IP address(es) associated with the domain, the authoritative DNS servers, and additional DNS records.

2. **Query Specific DNS Record Type:** dig recordtype domainname
Replace "recordtype" with the specific DNS record type you want to query, such as A, MX, CNAME, TXT, etc. This command will return the records of the specified type associated with the domain.

3. **Query Specific DNS Server:** dig domainname @dnsserver
Replace "dnsserver" with the IP address or hostname of the DNS server you want to query. This command directs the DIG query to a specific DNS server for the domain.

4**. Reverse DNS Lookup**: dig -x IPaddress
Replace "IPaddress" with the IP address you want to perform a reverse DNS lookup on. This command will return the domain name associated with the given IP address.

5. **Display More Detailed Output:** dig +nocmd +noall +answer domainname
This command provides a more concise and focused output, displaying only the answer section of the DNS query results.



```
┌──(sabarish㉿Sabarish)-[~]
└─$ dig 185.146.173.20

; <<>> DiG 9.16.11-Debian <<>> 185.146.173.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26105
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;185.146.173.20.                        IN      A

;; ANSWER SECTION:
185.146.173.20.         0       IN      A       185.146.173.20

;; Query time: 7 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jun 26 16:26:47 IST 2023
;; MSG SIZE  rcvd: 59
```

```
dig 185.146.173.20

; <<>> DiG 9.16.11-Debian <<>> 185.146.173.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26105
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;185.146.173.20.                IN      A
```

```
;; ANSWER SECTION:
185.146.173.20.        0      IN     A      185.146.173.20

;; Query time: 7 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jun 26 16:26:47 IST 2023
;; MSG SIZE  rcvd: 59
```

SUMMARY:
The DIG command was used to query the IP address 185.146.173.20. The summary of the output is as follows:

- The query was successful (status: NOERROR) and received an authoritative answer.
- The answer section states that the IP address 185.146.173.20 has an A record associated with it.
- The query was made to the DNS server at IP address 192.168.1.1.
- The query time was 7 milliseconds.
- The response was received on Monday, June 26, 2023, at 16:26:47 IST.
- The size of the received message was 59 bytes.

Overall, the output confirms that the IP address 185.146.173.20 has a corresponding A record indicating the same IP address.