

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

```
Session Actions Edit View Help
[~]@kali:~$ whois nmap.org
Domain Name: nmap.org
Registry Domain ID: REDACTED
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http://www.dynadot.com
Updated Date: 2025-01-18T05:00:15Z
Creation Date: 1999-01-18T05:00:00Z
Registry Expiry Date: 2029-01-18T05:00:00Z
Registrar: Dynadot Inc
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.508.316.6150
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://www.icann.org/wicf/
>>> Last update of WHOIS database: 2026-02-12T07:36:54Z ooo

For more information on whois status codes, please visit https://www.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 query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to e-mail, 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 Registrar of Record identified in this output may have an ARD service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

[~]@kali:~$
```

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

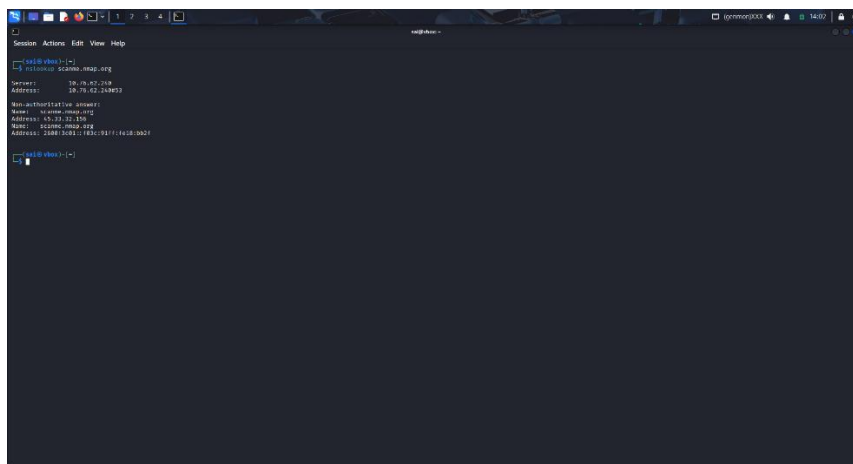
Explanation

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)



```
nslookup scanme.nmap.org
Server: 10.76.62.40
Address: 10.76.62.40#53

Non-authoritative answer:
Node: scanme.nmap.org
Address: 45.33.32.156
Node: scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
```

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

[illegible]

CIDR: 45.33.0.0/17

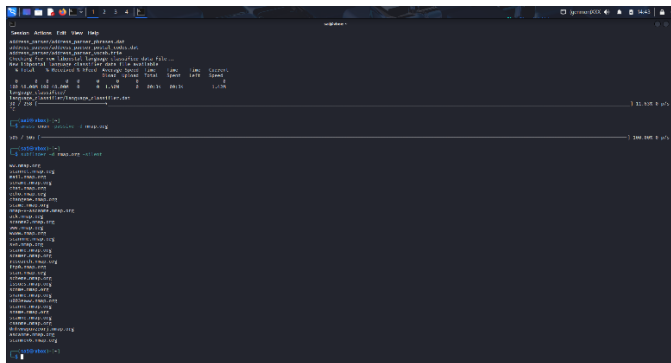
Parent Organization: Akamai Technologies, Inc.

Country: United States (US)

City: Philadelphia, PA

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.

2. Subdomain Enumeration

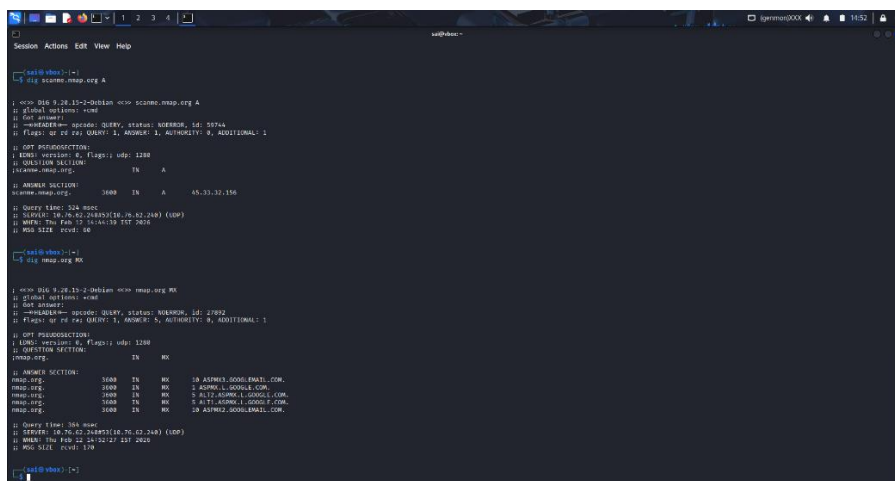


Some may be intentionally created for research/testing

Explanation

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.

3.DNS Information



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.

```

[~]
Session Actions Edit View Help

[~] [sal@rhua]~$ cat
[~] # dig nsap.org ns

; <> ID= 9.28.15-2-Dublin-ocso nsap.org NS
; GLOBAL OPTIONS: cmd
; Got answer!
; =====
; query: nsap.org: QUERY, Status: NOERROR, Id: 64338
; flags: qr rd ra QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1280
; QUESTION SECTION:
; nsap.org. IN NS

; ANSWER SECTION:
nsap.org. 3600 IN NS ns2.linode.com.
          3600 IN NS ns4.linode.com.
          3600 IN NS ns5.linode.com.
          3600 IN NS ns7.linode.com.
          3600 IN NS ns7.linode.com.

; Query time: 306 msec
; SERVER: 10.76.62.248(10.76.62.248) (UDP)
; WHEN: Thu Feb 22 14:52:15 IST 2024
; MSG SIZE  rcv= 137

[~] [sal@rhua]~$ cat
[~] # dig nsap.org txt

; <> ID= 9.28.15-2-Dublin-ocso nsap.org TXT
; GLOBAL OPTIONS: cmd
; Got answer!
; =====
; query: nsap.org: QUERY, Status: NOERROR, Id: 12924
; flags: qr rd ra QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1280
; QUESTION SECTION:
; nsap.org. IN TXT

; ANSWER SECTION:
nsap.org. 3600 IN TXT "google-site-verification=5r7y3nZnTccj2G5AXtLV-5CFj190u0t5Mw0fA"
          3600 IN TXT "wpfz x m p16 4w75b.126.8.126 4p4 2080-1481: f3a:52f:7ebf 4p4-2680:3d41c08b1dc1:4d6e/f041 include:sof.google.com -all"

; Query time: 376 msec
; SERVER: 10.76.62.248(10.76.62.248) (UDP)
; WHEN: Thu Feb 22 14:52:15 IST 2024
; MSG SIZE  rcv= 261

[~] [sal@rhua]~$ cat
[~]

```

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

[illegible]

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

```
(kali@vbox)~$ dig axfr dns1.linode.com mmap.org
;; Communications error to 92.123.94.2853: end of file
;; Communications error to 92.123.94.2853: end of file
;; Communications error to 92.123.94.2853: end of file
;; Connection to 2600:14c8:6::253(2600:14c8:6::2) for mmap.org failed: network unreachable.
;; No servers could be reached

(kali@vbox)~$ cp ~/Pictures/*.png /media/sf_kali-share/

(kali@vbox)~$ whatweb scanme.mmap.org
http://scanme.mmap.org [200 OK] Apache[2.4.7], Country[RESERVED][??], Google-Analytics[Universal][UA-118899417-1], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[65.33.32.156], Script, Title[Go ahead and ScanMe!]
ERROR Opening: https://scanme.mmap.org - connection refused - connect(1) for "65.33.32.156" port 443

(kali@vbox)~$
```

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

```
(kali@vbox)~$ gobuster dir -u http://scanme.mmap.org -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.0.2
by OJ Reeves (@theColonial) & Christian Mchlmauer (@firefart)

[+] Url: http://scanme.mmap.org
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.0.2
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

_.hta (Status: 403) [Size: 286]
_.htaccess (Status: 403) [Size: 291]
_.htpasswd (Status: 403) [Size: 291]
_.svn/entries (Status: 403) [Size: 294]
_.svn (Status: 200) [Size: 316] -> http://scanme.mmap.org/.svn/
favicon.ico (Status: 403) [Size: 293]
images (Status: 301) [Size: 318] -> http://scanme.mmap.org/images/
index (Status: 200) [Size: 6974]
index.html (Status: 200) [Size: 6974]
shared (Status: 301) [Size: 318] -> http://scanme.mmap.org/shared/
Progress: 3748 / 4613 (81.25%) INFO error on word self: timeout occurred during the request
Progress: 4111 / 4613 (89.12%) INFO error on word svn: 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/*.png /media/sf_kali-share/

(sai@vbox)-[~]
└─$ nmap -sV scanme.nmap.org

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

```
[kali@vbox: ~]$ nmap -A scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2026-02-12 15:16 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0040s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 664 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed  ssh
22/tcp    open   ssh
|_ ssh-hostkey:
|_ 1024 ac:0a:a8:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 2048 20:3d:2d:44:62:2a:b0:5a:9d:15:13:05:14:c2:a6:b2 (RSA)
|_ 256 90:a2:b0:b5:97:2a:1c:4e:45:74:56:4e:4a:2a:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
23/tcp    closed  telnet
33/tcp    closed  domain
80/tcp    open   http
|_ http-server: Modderz Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
|_ http-favicon: Nmap Project
111/tcp   closed  rpcbind
113/tcp   closed  ident
143/tcp   closed  imap
256/tcp   closed  fast-secureremote
534/tcp   closed  rtsp
587/tcp   closed  submission
993/tcp   closed  imaps
995/tcp   closed  pop3s
1025/tcp  closed  nfs-or-lls
1723/tcp  closed  pptp
1889/tcp  closed  ms-wbt-server
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sS
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.66 ms scanme.nmap.org (45.33.32.156)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address scanned by nmap.org on 2026-02-12.
```

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

```
[kali@vbox: ~]$ theHarvester -d nmap.org -b crtsh
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
theHarvester
*****
* theHarvester 4.9.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorellabedge-security.com
*****

[*] Target: nmap.org
[*] Searching CRTsh.
[*] No IPs found.
[*] No emails found.
[*] No people found.
[*] Hosts found: 2
-----
issues.nmap.org
svn.nmap.org
[kali@vbox: ~]$
```

No publicly indexed email addresses found

2 additional hosts discovered via certificate transparency logs:

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

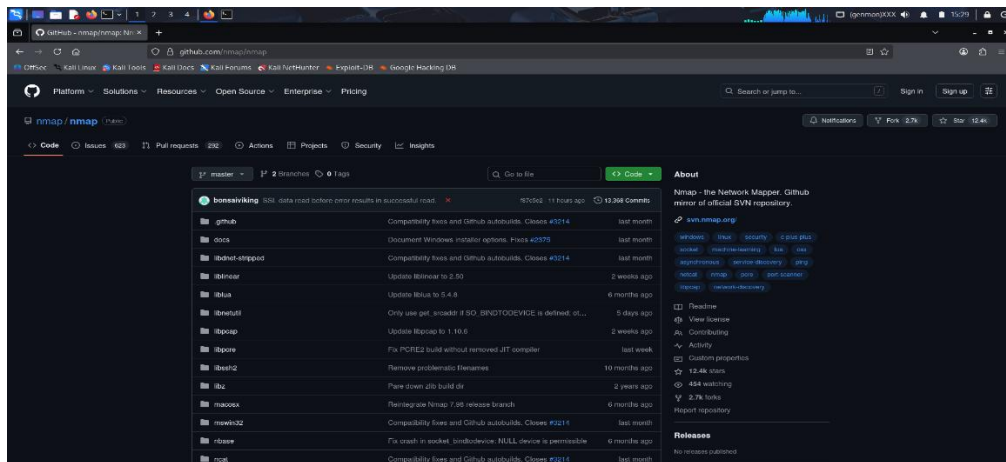
Email harvesting was conducted using theHarvester tool with passive sources including CRT.sh (Certificate Transparency logs).

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.