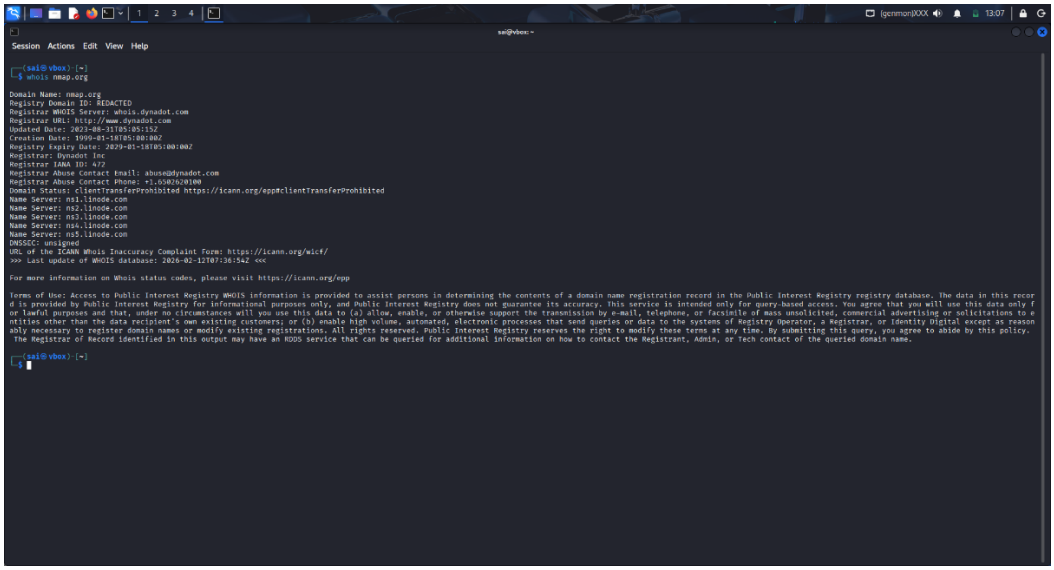
Information Gathering Report

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



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

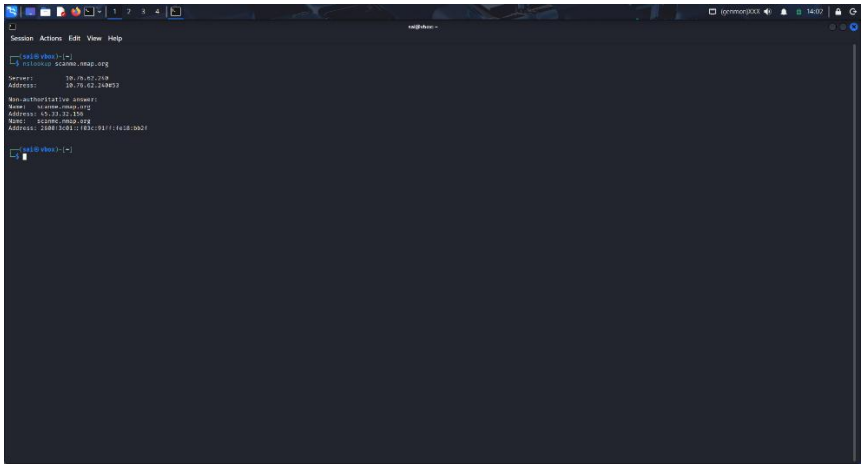
Explanation

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)



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

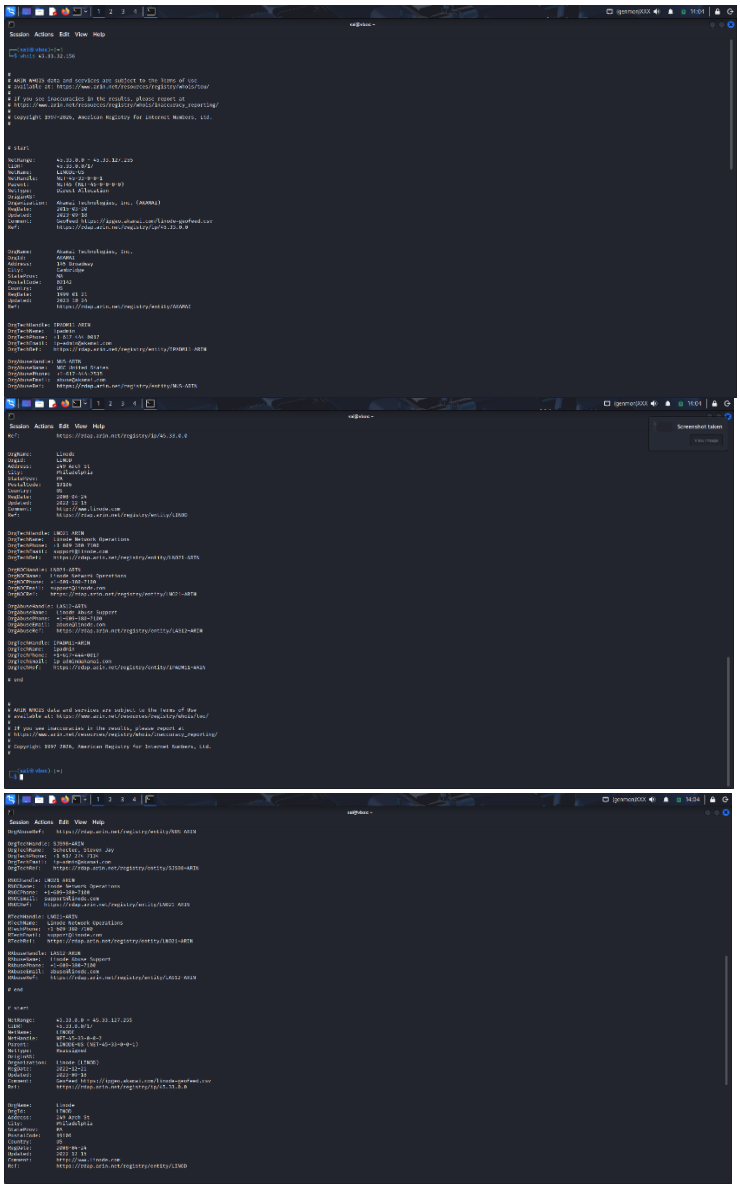
A DNS lookup was performed using the nslookup command to resolve the target domain scanme.nmap.org.

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



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

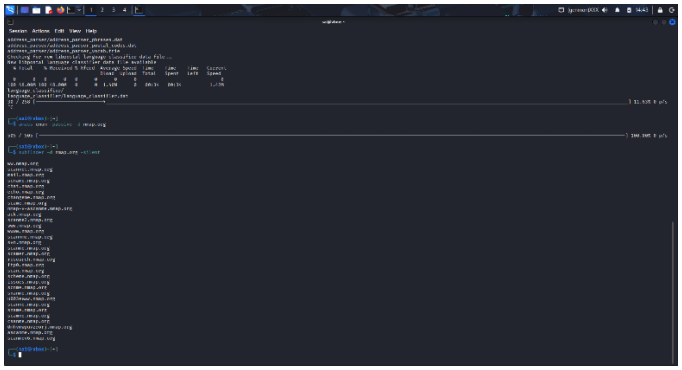
A WHOIS lookup was performed on the IP address 45.33.32.156 to identify the hosting provider and network ownership details.

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



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

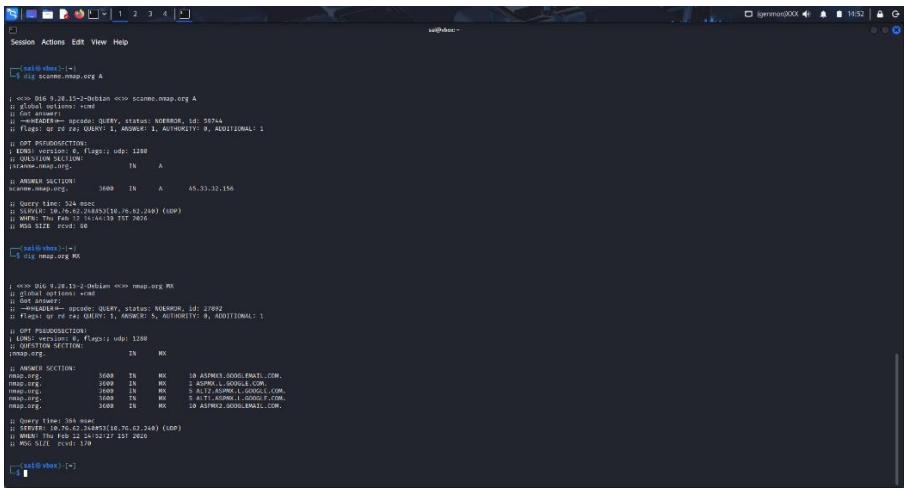
Explanation

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

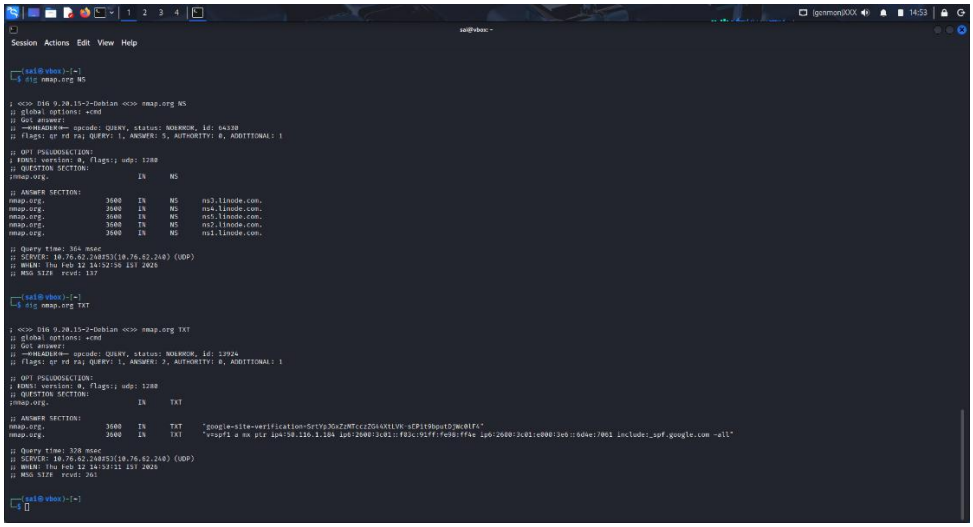


3.1 A Record (scanme.nmap.org)

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.



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

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

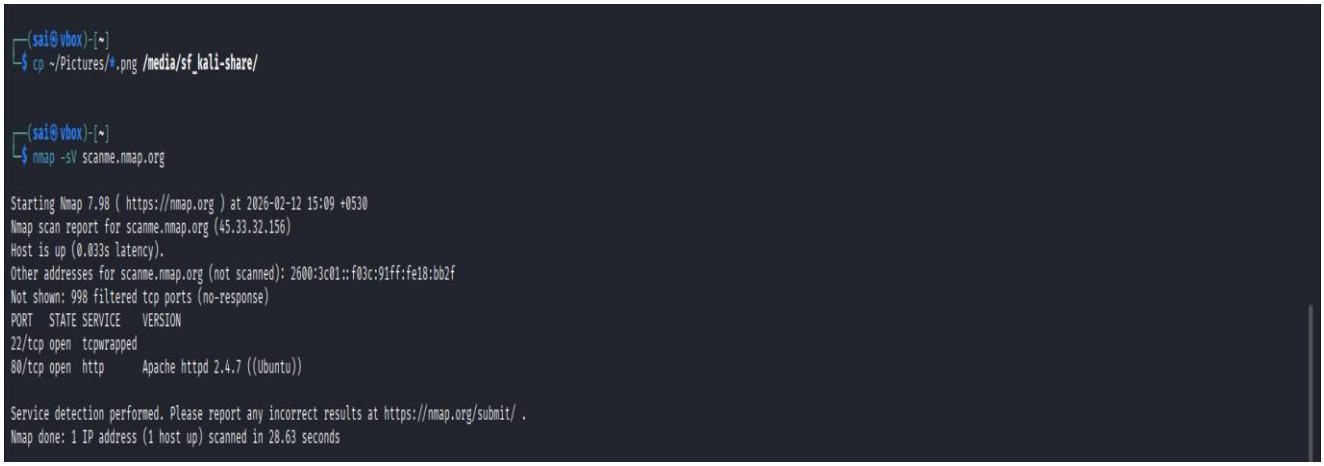
Directory enumeration was performed using Gobuster with a common wordlist.

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



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

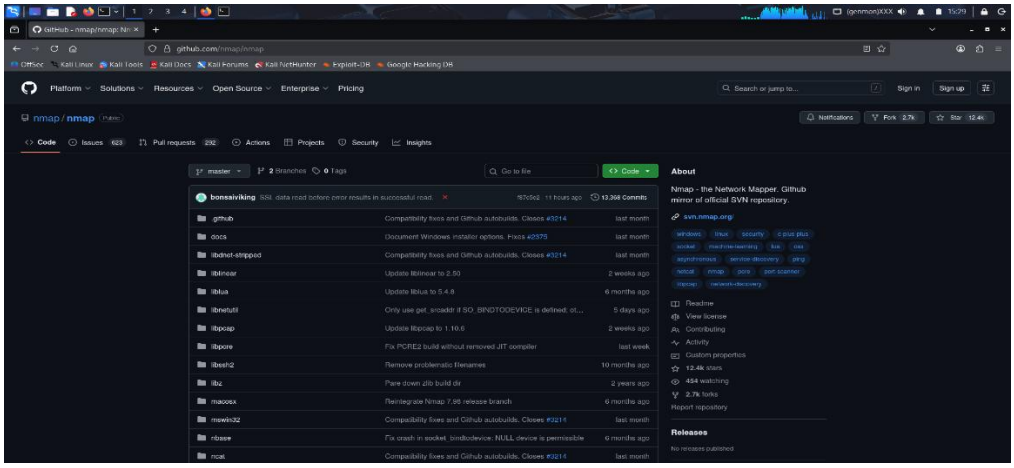
Email harvesting was conducted using theHarvester tool with passive sources including CRT.sh (Certificate Transparency logs).

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.