

Information Gathering Report

Target: scanme.nmap.org

Domain: nmap.org

Platform Used: Kali Linux

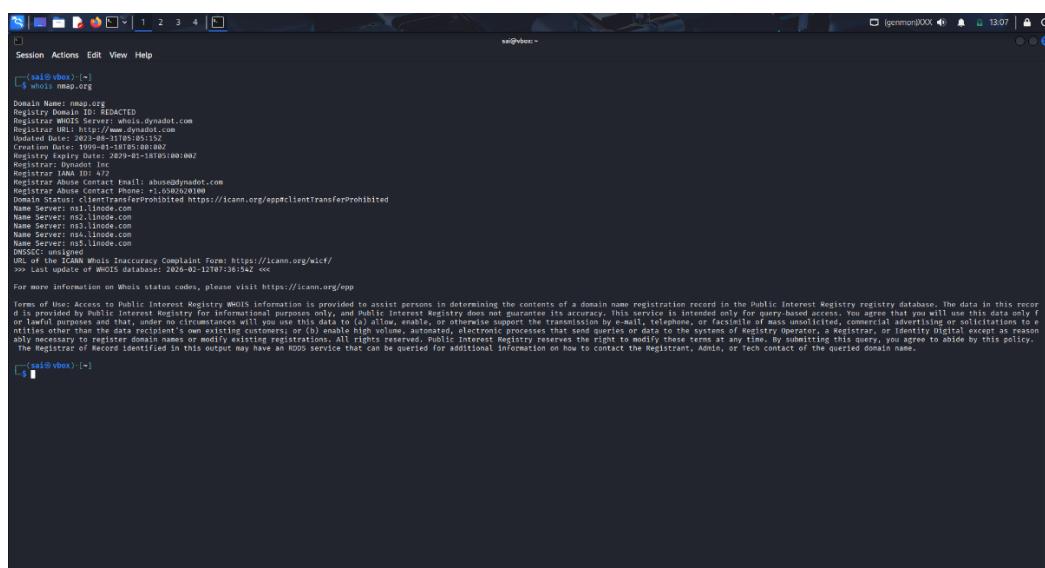
Tools Used: whois, nslookup, dig, subfinder, amass, whatweb, gobuster, nmap, theHarvester

Prepared By: Sai Vardhan

Date: 12 February 2026

Basic Information

1.1. Who is information



```
sai@vbox:~$ whois nmap.org
Domain Name: nmap.org
Registrar: Dynadot Inc [REDACTED]
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: https://www.dynadot.com
Updated Date: 2020-01-12T07:38:54Z
Creation Date: 1999-01-18T05:00:00Z
Expiration Date: 2029-01-18T05:00:00Z
Registrar IP: 67.202.123.222
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.650.526.1000
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ns1.linode.com
Name Server: ns2.linode.com
Name Server: ns3.linode.com
Name Server: ns4.linode.com
Name Server: ns5.linode.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/
>>> Last update of WHOIS database: 2020-01-12T07:38:54Z <<
For more information on Whois status codes, please visit https://icann.org/epp

Terms of Use: Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the Public Interest Registry registry database. The data in this record is provided by Public Interest Registry for informational purposes only, and Public Interest Registry does not guarantee its accuracy. This service is intended only for general-based access. You agree that you will use this data solely for the purpose of determining the contents of a domain name registration record in the Public Interest Registry registry database. You further agree that you will not (a) attempt to extract other information about other registrants by using automated means or processes, such as robots, spybots, screen scrapers, or the like, unless such processes are reasonably necessary to register domain names or modify existing registrations; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Identity Digital except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. Public Interest Registry reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.
The domain record identified in this output may have an ICANN service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
```

Domain Name: nmap.org

Registrar: Dynadot Inc

WHOIS Server: whois.dynadot.com

Creation Date: 1999-01-18

Expiry Date: 2029-01-18

Domain Status: clientTransferProhibited

Name Servers:

- ns1.linode.com
- ns2.linode.com

- ns3.linode.com
 - ns4.linode.com
 - ns5.linode.com

DNSSEC: unsigned

Explanation

The WHOIS lookup was performed on the parent domain nmap.org, since scanme.nmap.org is a subdomain and does not have separate WHOIS records.

The domain nmap.org is registered with Dynadot Inc and was originally created on January 18, 1999. The domain is currently active and protected with a clientTransferProhibited status, which prevents unauthorized domain transfers.

The authoritative name servers are hosted under linode.com, indicating that the DNS infrastructure is managed via Linode. DNSSEC is currently unsigned.

1.2 DNS Resolution (nslookup)

```
[root@vbox ~]# nslookup scanner.map.org
Server: 10.70.62.249#53
Address: 10.70.62.249#53

Non-authoritative answer:
Name: scanner.map.org
Name: scanner.map.org
Name: scanner.map.org
Address: 10.70.62.100:16181002

[root@vbox ~]#
```

DNS Server Used: 10.76.62.40

IPv4 Address: 45.33.32.156

IPv6 Address: 2600:3c01::f03c:91ff:fe18:bb2f

Response Type: Non-authoritative answer

Explanation

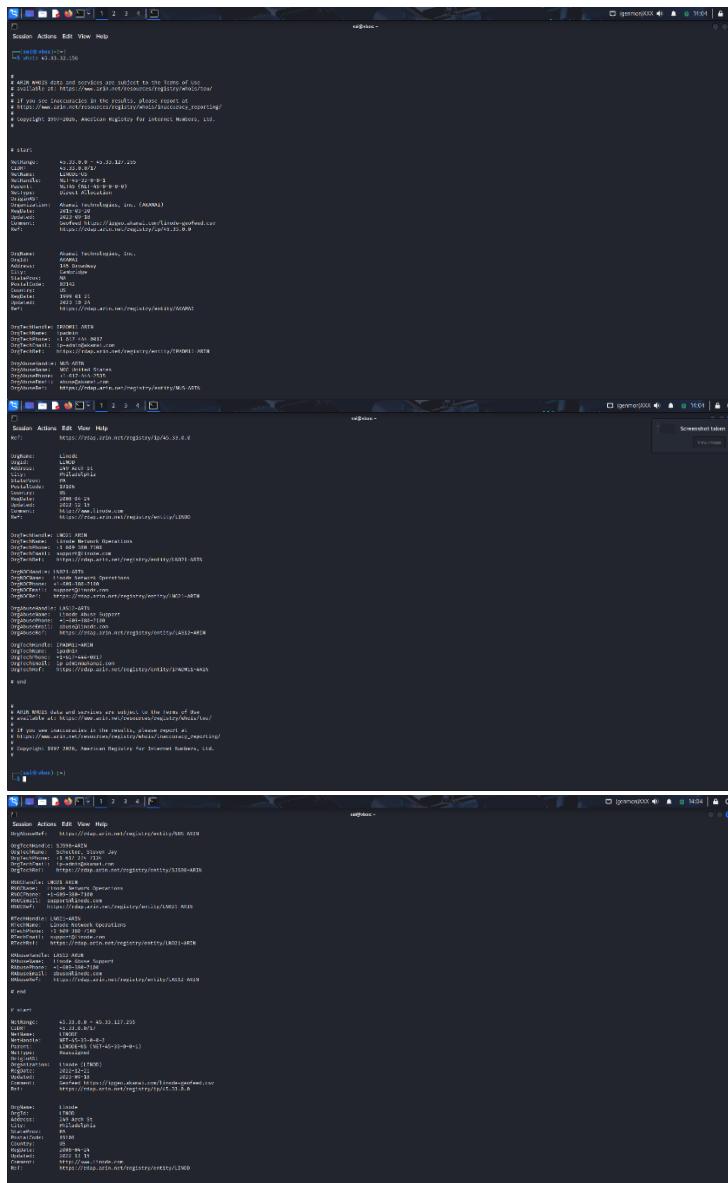
A DNS lookup was performed using the nslookup command to resolve the target domain scanme.nmap.org

The domain resolves to the IPv4 address 45.33.32.156 and an IPv6 address 2600:3c01::f03c:91ff:fe18:bb2f

The response was received as a non-authoritative answer, meaning the information was retrieved from a caching DNS server rather than directly from the authoritative name server.

The IP address 45.33.32.156 will be used in further reconnaissance activities such as port scanning and service enumeration.

1.3 — Hosting Provider & IP WHOIS



The image contains three vertically stacked terminal windows, each displaying WHOIS information for a specific IP address. The top window shows results for 45.33.32.156, the middle for 45.33.0.0, and the bottom for 45.33.127.255. The output is in plain text, listing various fields such as network, organization, and contact details.

```
Session Actions Edit View Help
└── whois 45.33.32.156

# Whois query and version are subject to the terms of use
# available at: https://www.iana.org/registry/whois/tos/
# If you see inaccuracies in the results, please report at
# https://www.iana.org/registry/whois/reporting/
# contact: American Registry for Internet Numbers, Inc.

# start
Network: 45.33.0.0 -> 45.33.255.255
CIDR: 45.33.0.0/17
NameServer: Linode.com
PortRange: 1024-65535
Protocol: TCP, UDP
Organization: Akamai Technologies, Inc. (Akamai)
Registrant: 2013-08-28
Comments: https://www.iana.org/registry/whois/45.33.0.0
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: Akamai Technologies, Inc.
Registrant: Akamai
Organization: Akamai
Address: 1000 Corporate Park Drive
City: Bedford
StateProv: MA
PostalCode: 01730
Latitude: 42.4564
Longitude: -71.0000
Email: https://www.akamai.com/contact-us/akamai@akamai.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC Operations
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC Support
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

# end

# Whois query and version are subject to the terms of use
# available at: https://www.iana.org/registry/whois/tos/
# If you see inaccuracies in the results, please report at
# https://www.iana.org/registry/whois/reporting/
# contact: American Registry for Internet Numbers, Inc.

# start
Network: 45.33.0.0 -> 45.33.255.255
CIDR: 45.33.0.0/17
NameServer: Linode.com
PortRange: 1024-65535
Protocol: TCP, UDP
Organization: Akamai Technologies, Inc. (Akamai)
Registrant: 2013-08-28
Comments: https://www.iana.org/registry/whois/45.33.0.0
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: Akamai Technologies, Inc.
Registrant: Akamai
Organization: Akamai
Address: 1000 Corporate Park Drive
City: Bedford
StateProv: MA
PostalCode: 01730
Latitude: 42.4564
Longitude: -71.0000
Email: https://www.akamai.com/contact-us/akamai@akamai.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC Operations
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC Support
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

Organization: LINODE INC
Registrant: LINODE INC
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.0.0

# end

# Whois query and version are subject to the terms of use
# available at: https://www.iana.org/registry/whois/tos/
# If you see inaccuracies in the results, please report at
# https://www.iana.org/registry/whois/reporting/
# contact: American Registry for Internet Numbers, Inc.

# start
Network: 45.33.127.255 -> 45.33.127.255
CIDR: 45.33.127.255/32
NameServer: Linode.com
PortRange: 1024-65535
Protocol: TCP, UDP
Organization: Akamai Technologies, Inc. (Akamai)
Registrant: 2013-08-28
Comments: https://www.iana.org/registry/whois/45.33.127.255
RefID: https://www.iana.org/registry/whois/45.33.127.255

Organization: Akamai Technologies, Inc.
Registrant: Akamai
Organization: Akamai
Address: 1000 Corporate Park Drive
City: Bedford
StateProv: MA
PostalCode: 01730
Latitude: 42.4564
Longitude: -71.0000
Email: https://www.akamai.com/contact-us/akamai@akamai.com
RefID: https://www.iana.org/registry/whois/45.33.127.255

Organization: LINODE INC
Registrant: LINODE INC Operations
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.127.255

Organization: LINODE INC
Registrant: LINODE INC Support
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.127.255

Organization: LINODE INC
Registrant: LINODE INC
Organization: LINODE INC
Address: 2474 46th St
City: San Francisco
StateProv: CA
PostalCode: 94158
Country: US
Email: support@linode.com
RefID: https://www.iana.org/registry/whois/45.33.127.255

# end
```

NetRange: 45.33.0.0 – 45.33.127.255

CIDR: 45.33.0.0/17

Organization: Linode (LINOD)

Parent Organization: Akamai Technologies, Inc.

Country: United States (US)

City: Philadelphia, PA

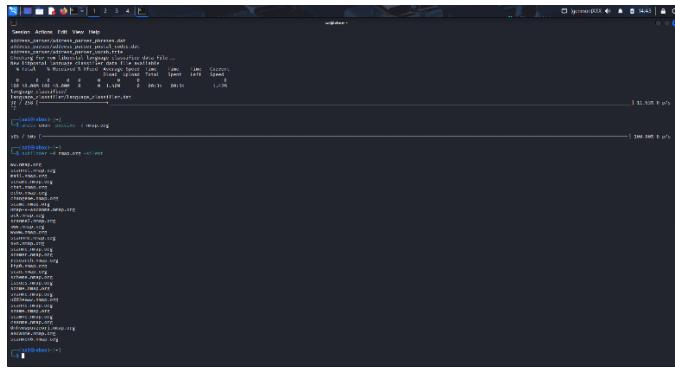
A WHOIS lookup was performed on the IP address 45.33.32.156 to identify the hosting provider and network ownership details.

The IP address belongs to the network range 45.33.0.0/17 and is registered under Linode (LINOD), which operates under Akamai Technologies, Inc.

The organization is located in the United States, specifically in Philadelphia, Pennsylvania.

This confirms that the target server is hosted on Linode infrastructure.

2. Subdomain Enumeration

A screenshot of a terminal window titled "Subfinder" showing the results of a scan. The output lists numerous subdomains of nmap.org, including "www.nmap.org", "scanme.nmap.org", "scanme2.nmap.org", "scanmev6.nmap.org", "research.nmap.org", "issues.nmap.org", "svn.nmap.org", and "mail.nmap.org". There are also many other subdomains listed that appear to be testing or typo variations.

Some subdomains appear to be **testing or typo variations**

Some may be intentionally created for research/testing

Presence of multiple “scanme” variants suggests controlled testing infrastructure

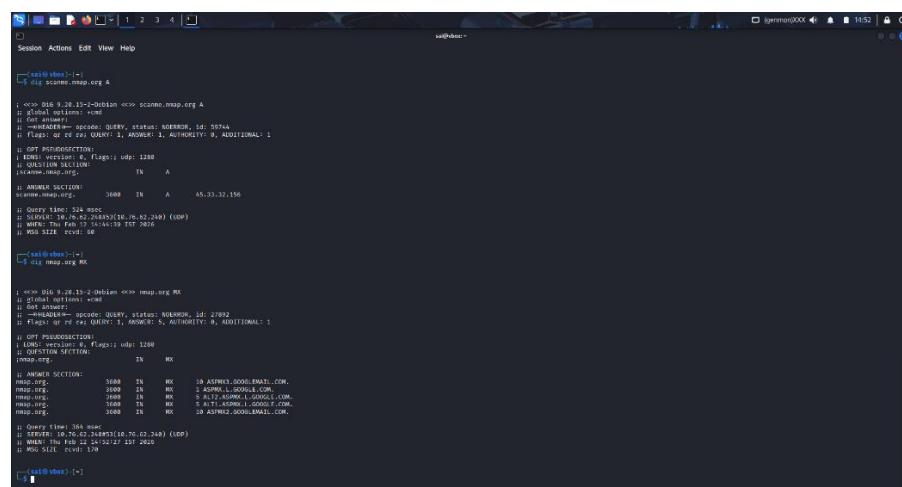
Explanation

Subdomain enumeration was performed using Subfinder in passive mode to identify publicly accessible subdomains of nmap.org.

The tool discovered multiple subdomains including www.nmap.org, scanme.nmap.org, scanme2.nmap.org, scanmev6.nmap.org, research.nmap.org, issues.nmap.org, svn.nmap.org, and mail.nmap.org.

Several typo-based and testing-related subdomains were also identified, indicating the presence of research and experimental infrastructure within the domain.

3.DNS Information

A screenshot of a terminal window titled "nslookup" showing DNS records for nmap.org. The output includes an A record pointing to 45.33.32.156, MX records for mx1.google.com and mx2.google.com, and CNAME records for aspmx.l.google.com, aspmx2.l.google.com, and aspmx3.l.google.com. It also shows a PTR record for 10.76.62.248 pointing to 10.76.62.248. The command used was "nslookup -type=MX nmap.org".

3.1 A Record (scanme.nmap.org)

The A record lookup for scanme.nmap.org resolved to the IPv4 address 45.33.32.156. This confirms the server hosting the target system and will be used for further network reconnaissance.

3.2 MX Record (Mail Servers)

The MX record lookup shows that nmap.org uses Google Mail servers (Google Workspace) for email handling. The presence of multiple Google MX servers indicates redundancy and professional email infrastructure.

```
[root@vbox: ~]# dig nsap.org NS

; <>> SIG 0.20.15-2-debian <>> nsap.org NS
;; global options: +rd
;; Got answer:
;; ->>>HEADER: opcode: QUERY, status: NOERROR, id: 6A32B
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PLS(UDS):
;; ANSWER SECTION:
nsap.org. IN NS
; <>>>HEADER: opcode: QUERY, status: NOERROR, id: 6A32B
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PLS(UDS):
;; ANSWER SECTION:
nsap.org. IN NS
ns1.linode.com.
ns2.linode.com.
ns3.linode.com.
ns4.linode.com.
ns5.linode.com.

;; Query time: 36 msec
;; SERVER: 10.76.62.248#53[10.76.62.248] (UDP)
;; WHEN: Thu Feb 11 14:52:50 IST 2024
;; MSG SIZE rcvd: 137

[root@vbox: ~]# dig nsap.org TXT

; <>> SIG 0.20.15-2-debian <>> nsap.org TXT
;; global options: +rd
;; Got answer:
;; ->>>HEADER: opcode: QUERY, status: NOERROR, id: 18926
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PLS(UDS):
;; ANSWER SECTION:
nsap.org. IN TXT
"noparse@linode-validation-GPU30-Z:~$ curl https://www.nsap.org"
"noparse@linode-validation-GPU30-Z:~$ curl https://www.nsap.org"

;; Query time: 379 msec
;; SERVER: 10.76.62.248#53[10.76.62.248] (UDP)
;; WHEN: Thu Feb 11 14:53:11 IST 2024
;; MSG SIZE rcvd: 261

[root@vbox: ~]#
```

3.3 NS Record (Name Servers)

The NS records indicate that DNS services for nmap.org are managed by Linode name servers. This confirms that Linode is responsible for DNS resolution and domain infrastructure.

3.4 TXT Record

The TXT records include a Google site verification token and an SPF (Sender Policy Framework) record. The SPF record specifies authorized mail servers, including Google's infrastructure, helping prevent email spoofing and phishing attacks.

3.5 Zone Transfer Test

A DNS zone transfer attempt was conducted using the AXFR query against the authoritative name server.

The request failed and no servers could be reached, indicating that the DNS server does not allow unauthorized zone transfers.

This demonstrates proper DNS security configuration and protection against information disclosure.

4. Technology Fingerprinting

The server is running:

- Apache 2.4.7
 - Ubuntu Linux

HTTPS (443) is closed:

- Only HTTP (80) is active
 - This is intentional for scan testing

Google Analytics tracking is enabled.

Technology fingerprinting was performed using WhatWeb to identify the web technologies used by the target.

The scan revealed that the server is running Apache version 2.4.7 on Ubuntu Linux. The website returns an HTTP 200 OK response and supports HTML5.

Google Analytics tracking is enabled on the website.

The HTTPS service on port 443 was not accessible, as the connection attempt was refused, indicating that the server is primarily configured to operate over HTTP.

5. Directory and File Discovery

```
[+] Url: http://scanne.nmap.org
[+] Method: GET
[+] Threads: 10
[*] Wordlist: /usr/share/wordlists/dirb/common.txt
[*] Negative Status codes: 
[*] Timeout: 10s
[*] User Agent: gobuster/3.0.2
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
=====
[+]: http://scanne.nmap.org/.htaccess (Status: 403) [Size: 286]
[+]: http://scanne.nmap.org/.htpasswd (Status: 403) [Size: 201]
[+]: http://scanne.nmap.org/.svnentries (Status: 403) [Size: 294]
[+]: http://scanne.nmap.org/.svn/ (Status: 306) [→ http://scanne.nmap.org/.svn/]
[+]: http://scanne.nmap.org/.icon (Status: 403) [Size: 201]
[+]: http://scanne.nmap.org/images (Status: 101) [Size: 358] [→ http://scanne.nmap.org/images/]
[+]: http://scanne.nmap.org/index (Status: 200) [Size: 6974]
[+]: http://scanne.nmap.org/index.html (Status: 200) [Size: 6974]
[+]: http://scanne.nmap.org/shared (Status: 101) [Size: 358] [→ http://scanne.nmap.org/shared/]
Progress: 3748 / 4613 (81.25%) [ERROR] error on word self: timeout occurred during the request
Progress: 4111 / 4613 (89.12%) [ERROR] error on word svr: timeout occurred during the request
Progress: 4613 / 4613 (100.00%)
Finished
```

403 Status

Access denied (server protected).

Example:

- .htaccess
- .htpasswd

This is good security.

301 Status

Redirected resource exists.

Example:

- /svn
- /images
- /shared

This means those directories exist.

200 Status

Page exists and accessible.

Example:

- /index
- /index.html

Directory enumeration was performed using Gobuster with a common wordlist.

Several directories and files were identified including /images, /svn, /shared, /index, and /index.html.

Sensitive configuration files such as .htaccess and .htpasswd returned HTTP 403 status codes, indicating that access is properly restricted.

The presence of redirected directories (HTTP 301) confirms that these resources exist on the server.

6. Open Ports and Services

```
(sai㉿vbox)-[~]
$ cp ~/Pictures/*.* /media/sf_kali-share/

(sai㉿vbox)-[~]
$ nmap -sV scanne.nmap.org

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 15:09 +0530
Nmap scan report for scanne.nmap.org (45.33.32.156)
Host is up (0.033s latency).
Other addresses for scanne.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  tcpwrapped
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.63 seconds
```

```
(sal@vbox: ~) ->
 3 nmap -A scansme.map.org

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 15:16 +0530
Nmap scan report for scansme.map.org (45.33.32.156)
Host is up (pingable).
Other addresses for scansme.map.org (not scanned): 2600:13c0:1::f03c:91ff:fe18:bb2f
Not shown: 984 filtered TCP ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 13.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ecdsa-sha2-nistp256-sha256:199d:6cf72b34:k4:7575 [DSS]
|   1024 rsa-sha2-256:9e:2a:5b:96d5:b2:80:54:1c:24:6b92 [RSA]
|_  256 sha256+sshd:57:5a4c:45:2f56:ac:4a:24:b2:57 [ECDSA]
23/tcp    closed  telnet
53/tcp    closed  domain
80/tcp    open   http    Apache httpd/2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
| http-favicon: Nmap Project
8080/tcp  closed  httpd
113/tcp   closed  rrdcached
137/tcp   closed  netlink
143/tcp   closed  imap
256/tcp   closed  fw-isecureremote
352/tcp   closed  vnc
387/tcp   closed  submission
993/tcp   closed  imaps
995/tcp   closed  pop3s
1025/tcp  closed  proftpd
1723/tcp  closed  pptp
3889/tcp closed  msrpc-dll-server
8089/tcp  closed  httpd-ssl
No matches for host
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTER (using port 80/tcp)
Hop RTT      ADDRESS
  0.66 ms  scansme.map.org (45.33.32.156)

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

Port 22 → Open (SSH service)

Port 80 → Open (HTTP service running Apache 2.4.7)

21/tcp → Closed (FTP)

22/tcp → Open → OpenSSH 6.6.1p1 (Ubuntu)

80/tcp → Open → Apache 2.4.7 (Ubuntu)

Many other ports → Closed

Port scanning was conducted using Nmap with service version detection and aggressive scanning options enabled.

The scan identified two open ports:

- Port 22 (SSH) running OpenSSH 6.6.1p1 on Ubuntu Linux.
 - Port 80 (HTTP) running Apache HTTP Server version 2.4.7 on Ubuntu.

Several other common ports were found closed.

OS detection indicates that the system is running Linux. The web server title confirms that this is the official ScanMe test environment maintained by the Nmap Project.

7. Email Harvesting

No publicly indexed email addresses found

2 additional hosts discovered via certificate transparency logs:

- issues.nmap.org
- svn.nmap.org

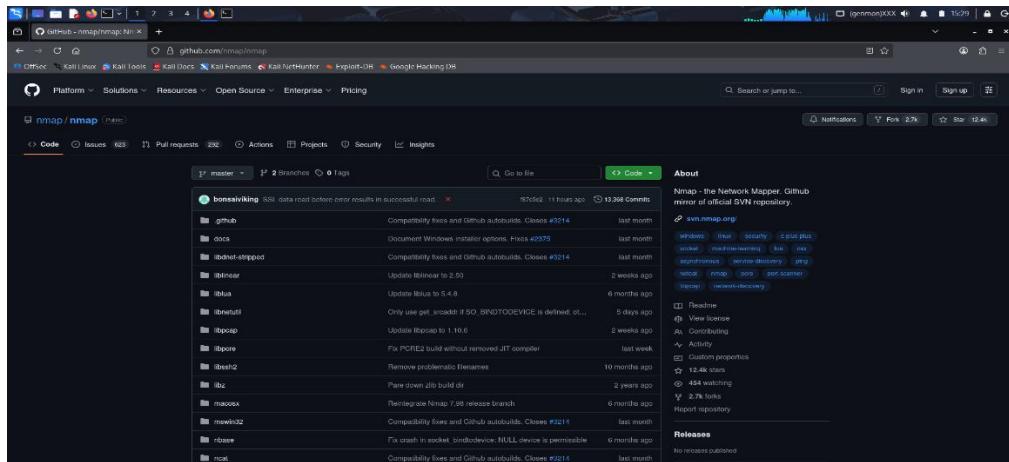
Email harvesting was conducted using theHarvester tool with passive sources including CRT.sh (Certificate Transparency logs).

No publicly indexed email addresses associated with nmap.org were discovered.

However, certificate transparency logs revealed additional subdomains including issues.nmap.org and svn.nmap.org.

The absence of publicly exposed email addresses suggests good information security practices and limited exposure of contact information.

8. Social Media and Public Data



Public footprint analysis was conducted to identify the organization's online presence.

The Nmap Project maintains an official GitHub repository (github.com/nmap/nmap), which hosts the source code and development resources. The repository is publicly accessible and actively maintained.

The public presence reflects transparency, active development, and community involvement.

- This information gathering assessment was conducted using passive and authorized active reconnaissance techniques in accordance with ethical hacking guidelines. No exploitation or unauthorized access attempts were performed. The findings demonstrate controlled infrastructure exposure and proper security configurations within the target environment.