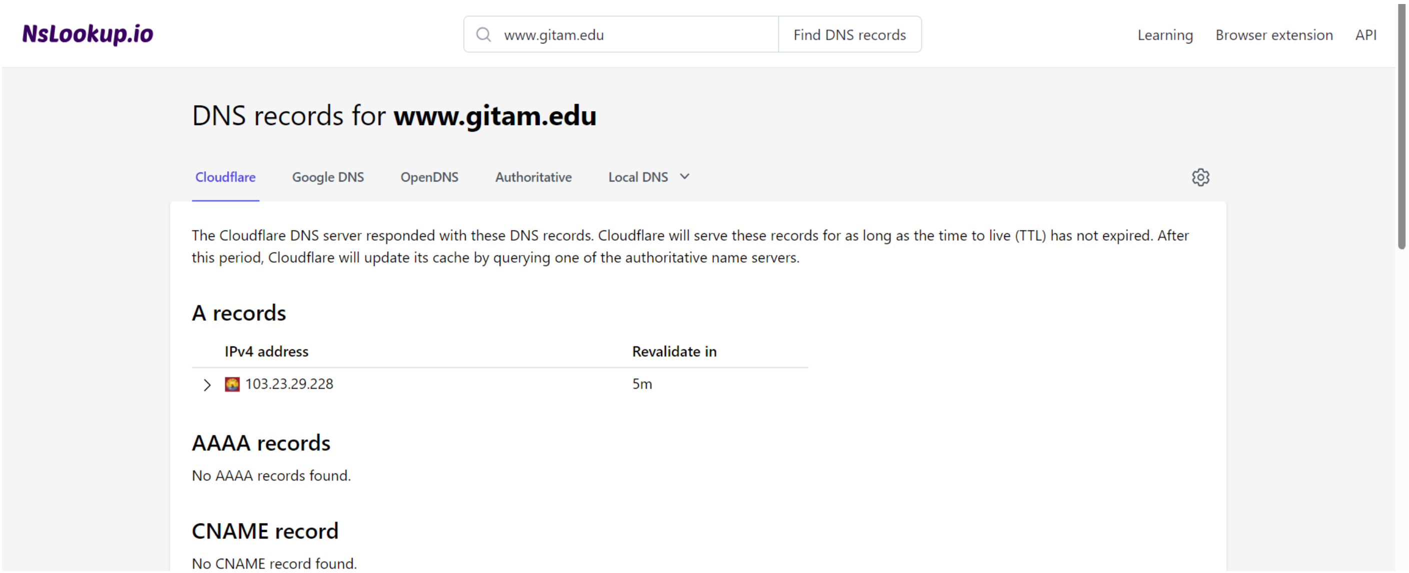
TASK 5 (04-09-23)

Overview of the assignment : Select any website and collect footprint reconnaissance information about it . Do passive reconnaissance . (nslookup.io , nessus and shodan)

What is nslookup.io?

nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address, or other DNS records.It stands for "Name Server Lookup." This tool is available on various operating systems, including Windows, macOS, and Linux.



DNS records for **www.gitam.edu**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
103.23.29.228	5m

AAAA records

No AAAA records found.

CNAME record

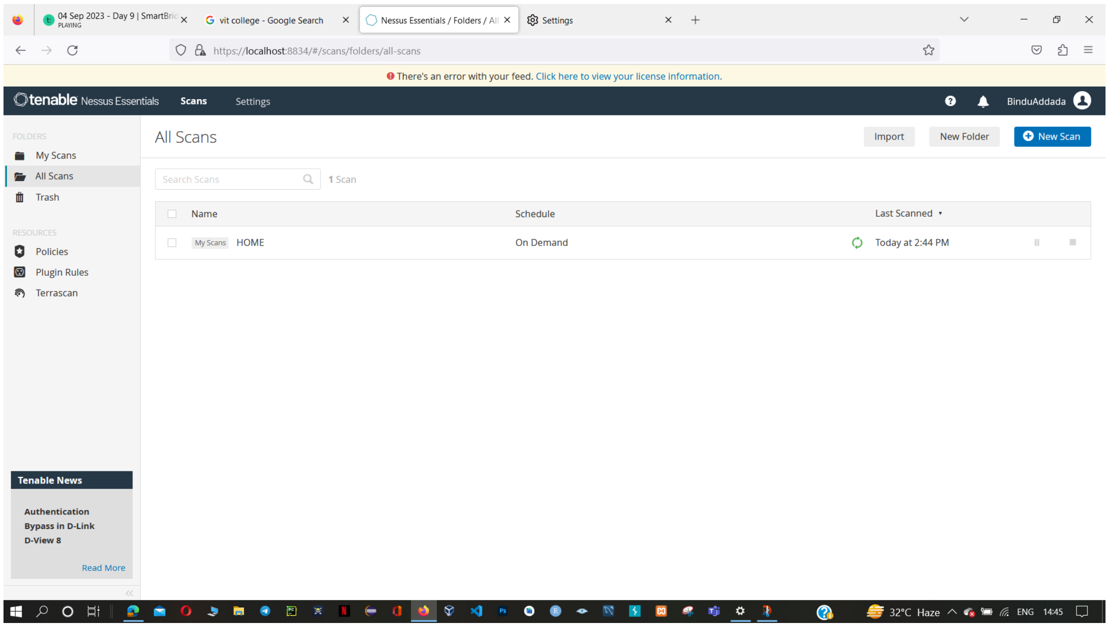
No CNAME record found.

Here I am using the nslookup to find out the ip address associated with the website, which will help us further in gathering the information about the network.

What is NESSUS ?

Nessus is a popular and widely used vulnerability scanning tool. It is designed to identify vulnerabilities, misconfigurations, and security issues in computer systems and networks. Nessus is commonly employed by security professionals, penetration testers, and system administrators to assess the security posture of their systems and networks.

Here I will be scanning my home network to show how nessus produces a scan and I am going for a basic network scan



https://localhost:8834/#/scans/folders/all-scans

There's an error with your feed. Click here to view your license information.

All Scans

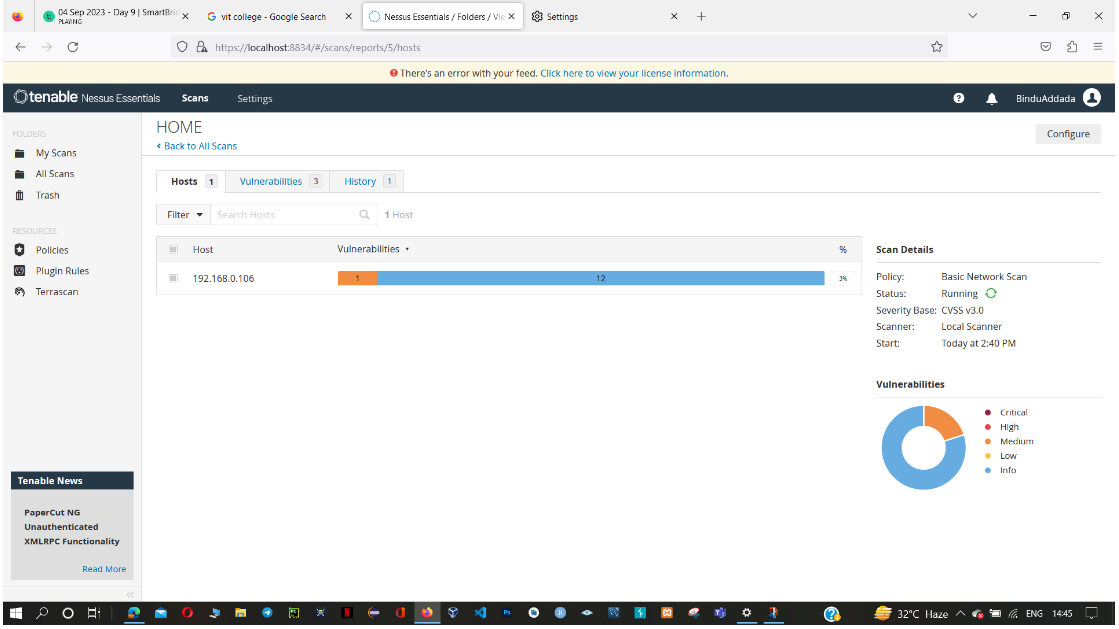
1 Scan

Name	Schedule	Last Scanned
My Scans HOME	On Demand	Today at 2:44 PM

Tenable News

Authentication Bypass in D-Link D-View 8

32°C Haze ENG 14:45



https://localhost:8834/#/scans/reports/5/hosts

There's an error with your feed. Click here to view your license information.

HOME

Back to All Scans

1 Host

Host	Vulnerabilities	%
192.168.0.106	1 12	3%

Scan Details

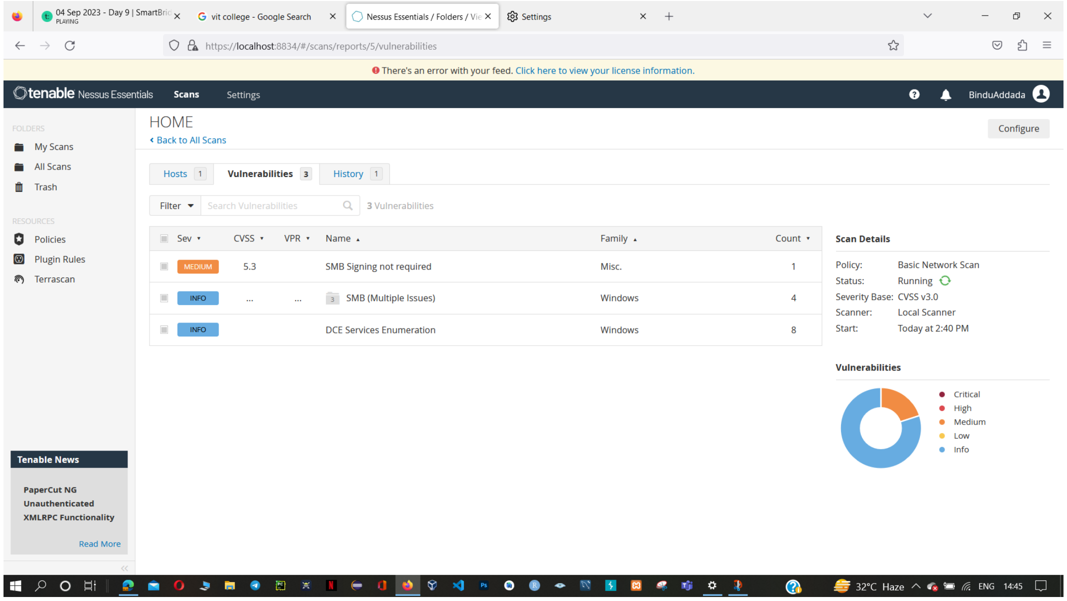
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:40 PM

Vulnerabilities

Tenable News

PaperCut NG Unauthenticated XMLRPC Functionality

32°C Haze ENG 14:45



There's an error with your feed. Click here to view your license information.

HOME

‹ Back to All Scans

3 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MEDIUM	5.3		SMB Signing not required	Misc.	1
INFO	...	...	3 SMB (Multiple Issues)	Windows	4
INFO			DCE Services Enumeration	Windows	8

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 2:40 PM

Vulnerabilities

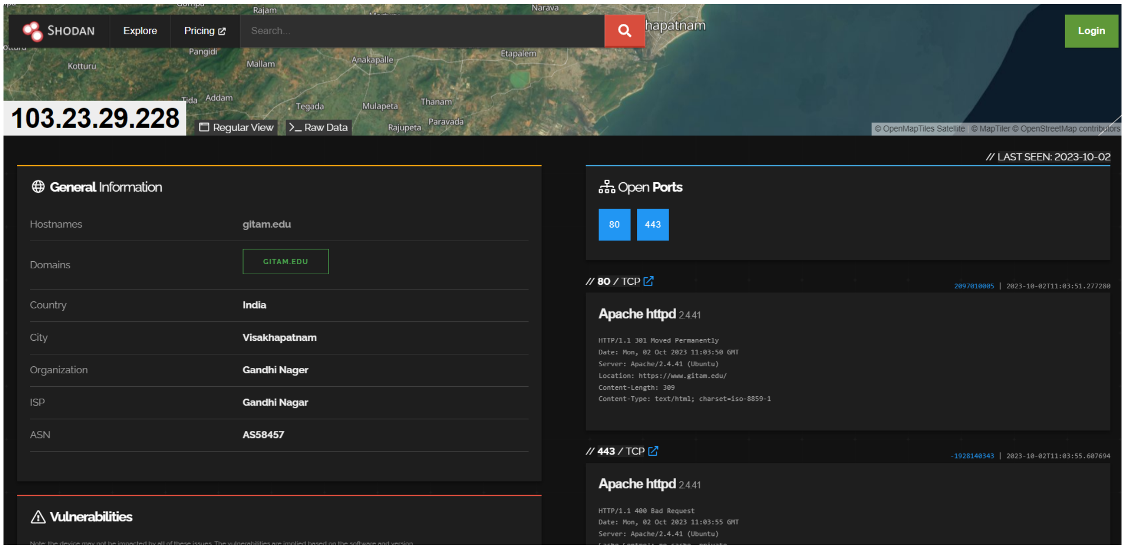
PaperCut NG Unauthenticated XMLRPC Functionality

What is SHODAN ?

This is another website that can be used to check the open ports on different IP addresses.It takes an ip address as the input and gives information about that website.

Shodan is a search engine designed to find and index internet-connected devices and systems. It's often referred to as the "search engine for hackers" because it can be used to discover devices and services that may have security vulnerabilities

Here is an example of information we could get by using the shodan : (I will be using gitam.edu ip address we attained through the nslookup)



103.23.29.228

// LAST SEEN: 2023-10-02

General Information

Hostnames	gitam.edu
Domains	GITAM.EDU
Country	India
City	Visakhapatnam
Organization	Gandhi Nager
ISP	Gandhi Nagar
ASN	AS58457

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

Open Ports

80 443

// 80 / TCP 2097010005 | 2023-10-02T11:03:51.277280

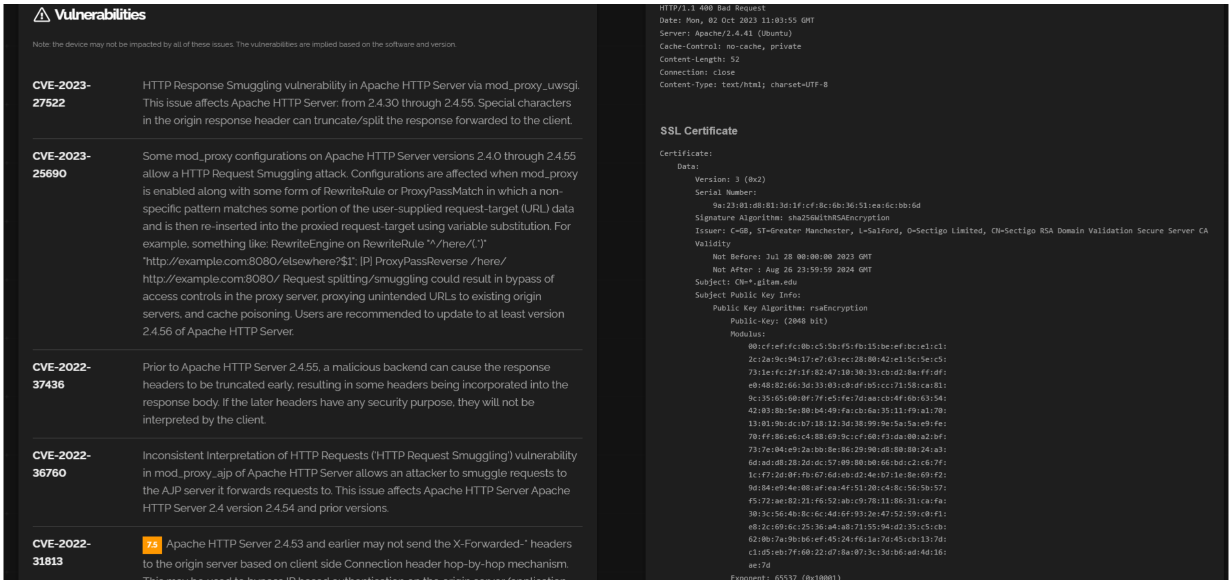
Apache httpd 2.4.41

```
HTTP/1.1 301 Moved Permanently
Date: Mon, 02 Oct 2023 11:03:50 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: https://www.gitam.edu/
Content-Length: 309
Content-Type: text/html; charset=iso-8859-1
```

// 443 / TCP -1928140343 | 2023-10-02T11:03:55.607694

Apache httpd 2.4.41

```
HTTP/1.1 400 Bad Request
Date: Mon, 02 Oct 2023 11:03:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
```



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-27522	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.
CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2022-37436	Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
CVE-2022-36760	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
CVE-2022-31813	7.5 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism.

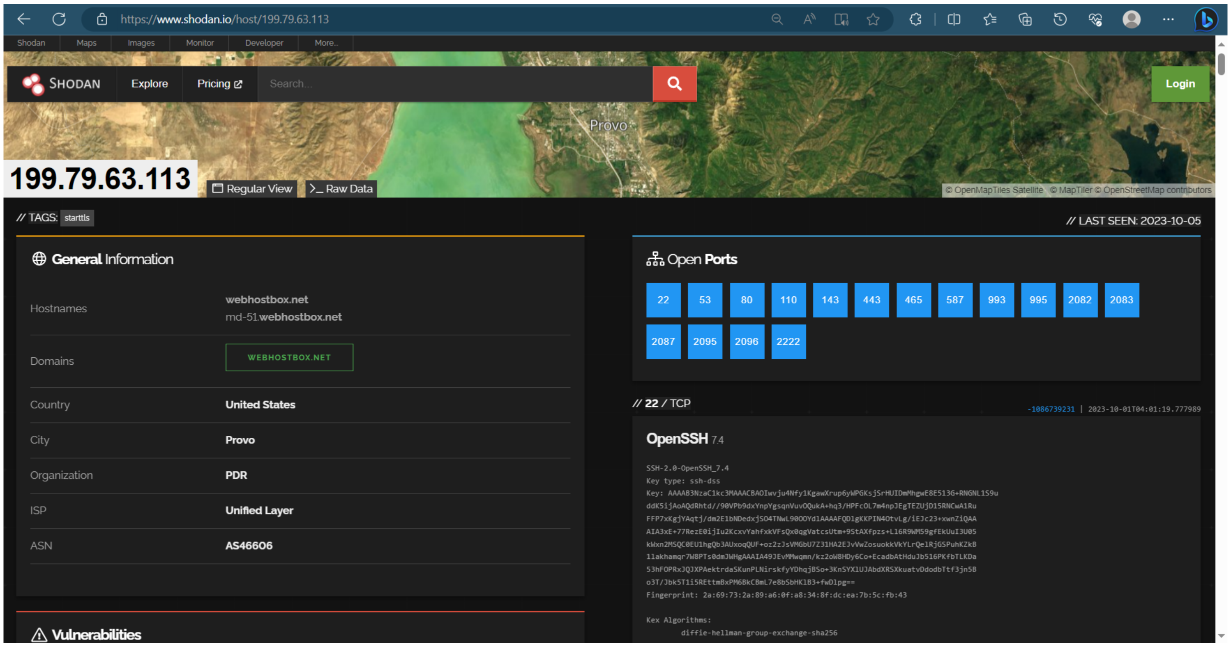
```
HTTP/1.1 400 Bad Request
Date: Mon, 02 Oct 2023 11:03:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
Content-Length: 52
Connection: close
Content-Type: text/html; charset=UTF-8
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9a:23:01:d8:81:3d:1f:cf:8c:6b:36:51:ea:6c:bb:6d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
        Validity
            Not Before: Jul 28 00:00:00 2023 GMT
            Not After : Aug 26 23:59:59 2024 GMT
        Subject: CN=*.gitam.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cf:ef:fc:0b:c5:5b:f5:fb:15:be:ef:bc:e1:c1:
                    2c:2a:9c:94:17:e7:63:ec:28:80:42:e1:5c:5e:c5:
                    73:1e:fc:2f:1f:82:47:10:30:33:cb:d2:8a:ff:df:
                    e0:48:82:66:3d:33:03:c0:df:b5:cc:71:58:ca:81:
                    9c:35:65:60:0f:7f:e5:fe:7d:aa:cb:4f:6b:63:54:
                    42:03:8b:5e:80:b4:49:fa:cb:6a:35:11:f9:a1:70:
                    13:01:9b:dc:b7:18:12:3d:38:99:9e:5a:5a:e9:fe:
                    70:ff:86:e6:c4:88:69:9c:cf:60:f3:da:00:a2:bf:
                    73:7e:04:e9:2a:bb:8e:86:29:90:d8:80:80:24:a3:
                    6d:ad:d8:28:2d:dc:57:09:80:b0:66:bd:c2:c6:7f:
                    1c:f7:2d:0f:fb:67:6d:eb:d2:4e:b7:1e:8e:69:f2:
                    9d:84:e9:4e:08:af:ea:4f:51:20:c4:8c:56:5b:57:
                    f5:72:ae:82:21:f6:52:ab:c9:78:11:86:31:ca:fa:
                    30:3c:56:4b:8c:6c:4d:6f:93:2e:47:52:59:c0:f1:
                    e8:2c:69:6c:25:36:a4:a8:71:55:94:d2:35:c5:cb:
                    62:0b:7a:9b:b6:ef:45:24:f6:1a:7d:45:cb:13:7d:
                    c1:d5:eb:7f:60:22:d7:8a:07:3c:3d:b6:ad:4d:16:
                    ae:7d
                Exponent: 65537 (0x10001)
```

Through SHODAN we can see the ports that are currently open and possible vulnerabilities that could be exploited.It doesn't however provide the information about the service at times and it only shows the open ports.

Example of a website which might be vulnerable to attacks because of too many open ports :


https://www.shodan.io/host/199.79.63.113
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Pricing
Search...
Login
Provo
© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors
Regular View
>_ Raw Data

199.79.63.113

// TAGS: starttls

// LAST SEEN: 2023-10-05

General Information

Hostnames	webhostbox.net md-51.webhostbox.net
Domains	WEBHOSTBOX.NET
Country	United States
City	Provo
Organization	PDR
ISP	Unified Layer
ASN	AS46606

Vulnerabilities

Open Ports

22 53 80 110 143 443 465 587 993 995 2082 2083 2087 2095 2096 2222

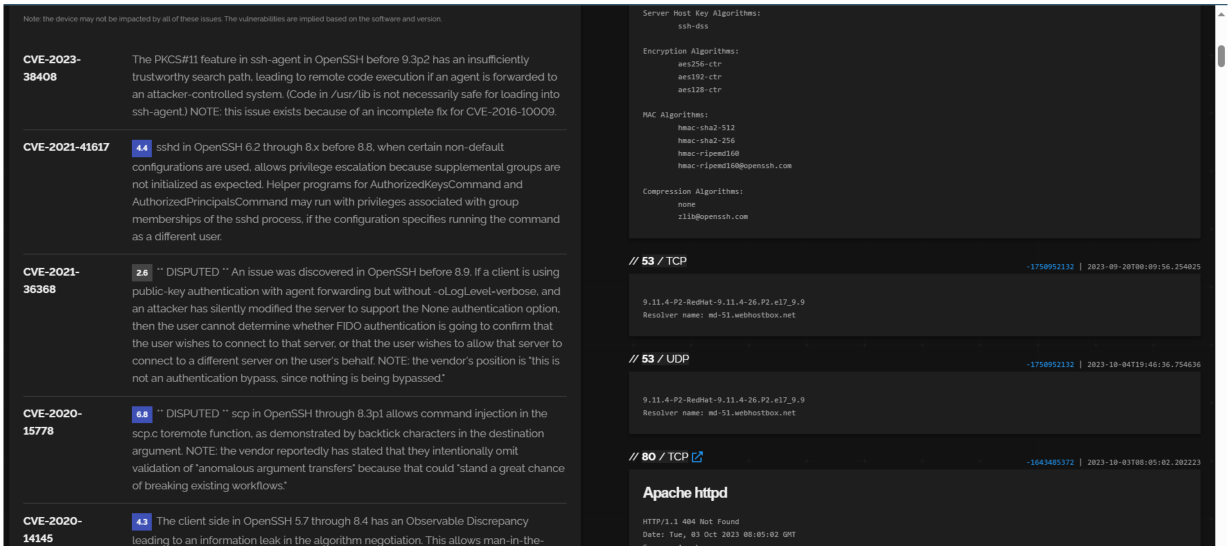
// 22 / TCP

-1086739231 | 2023-10-01T04:01:19.777989

OpenSSH 7.4

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-dss
Key: AAAAB3NzaC1kc3MAAACBAOIwvju4Nfy1KgawXrup6yWPGKsjSrHUIDmMhgwE8E513G+RNGNL1S9u
ddK5ijAoAQdRhtd//90VPb9dxYnpYgsqnVuvOQukA+hq3/HPFcOL7m4npJEgTEZUjD15RNCwA1Ru
FFP7xKgjYAqtj/dm2E1bNDedxjSO4TNwL90OOYdlAAAAFQDlgKKPIN4OtvLg/iEJc23+xwnZiQAA
AIA3xE+77RezE0ijIu2KcxvYahfxkVFsQx0qgVatcsUtm+9StAXfpzs+Ll6R9WM59gfEkUuI3U05
kWxn2MSQC0EU1hgQb3AUxoqQUF+oz2zJsVMGbU7Z31HA2EJvVwZosuokkVkYLrQelRjGSPuhKZkB
1lakhamqr7W8PTs0dmJWHgAAAIA49JEvMMwqmn/kz2oW8HDy6Co+EcadbAtHduJb516PKfbTLKDa
53hFOPRxJQJXPAektrdaSKunPLNirskfyYDhqjBSo+3KnSYXlUJAbdXRSXkuatvDdodbTtf3jn5B
o3T/Jbk5T1i5REttmBxPM6BkCBmL7e8bSbHKlB3+fwDlpg==
Fingerprint: 2a:69:73:2a:89:a6:0f:a8:34:8f:dc:ea:7b:5c:fb:43

Kex Algorithms:
        diffie-hellman-group-exchange-sha256
```



Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-38408 The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

CVE-2021-41617 4.4 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

CVE-2021-36368 2.6 ** DISPUTED ** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

CVE-2020-15778 6.8 ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

CVE-2020-14145 4.3 The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-

```
Server Host Key Algorithms:
        ssh-dss

Encryption Algorithms:
        aes256-ctr
        aes192-ctr
        aes128-ctr

MAC Algorithms:
        hmac-sha2-512
        hmac-sha2-256
        hmac-ripemd160
        hmac-ripemd160@openssh.com

Compression Algorithms:
        none
        zlib@openssh.com
```

// **53** / TCP

-1750952132 | 2023-09-20T00:09:56.254025

```
9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
Resolver name: md-51.webhostbox.net
```

// **53** / UDP

-1750952132 | 2023-10-04T19:46:36.754636

```
9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
Resolver name: md-51.webhostbox.net
```

// **80** / TCP

-1643485372 | 2023-10-03T08:05:02.202223

Apache httpd

```
HTTP/1.1 404 Not Found
Date: Tue, 03 Oct 2023 08:05:02 GMT
```