Name : K .Monika

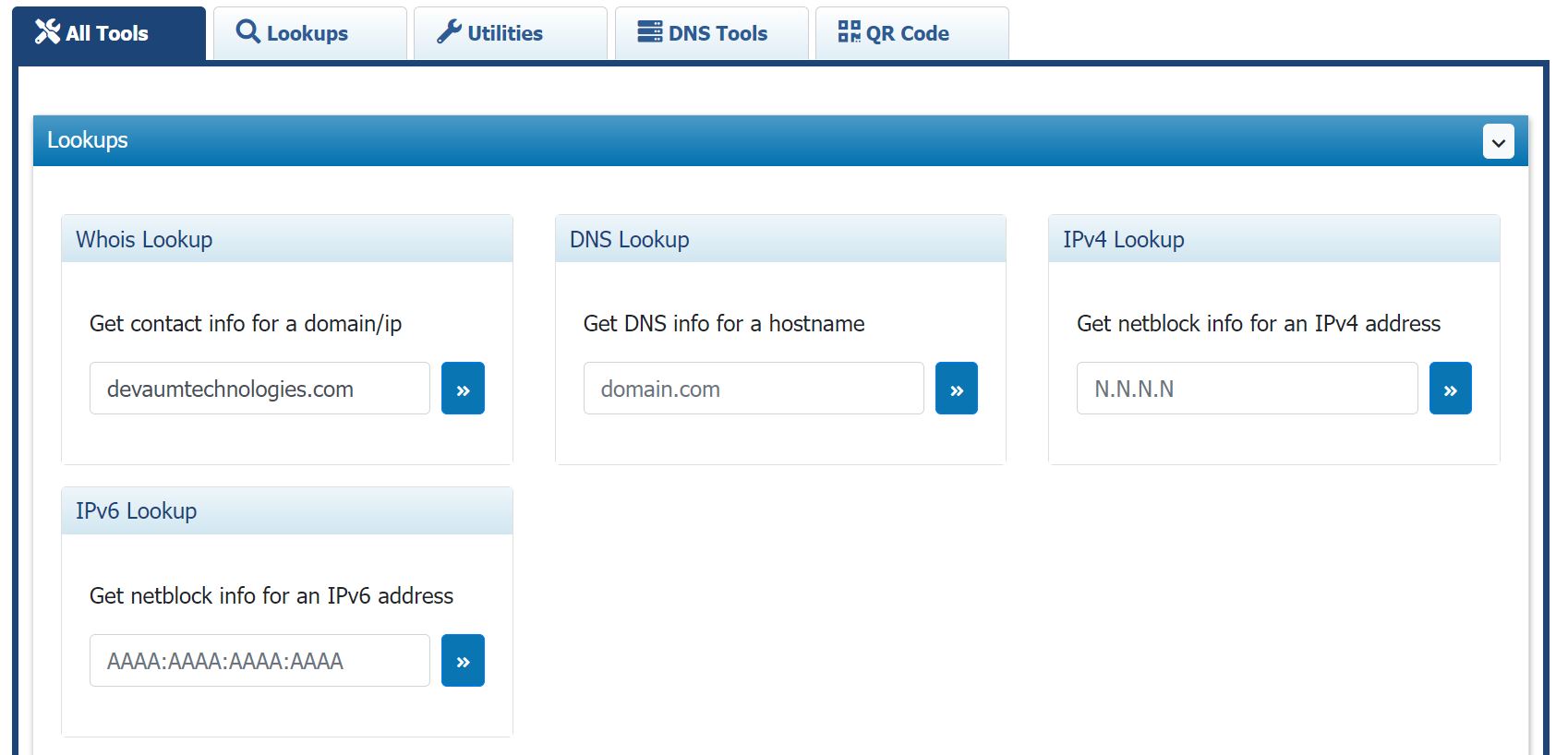
Branch : Computer Science & Engineering

RollNo : 226W1A0527

UNIT 03-(LABS) INTRODUCTION TO HACKING PROCESS

Task 1 :Need to be Performed

1. Foot Printing using tool: <https://domainhelp.com/>



Output:

DEVAUMTECHNOLOGIES.COM whois record

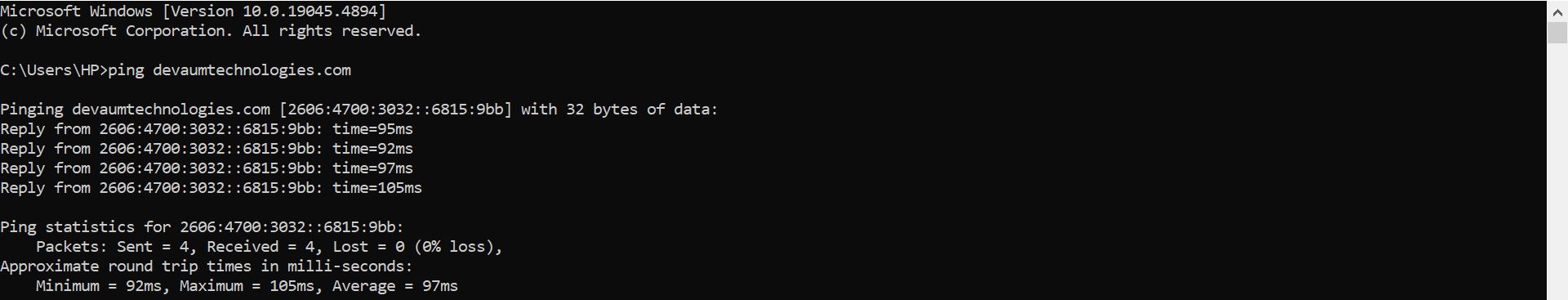
Domain Name: DEVAUMTECHNOLOGIES.COM  
Registry Domain ID: 2378576577\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.godaddy.com  
Registrar URL: http://www.godaddy.com  
Updated Date: 2022-10-26T04:31:14Z  
Creation Date: 2019-04-10T08:16:02Z  
Registry Expiry Date: 2025-04-10T08:16:02Z  
Registrar: GoDaddy.com, LLC  
Registrar IANA ID: 146  
Registrar Abuse Contact Email: abuse@godaddy.com  
Registrar Abuse Contact Phone: 480-624-2505  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Name Server: CHAN.NS.CLOUDFLARE.COM  
Name Server: HUGH.NS.CLOUDFLARE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2024-09-23T05:35:49Z  
  
For more information on Whois status codes, please visit https://icann.org/epp  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
Domain Name: devaumtechnologies.com  
Registry Domain ID: 2378576577\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.godaddy.com  
Registrar URL: https://www.godaddy.com  
Updated Date: 2022-04-05T08:32:36Z  
Creation Date: 2019-04-10T03:16:02Z  
Registrar Registration Expiration Date: 2025-04-10T03:16:02Z  
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: 100 S. Mill Ave, Suite 1600  
Registrant City: Tempe  
Registrant State/Province: Arizona  
Registrant Postal Code: 85281  
Registrant Country: US  
Registrant Phone: +1.4806242599  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=devaumtechnologies.com  
Registry Admin ID: Not Available From Registry  
Admin Name: Registration Private  
Admin Organization: Domains By Proxy, LLC  
Admin Street: DomainsByProxy.com  
Admin Street: 100 S. Mill Ave, Suite 1600  
Admin City: Tempe  
Admin State/Province: Arizona  
Admin Postal Code: 85281  
Admin Country: US  
Admin Phone: +1.4806242599  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:  
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=devaumtechnologies.com  
Registry Tech ID: Not Available From Registry  
Tech Name: Registration Private  
Tech Organization: Domains By Proxy, LLC  
Tech Street: DomainsByProxy.com  
Tech Street: 100 S. Mill Ave, Suite 1600  
Tech City: Tempe  
Tech State/Province: Arizona  
Tech Postal Code: 85281  
Tech Country: US  
Tech Phone: +1.4806242599  
Tech Phone Ext:  
Tech Fax:  
Tech Fax Ext:  
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=devaumtechnologies.com  
Name Server: CHAN.NS.CLOUDFLARE.COM  
Name Server: HUGH.NS.CLOUDFLARE.COM  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/  
>>> Last update of WHOIS database: 2024-09-23T05:36:09Z

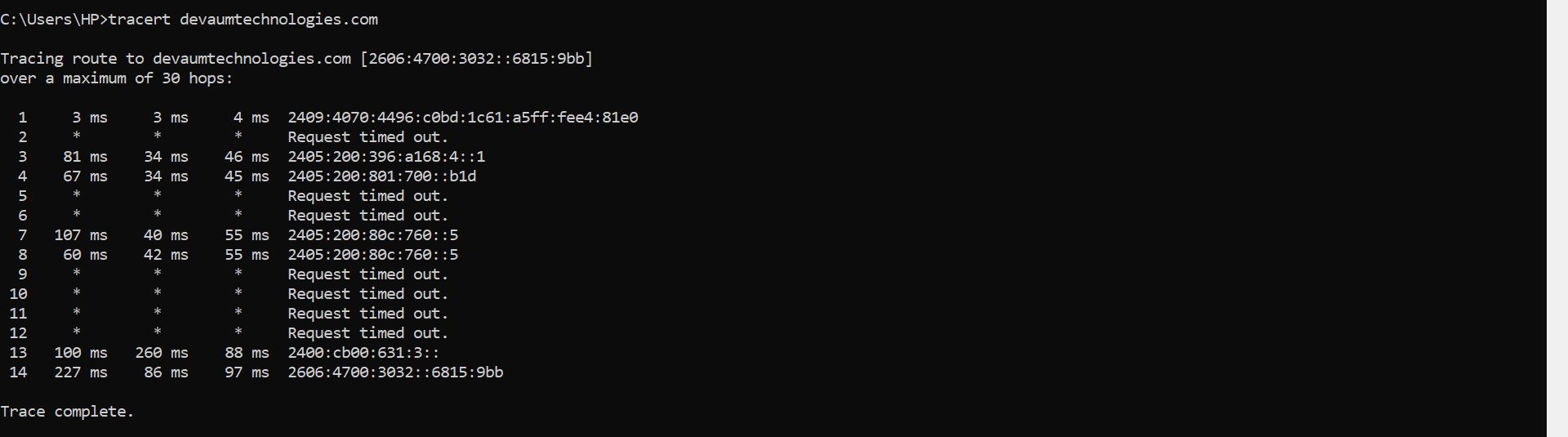
Task 2

Gather the information with respect to Network

Check networking Connectivity

Ping

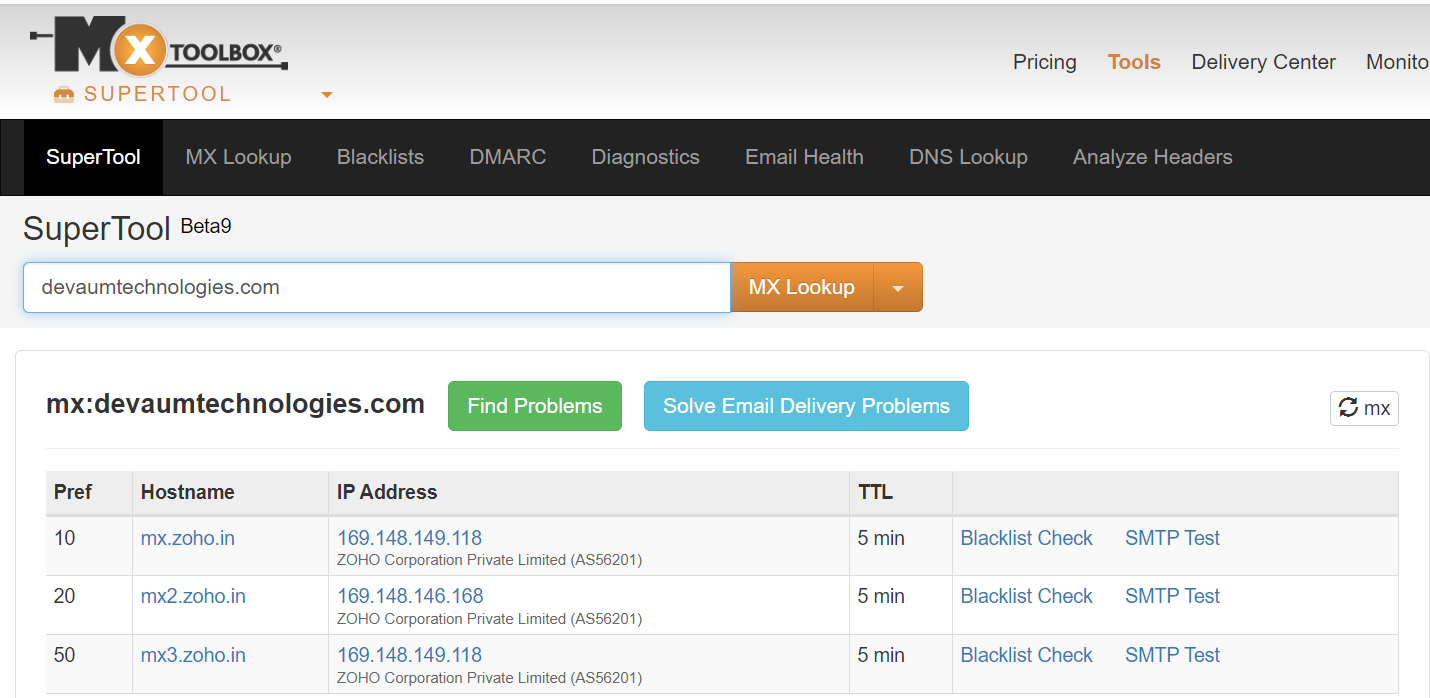


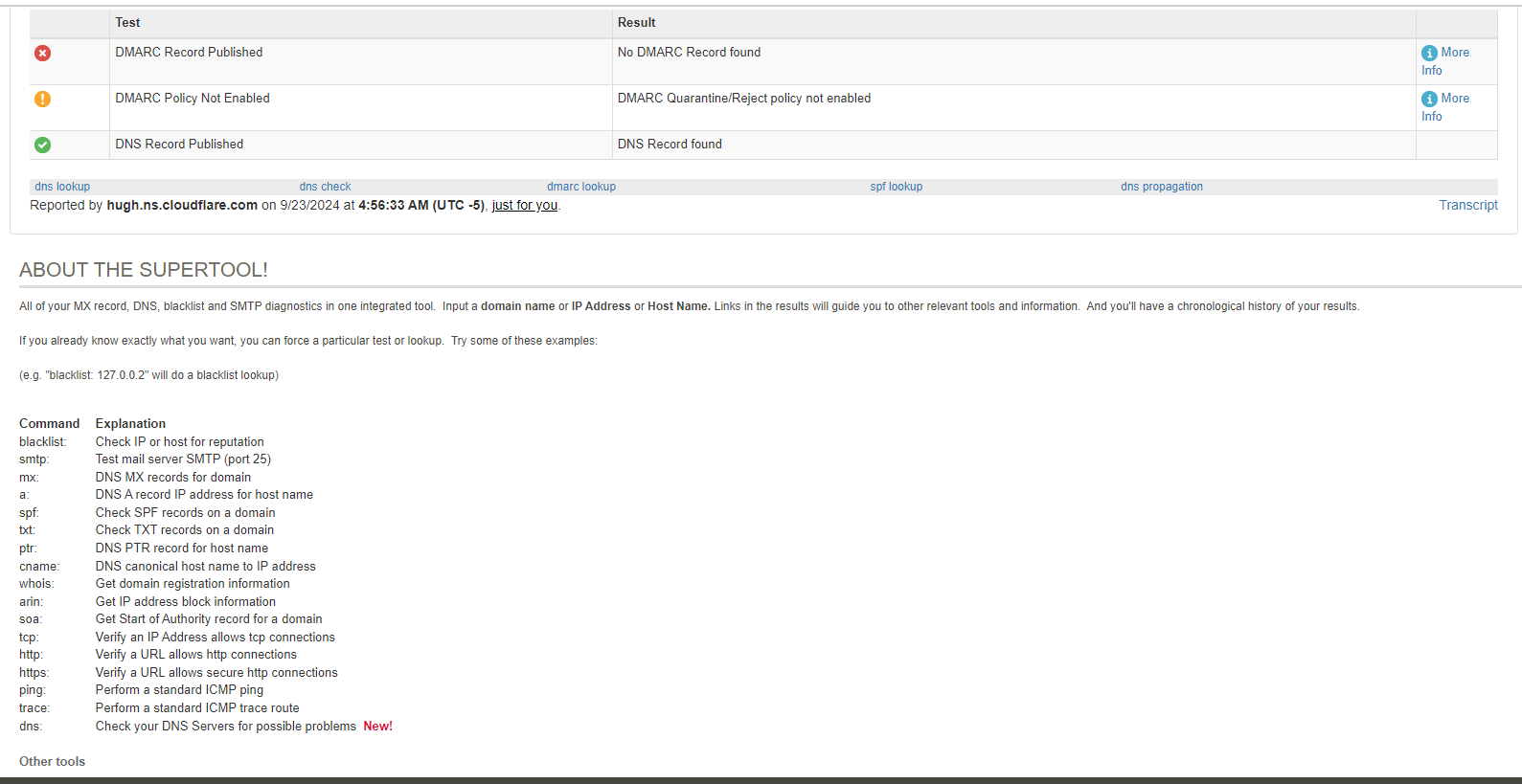
Tracert :  


Nslookup



Mail server Details:





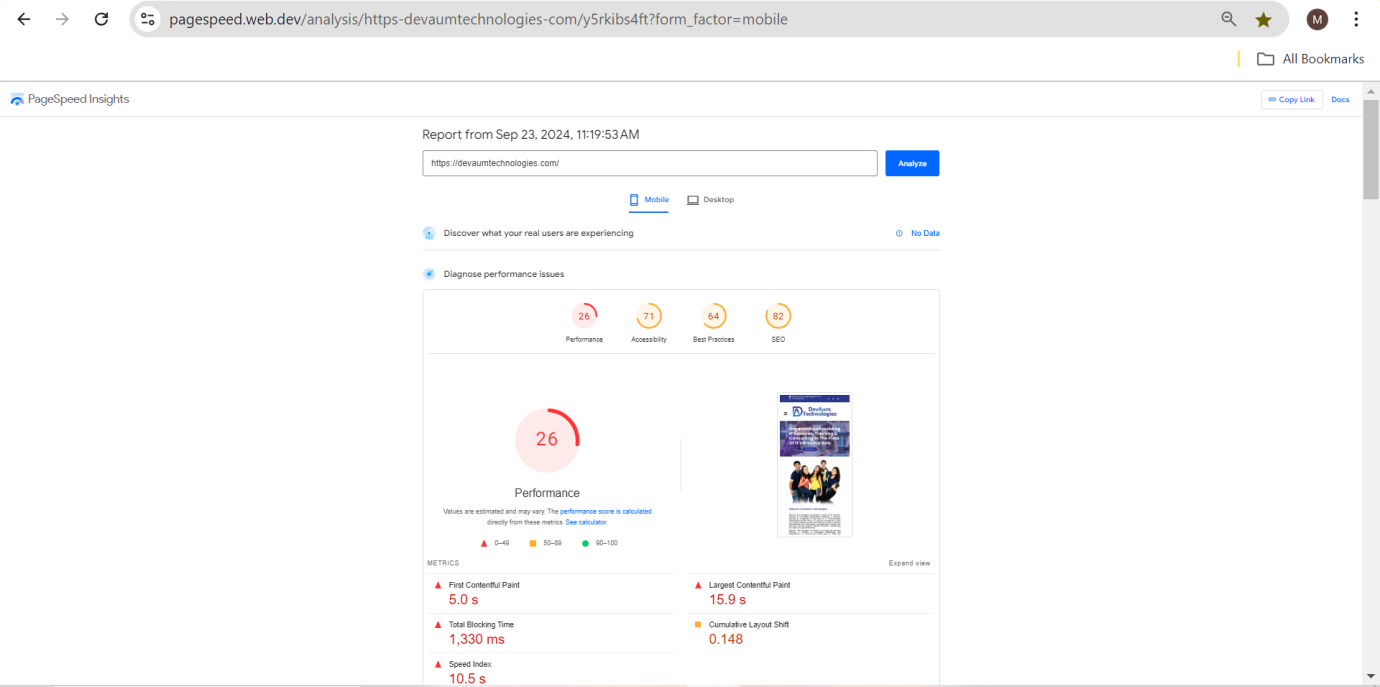
Lab Questions

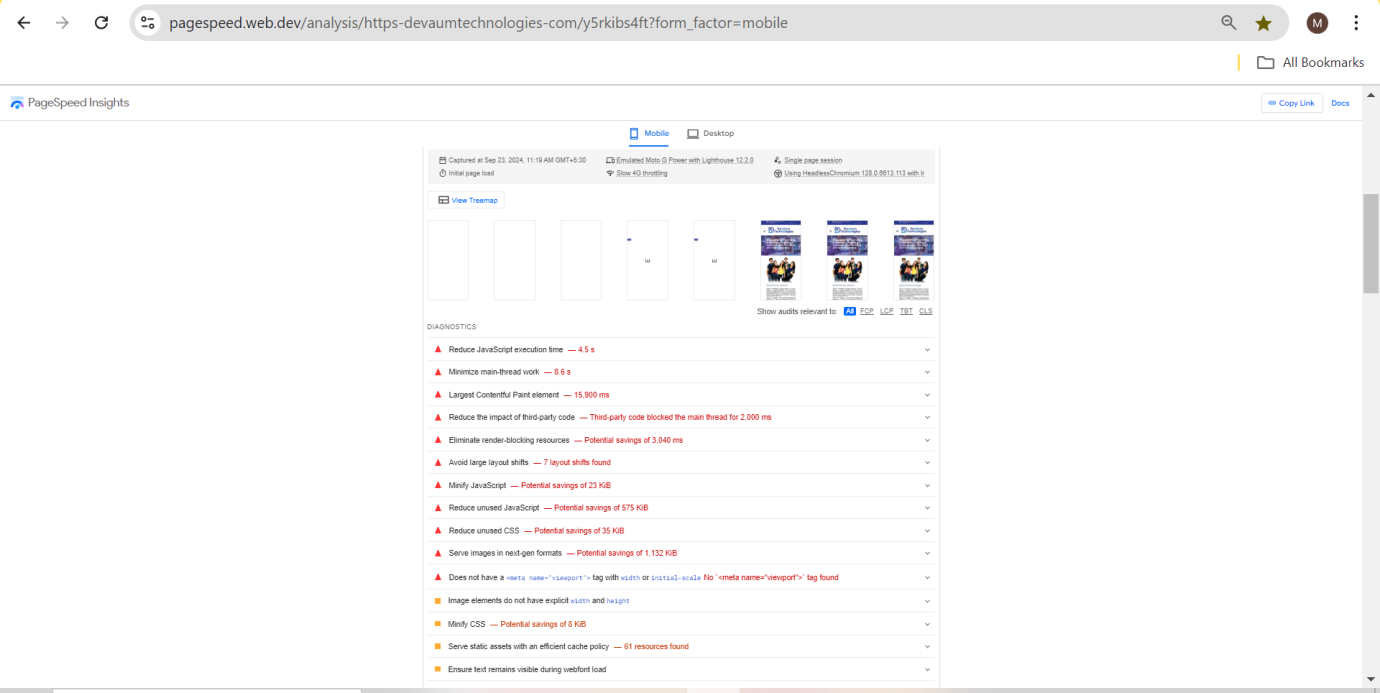
1. What is foot printing in the context of cyber security, and why is it essential for reconnaissance?

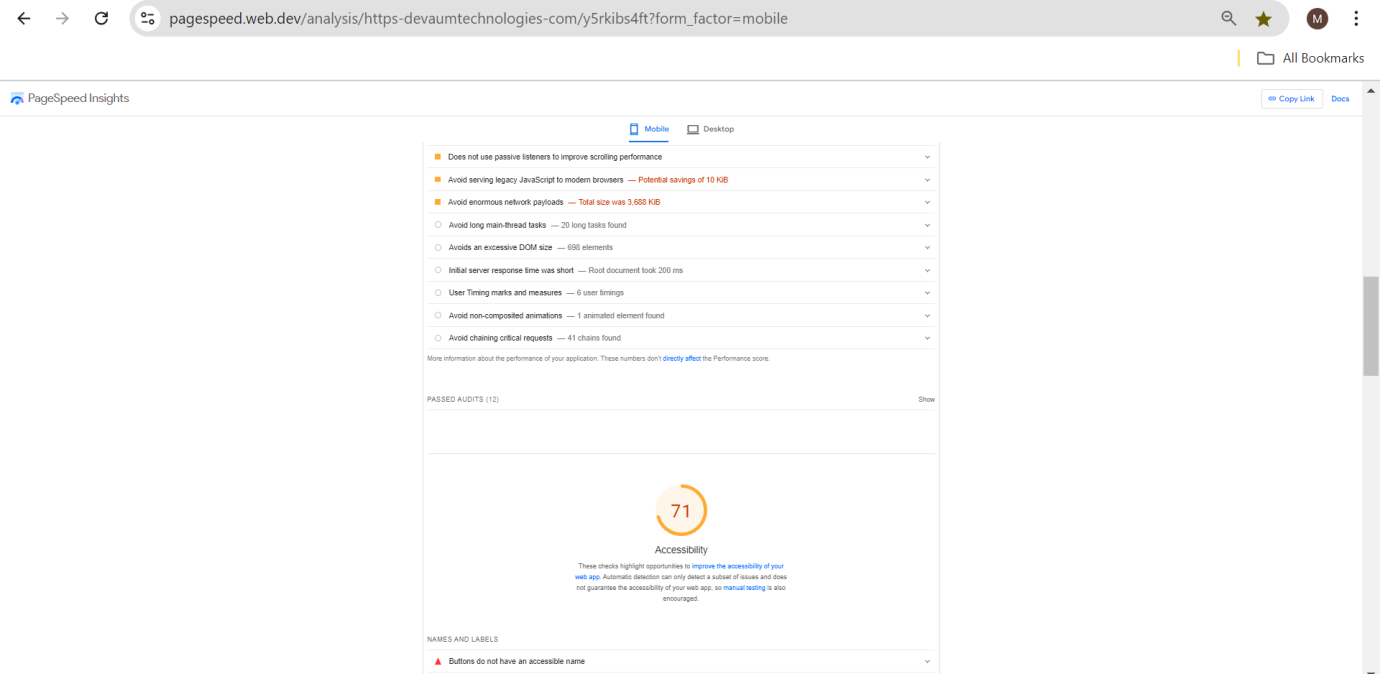
Foot printing in the context of cyber security refers to the process of gathering information about a target system, network, or organization to identify vulnerabilities that can be exploited during a cyber attack. It is the first phase of the reconnaissance process, where an attacker or security professional collects as much data as possible about the target without actively interacting with it in a way that could alert the target to their presence.

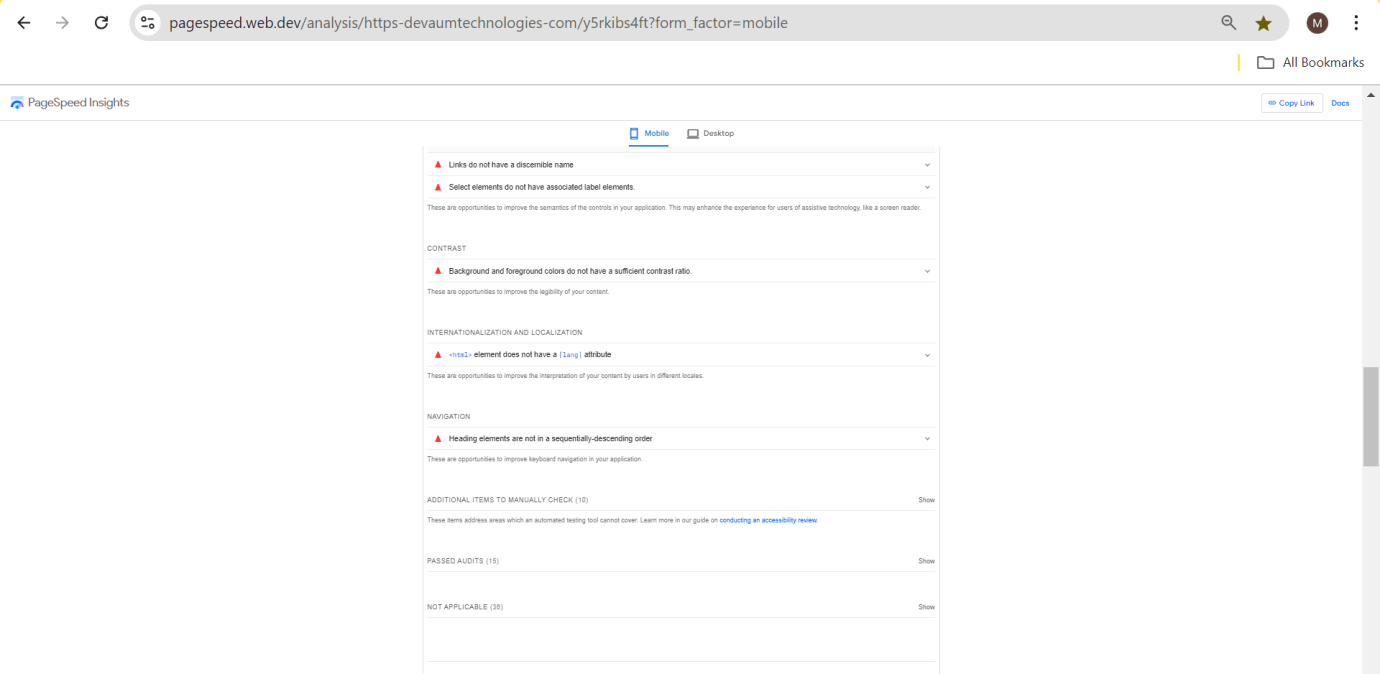
1. **Foundation for Further Attacks**: Foot printing provides a comprehensive understanding of the target’s environment, including network structures, operating systems, domain names, IP addresses, and more. This information is crucial for planning and executing subsequent stages of an attack, such as scanning and exploitation.
2. **Identification of Weak Points**: By mapping out the target's infrastructure, attackers can identify potential vulnerabilities, such as out dated software, unpatched systems, or misconfigured services that can be exploited.
3. **Minimizing Detection Risk**: Passive foot printing techniques (e.g., whois lookups, DNS queries, or searching publicly available information) allow attackers to gather significant data without directly interacting with the target system, reducing the risk of detection.
4. **Informed Decision-Making**: For ethical hackers or penetration testers, foot printing helps in prioritizing which systems or applications to target based on their potential vulnerabilities, leading to more effective security assessments.
5. **Defensive Strategies**: For defenders, understanding the methods used in foot printing can help in identifying early signs of reconnaissance and implementing measures to protect sensitive information from being easily accessible.

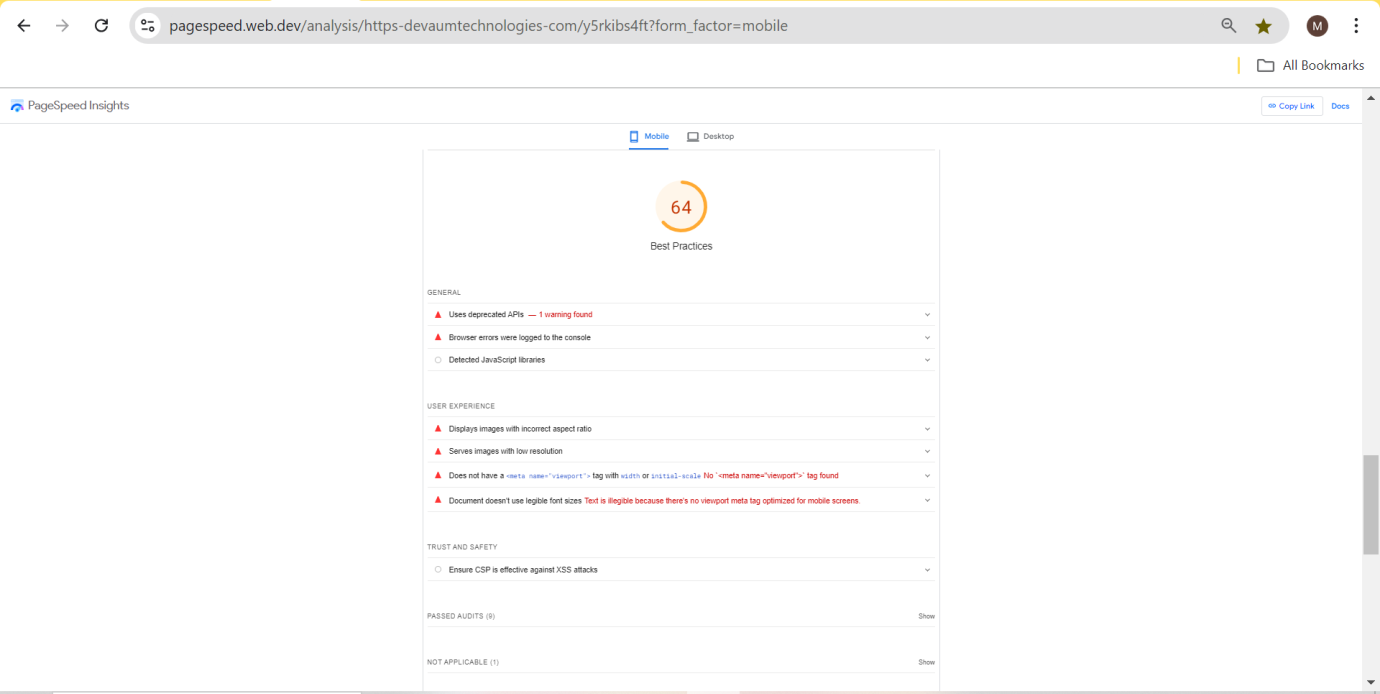
2. Get the website grading and coding error ( sitechecker.pro)

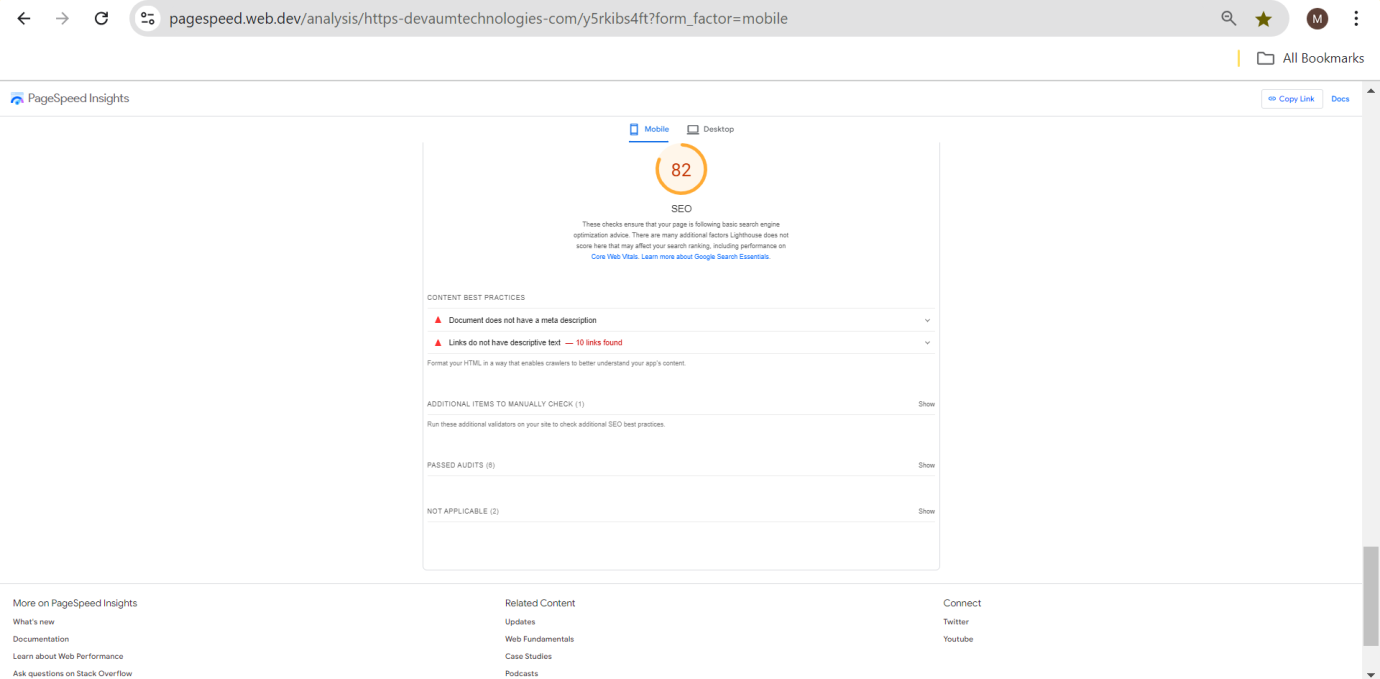






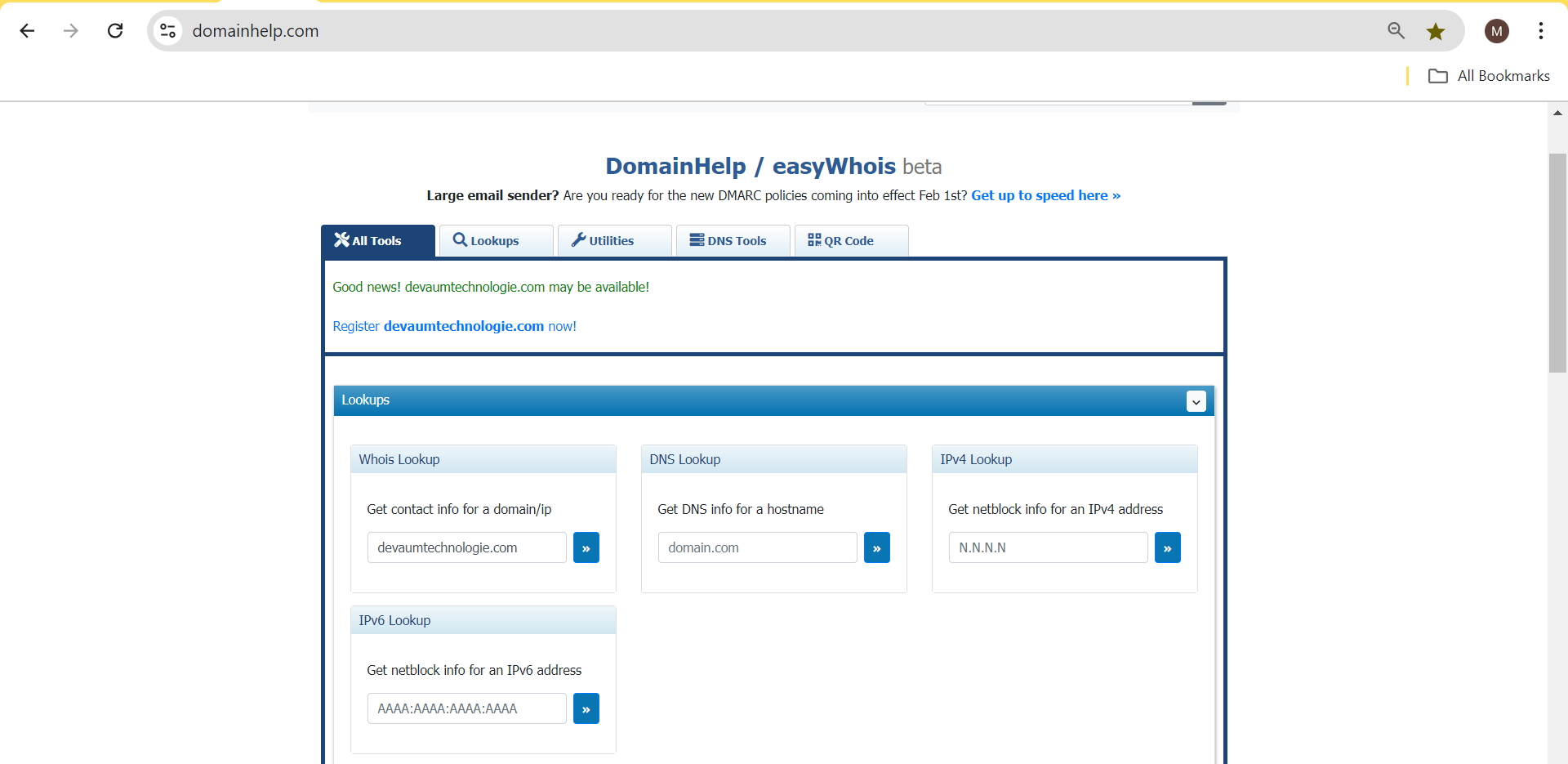






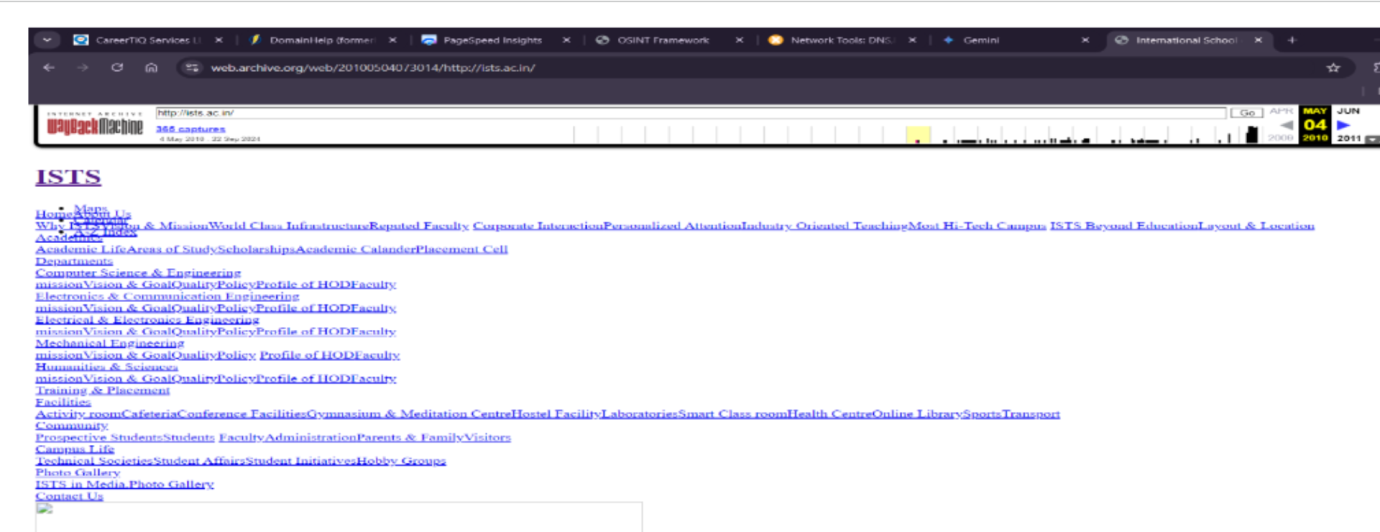
3. Get the details about the website ..(whois)

Domain Name: DEVAUMTECHNOLOGIES.COM  
Registry Domain ID: 2378576577\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.godaddy.com  
Registrar URL: http://www.godaddy.com  
Updated Date: 2022-10-26T04:31:14Z  
Creation Date: 2019-04-10T08:16:02Z  
Registry Expiry Date: 2025-04-10T08:16:02Z  
Registrar: GoDaddy.com, LLC  
Registrar IANA ID: 146  
Registrar Abuse Contact Email: abuse@godaddy.com  
Registrar Abuse Contact Phone: 480-624-2505  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Name Server: CHAN.NS.CLOUDFLARE.COM  
Name Server: HUGH.NS.CLOUDFLARE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2024-09-23T05:35:49Z  
  
For more information on Whois status codes, please visit https://icann.org/epp  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
Domain Name: devaumtechnologies.com  
Registry Domain ID: 2378576577\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.godaddy.com  
Registrar URL: https://www.godaddy.com  
Updated Date: 2022-04-05T08:32:36Z  
Creation Date: 2019-04-10T03:16:02Z  
Registrar Registration Expiration Date: 2025-04-10T03:16:02Z  
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: 100 S. Mill Ave, Suite 1600  
Registrant City: Tempe  
Registrant State/Province: Arizona  
Registrant Postal Code: 85281  
Registrant Country: US  
Registrant Phone: +1.4806242599  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=devaumtechnologies.com  
Registry Admin ID: Not Available From Registry  
Admin Name: Registration Private  
Admin Organization: Domains By Proxy, LLC  
Admin Street: DomainsByProxy.com  
Admin Street: 100 S. Mill Ave, Suite 1600  
Admin City: Tempe  
Admin State/Province: Arizona  
Admin Postal Code: 85281  
Admin Country: US  
Admin Phone: +1.4806242599  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:  
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=devaumtechnologies.com  
Registry Tech ID: Not Available From Registry  
Tech Name: Registration Private  
Tech Organization: Domains By Proxy, LLC  
Tech Street: DomainsByProxy.com  
Tech Street: 100 S. Mill Ave, Suite 1600  
Tech City: Tempe  
Tech State/Province: Arizona  
Tech Postal Code: 85281  
Tech Country: US  
Tech Phone: +1.4806242599  
Tech Phone Ext:  
Tech Fax:  
Tech Fax Ext:  
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=devaumtechnologies.com  
Name Server: CHAN.NS.CLOUDFLARE.COM  
Name Server: HUGH.NS.CLOUDFLARE.COM  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/  
>>> Last update of WHOIS database: 2024-09-23T05:36:09Z

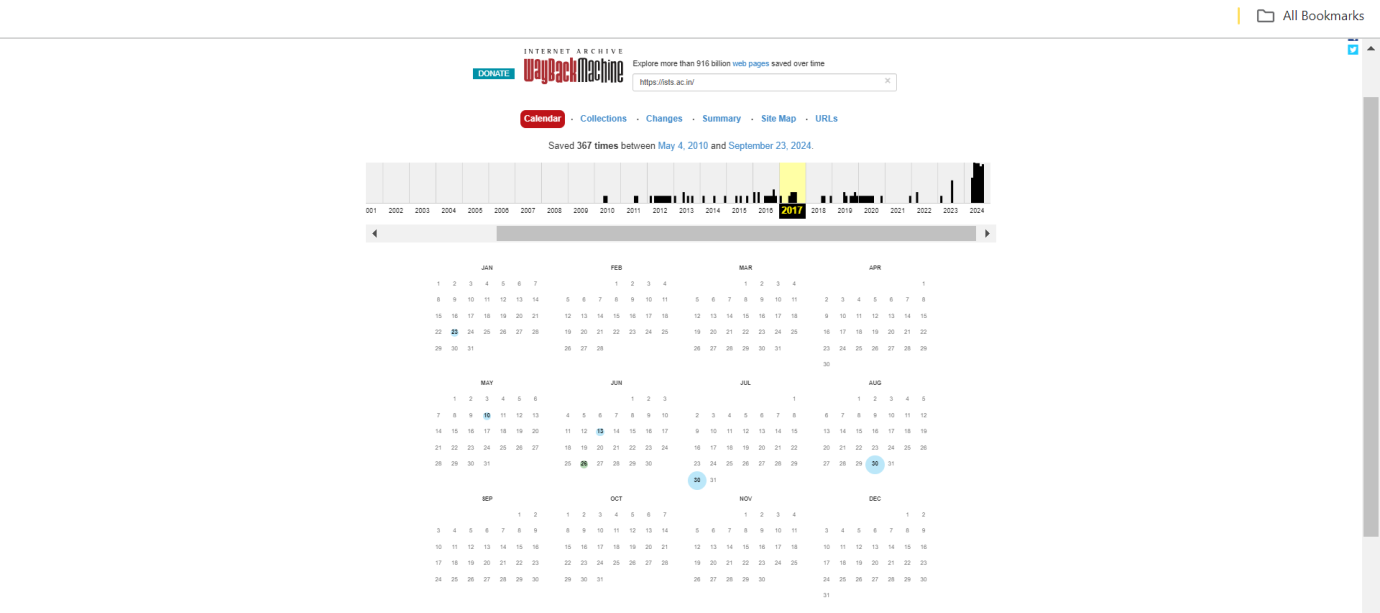


4.Get the history about the website(archeive.org)

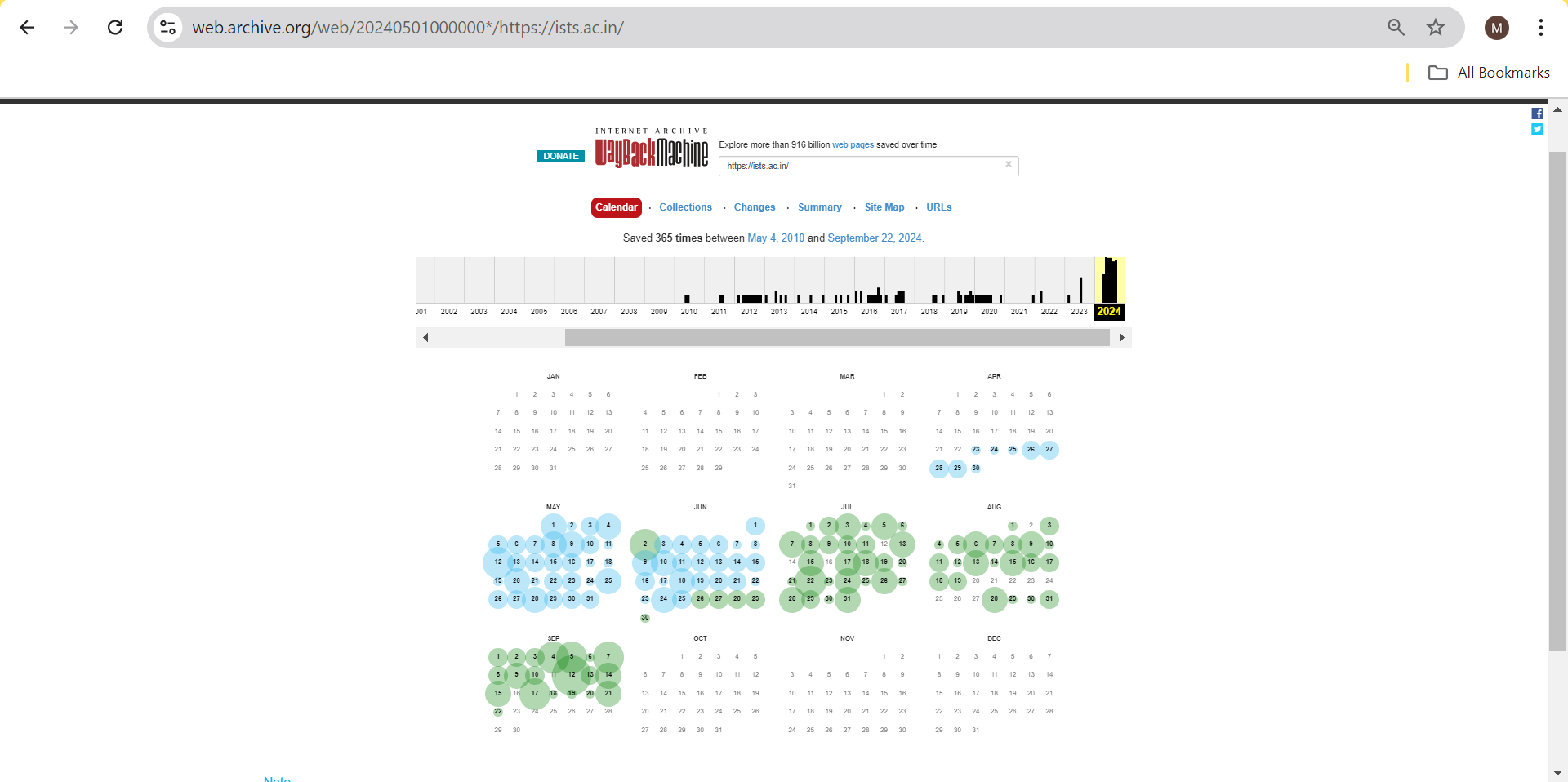
First snapshot on 2010



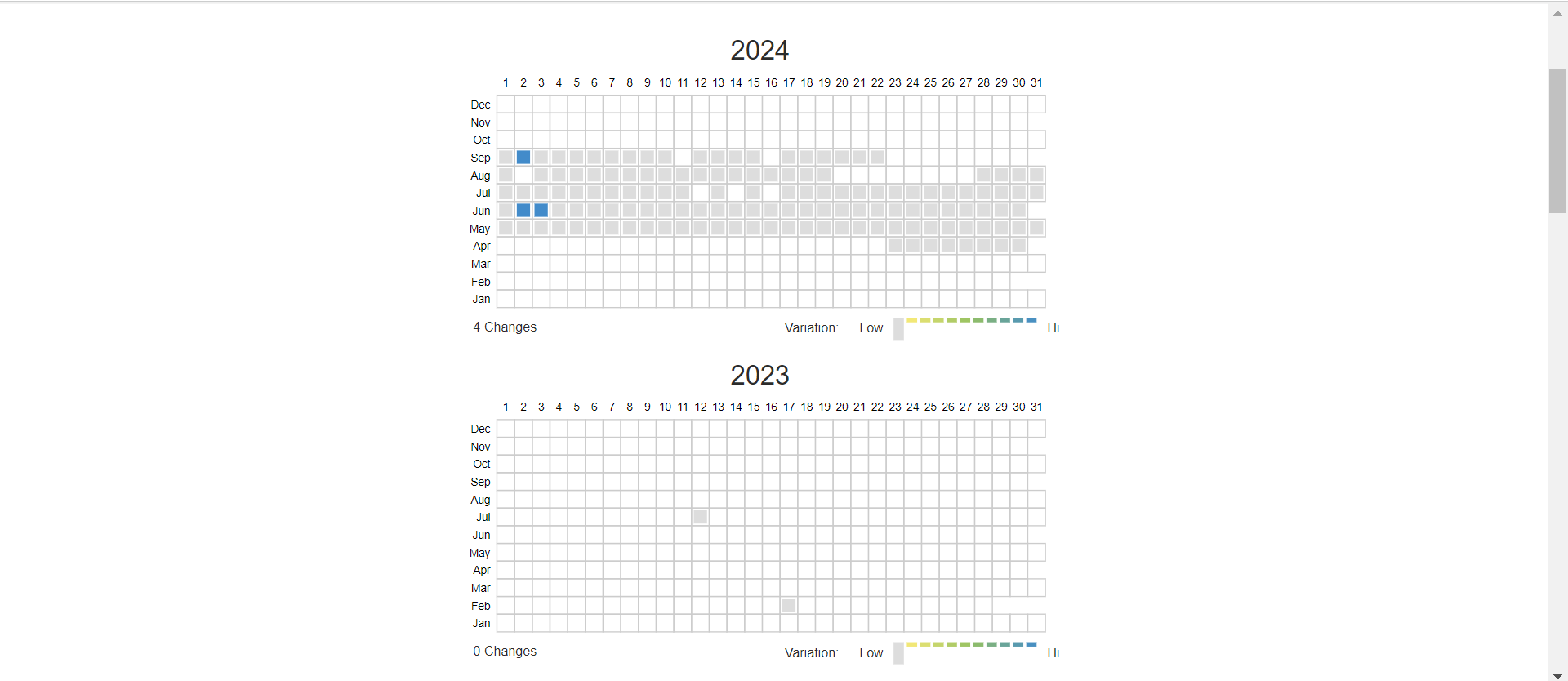
The website is updated 8 times in 2017



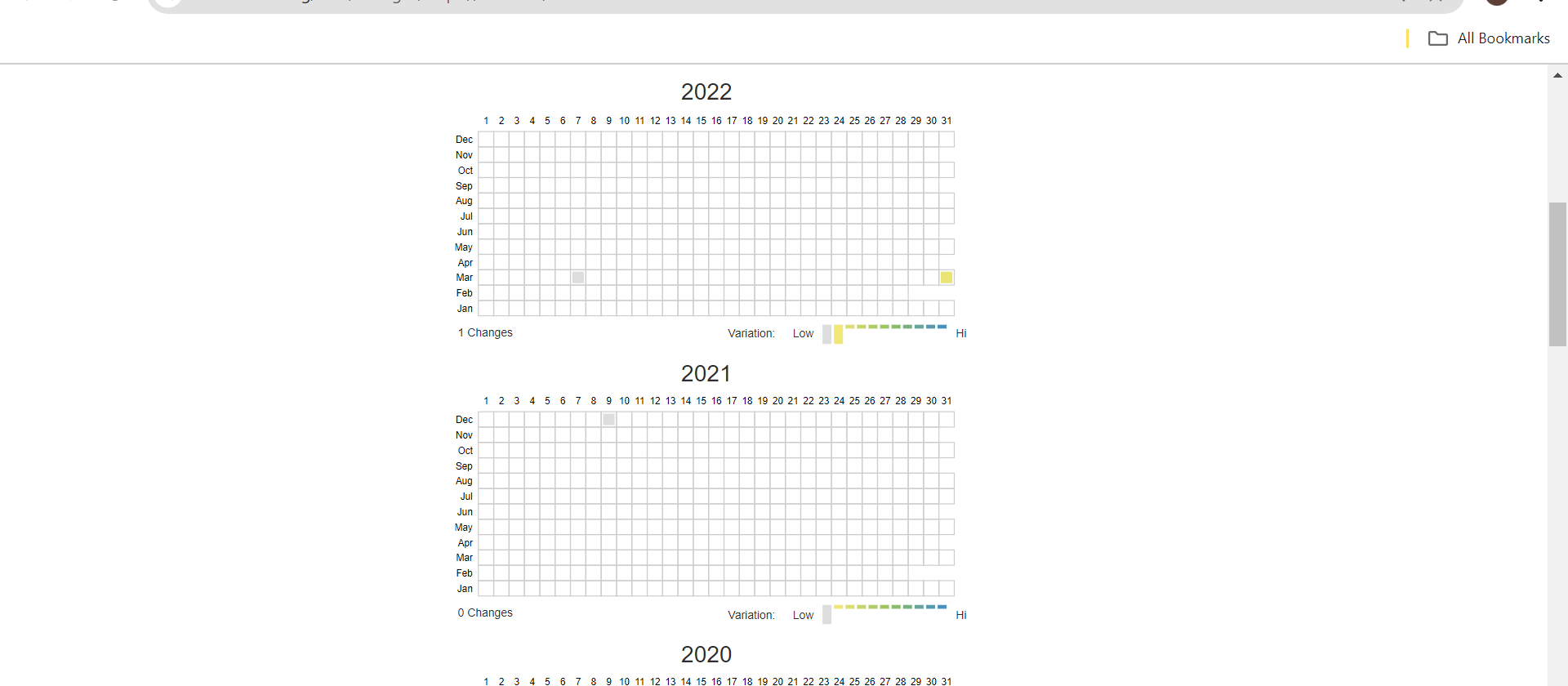
In 2024 around 150 times website was updated:



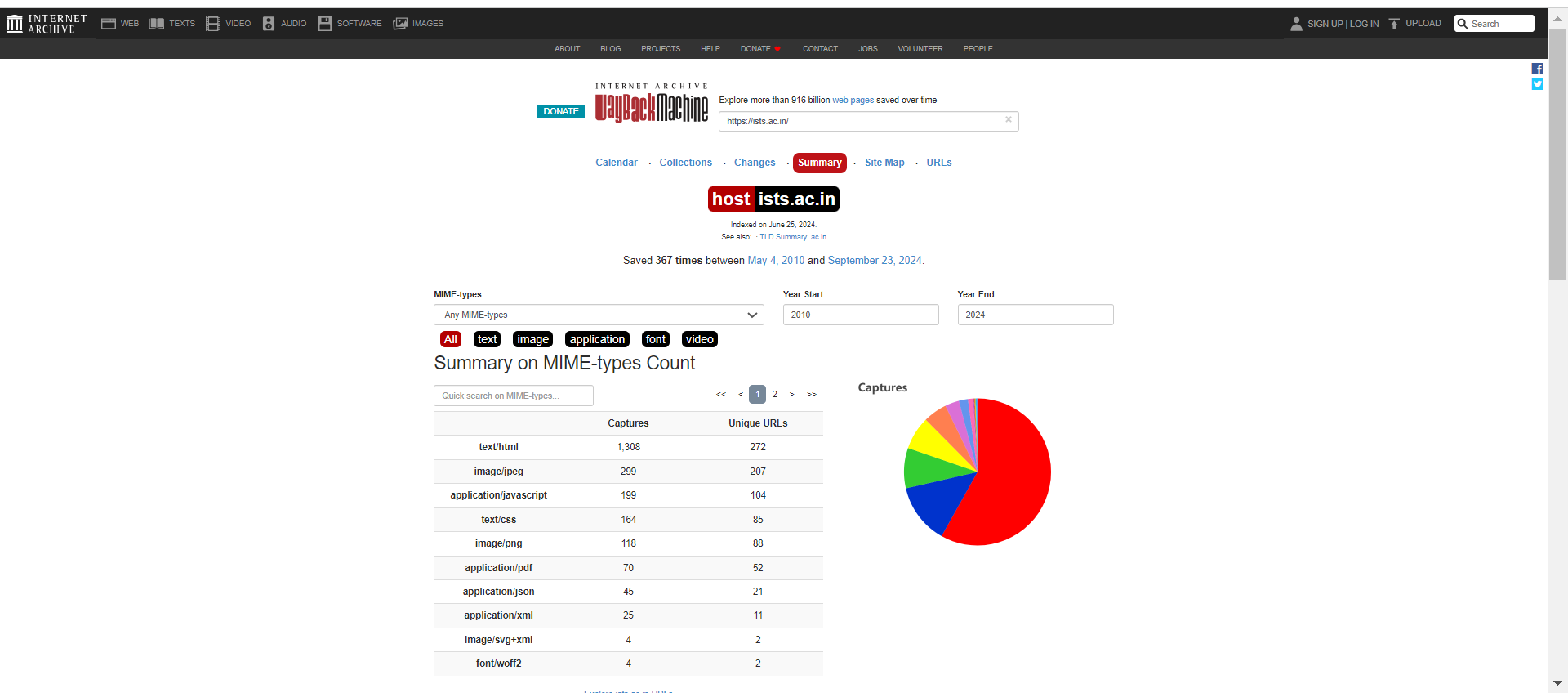
No.of changes made in 2023 to 2024

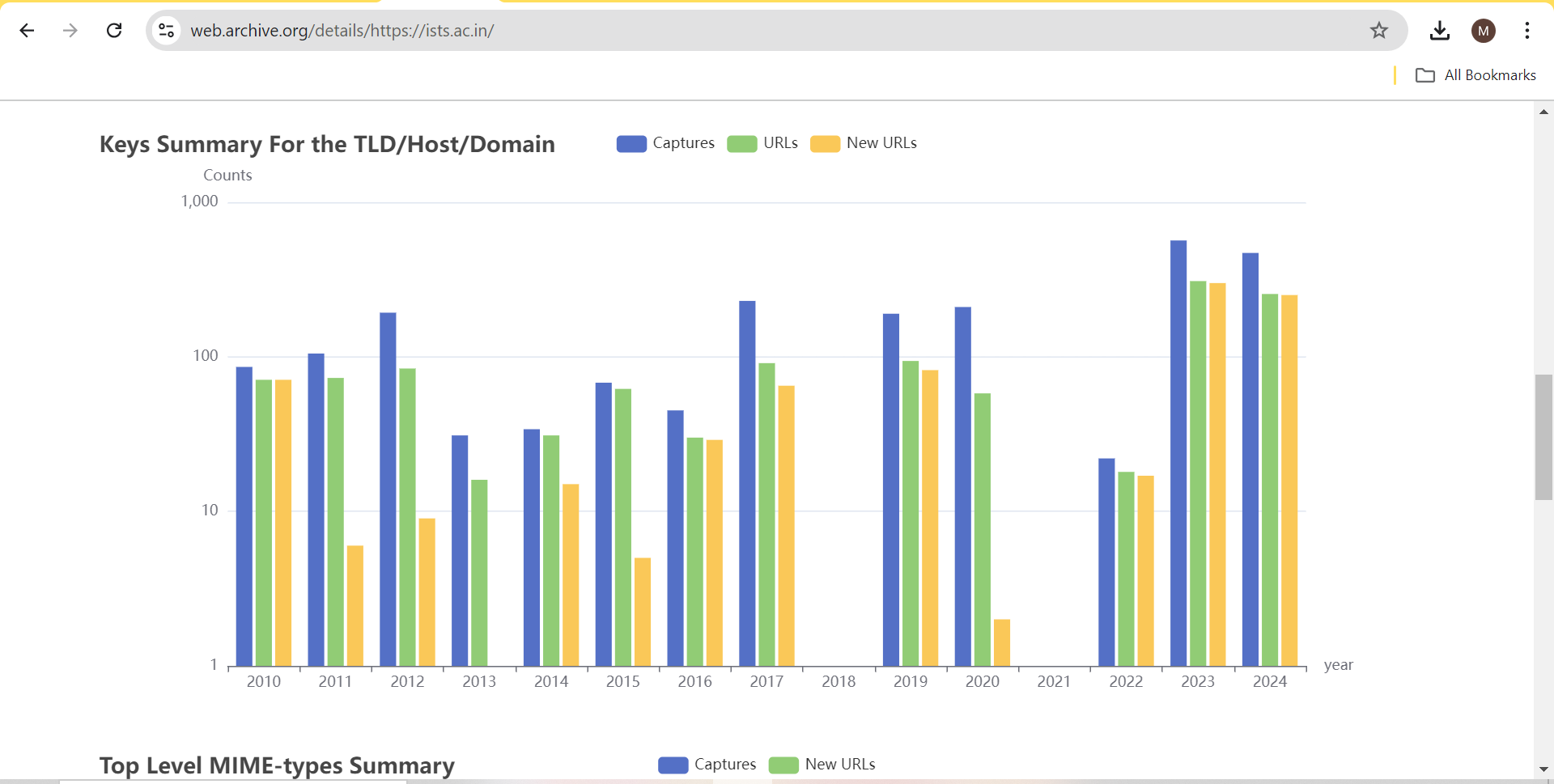


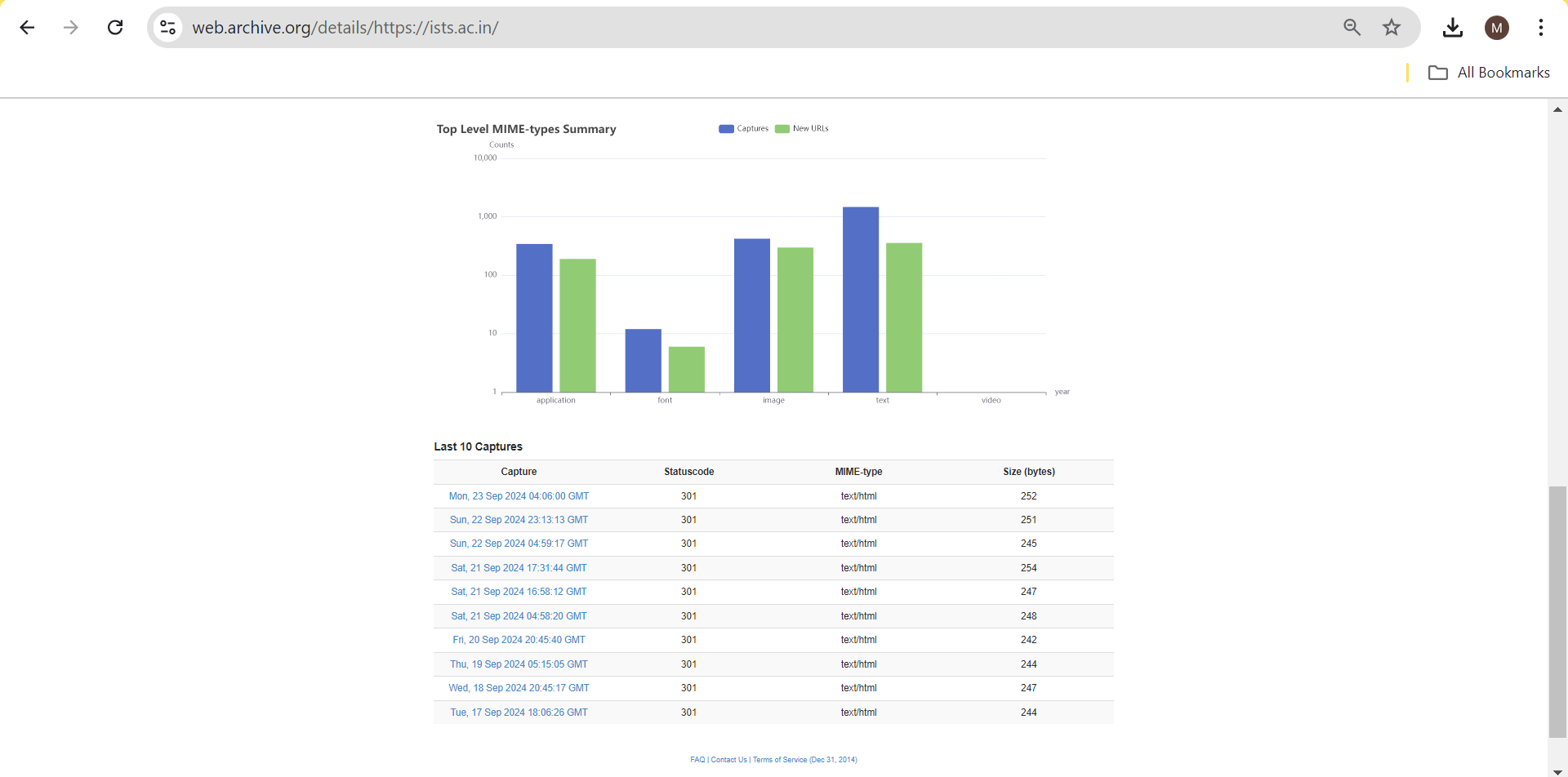
Changes 2022 to2024

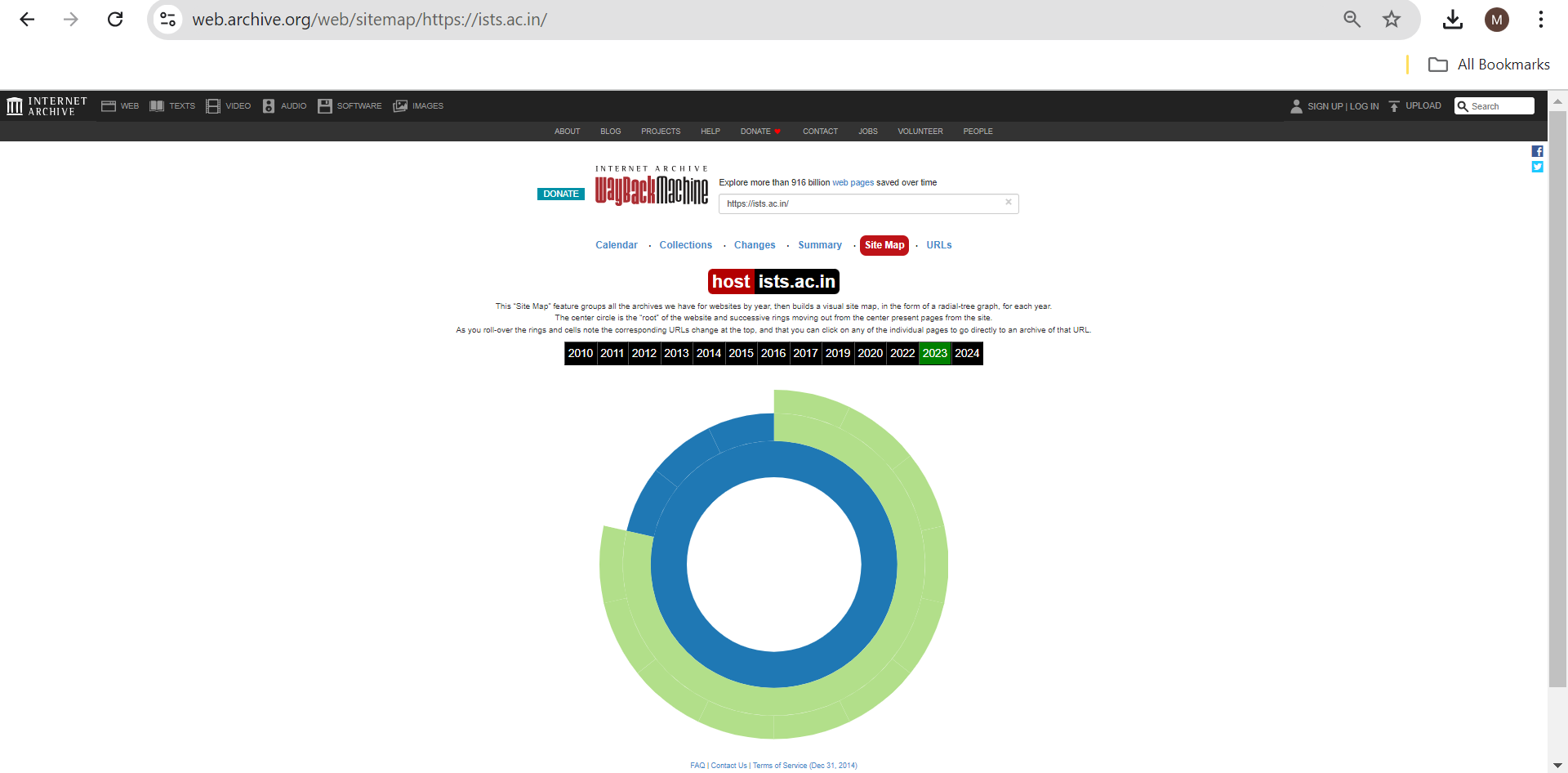


Different changes in summary







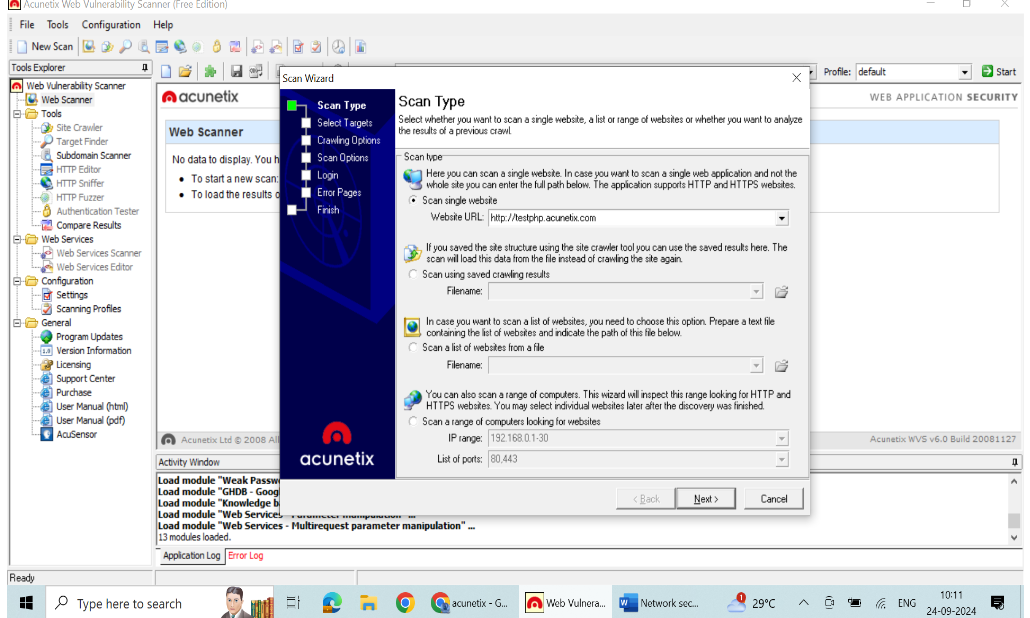


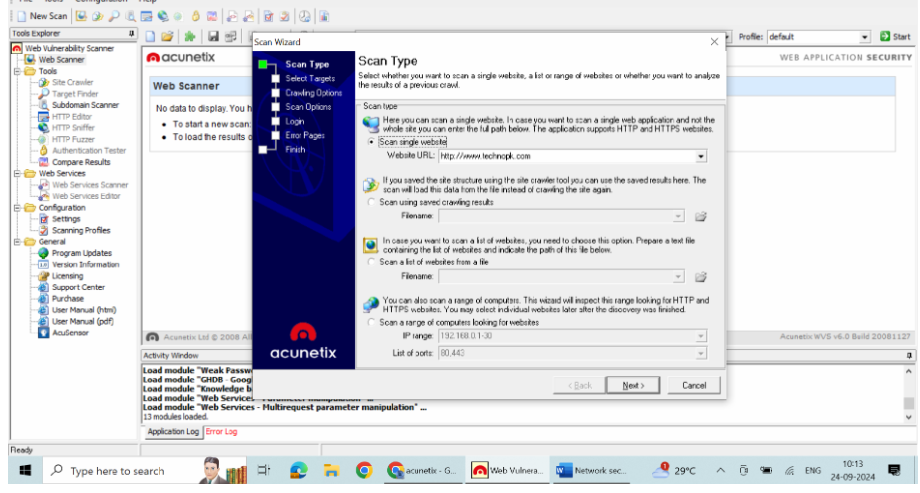
UNIT 04-(LABS) INTRODUCTION TO ATTACKS

Task 1

Scanning a website

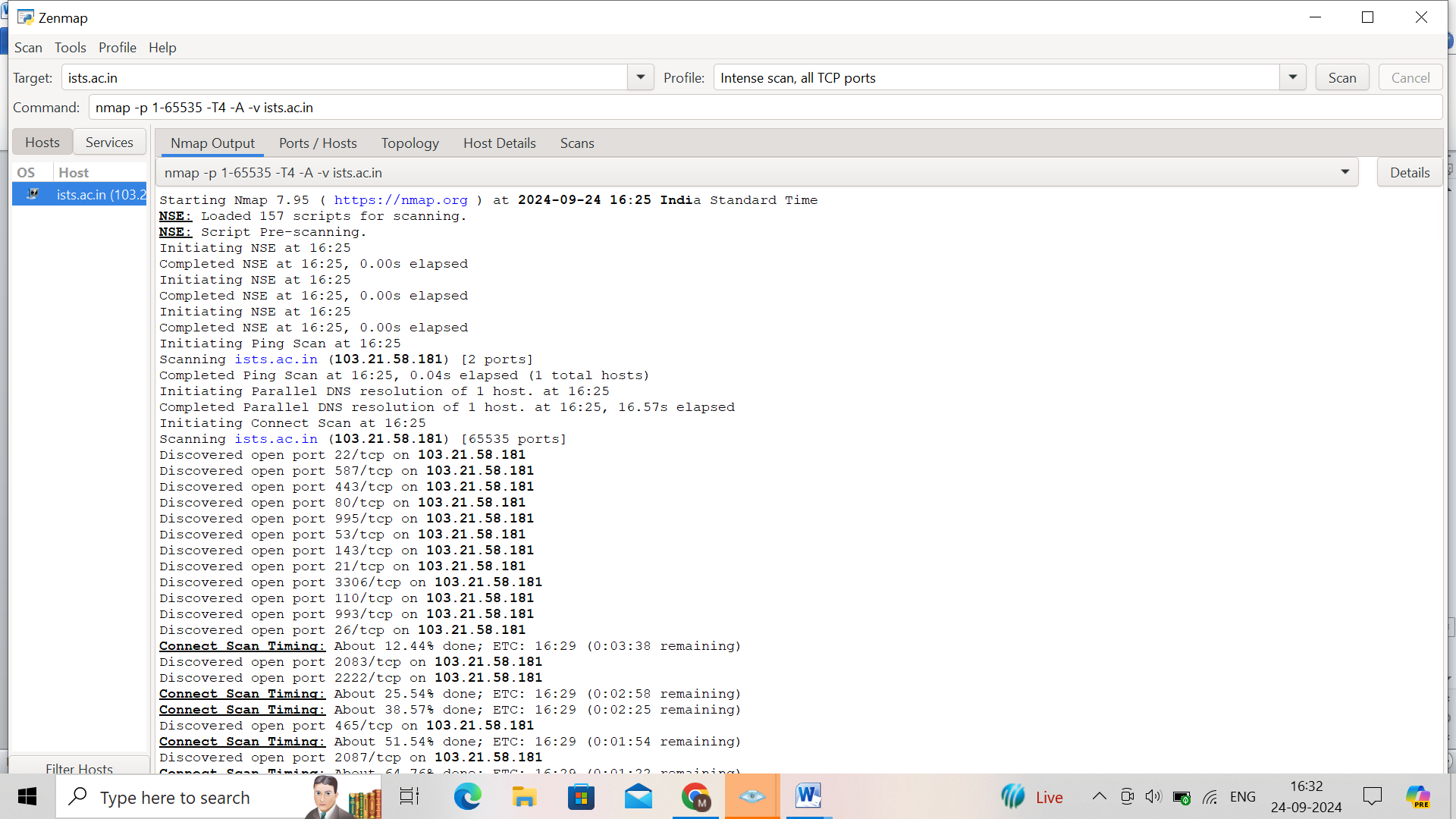
To do the port scanning which ports are open and which ports are closed





Task 2

Scanning a network which host are open and which host are closed bu using nmap tool



Connect Scan Timing: About 25.54% done; ETC: 16:29 (0:02:58 remaining)

Connect Scan Timing: About 38.57% done; ETC: 16:29 (0:02:25 remaining)

Discovered open port 465/tcp on 103.21.58.181

Connect Scan Timing: About 51.54% done; ETC: 16:29 (0:01:54 remaining)

Discovered open port 2087/tcp on 103.21.58.181

Connect Scan Timing: About 64.76% done; ETC: 16:29 (0:01:22 remaining)

Discovered open port 2077/tcp on 103.21.58.181

Discovered open port 2096/tcp on 103.21.58.181

Connect Scan Timing: About 77.92% done; ETC: 16:29 (0:00:51 remaining)

Discovered open port 2082/tcp on 103.21.58.181

Discovered open port 2095/tcp on 103.21.58.181

Discovered open port 2078/tcp on 103.21.58.181

Discovered open port 2086/tcp on 103.21.58.181

Completed Connect Scan at 16:29, 231.93s elapsed (65535 total ports)

Initiating Service scan at 16:29

Scanning 22 services on ists.ac.in (103.21.58.181)

Service scan Timing: About 72.73% done; ETC: 16:31 (0:00:32 remaining)

Completed Service scan at 16:31, 89.45s elapsed (22 services on 1 host)

NSE: Script scanning 103.21.58.181.

Initiating NSE at 16:31

Completed NSE at 16:31, 31.55s elapsed

Initiating NSE at 16:31

Completed NSE at 16:32, 28.54s elapsed

Initiating NSE at 16:32

Completed NSE at 16:32, 0.01s elapsed

Nmap scan report for ists.ac.in (103.21.58.181)

Host is up (0.042s latency).

Not shown: 65513 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

21/tcp open ftp Pure-FTPd

| ssl-cert: Subject: commonName=\*.webhostbox.net

| Subject Alternative Name: DNS:\*.webhostbox.net, DNS:webhostbox.net

| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-05-09T00:00:00

| Not valid after: 2025-05-09T23:59:59

| MD5: 2c90:81eb:2ed3:d5d7:63aa:0c24:a7c0:0a0b

|\_SHA-1: 77f3:d88e:0fdb:3c8d:6337:5cf2:d063:0e1a:7fae:b392

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

26/tcp open smtp Exim smtpd 4.96.2

|\_smtp-commands: Couldn't establish connection on port 26

53/tcp open domain ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)

| dns-nsid:

|\_ bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7\_9.5

80/tcp open http Apache httpd

| http-server-header:

| Apache

|\_ nginx/1.23.4

110/tcp open pop3 Dovecot pop3d

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

143/tcp open imap Dovecot imapd

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

443/tcp open ssl/http Apache httpd

| http-server-header:

| Apache

|\_ nginx/1.23.4

|\_ssl-date: TLS randomness does not represent time

| http-methods:

|\_ Supported Methods: HEAD POST

|\_http-title: ISTS

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

465/tcp open ssl/smtp Exim smtpd 4.96.2

| smtp-commands: bh-in-14.webhostbox.net Hello ists.ac.in [117.250.213.117], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP

|\_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

587/tcp open smtp Exim smtpd 4.96.2

|\_smtp-commands: Couldn't establish connection on port 587

993/tcp open imaps?

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

995/tcp open pop3s?

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

2077/tcp open tsrmagt?

2078/tcp open ssl/http cPanel httpd (unauthorized)

|\_http-server-header: cPanel

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

|\_ssl-date: TLS randomness does not represent time

2082/tcp open infowave?

2083/tcp open ssl/radsec?

| fingerprint-strings:

| GetRequest:

| HTTP/1.0 200 OK

| Connection: close

| Content-Type: text/html; charset="utf-8"

| Date: Tue, 24 Sep 2024 10:59:59 GMT

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Set-Cookie: cpsession=%3a\_LSYwn3SsIGQtTes%2ccb6c01e93048231bda2eee243633b0b0; HttpOnly; path=/; port=2083; secure

| Set-Cookie: roundcube\_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Set-Cookie: roundcube\_sessauth=expired; HttpOnly; domain=bh-in-14.webhostbox.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Set-Cookie: PPA\_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| X-Frame-Options: SAMEORIGIN

| X-Content-Type-

| HTTPOptions:

| HTTP/1.0 200 OK

| Connection: close

| Content-Type: text/html; charset="utf-8"

| Date: Tue, 24 Sep 2024 11:00:00 GMT

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Set-Cookie: cpsession=%3a5aZqRBO6IZm6ucs1%2ca85b09b3c94f0e6bd75ac65f6bd900cb; HttpOnly; path=/; port=2083; secure

| Set-Cookie: roundcube\_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Set-Cookie: roundcube\_sessauth=expired; HttpOnly; domain=bh-in-14.webhostbox.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Set-Cookie: PPA\_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| X-Frame-Options: SAMEORIGIN

|\_ X-Content-Type-

|\_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

2086/tcp open gnunet?

2087/tcp open ssl/eli?

|\_ssl-date: TLS randomness does not represent time

| fingerprint-strings:

| GetRequest:

| HTTP/1.0 200 OK

| Connection: close

| Content-Type: text/html; charset="utf-8"

| Date: Tue, 24 Sep 2024 10:59:59 GMT

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Set-Cookie: whostmgrsession=%3as6rY3V88xKYstGfq%2c92d5d02e9d5048b8133158649bed0754; HttpOnly; path=/; port=2087; secure

| Set-Cookie: roundcube\_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Set-Cookie: roundcube\_sessauth=expired; HttpOnly; domain=bh-in-14.webhostbox.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Set-Cookie: PPA\_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| X-Frame-Options: SAMEORIGIN

| HTTPOptions:

| HTTP/1.0 200 OK

| Connection: close

| Content-Type: text/html; charset="utf-8"

| Date: Tue, 24 Sep 2024 11:00:00 GMT

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Set-Cookie: whostmgrsession=%3aPQIctJLoThvAgNBo%2c823dea6b6dc9b3d654bbbc8969d09ebf; HttpOnly; path=/; port=2087; secure

| Set-Cookie: roundcube\_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Set-Cookie: roundcube\_sessauth=expired; HttpOnly; domain=bh-in-14.webhostbox.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Set-Cookie: PPA\_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

|\_ X-Frame-Options: SAMEORIGIN

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

2095/tcp open nbx-ser?

2096/tcp open ssl/nbx-dir?

| fingerprint-strings:

| GetRequest:

| HTTP/1.0 200 OK

| Connection: close

| Content-Type: text/html; charset="utf-8"

| Date: Tue, 24 Sep 2024 11:00:05 GMT

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: webmailsession=%3al4WX5TQZ31MqkyFV%2c7dfd18fd5d70f250f2f6d9bd07559b94; HttpOnly; path=/; port=2096; secure

| Set-Cookie: roundcube\_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: roundcube\_sessauth=expired; HttpOnly; domain=bh-in-14.webhostbox.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: PPA\_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: roundcube\_cookies=enabled; HttpOnly; expires=Wed, 24-Sep-2025 11:00:05 GMT; path=/; port=2096; secure

| HTTPOptions:

| HTTP/1.0 200 OK

| Connection: close

| Content-Type: text/html; charset="utf-8"

| Date: Tue, 24 Sep 2024 11:00:06 GMT

| Cache-Control: no-cache, no-store, must-revalidate, private

| Pragma: no-cache

| Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: webmailsession=%3avnouRbDcHdbnD7El%2c76f472cfbf93348c626b0a2761660684; HttpOnly; path=/; port=2096; secure

| Set-Cookie: roundcube\_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: roundcube\_sessauth=expired; HttpOnly; domain=bh-in-14.webhostbox.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

| Set-Cookie: PPA\_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure

|\_ Set-Cookie: roundcube\_cookies=enabled; HttpOnly; expires=Wed, 24-Sep-2025 11:00:06 GMT; path=/; port=2096; secure

|\_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=\*.ists.ac.in

| Subject Alternative Name: DNS:\*.ists.ac.in, DNS:ists.ac.in, DNS:www.edu.ists.ac.in

| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-08-20T04:29:20

| Not valid after: 2024-11-18T04:29:19

| MD5: 31a3:6326:5612:01e3:4a1b:dcf8:9b79:80b1

|\_SHA-1: d471:040e:ec16:4867:66d8:86bd:ecba:033c:2f12:9718

2222/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

|\_ 1024 e0:ae:22:b9:bc:53:e5:e7:51:0c:db:f0:ac:01:f5:4f (DSA)

3306/tcp open mysql MySQL 5.7.23-23

|\_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=\*.webhostbox.net

| Subject Alternative Name: DNS:\*.webhostbox.net, DNS:webhostbox.net

| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2024-05-09T00:00:00

| Not valid after: 2025-05-09T23:59:59

| MD5: 2c90:81eb:2ed3:d5d7:63aa:0c24:a7c0:0a0b

|\_SHA-1: 77f3:d88e:0fdb:3c8d:6337:5cf2:d063:0e1a:7fae:b392

3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port2083-TCP:V=7.95%T=SSL%I=7%D=9/24%Time=66F29BAF%P=i686-pc-windows-wi

SF:ndows%r(GetRequest,4000,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close

SF:\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nDate:\x20Tue,\x

SF:2024\x20Sep\x202024\x2010:59:59\x20GMT\r\nCache-Control:\x20no-cache,\x

SF:20no-store,\x20must-revalidate,\x20private\r\nPragma:\x20no-cache\r\nSe

SF:t-Cookie:\x20cprelogin=no;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\

SF:x2000:00:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x

SF:20cpsession=%3a\_LSYwn3SsIGQtTes%2ccb6c01e93048231bda2eee243633b0b0;\x20

SF:HttpOnly;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20roundcub

SF:e\_sessid=expired;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\x2000:00:

SF:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20roundcu

SF:be\_sessauth=expired;\x20HttpOnly;\x20domain=bh-in-14\.webhostbox\.net;\

SF:x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2

SF:083;\x20secure\r\nSet-Cookie:\x20PPA\_ID=expired;\x20HttpOnly;\x20expire

SF:s=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2083;\x20s

SF:ecure\r\nCache-Control:\x20no-cache,\x20no-store,\x20must-revalidate,\x

SF:20private\r\nPragma:\x20no-cache\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX

SF:-Content-Type-")%r(HTTPOptions,4000,"HTTP/1\.0\x20200\x20OK\r\nConnecti

SF:on:\x20close\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nDat

SF:e:\x20Tue,\x2024\x20Sep\x202024\x2011:00:00\x20GMT\r\nCache-Control:\x2

SF:0no-cache,\x20no-store,\x20must-revalidate,\x20private\r\nPragma:\x20no

SF:-cache\r\nSet-Cookie:\x20cprelogin=no;\x20HttpOnly;\x20expires=Thu,\x20

SF:01-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nS

SF:et-Cookie:\x20cpsession=%3a5aZqRBO6IZm6ucs1%2ca85b09b3c94f0e6bd75ac65f6

SF:bd900cb;\x20HttpOnly;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:

SF:\x20roundcube\_sessid=expired;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-19

SF:70\x2000:00:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie

SF::\x20roundcube\_sessauth=expired;\x20HttpOnly;\x20domain=bh-in-14\.webho

SF:stbox\.net;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=

SF:/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20PPA\_ID=expired;\x20HttpOnl

SF:y;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20por

SF:t=2083;\x20secure\r\nCache-Control:\x20no-cache,\x20no-store,\x20must-r

SF:evalidate,\x20private\r\nPragma:\x20no-cache\r\nX-Frame-Options:\x20SAM

SF:EORIGIN\r\nX-Content-Type-");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port2087-TCP:V=7.95%T=SSL%I=7%D=9/24%Time=66F29BAF%P=i686-pc-windows-wi

SF:ndows%r(GetRequest,9463,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close

SF:\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nDate:\x20Tue,\x

SF:2024\x20Sep\x202024\x2010:59:59\x20GMT\r\nCache-Control:\x20no-cache,\x

SF:20no-store,\x20must-revalidate,\x20private\r\nPragma:\x20no-cache\r\nSe

SF:t-Cookie:\x20whostmgrrelogin=no;\x20HttpOnly;\x20expires=Thu,\x2001-Jan

SF:-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2087;\x20secure\r\nSet-Coo

SF:kie:\x20whostmgrsession=%3as6rY3V88xKYstGfq%2c92d5d02e9d5048b8133158649

SF:bed0754;\x20HttpOnly;\x20path=/;\x20port=2087;\x20secure\r\nSet-Cookie:

SF:\x20roundcube\_sessid=expired;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-19

SF:70\x2000:00:01\x20GMT;\x20path=/;\x20port=2087;\x20secure\r\nSet-Cookie

SF::\x20roundcube\_sessauth=expired;\x20HttpOnly;\x20domain=bh-in-14\.webho

SF:stbox\.net;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=

SF:/;\x20port=2087;\x20secure\r\nSet-Cookie:\x20PPA\_ID=expired;\x20HttpOnl

SF:y;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20por

SF:t=2087;\x20secure\r\nCache-Control:\x20no-cache,\x20no-store,\x20must-r

SF:evalidate,\x20private\r\nPragma:\x20no-cache\r\nX-Frame-Options:\x20SAM

SF:EORIGIN\r\nX-C")%r(HTTPOptions,9463,"HTTP/1\.0\x20200\x20OK\r\nConnecti

SF:on:\x20close\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nDat

SF:e:\x20Tue,\x2024\x20Sep\x202024\x2011:00:00\x20GMT\r\nCache-Control:\x2

SF:0no-cache,\x20no-store,\x20must-revalidate,\x20private\r\nPragma:\x20no

SF:-cache\r\nSet-Cookie:\x20whostmgrrelogin=no;\x20HttpOnly;\x20expires=Th

SF:u,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2087;\x20secur

SF:e\r\nSet-Cookie:\x20whostmgrsession=%3aPQIctJLoThvAgNBo%2c823dea6b6dc9b

SF:3d654bbbc8969d09ebf;\x20HttpOnly;\x20path=/;\x20port=2087;\x20secure\r\

SF:nSet-Cookie:\x20roundcube\_sessid=expired;\x20HttpOnly;\x20expires=Thu,\

SF:x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2087;\x20secure\r

SF:\nSet-Cookie:\x20roundcube\_sessauth=expired;\x20HttpOnly;\x20domain=bh-

SF:in-14\.webhostbox\.net;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20G

SF:MT;\x20path=/;\x20port=2087;\x20secure\r\nSet-Cookie:\x20PPA\_ID=expired

SF:;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20pa

SF:th=/;\x20port=2087;\x20secure\r\nCache-Control:\x20no-cache,\x20no-stor

SF:e,\x20must-revalidate,\x20private\r\nPragma:\x20no-cache\r\nX-Frame-Opt

SF:ions:\x20SAMEORIGIN\r\nX-C");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port2096-TCP:V=7.95%T=SSL%I=7%D=9/24%Time=66F29BB5%P=i686-pc-windows-wi

SF:ndows%r(GetRequest,4000,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close

SF:\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nDate:\x20Tue,\x

SF:2024\x20Sep\x202024\x2011:00:05\x20GMT\r\nCache-Control:\x20no-cache,\x

SF:20no-store,\x20must-revalidate,\x20private\r\nPragma:\x20no-cache\r\nSe

SF:t-Cookie:\x20webmailrelogin=no;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-

SF:1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2096;\x20secure\r\nSet-Cook

SF:ie:\x20webmailsession=%3al4WX5TQZ31MqkyFV%2c7dfd18fd5d70f250f2f6d9bd075

SF:59b94;\x20HttpOnly;\x20path=/;\x20port=2096;\x20secure\r\nSet-Cookie:\x

SF:20roundcube\_sessid=expired;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970

SF:\x2000:00:01\x20GMT;\x20path=/;\x20port=2096;\x20secure\r\nSet-Cookie:\

SF:x20roundcube\_sessauth=expired;\x20HttpOnly;\x20domain=bh-in-14\.webhost

SF:box\.net;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;

SF:\x20port=2096;\x20secure\r\nSet-Cookie:\x20PPA\_ID=expired;\x20HttpOnly;

SF:\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=

SF:2096;\x20secure\r\nSet-Cookie:\x20roundcube\_cookies=enabled;\x20HttpOnl

SF:y;\x20expires=Wed,\x2024-Sep-2025\x2011:00:05\x20GMT;\x20path=/;\x20por

SF:t=2096;\x20secure")%r(HTTPOptions,4000,"HTTP/1\.0\x20200\x20OK\r\nConne

SF:ction:\x20close\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\n

SF:Date:\x20Tue,\x2024\x20Sep\x202024\x2011:00:06\x20GMT\r\nCache-Control:

SF:\x20no-cache,\x20no-store,\x20must-revalidate,\x20private\r\nPragma:\x2

SF:0no-cache\r\nSet-Cookie:\x20webmailrelogin=no;\x20HttpOnly;\x20expires=

SF:Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2096;\x20sec

SF:ure\r\nSet-Cookie:\x20webmailsession=%3avnouRbDcHdbnD7El%2c76f472cfbf93

SF:348c626b0a2761660684;\x20HttpOnly;\x20path=/;\x20port=2096;\x20secure\r

SF:\nSet-Cookie:\x20roundcube\_sessid=expired;\x20HttpOnly;\x20expires=Thu,

SF:\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2096;\x20secure\

SF:r\nSet-Cookie:\x20roundcube\_sessauth=expired;\x20HttpOnly;\x20domain=bh

SF:-in-14\.webhostbox\.net;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20

SF:GMT;\x20path=/;\x20port=2096;\x20secure\r\nSet-Cookie:\x20PPA\_ID=expire

SF:d;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20p

SF:ath=/;\x20port=2096;\x20secure\r\nSet-Cookie:\x20roundcube\_cookies=enab

SF:led;\x20HttpOnly;\x20expires=Wed,\x2024-Sep-2025\x2011:00:06\x20GMT;\x2

SF:0path=/;\x20port=2096;\x20secure");

Service Info: Host: bh-in-14.webhostbox.net; OS: Linux; CPE: cpe:/o:redhat:enterprise\_linux:7

NSE: Script Post-scanning.

Initiating NSE at 16:32

Completed NSE at 16:32, 0.01s elapsed

Initiating NSE at 16:32

Completed NSE at 16:32, 0.00s elapsed

Initiating NSE at 16:32

Completed NSE at 16:32, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 399.07 seconds

Task 3  
 Create a Vulnerability assessment report  
Tools used – Acunetix to do vulnerability scanning  
Finding – Risk Levels – High , Moderate and low  
TOOLS FOR LIVE NETWORK SCANNING

