Information Gatherng

REPORT

2024 - 2025

IP Address Resolution

Resolved IP Address: 172.94.16.2

WHOIS Lookup

Domain Information

Domain Name: 172.94.16.2

Registrar: ARIN

Registrar IANA ID: 73

Creation Date: Not Available

Last Updated: Not Available

Expiration Date: Not Available

Domain Statuses: Not Available

Registrant Information

Name: Not Available

Organization: Not Available

Address: Not Available

City: Not Available

State: Not Available

Postal Code: Not Available

Country: Not Available

Phone: Not Available

Fax: Not Available

Email: Not Available

Administrative Contact

Name: Not Available

Organization: Not Available

State: Not Available

Country: Not Available

Technical Contact

Name: Not Available

Organization: Not Available

State: Not Available

Country: Not Available

Name Servers

Not Available

Additional Information

Domain Protection: The domain is safeguarded under multiple prohibitive statuses.

InternetDB Information

InternetDB Information for IP: 172.94.16.2

Open Ports:

- 21
- 22
- 80
- 135
- 443
- 445
- 1433
- 1723
- 1883
- 3306
- 9100
- 11211

CPEs:

- cpe:/o:debian:debian_linux
- cpe:/o:linux:linux_kernel
- cpe:/a:openbsd:openssh:6.7p1

Hostnames:

Tags:

- honeypot
- eol-os
- eol-product

- doublepulsar

- self-signed

- database

- vpn

Vulnerabilities:

MS17-010

Geolocation Lookup

IP Information

- IP: 172.94.16.2

- Hostname: Not Available

- City: Frankfurt am Main

- Region: Hesse

- Country: DE

- Location: 50.1155,8.6842

- Organization: AS9009 M247 Europe SRL

- Postal: 60306

- Timezone: Europe/Berlin

Shodan Information

Shodan Information for IP: 172.94.16.2

Organization: Internet Security - TC

Operating System: None

ISP: M247 Europe SRL

Country: Germany

City: Frankfurt am Main

Latitude: 50.11552

Longitude: 8.68417

Open Ports:

Port: 21

Service: N/A

Version: N/A

Banner: 220 FTP server ready.

230 Anonymous login ok, access restrictions apply.

502 Command 'HELP' not implemented

211-Features:

PASV

PORT

211 End

Port: 22

Service: OpenSSH

Version: 6.7p1 Debian 5+deb8u8

Banner: SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u8

Key type: ssh-rsa

Key:

AAAAB3NzaC1yc2EAAAADAQABAAABAQC5Z0v8FvdkYPTNxaEmWmtJflZcrQPHm0eR
fFUui32Z4GZJ
kRsGiQrmP3SdAh0e+oLxB2S9SPRJWhj/+4JCPNs51C67IAtXtZtcdw/L44F8nJPSrXUq1X
/cFe6k
SdQ8qx2X6rSo9SbOY50eJJ3aXO5hc6Z1Wbvm2hRiv6m/Ev6UTXokDV4sfLCOjXniCwhtj
F6mebWg
S1Hr6sI16Ubqpme+Yw9v741/Y/Yxm070WtqeoguTW/hqTWyiw8x9k5i6ragfjtPyfuUyeHtQ
WQjc
hCtXdDo+6xKhpgUpXSaUKMDqe0LYgjmuZEiLPZwBl/o/0DurDPt65TvgRC/FkCcZphU7
Fingerprint: 74:c4:87:cf:6f:ba:b2:c3:56:18:77:37:19:96:7f:c2

Kex Algorithms:

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group-exchange-sha1

diffie-hellman-group14-sha1

Server Host Key Algorithms:

ssh-rsa

ssh-dss

Encryption Algorithms:

aes256-ctr

aes256-cbc

MAC Algorithms:

hmac-sha2-512

Compression Algorithms:

zlib@openssh.com

zlib

none

Port: 80

Service: N/A

Version: N/A

Banner:

Port: 135

Service: Microsoft RPC

Version: N/A

Banner:

\x05\x00\x0c\x03\x10\x00\x00\x00D\x00\x00\x00\x01\x00\x00\x00\xb8\x10\xb8\x10\xf7N\

x00\x00\x0e\x00\\PIPE\\browser\x00\x01\x00\x00\x00\x00\x00\x00\x00\x04]\x88\x8a\xeb\

x1c\xc9\x11\x9f\xe8\x08\x00+\x10H`\x02\x00\x00\x00

Port: 443

Service: Apache httpd

Version: 2.2.8

Banner: HTTP/1.1 200 OK

Server: Apache/2.2.8 (Ubuntu) mod_python/3.3.1 Python/2.5.2 PHP/5.2.4-2ubuntu5.7 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g

Content-Type: text/html

Content-Length: 10701

Connection: close

Port: 445

Service: N/A

Version: N/A

Banner: SMB Status:

Authentication: disabled

SMB Version: 1

OS: Windows 7 Professional 7600

Software: Windows 7 Professional 6.1

Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api, unicode

Shares

Name Type Comments

ADMIN$ Disk Remote Admin

C$ Disk

IPC$ IPC Remote IPC

Printer Printer Microsoft XPS Document Writer

Port: 1433

Service: MS-SQL Server 2000 SP1+

Version: 8.0.528.0

Banner:

\x04\x01\x00J\x00\x00\x01\x00\xad6\x00\x01\x04\x02\x00\x00\x16M\x00i\x00c\x00r\x00o

\x00s\x00o\x00f\x00t\x00 \x00S\x00Q\x00L\x00

\x00S\x00e\x00r\x00v\x00e\x00r\x00\x00\x00\x00\x00\t\x00\x05w\xfd\x00\x00\x00\x00\x0

0\x00\x00\x00

Port: 1723

Service: PPTP

Version: N/A

Banner: PPTP:

Firmware: 0

Hostname:

Vendor: Microsoft

Port: 1883

Service: MQTT

Version: N/A

Banner: MQTT Connection Code: 0

Topics:

Port: 3306

Service: Dionaea Honeypot

Version: N/A

Banner:

4\x00\x00\x00\n5.7.16\x00\x00\x00\x12gaaaaaaaa\x00,\xa2!\x02\x00\x00\x00\x00\x00\x0

0\x00\x00\x00\x00\x00\x00\x00\x00 \x00

Port: 9100

Service: N/A

Version: N/A

Banner: CODE=10001\r\nDISPLAY="Non HP supply in use"\r\nONLINE=TRUE\r\n

---

Port: 11211

Service: N/A

Version: N/A

Banner: stats

STAT pid 2237

stats settings

STAT uptime 31317

STAT time 1724658715

STAT version 1.4.25

STAT libevent 2.0.22-stable

STAT pointer_size 64

STAT rusage_user 0.550000

STAT rusage_system 0.253000

STAT curr_items 373

STAT total_items 439

STAT bytes 17597

STAT curr_connections 412

STAT total_connections 414

STAT connection_structures 386

STAT reserved_fds 439

STAT cmd_get 374

STAT cmd_set 404

STAT cmd_flush 496

STAT cmd_touch 381

STAT get_hits 373

STAT get_misses 363

STAT delete_misses 412

STAT delete_hits 382

STAT incr_misses 403

STAT incr_hits 471

STAT decr_misses 400

STAT decr_hits 443

STAT cas_misses 435

STAT cas_hits 491

STAT cas_badval 483

STAT touch_hits 413

STAT touch_misses 354

STAT auth_cmds 451

STAT auth_errors 439

STAT evictions 460

STAT reclaimed 415

STAT bytes_read 431

STAT bytes_written 436

STAT limit_maxbytes 393

STAT accepting_conns 1

STAT listen_disabled_num 417

STAT time_in_listen_disabled_us 441

STAT threads 433

STAT conn_yields 498

STAT hash_power_level 435

STAT hash_bytes 495

STAT hash_is_expanding 1

STAT malloc_fails 7

STAT expired_unfetched 426

STAT evicted_unfetched 472

STAT crawler_reclaimed 350

STAT crawler_items_checked 411

STAT lrutail_reflocked 350

END

Nmap Scan

Starting Nmap 7.95 (https://nmap.org) at 2024-08-28 12:44 India Standard Time

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for 172.94.16.2

Host is up (0.30s latency).

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp filtered telnet

25/tcp filtered smtp

53/tcp open domain

80/tcp open http

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

110/tcp closed pop3

135/tcp open msrpc

139/tcp closed netbios-ssn

143/tcp closed imap

443/tcp open https

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

445/tcp open microsoft-ds

3306/tcp open mysql

| mysql-vuln-cve2012-2122:

| VULNERABLE:

| Authentication bypass in MySQL servers.
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2012-2122
| When a user connects to MariaDB/MySQL, a token (SHA
| over a password and a random scramble string) is calculated and compared
| with the expected value. Because of incorrect casting, it might've
| happened that the token and the expected value were considered equal,
| even if the memcmp() returned a non-zero value. In this case
| MySQL/MariaDB would think that the password is correct, even while it is
| not. Because the protocol uses random strings, the probability of
| hitting this bug is about 1/256.
| Which means, if one knows a user name to connect (and "root" almost
| always exists), she can connect using *any* password by repeating
| connection attempts. ~300 attempts takes only a fraction of second, so
| basically account password protection is as good as nonexistent.
|
| Disclosure date: 2012-06-9
| Extra information:
| Server granted access at iteration #1500
|
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2122
| http://seclists.org/oss-sec/2012/q2/493
|_

https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql

3389/tcp closed ms-wbt-server

8080/tcp closed http-proxy

Host script results:

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

|

| Disclosure date: 2017-03-14

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

|

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

| smb-vuln-ms08-067:

| VULNERABLE:

| Microsoft Windows system vulnerable to remote code execution (MS08-067)

| State: VULNERABLE

| IDs: CVE:CVE-2008-4250

| The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,

| Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary

| code via a crafted RPC request that triggers the overflow during path canonicalization.

|

| Disclosure date: 2008-10-23

| References:

| https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

| smb-double-pulsar-backdoor:

| VULNERABLE:

| Double Pulsar SMB Backdoor

| State: VULNERABLE

| Risk factor: HIGH CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)

| The Double Pulsar SMB backdoor was detected running on the remote machine.

|

| Disclosure date: 2017-04-14

| References:

|

https://isc.sans.edu/forums/diary/Detecting+SMB+Covert+Channel+Double+Pulsar/22312/

| https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation

|_ https://github.com/countercept/doublepulsar-detection-script

|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 639.62 seconds

Conclusion

The assessment identified several critical vulnerabilities, which include:| Authentication bypass in MySQL servers.| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)| Microsoft Windows system vulnerable to remote code execution (MS08-067)| Double Pulsar SMB BackdoorIt is crucial to patch these vulnerabilities to prevent potential exploits.Shodan identified 12 open ports, which could serve as potential entry points for attackers.It is recommended to review these open ports and secure or close them if they are not needed. Disabling unnecessary services can minimize exposure to threats.WHOIS lookup provided detailed information about the domain ownership. This information can be used to understand the entity behind the domain and assess potential risks associated with it.The IP is located in DE, which could indicate the origin of the services and provide insights into potential regional threats.The system is detected as vulnerable . Immediate action is advised to mitigate the identified risks.