TEAM 2.3

Web Application Penetration Testing

TEAM MEMBERS

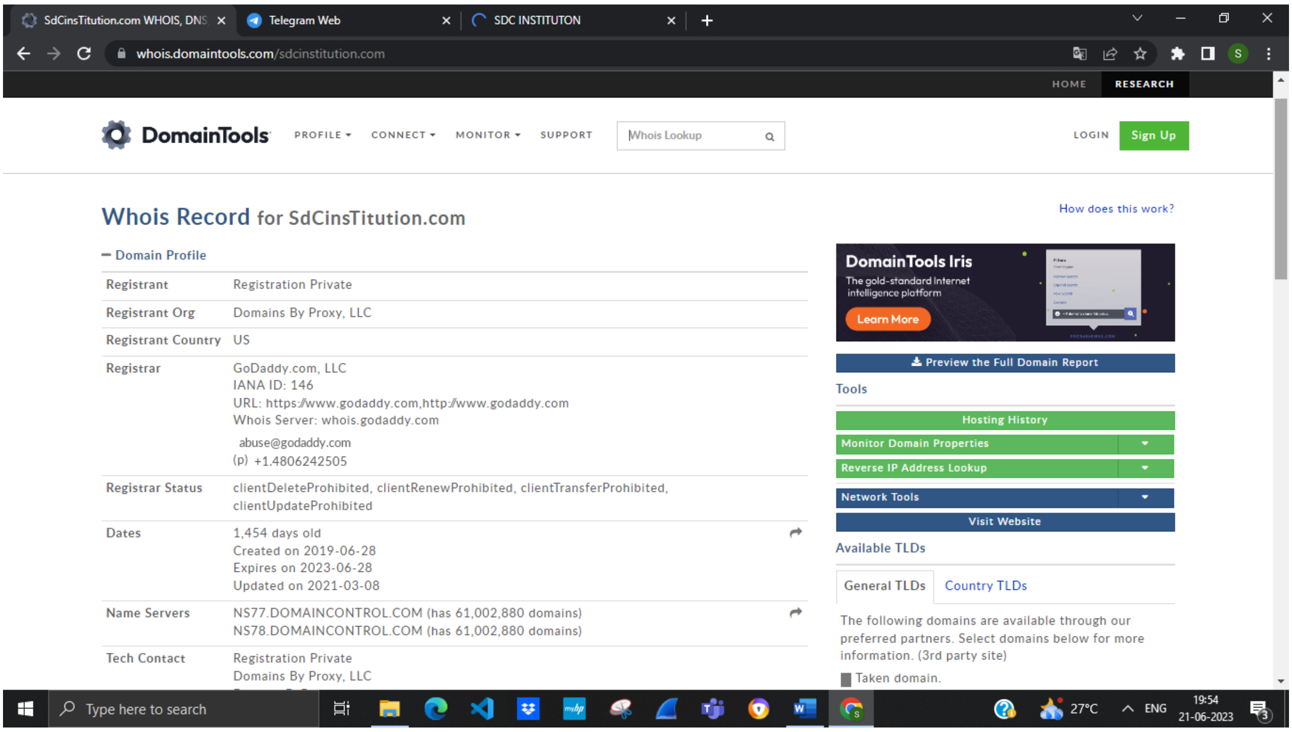
- **PRATHEESH KUMAR N - 20BCI0195**
- **SANDHIYA N - 20BCI0196**
- **MUKUNDHAN D - 20BCI0291**

Target/Main : www.sdcinstitution.com

1. Information Gathering Reconnaissance :

Passive Reconnaissance :

Tool used : whois



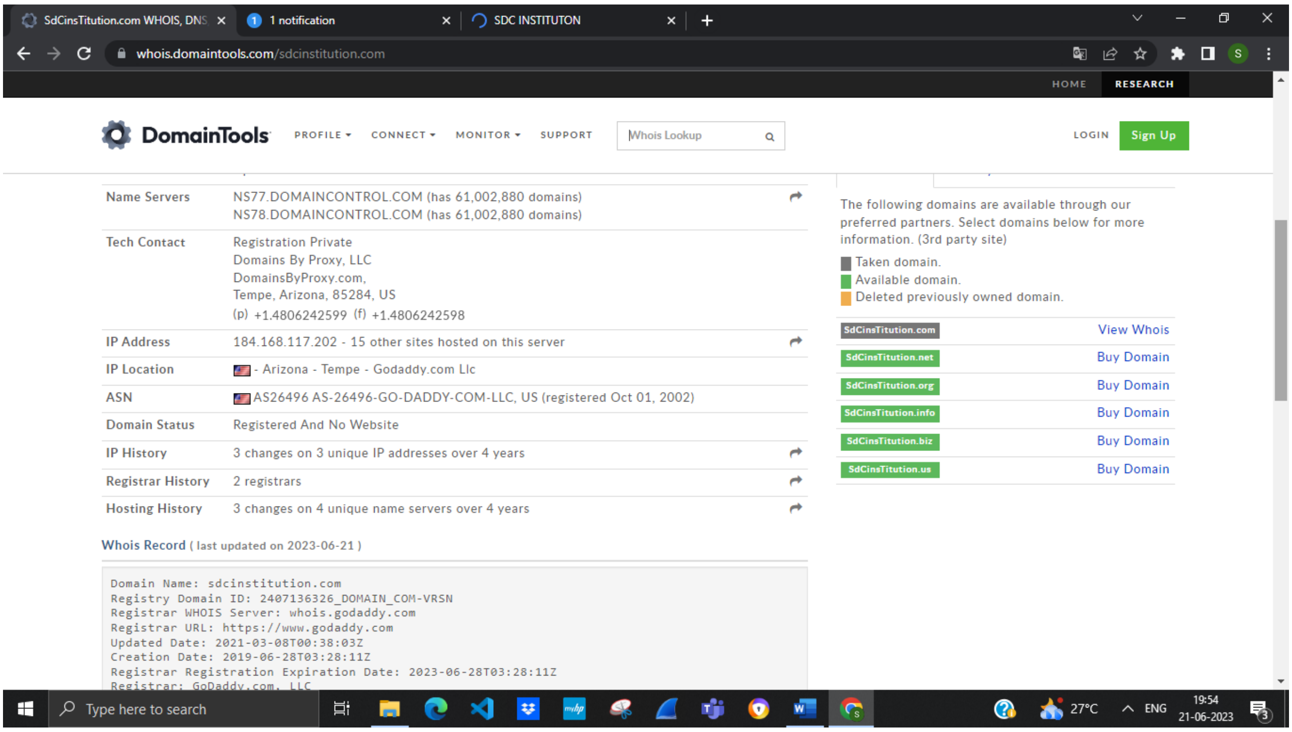
Whois Record for SdCinsTitution.com

– Domain Profile

Registrant	Registration Private
Registrant Org	Domains By Proxy, LLC
Registrant Country	US
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: https://www.godaddy.com,http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) +1.4806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	1,454 days old Created on 2019-06-28 Expires on 2023-06-28 Updated on 2021-03-08
Name Servers	NS77.DOMAINCONTROL.COM (has 61,002,880 domains) NS78.DOMAINCONTROL.COM (has 61,002,880 domains)
Tech Contact	Registration Private Domains By Proxy, LLC

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▆ Taken domain.



Name Servers	NS77.DOMAINCONTROL.COM (has 61,002,880 domains) NS78.DOMAINCONTROL.COM (has 61,002,880 domains)
Tech Contact	Registration Private Domains By Proxy, LLC DomainsByProxy.com, Tempe, Arizona, 85284, US (p) +1.4806242599 (f) +1.4806242598
IP Address	184.168.117.202 - 15 other sites hosted on this server
IP Location	- Arizona - Tempe - Godaddy.com Llc
ASN	AS26496 AS-26496-GO-DADDY-COM-LLC, US (registered Oct 01, 2002)
Domain Status	Registered And No Website
IP History	3 changes on 3 unique IP addresses over 4 years
Registrar History	2 registrars
Hosting History	3 changes on 4 unique name servers over 4 years

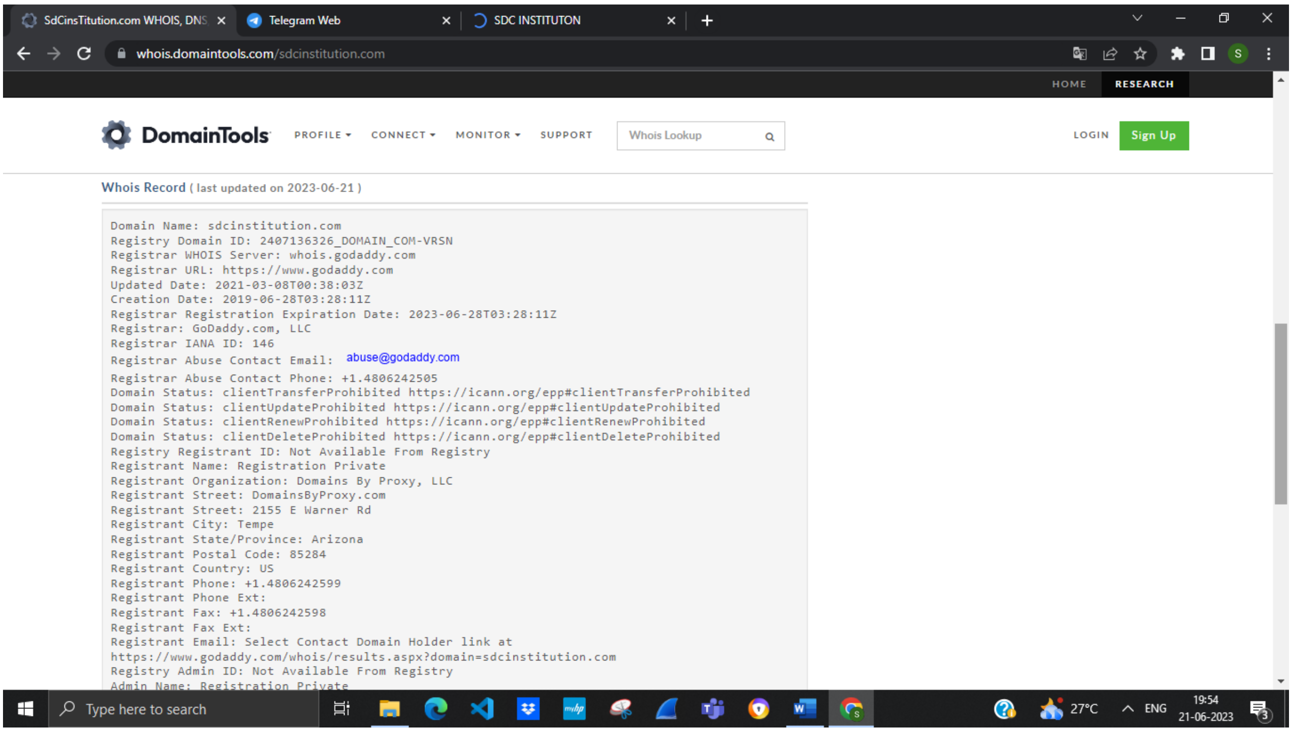
The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▇ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

SdCinsTitution.com	View Whois
SdCinsTitution.net	Buy Domain
SdCinsTitution.org	Buy Domain
SdCinsTitution.info	Buy Domain
SdCinsTitution.biz	Buy Domain
SdCinsTitution.us	Buy Domain

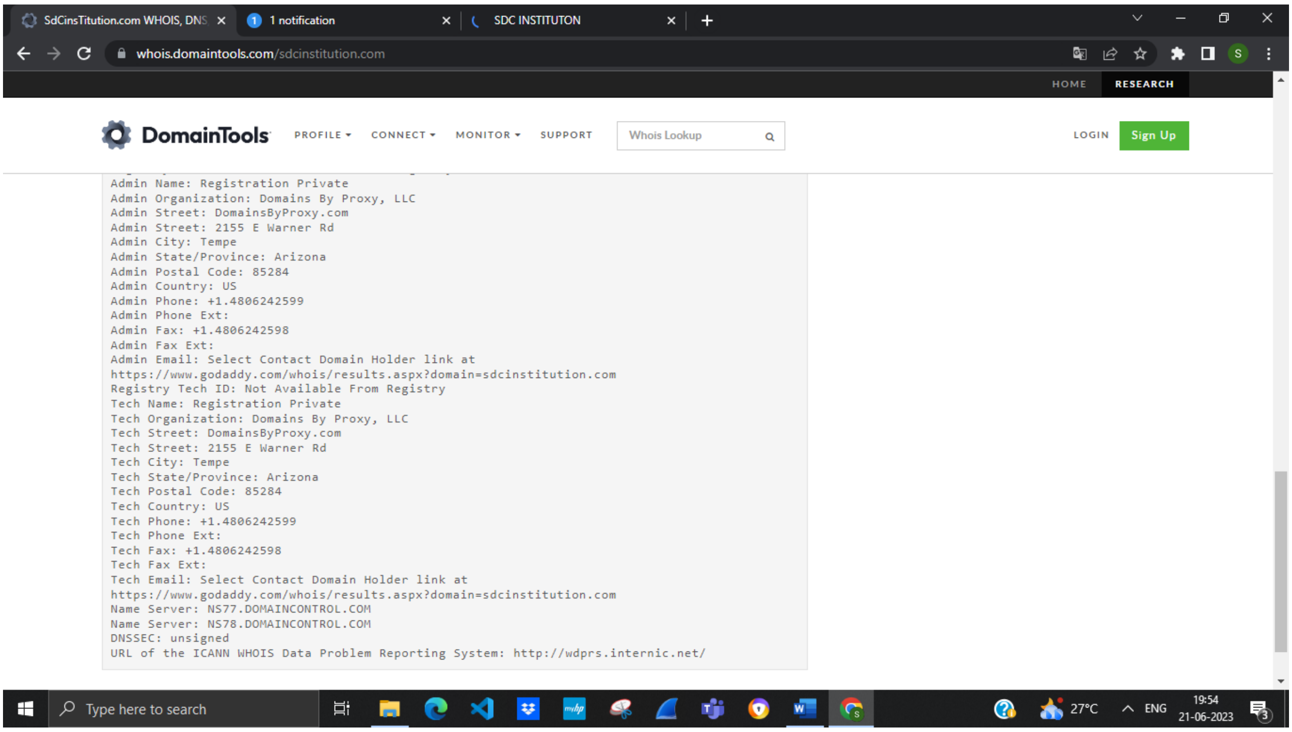
Whois Record (last updated on 2023-06-21)

```
Domain Name: sdcinstitution.com
Registry Domain ID: 2407136326_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2021-03-08T00:38:03Z
Creation Date: 2019-06-28T03:28:11Z
Registrar Registration Expiration Date: 2023-06-28T03:28:11Z
Registrar: GoDaddy.com, LLC
```



Whois Record (last updated on 2023-06-21)

```
Domain Name: sdcinstitution.com
Registry Domain ID: 2407136326_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2021-03-08T00:38:03Z
Creation Date: 2019-06-28T03:28:11Z
Registrar Registration Expiration Date: 2023-06-28T03:28:11Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:  abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=sdcinstitution.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
```



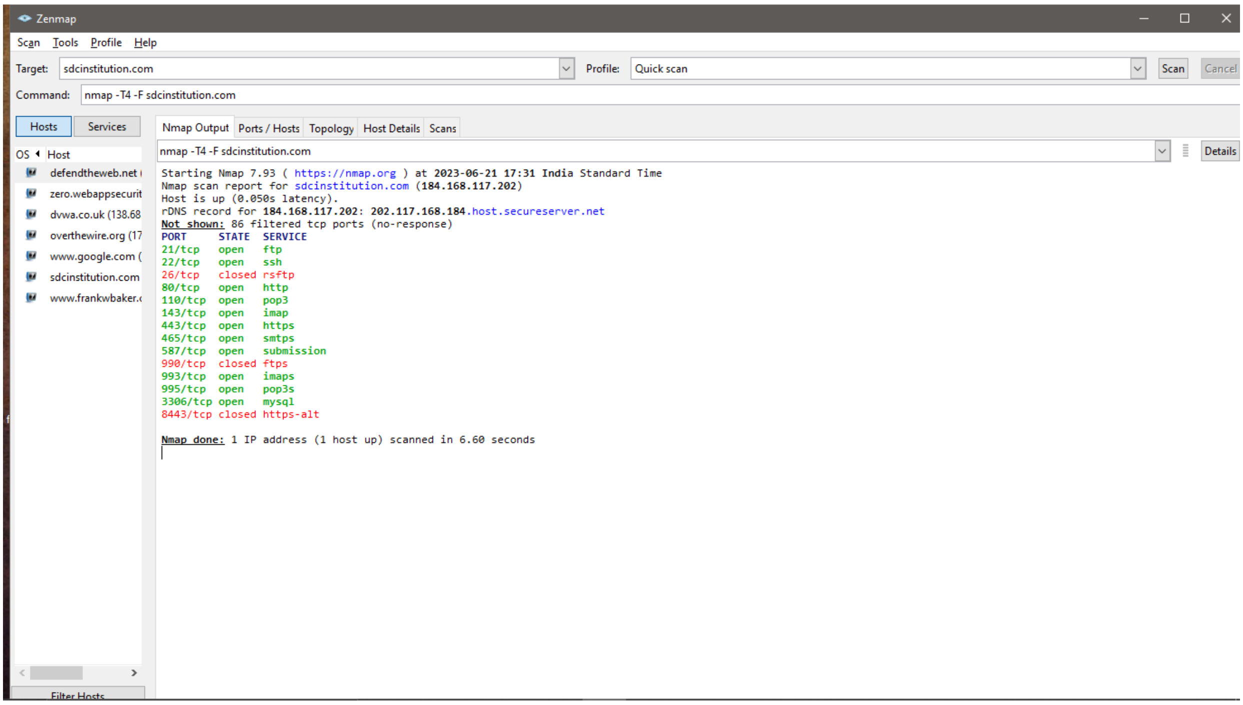
```
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=sdcinstitution.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=sdcinstitution.com
Name Server: NS77.DOMAINCONTROL.COM
Name Server: NS78.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

2. Active Reconnaissance :

Tool used : nmap

Port Scanning:

Scanning web target for open ports



Target: sdcinstitution.com

Profile: Quick scan

Command: nmap -T4 -F sdcinstitution.com

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 17:31 India Standard Time
Nmap scan report for sdcinstitution.com (184.168.117.202)
Host is up (0.050s latency).
rDNS record for 184.168.117.202: 202.117.168.184.host.secureserver.net
Not shown: 86 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
26/tcp   closed rsftp
80/tcp   open   http
110/tcp  open   pop3
143/tcp  open   imap
443/tcp  open   https
465/tcp  open   smtps
587/tcp  open   submission
990/tcp  closed ftps
993/tcp  open   imaps
995/tcp  open   pop3s
3306/tcp open   mysql
8443/tcp closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds
```

Here there is the presence of 11 open ports uses and vulnerability of all 11 ports are mentioned below :

1. **Port 21/TCP (FTP - File Transfer Protocol):**
   - Vulnerabilities: Weak authentication mechanisms, plaintext transmission, potential for brute-force attacks.
   - Uses: FTP servers for file transfers, commonly used in web development and file sharing.
2. **Port 22/TCP (SSH - Secure Shell):**
   - Vulnerabilities: Weak passwords, outdated SSH versions, SSH brute-force attacks.
   - Uses: Secure remote administration and secure file transfers over a network.

3.Port 80/TCP (HTTP - Hypertext Transfer Protocol):

- Vulnerabilities: Web application vulnerabilities (e.g., SQL injection, cross-site scripting), outdated software, misconfigured permissions.
- Uses: Standard port for web traffic, used for accessing websites and web services.

4.Port 110/TCP (POP3 - Post Office Protocol version 3):

- Vulnerabilities: Weak authentication, lack of encryption, potential for eavesdropping.
- Uses: Email retrieval from a mail server, commonly used by email clients.

5.Port 143/TCP (IMAP - Internet Message Access Protocol):

- Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized access.
- Uses: Email retrieval and manipulation, commonly used by email clients.

6.Port 443/TCP (HTTPS - Hypertext Transfer Protocol Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak cipher suites.
- Uses: Encrypted web traffic using SSL/TLS, commonly used for secure transactions and sensitive data transfer.

7.Port 465/TCP (SMTPS - Simple Mail Transfer Protocol Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Secure SMTP communication using SSL/TLS, commonly used for outgoing email delivery.

8.Port 587/TCP (Submission - Mail Submission Agent):

- Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized relaying.
- Uses: SMTP communication for email submission by mail clients, often used with STARTTLS for encryption.

9.Port 993/TCP (IMAPS - Internet Message Access Protocol Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Encrypted email retrieval and manipulation using IMAP over SSL/TLS.

10.Port 995/TCP (POP3S - Post Office Protocol version 3 Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Secure email retrieval using POP3 over SSL/TLS.

11.Port 3306/TCP (MySQL - MySQL Database):

- Vulnerabilities: Weak or default credentials, SQL injection, remote code execution.
- Uses: Database server for MySQL, commonly used in web applications and content management systems.

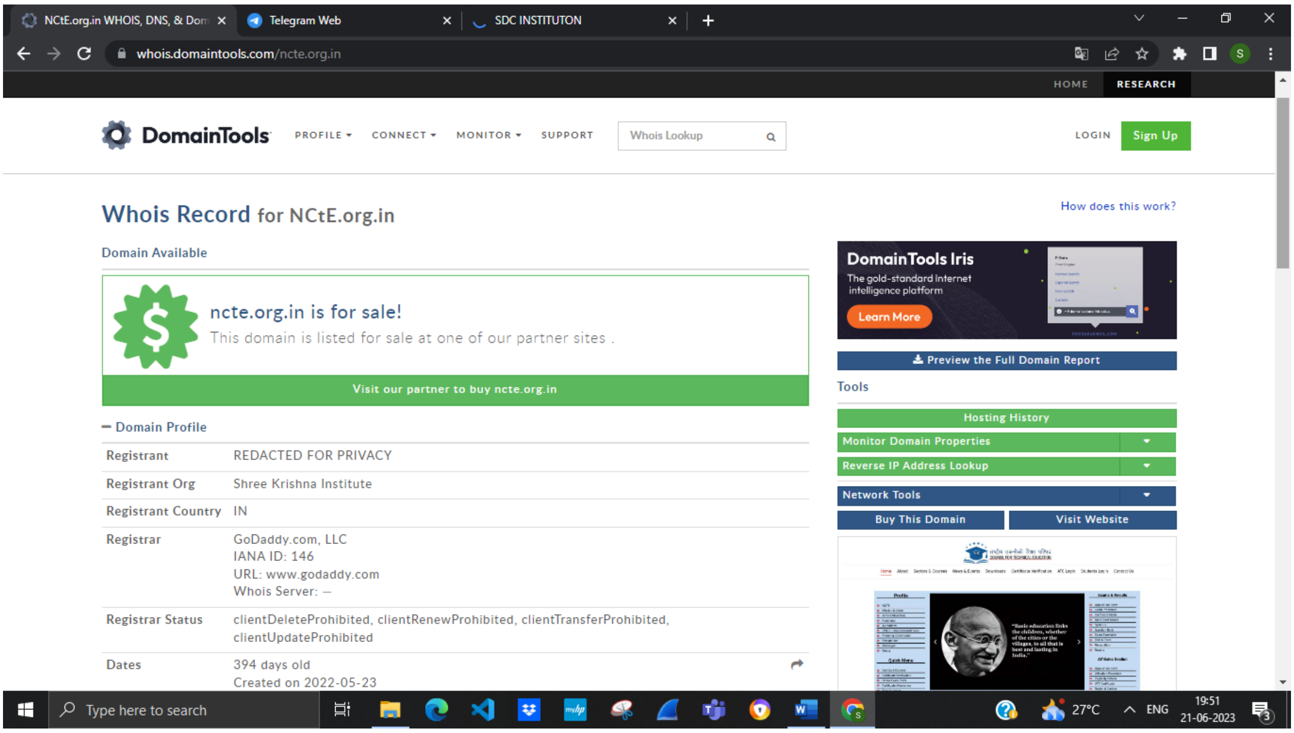
12. It's important to note that these vulnerabilities and uses are not exhaustive, and there may be additional specific vulnerabilities based on the software and configurations in use on these ports. Regular security updates, strong authentication mechanisms, and encryption are crucial to mitigate these vulnerabilities.

Test/Practice website : https://ncte.org.in/

1. Information Gathering Reconnaissance :

Passive Reconnaissance :

Tool used : whois



Whois Record for NCtE.org.in

How does this work?

Domain Available

ncte.org.in is for sale!

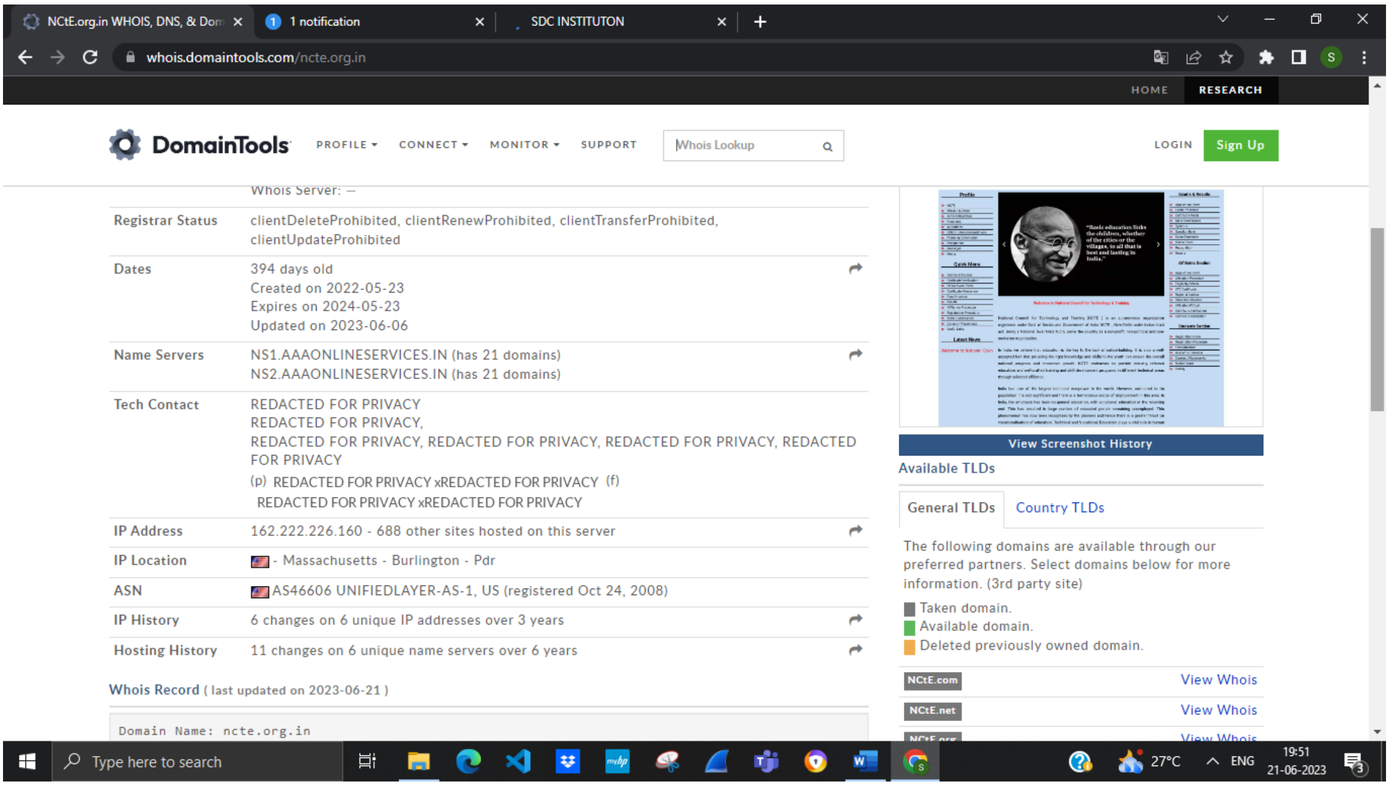
This domain is listed for sale at one of our partner sites .

Visit our partner to buy ncte.org.in

DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Buy This Domain
Visit Website

− Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	Shree Krishna Institute
Registrant Country	IN
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: www.godaddy.com Whois Server: –
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	394 days old Created on 2022-05-23



	Whois Server: –
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	394 days old Created on 2022-05-23 Expires on 2024-05-23 Updated on 2023-06-06
Name Servers	NS1.AAAONLINESERVICES.IN (has 21 domains) NS2.AAAONLINESERVICES.IN (has 21 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY (f) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY
IP Address	162.222.226.160 - 688 other sites hosted on this server
IP Location	- Massachusetts - Burlington - Pdr
ASN	AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
IP History	6 changes on 6 unique IP addresses over 3 years
Hosting History	11 changes on 6 unique name servers over 6 years

Available TLDs

General TLDs | Country TLDs

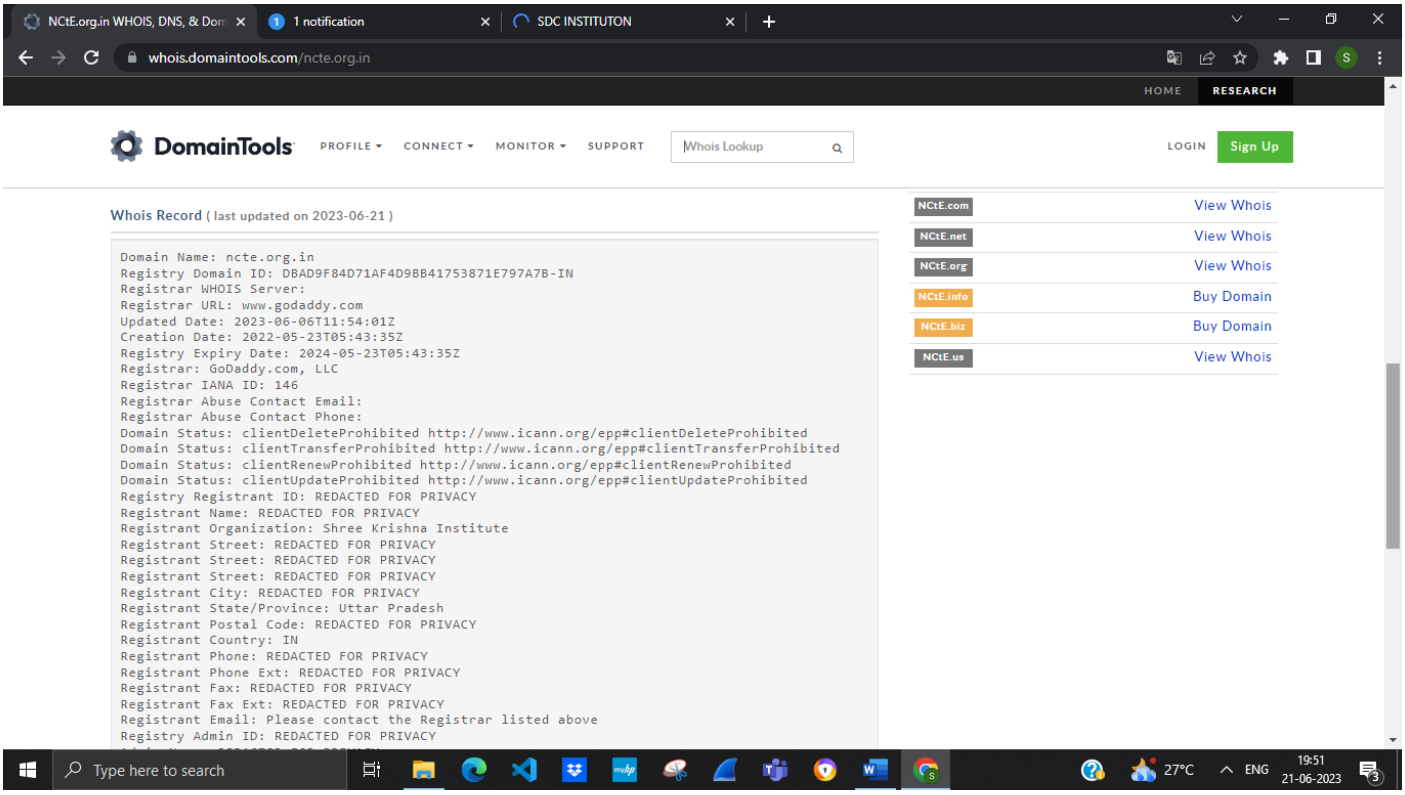
The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▨ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

NCtE.com	View Whois
NCtE.net	View Whois

Whois Record (last updated on 2023-06-21)

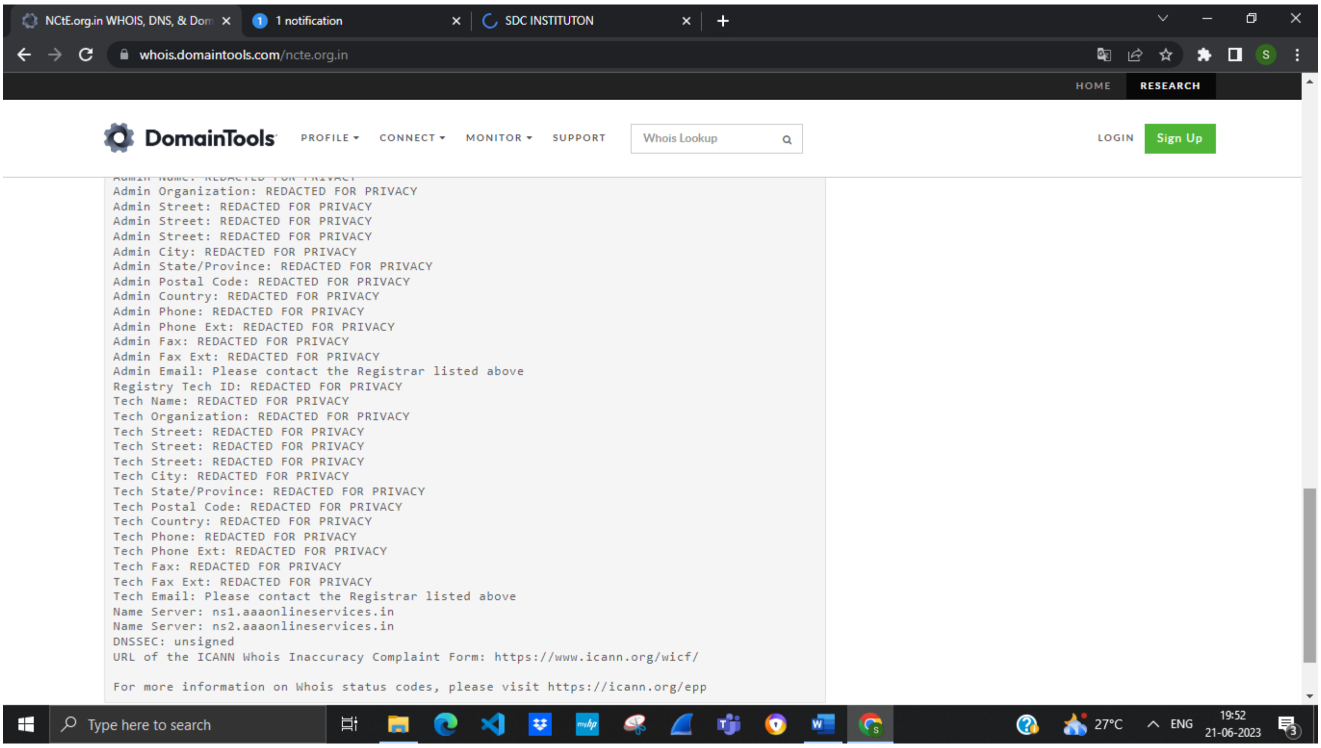
```
Domain Name: ncte.org.in
```



Whois Record (last updated on 2023-06-21)

```
Domain Name: ncte.org.in
Registry Domain ID: DBAD9F84D71AF4D9BB41753871E797A7B-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2023-06-06T11:54:01Z
Creation Date: 2022-05-23T05:43:35Z
Registry Expiry Date: 2024-05-23T05:43:35Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Shree Krishna Institute
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Uttar Pradesh
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
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
```

NCtE.com	View Whois
NCtE.net	View Whois
NCtE.org	View Whois
NCtE.info	Buy Domain
NCtE.biz	Buy Domain
NCtE.us	View Whois



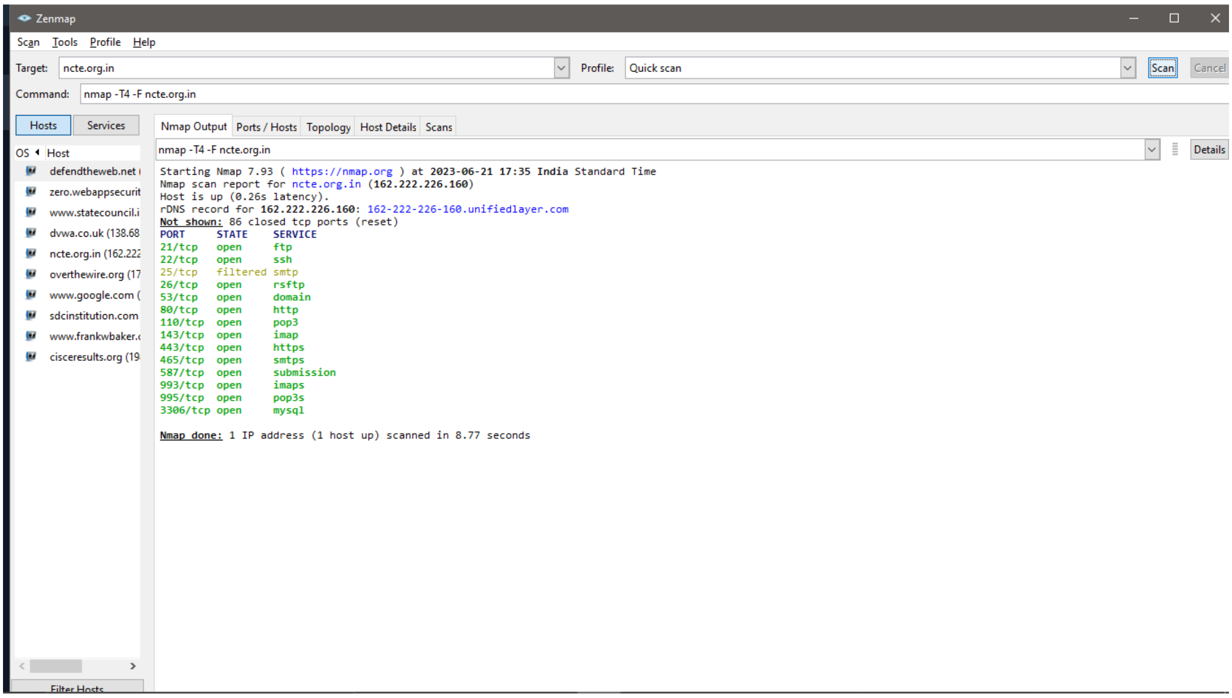
```
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin 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: ns1.aaaonlineservices.in
Name Server: ns2.aaaonlineservices.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

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

2. Active Reconnaissance :

Tool used : nmap

Port Scanning:

Scanning web target for open ports



Target: ncte.org.in

Profile: Quick scan

Command: nmap -T4 -F ncte.org.in

```
nmap -T4 -F ncte.org.in

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 17:35 India Standard Time
Nmap scan report for ncte.org.in (162.222.226.160)
Host is up (0.26s latency).
rDNS record for 162.222.226.160: 162-222-226-160.unifiedlayer.com
Not shown: 86 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   filtered smtp
26/tcp   open     rsftp
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
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 8.77 seconds
```

Here there is the presence of 13 open ports uses and vulnerability of all 13 ports are mentioned below :

1.Port 21/TCP (FTP - File Transfer Protocol):

- Vulnerabilities: Weak authentication mechanisms, plaintext transmission, potential for brute-force attacks.
- Uses: FTP servers for file transfers, commonly used in web development and file sharing.

2.Port 22/TCP (SSH - Secure Shell):

- Vulnerabilities: Weak passwords, outdated SSH versions, SSH brute-force attacks.
- Uses: Secure remote administration and secure file transfers over a network.

3.Port 26/TCP:

- This port is typically unassigned and doesn't have any specific vulnerabilities or uses associated with it. It's not commonly used for any particular service.

4.Port 53/TCP (DNS - Domain Name System):

- Vulnerabilities: DNS cache poisoning, DDoS attacks, zone transfer issues.
- Uses: DNS server communication for domain name resolution and mapping domain names to IP addresses.

5.Port 80/TCP (HTTP - Hypertext Transfer Protocol):

- Vulnerabilities: Web application vulnerabilities (e.g., SQL injection, cross-site scripting), outdated software, misconfigured permissions.
- Uses: Standard port for web traffic, used for accessing websites and web services.

6.Port 110/TCP (POP3 - Post Office Protocol version 3):

- Vulnerabilities: Weak authentication, lack of encryption, potential for eavesdropping.
- Uses: Email retrieval from a mail server, commonly used by email clients.

7.Port 143/TCP (IMAP - Internet Message Access Protocol):

- Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized access.

- Uses: Email retrieval and manipulation, commonly used by email clients.

8.Port 443/TCP (HTTPS - Hypertext Transfer Protocol Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak cipher suites.
- Uses: Encrypted web traffic using SSL/TLS, commonly used for secure transactions and sensitive data transfer.

9.Port 465/TCP (SMTPS - Simple Mail Transfer Protocol Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Secure SMTP communication using SSL/TLS, commonly used for outgoing email delivery.

10.Port 587/TCP (Submission - Mail Submission Agent):

- Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized relaying.
- Uses: SMTP communication for email submission by mail clients, often used with STARTTLS for encryption.

11.Port 993/TCP (IMAPS - Internet Message Access Protocol Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Encrypted email retrieval and manipulation using IMAP over SSL/TLS.

12.Port 995/TCP (POP3S - Post Office Protocol version 3 Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Secure email retrieval using POP3 over SSL/TLS.

13.Port 3306/TCP (MySQL - MySQL Database):

- Vulnerabilities: Weak or default credentials, SQL injection, remote code execution.
- Uses: Database server for MySQL, commonly used in web applications and content management systems.

NOTE : SIR WE WOULD LIKE TO CHANGE THE TEST WEBSITE TO THE GIVEN LINK FOR THE BETTER MENT BECAUSE WE COULD FIND BETTER RESULTS IN THE NEWLY UPDATED TEST WEBSITE COMPARED TO THE PREVIOUS ONE SO DO CONSIDER THE REQUEST SIR

THE END