

Name: Rasmi Ranjan Nayak

Project 2 : Footprinting

Footprinting:

Footprinting, the first step in ethical hacking or penetration testing refers to a process of target website, web application, network and it's environment.

Considering the website :<https://nmap.org>

Below is the result through different tools

Footprinting using netcraft

Site report for https://scanme.nmap.org

site report.netcraft.com/?url=https%3A%2F%2Fscanme.nmap.org

NETCRAFT






Services Solutions News Company Resources

Discover More


Report Fraud

Site report for https://scanme.nmap.org


Look up another site?

Share:     

Background

Site title	Go ahead and ScanMe!	Date first seen	October 2005
Site rank	69725	Netcraft Risk Rating ?	0/10 
Description	Not Present	Primary language	English

Network

Site	https://scanme.nmap.org	Domain	nmap.org
Netblock Owner	Linode	Nameserver	ns1.linode.com
Hosting company	Linode - Fremont	Domain registrar	plr.org
Hosting country	 us	Nameserver organisation	whois.name.com
IPv4 address	45.33.32.156 View Total IP's	Organisation	Insecure.Com LLC, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED







28°C Cloudy



20:23 09-08-2022








Network

Site	https://scanme.nmap.org 	Domain	nmap.org
Netblock Owner	Linode	Nameserver	ns1.linode.com
Hosting company	Linode - Fremont	Domain registrar	pir.org
Hosting country	 us 	Nameserver organisation	whois.name.com
IPv4 address	45.33.32.156 (VirusTotal 	Organisation	Insecure.Com LLC, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, US
IPv4 autonomous systems	AS63949 	DNS admin	hostmaster@insecure.org
IPv6 address	2600:3c01:0:0:f03c:91ff:fe18:bb2f	Top Level Domain	Organization entities (.org)
IPv6 autonomous systems	AS63949 	DNS Security Extensions	unknown
Reverse DNS	scanme.nmap.org		

IP delegation

IPv4 address (45.33.32.156)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	 United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
 45.0.0.0-45.255.255.255	 United States	NET45	American Registry for Internet Numbers
 45.33.0.0-45.33.127.255	 United States	LINODE-US	Linode

[Services](#)[Solutions](#)[News](#)[Company](#)[Resources](#)[Discover More](#)[Report Fraud](#)

IPv6 autonomous systems

[AS63949](#)

DNS Security
Extensions

unknown

Reverse DNS

scanme.nmap.org

IP delegation

IPv4 address (45.33.32.156)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
45.0.0.0-45.255.255.255	United States	NET45	American Registry for Internet Numbers
45.33.0.0-45.33.127.255	United States	LINODE-US	Linode
45.33.32.156	United States	LINODE-US	Linode

IPv6 address (2600:3c01:0:0:f03c:91ff:fe18:bb2f)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
2600::/12	United States	NET6-2600	American Registry for Internet Numbers
2600:3c00::/28	United States	LINODE-US	Linode
2600:3c01:0:0:f03c:91ff:fe18:bb2f	United States	LINODE-US	Linode

Hosting History

This host does not have any history data.



IPv6 autonomous systems

AS63949

DNS Security
Extensions

unknown

Reverse DNS

scanme.nmap.org

IP delegation

IPv4 address (45.33.32.156)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
45.0.0.0-45.255.255.255	United States	NET45	American Registry for Internet Numbers
45.33.0.0-45.33.127.255	United States	LINODE-US	Linode
45.33.32.156	United States	LINODE-US	Linode

IPv6 address (2600:3c01:0:0:f03c:91ff:fe18:bb2f)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
2600::/12	United States	NET6-2600	American Registry for Internet Numbers
2600:3c00::/28	United States	LINODE-US	Linode
2600:3c01:0:0:f03c:91ff:fe18:bb2f	United States	LINODE-US	Linode

Hosting History

This host does not have any history data.



Services ▾

Solutions ▾

News

Company ▾

Resources ▾

Q ▾

Discover More

Report Fraud ↗

▴ Hosting History

This host does not have any history data.

▴ Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#) ↗. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#) ↗.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on nmap.org: Check the [site report](#).

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any [mail-enabled subdomains](#) ↗. It is recommended to add an SPF record to any subdomain with an MX record.

▴ DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see [dmarc.org](#) ↗.

This host does not have a DMARC record. There may be a DMARC record on the site report for nmap.org: Check the [site report](#).

▴ Web Trackers

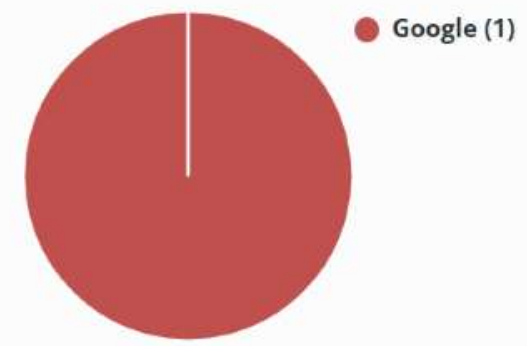
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.



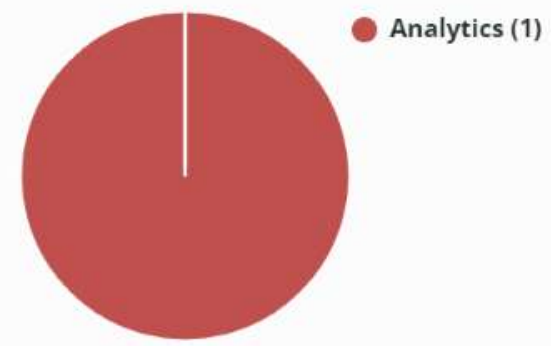
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

1 known tracker was identified.

Companies



Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Google	Analytics	Google Analytics	www.researchgate.net, www.homedepot.com, www.aliexpress.com

Site Technology (fetched 9 days ago)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
------------	-------------	-------------------------------------

Site Technology (fetched 9 days ago)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Apache	Web server software	www.internetdownloadmanager.com, www.victoriaweather.ca, www.majorgeeks.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	discord.com, accounts.google.com, my308053-sso.crm.ondemand.com

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
------------	-------------	-------------------------------------



side dynamic content on websites

sso.crm.ondemand.com

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.sozcu.com.tr, www.seznam.cz, www.pole-emploi.fr

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	www.instagram.com, www.google.com, web.whatsapp.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	teams.microsoft.com, docs.microsoft.com, mail.google.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as



A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External ↗	Styles defined within an external CSS file	www.linkedin.com , www.twitch.tv , www.msn.com

Looking for similar sites?

Using Nmmapper

Site report for https://scanme.nmap.org | Pentest tools from Nmap online

nmmapper.com

Nmmapper

Osint Tools | Bug Bounty Tools | Web Applications | Nmap | Subdomain finder | theHarvester | Pricing | API

Account | Resources

Subdomain Finder, theHarvester

https://scanme.nmap.org Start scan

Web application firewall | **Nmap** | Subdomain finder | Ping tool | Cipherscan | IP ASN Lookup | IP Geo Location

Nmap scan options

- ☒ Nmap common ports
- > Nmap Online OS Detection
- > Nmap Online Version Detection

Host	Protocol	Port	State	Service	Version
scanme.nmap.org	tcp	21	closed	ftp	
scanme.nmap.org	tcp	22	open	ssh	
scanme.nmap.org	tcp	23	closed	telnet	
scanme.nmap.org	tcp	25	closed	smtp	
scanme.nmap.org	tcp	80	open	http	
scanme.nmap.org	tcp	110	closed	pop3	
scanme.nmap.org	tcp	139	closed	netbios-ssn	

A curated list of OSINT tools

28°C Cloudy

ENG IN

20:27 09-08-2022



Subdomain Finder, theHarvester


Start scan

Web application firewall	Nmap	Subdomain finder	Ping tool	Cipherscan	IP ASN Lookup	IP Geo Location	
Nmap scan options			scanme.nmap.org	tcp	23	closed	telnet
<input checked="" type="radio"/> Nmap common ports			scanme.nmap.org	tcp	25	closed	smtp
> Nmap Online OS Detection			scanme.nmap.org	tcp	80	open	http
> Nmap Online Version Detection			scanme.nmap.org	tcp	110	closed	pop3
			scanme.nmap.org	tcp	139	closed	netbios-ssn
			scanme.nmap.org	tcp	443	closed	https
			scanme.nmap.org	tcp	445	closed	microsoft-ds
			scanme.nmap.org	tcp	3389	closed	ms-wbt-server

A curated list of OSINT tools



Using Buitwith



[Site Search](#)

[Download](#)
[Reference Guide](#)
[Book](#)
[Docs](#)
[Zenmap](#)

[Get Nmap 7.92 here](#)

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on [Npcap.com](#), [Seclists.org](#), [In](#)
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, enhancements! [\[Release Announcement\]](#) [\[Download page\]](#)
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap [\[Announcement\]](#) [\[Download page\]](#)
- Nmap 7.80 was released for DEFCON 27! [\[release notes\]](#) [\[download\]](#)
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading [the original Phrack #51 article](#).
- Nmap 7.50 is now available! [\[release notes\]](#) [\[download\]](#)
- Nmap 7 is now available! [\[release notes\]](#) [\[download\]](#)
- We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive collection of the Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also in [Joe: Retaliation!](#)
- We're delighted to announce Nmap 6.40 with 14 new [NSE scripts](#), hundreds of new [OS](#) and [version detection](#) new features! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with [Nmap 6.01!](#)
- Nmap 6 is now available! [\[release notes\]](#) [\[download\]](#)
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of like Yelp for security tools. Are you familiar with all of the [49 new tools](#) in this edition?
- Nmap 5.50 Released:** Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS

NMAP.ORG

	Analytics and Tracking	First Detected	Last Detected
	Google Analytics Application Performance · Audience Measurement · Visitor Count Tracking	Jan 2011	Aug 2022
	Google Universal Analytics	Jan 2015	Aug 2022
	Gemius PL Audience Measurement	Aug 2018	Jan 2020
	Gemius Audience Measurement	Aug 2019	Jan 2020
	Everest Technologies	Sep 2017	Jan 2020
	Efficient Frontier Marketing Automation	Sep 2017	Jan 2020
	Rapleaf Marketing Automation	Aug 2018	Dec 2019
	MediaMath Advertiser Tracking	Aug 2015	Aug 2019
	Moat Advertiser Tracking	Mar 2015	Jun 2019
	comScore Advertiser Tracking · Audience Measurement · Conversion Optimization · Site Optimization · Visitor Count Tracking	Nov 2017	Mar 2019
	Quantcast Measurement	Nov 2017	Mar 2019

Using Wappalyzer(Addon)

The screenshot shows a web browser window with the Nmap.org website. The Wappalyzer addon is active, displaying a sidebar with technology detection results. The browser's address bar shows the URL https://nmap.org. The website's navigation bar includes links for Download, Reference Guide, Book, Docs, and Zenmap. A prominent button reads "Get Nmap 7.92 here". The "News" section contains a list of updates, including the redesign of Nmap.org, the release of Nmap 7.90, and the announcement of Nmap 6.40. The Wappalyzer sidebar lists detected technologies: Analytics (Google Analytics), Operating systems (CentOS), and Web servers (Apache 2.4.6). It also includes a link to "Automate technology lookups" and a "Compare APIs" button.

Nmap: the Network Mapper - F X

https://nmap.org

Getting Started CSS first steps - Learn ... Assignments - thetech...

Npcap.com Seclists.org

Site Search

Download Reference Guide Book Docs Zenmap

Get Nmap 7.92 here

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on [Npcap.com](#), [Seclists.org](#), [I](#)
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements enhancements! [\[Release Announcement\]](#) [\[Download page\]](#)
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Np [Announcement](#) [\[Download page\]](#)
- Nmap 7.80 was released for DEFCON 27! [\[release notes\]](#) [\[download\]](#)
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading [the original Phrack #51 article](#)
- Nmap 7.50 is now available! [\[release notes\]](#) [\[download\]](#)
- Nmap 7 is now available! [\[release notes\]](#) [\[download\]](#)
- We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive c Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also to [launch nuclear missiles in G.I. Joe: Retaliation](#)!
- We're delighted to announce Nmap 6.40 with 14 new [NSE scripts](#), hundreds of new [OS](#) and [version detection](#) signatures, and many great new features! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with [Nmap 6.01](#)!
- Nmap 6 is now available! [\[release notes\]](#) [\[download\]](#)
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of like Yelp for security tools. Are you familiar with all of the [49 new tools](#) in this edition?
- **Nmap 5.50 Released:** Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS

Wappalyzer

TECHNOLOGIES MORE INFO Export

Analytics

[Google Analytics](#)

Operating systems

[CentOS](#)

Web servers

[Apache](#) 2.4.6

[Something wrong or missing?](#)

Automate technology lookups

Our APIs provide instant access to website technology stacks, contact details and social media profiles.

[Compare APIs](#)

28°C Cloudy

20:30 09-08-2022

Using DNS Checker

DNS Propagation Checker - Glo...

←

→

↺

https://www.whatsmydns.net/#A/scanme.nmap.org

☆


✉

🔔

23

☰

Getting StartedCSS first steps - Learn ...Assignments – thetech...

whatsmysdns.net
Global DNS Propagation Checker

GoDaddy
Get ahead of price increases and entrust your domain to the world's leading registrar
[LEARN MORE](#)

scanme.nmap.org

A

⚙️


🔍 Search

[Donate](#)[Twitter](#)[Facebook](#)

Holtsville NY, United States OpenDNS	45.33.32.156	✓
Kansas City, United States WholeSale Internet	45.33.32.156	✓
Dothan AL, United States Comodo		✗
Miami FL, United States AT&T	45.33.32.156	✓
Boston MA, United States Speakeasy	45.33.32.156	✓
St. John's, Canada Memorial University of Newfoundland	45.33.32.156	✓
Culiacan, Mexico Megacable	45.33.32.156	✓
Diadema, Brazil Trufer Comercio de Sucatas	45.33.32.156	✓
Paterna de Rivera, Spain ServiHosting	45.33.32.156	✓
London, United Kingdom InterNAP	45.33.32.156	✓
Lille, France Completel SAS	45.33.32.156	✓
Amsterdam, Netherlands Routit	45.33.32.156	✓
Glostrup, Denmark Sentia	45.33.32.156	✓

DNS Propagation Checker


whatsmydns.net lets you instantly perform a DNS lookup to check a domain name's current IP address and DNS record information against multiple nameservers located in different parts of the world.




Limited offer on domains.

GoDaddy

28°C
Cloudy



ENG
IN



20:32
09-08-2022

DNS Propagation Checker - Glo...

+

← → ↺

https://www.whatsmydns.net/#A/scanme.nmap.org

☆

Getting Started

CSS first steps - Learn ...

Assignments – thetech...

whatsmydns.net

Global DNS Propagation Checker

scanme.nmap.org

A

⚙

🔍 Search

Donate

Comptel SAS

45.33.32.156

✓

Amsterdam, Netherlands

Routit

45.33.32.156

✓

Glostrup, Denmark

Sentia

45.33.32.156

✓

Merzig, Germany

Probe Networks

✗

Zizers, Switzerland

Oskar Emmenegger

45.33.32.156

✓

Sassuolo, Italy

Telecom Italia

45.33.32.156

✓

Cullinan, South Africa

Liquid

45.33.32.156

✓

Antalya, Turkey

Teknet Yazlim

✗

St Petersburg, Russia

Yandex

45.33.32.156

✓

Peshawar, Pakistan

PTCL

45.33.32.156

✓

Ariyalur, India

Railwire

45.33.32.156

✓

Bangkok, Thailand

Loxley

45.33.32.156

✓

Petaling Jaya, Malaysia

Clear-Comm

45.33.32.156

✓

Singapore, Singapore

M1 Net

45.33.32.156

✓

Limited offer on domains.

GoDaddy

28°C Cloudy

20:32

09-08-2022

DNS Propagation Checker - Global

← → ↺

https://www.whatsmydns.net/#A/scanme.nmap.org

☆

📧 🔔 🌐 23 ☰

Getting Started 🌐 CSS first steps - Learn ... 🌐 Assignments – thetech...

whatsmydns.net

Global DNS Propagation Checker

scanme.nmap.org

A ▾ ⚙️ 🔍 Search

Donate

🐦

f

🇩🇪 Merzig, Germany

Probe Networks

✖

🇨🇭 Zizers, Switzerland

Oskar Emmenegger

45.33.32.156 ✔

🇮🇹 Sassuolo, Italy

Telecom Italia

45.33.32.156 ✔

🇿🇦 Cullinan, South Africa

Liquid

45.33.32.156 ✔

🇹🇷 Antalya, Turkey

Teknet Yazlim

✖

🇷🇺 St Petersburg, Russia

Yandex

45.33.32.156 ✔

🇵🇰 Peshawar, Pakistan

PTCL

45.33.32.156 ✔

🇮🇳 Ariyalur, India

Railwire

45.33.32.156 ✔

🇹🇭 Bangkok, Thailand

Loxley

45.33.32.156 ✔

🇲🇾 Petaling Jaya, Malaysia

Clear-Comm

45.33.32.156 ✔

🇸🇬 Singapore, Singapore

M1 Net

45.33.32.156 ✔

🇨🇳 Beijing, China

CNNIC

45.33.32.156 ✔

🇰🇷 Seoul, South Korea

LG Dacom

45.33.32.156 ✔

🇯🇵 Tokyo, Japan

Timed Out

✖

← back to map view

🇮🇳 Ariyalur, India

Railwire

id 6377

opcode QUERY

rcode NOERROR

flags QR RD RA

;QUESTION

scanme.nmap.org. IN A

;ANSWER

scanme.nmap.org. 3600 IN A 45.33.32.156

;AUTHORITY

;ADDITIONAL

Limited offer on domains.

GoDaddy

28°C Cloudy

🪟 🔍 📁 🗓️ 📧 📄 🌐 🔥 🌐 🌐 📶 📶 📶

20:32 09-08-2022 3

Currently detecting 1326 website powering technologies

https://nmap.org

Q Detect CMS

✓ Success

JSON

We didn't find a CMS for nmap.org but we did find the following technologies

Category	Software	Version
Web Server	Apache	2.4.6
Operating System	CentOS	
Social Media		
Network	Profile	Url
Twitter	hashtag	https://twitter.com/hashtag/
Twitter	nmap	https://twitter.com/nmap
Facebook	nmap	https://facebook.com/nmap

Help us improve these results

Top 5 Leader
TestGorilla
Interview

**Skills Test First.
CV Second.**

TestGorilla

Pre-employment
Screening Tests And
Assessments |
TestGorilla

>

Timed Out

Using WayBack Machine

dns checker.com - Google Search X W Detect which CMS a site is using X Insecure.org -- Computer Security, h X +

← → ↺ web.archive.org/web/20000816230522/http://www.nmap.org/ [Go] 1999 AUG 16 2000 2001 About this capture

Getting Started CSS first steps - Learn ... Assignments - thetech...

INTERNET ARCHIVE **wayBack Machine** [http://www.nmap.org/](#) 3,177 captures 16 Aug 2000 - 6 Aug 2022

FREE KEVIN
Welcome to
Insecure.Org
GNU

Last modified: Monday, 14-Aug-2000 11:47:35 PDT

Nmap Free Security Scanner
Network-wide ping sweep, portscan, OS Detection
Audit your network security before the bad guys do

Featured News

Lists.Insecure.Org open for Business

Many people have asked us about a web archive of some of our security lists such as Nmap-hackers and Nmap-dev. I have finally made one available [here](#). And while I was at it, I added real-time updating archives for a bunch of other cool lists such as Bugtraq and ISN. The next step is to fix some rough edges and to make all the lists searchable. If you was to suggest other quality lists (especially if you have mbox-style archives), [drop me a line](#).
[[List.Insecure.Org Security List Archive](#)]

Top 50 Security Tools Survey Results

We conducted a survey of 1200 [Nmap](#) users from the nmap-hackers mailing list to determine their favorite security commercial or open source security tools on any platform. Each respondent could list up to 5. I was so impressed by the list they created that I am putting the top 50 up [here](#) where everyone can benefit from them. I think anyone in the security field would be well advised to go over [the list](#) and investigate any tools they are unfamiliar with. I also plan to point newbies to this page whenever they write me saying "I do not know where to start".

Nmap 2.50 Released

Insecure.Org is pleased to announce the immediate, free availability of the Nmap Security Scanner version 2.50 from <http://www.insecure.org/nmap/>.

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), and TCP/IP fingerprinting (remote host operating system identification). Nmap also offers flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, sunRPC scanning, reverse-identd scanning, and more. Console and X-Window versions are available.
[[Press release](#)]
[[Nmap home page](#)]

OpenDVD Project Launched

The code has been cracked! For years, users of Linux (and other systems) have been unable to play DVD Video on their computers. The DVD Forum made up an [encryption scheme](#) for the data and only licensed it for players on operating systems they consider economically viable. Further, it prevented users from exercising many forms of legally protected "fair use". And it enabled the much-hated [region codes](#), which are an artificial compatibility restraint preventing DVDs purchased in one geographic region from functioning with players in another region. This allows the MPAA to introduce movies in Europe 6 months late and charge people different prices based on the country they live in.

28°C Cloudy 20:36 09-08-2022

- **Nmap 5.50 Released:** Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [[Download page](#) | [Release notes](#)]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam—all in 38 minutes! ([Presentation video](#))
- *Icons of the Web:* explore favicons for the top million web sites with our [new poster](#) and [online viewer](#).
- We're delighted to announce the immediate, free availability of the [Nmap Security Scanner version 5.00](#). Don't miss the [top 5 improvements in Nmap 5](#).
- After years of effort, we are delighted to release [Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!](#)
- We now have an active Nmap [Facebook page](#) and [Twitter feed](#) to augment the [mailing lists](#). All of these options offer RSS feeds as well.

Nmap ("Network Mapper") is a free and open source ([license](#)) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer ([Zenmap](#)), a flexible data transfer, redirection, and debugging tool ([Ncat](#)), a utility for comparing scan results ([Ndiff](#)), and a packet generation and response analysis tool ([Nping](#)).

Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in [twelve movies](#), including [The Matrix Reloaded](#), [Die Hard 4](#), [Girl With the Dragon Tattoo](#), and [The Bourne Ultimatum](#).

Nmap is ...

- **Flexible:** Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many [port scanning](#) mechanisms (both TCP & UDP), [OS detection](#), [version detection](#), ping sweeps, and more. See the [documentation page](#).
- **Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable:** Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- **Easy:** While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- **Free:** The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for [free download](#), and also comes with full source code that you may modify and redistribute under the terms of the [license](#).
- **Well Documented:** Significant effort has been put into comprehensive and up-to-date man pages, [whitpapers](#), [tutorials](#), and even a whole book! Find them in multiple languages [here](#).

dns checker.com - Google Search X

W Detect which CMS a site is using X

Nmap - Free Security Scanner F X

+

← → ↺

web.archive.org/web/20130403232041/http://nmap.org/

📄 ☆

📧 🔔 🌐 13 ☰

Getting Started 🌐 CSS first steps - Learn ... 🌐 Assignments – thetech...

INTERNET ARCHIVE
Wayback Machine

http://nmap.org/

Go

MAR 2012

APR 03 2013

MAY 2014

👤 ? ✕

f t

About this capture

several movies, dozens of books, and one comic book series. Visit the [press page](#) for further details.

- **Popular:** Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

Communication

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (4 posts in 2009), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join more than 75,000 current subscribers by submitting your email address here:

Subscribe to Nmap-hackers

(or subscribe with custom options from the [Nmap-hackers list info page](#))

We also have a development list for more hardcore members (especially programmers) who are interested in helping the project by helping with coding, testing, feature ideas, etc. New (test/beta) versions of Nmap are sometimes released here prior to general availability for QA purposes. You can subscribe at the [Nmap-dev list info page](#).

Both lists are archived (along with many other security lists) at [Seclists.org](#).

Though it isn't nearly as active as the mailing lists, the official IRC channel is #nmap on [Freenode](#) (irc.freenode.net).

Nmap Site Navigation

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

[[Nmap](#) | [Sec Tools](#) | [Mailing Lists](#) | [Site News](#) | [About/Contact](#) | [Advertising](#) | [Privacy](#)]

Search

28°C
Cloudy

🪟 🔍 📁 🗨️ 📅 📧 📄

🔥 🌐 🌀 🛡️ 📌

ENG IN 🔊 🔌 🔋

20:37
09-08-2022 3