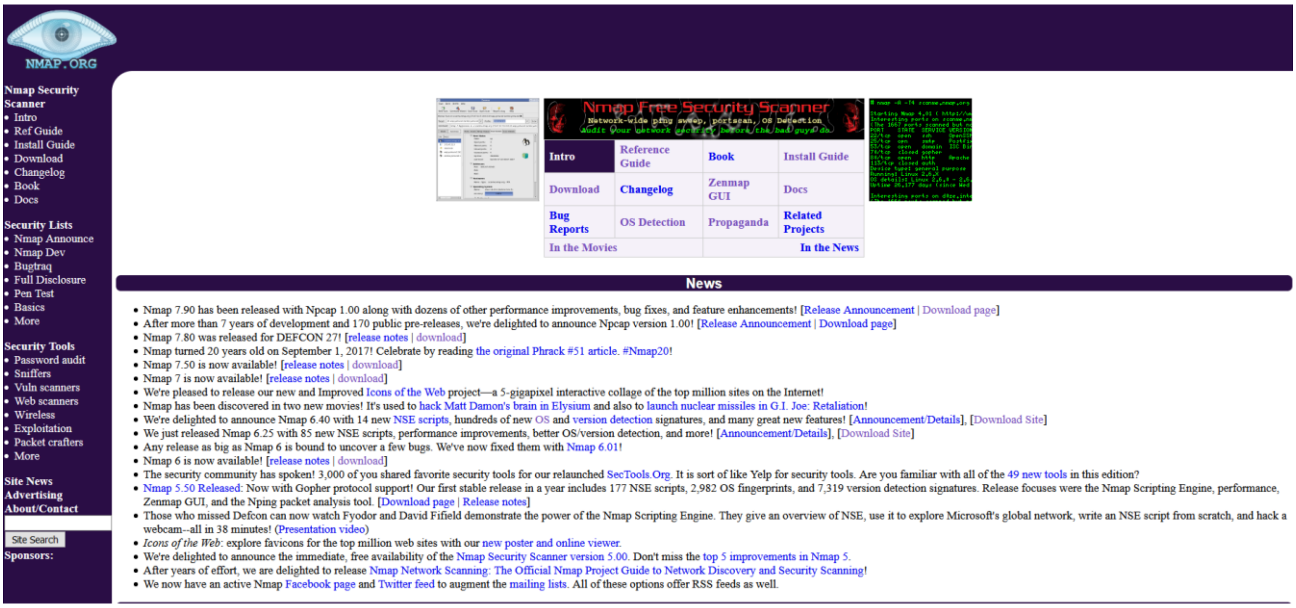
Zenmap /Nmap



NMAP.ORG

Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News
Advertising
About/Contact

Site Search

Sponsors:

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

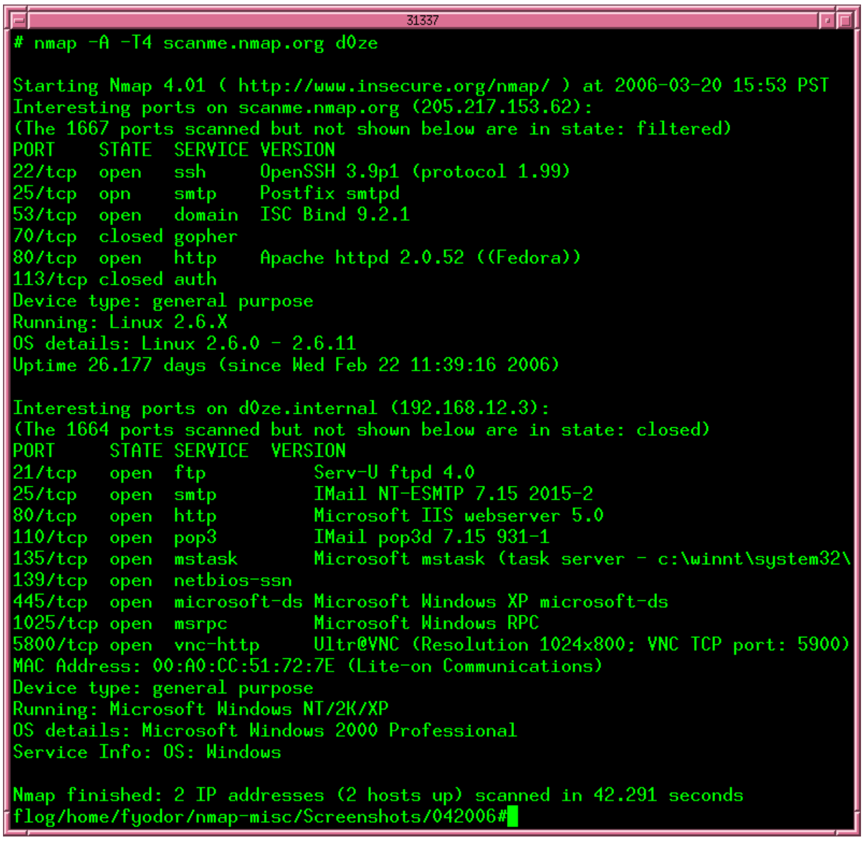
Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies		In the News	

News

- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Announcement | Download page]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release 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. #Nmap20!
- 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 collage of the top million sites on the 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 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.

What is Nmap ?

Nmap is a security scanner developed by computer networking expert Gordon Lyon (Nickname Fyodor). It can map the scanned network (topography) and observe the status of services running on network machines, operating systems, ports.



31337

```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Interface of Nmap

General features

With Nmap, you can learn the devices connected to the network, the operating systems of the devices, the operating times of the devices, the versions of the operating systems, whether there is a firewall or even the name of the network card manufacturer.

Nmap codded with

C,c++,python and lua

Supported Operating Systems (cross platform)

Windows

Linux distributions (Most of them)

Mac Os

Solaris

FreeBSD, OpenBSD, ve NetBSD vb.

License

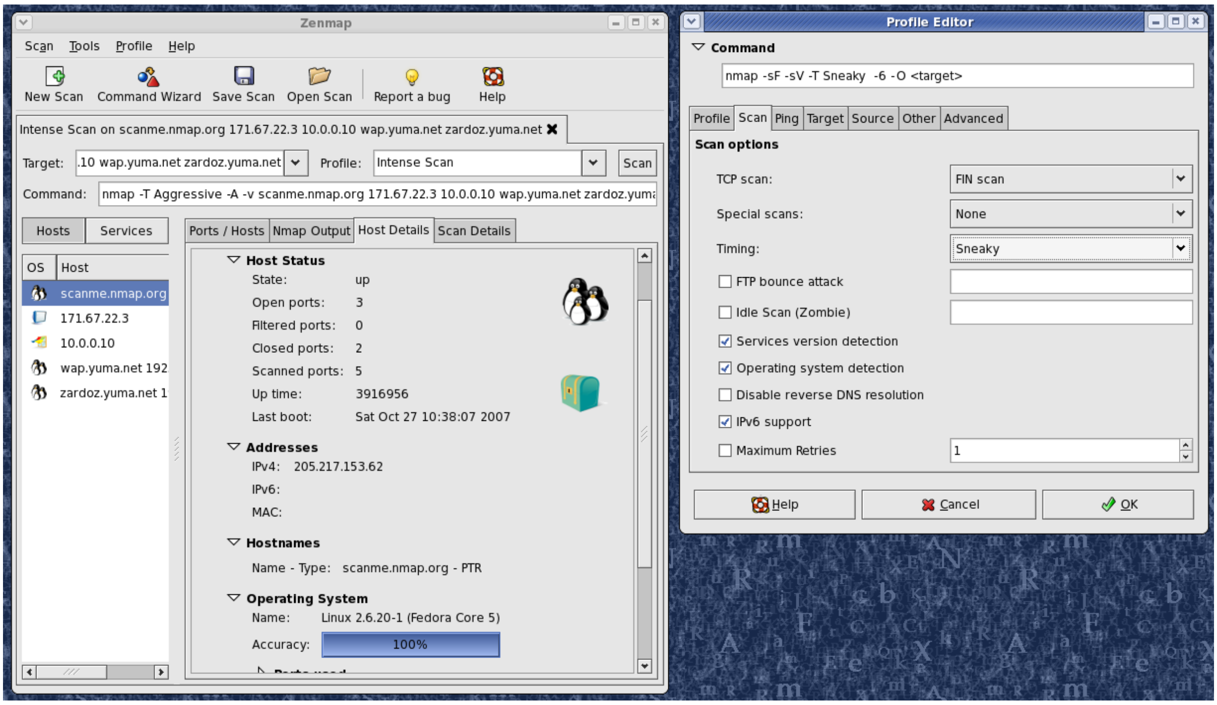
Nmap/Zenmap is completely free under the GPL v2 license. There is no harm in copying, distributing and changing, you can access the source codes.

What is Zenmap ?

Zenmap is the graphical interface (gui) version of nmap. In Zenmap, unlike nmap, frequently used scanning methods are registered with the profile system. At the same time, you can create your own profile with zenmap or edit existing profiles. Zenmap is supported by Windows ,MacOS and Linux platforms.

Zenmap

Originally coded by Kanchan and called NmapFE, it was the official GUI of Nmap from versions 2.2 to 4.22, later replaced by Zenmap, a new UMIT-based graphical user interface developed by Monteiro Marques as of Nmap 4.50.



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .10 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

Host Status

State:	up
Open ports:	3
Filtered ports:	0
Closed ports:	2
Scanned ports:	5
Up time:	3916956
Last boot:	Sat Oct 27 10:38:07 2007

Addresses

IPv4: 205.217.153.62

IPv6:

MAC:

Hostnames

Name - Type: scanme.nmap.org - PTR

Operating System

Name: Linux 2.6.20-1 (Fedora Core 5)

Accuracy: 100%

Command

nmap -sF -sV -T Sneaky -6 -O <target>

Scan options

TCP scan: FIN scan

Special scans: None

Timing: Sneaky

□ FTP bounce attack

□ Idle Scan (Zombie)

☑ Services version detection

☑ Operating system detection

□ Disable reverse DNS resolution

☑ IPv6 support

□ Maximum Retries 1

Interface of Zenmap

Why use Nmap/Zenmap?

For testing necessary settings during network setup and preparation.

Network inventory holding, mapping, maintenance and management.

By identifying new unknown servers, we can use them to perform security audits.

It can be used for vulnerability detection. (For penetration tests)

It can be used to get information about the scanned network. (Port information etc.)

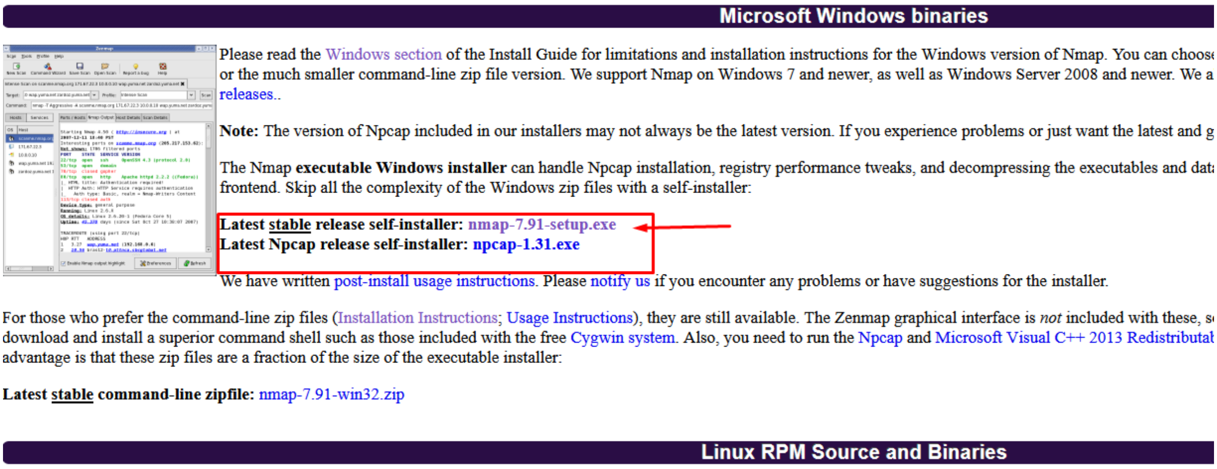
How to install Zenmap

For Windows

Step-1 (Go there)

https://nmap.org/download.html

Step-2



Microsoft Windows binaries

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We a releases..

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and g

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, and decompressing the executables and data frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest stable release self-installer: nmap-7.91-setup.exe
Latest Npcap release self-installer: **npcap-1.31.exe**

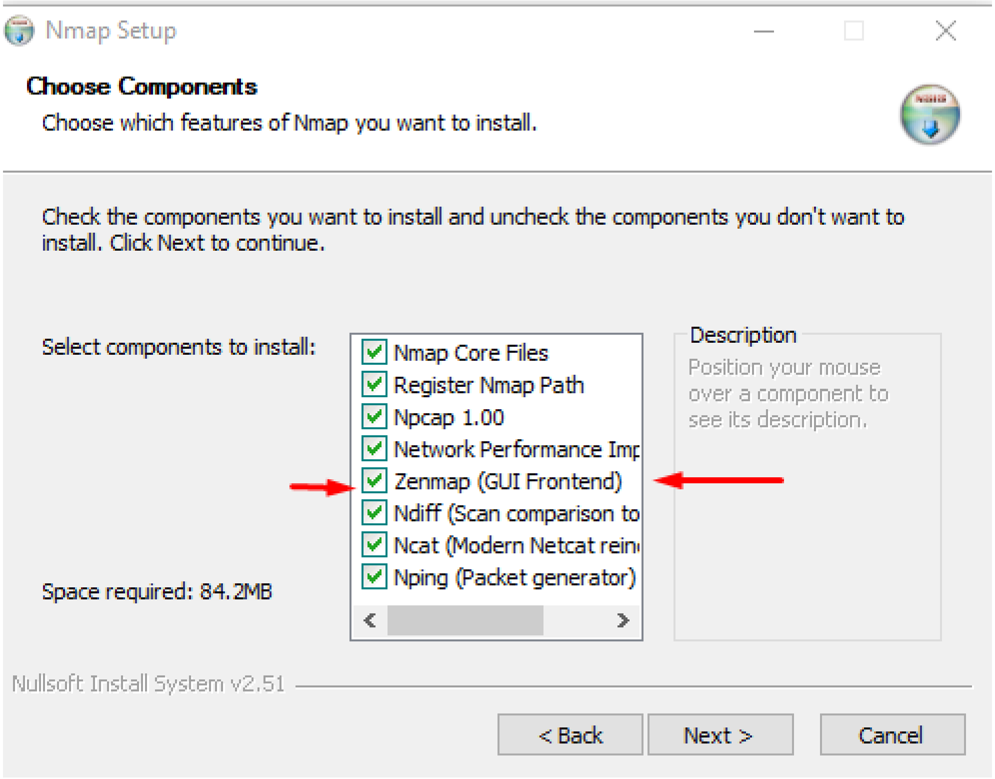
We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), they are still available. The Zenmap graphical interface is *not* included with these, so download and install a superior command shell such as those included with the free Cygwin system. Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributab advantage is that these zip files are a fraction of the size of the executable installer:

Latest stable command-line zipfile: nmap-7.91-win32.zip

Linux RPM Source and Binaries

Step-3



Nmap Setup

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Nmap Core Files
☑ Register Nmap Path
☑ Npcap 1.00
☑ Network Performance Imp
☑ Zenmap (GUI Frontend)
☑ Ndiff (Scan comparison to
☑ Ncat (Modern Netcat rein
☑ Nping (Packet generator)

Space required: 84.2MB

Description

Position your mouse over a component to see its description.

Warning: Run as administrator

For Linux

From terminal

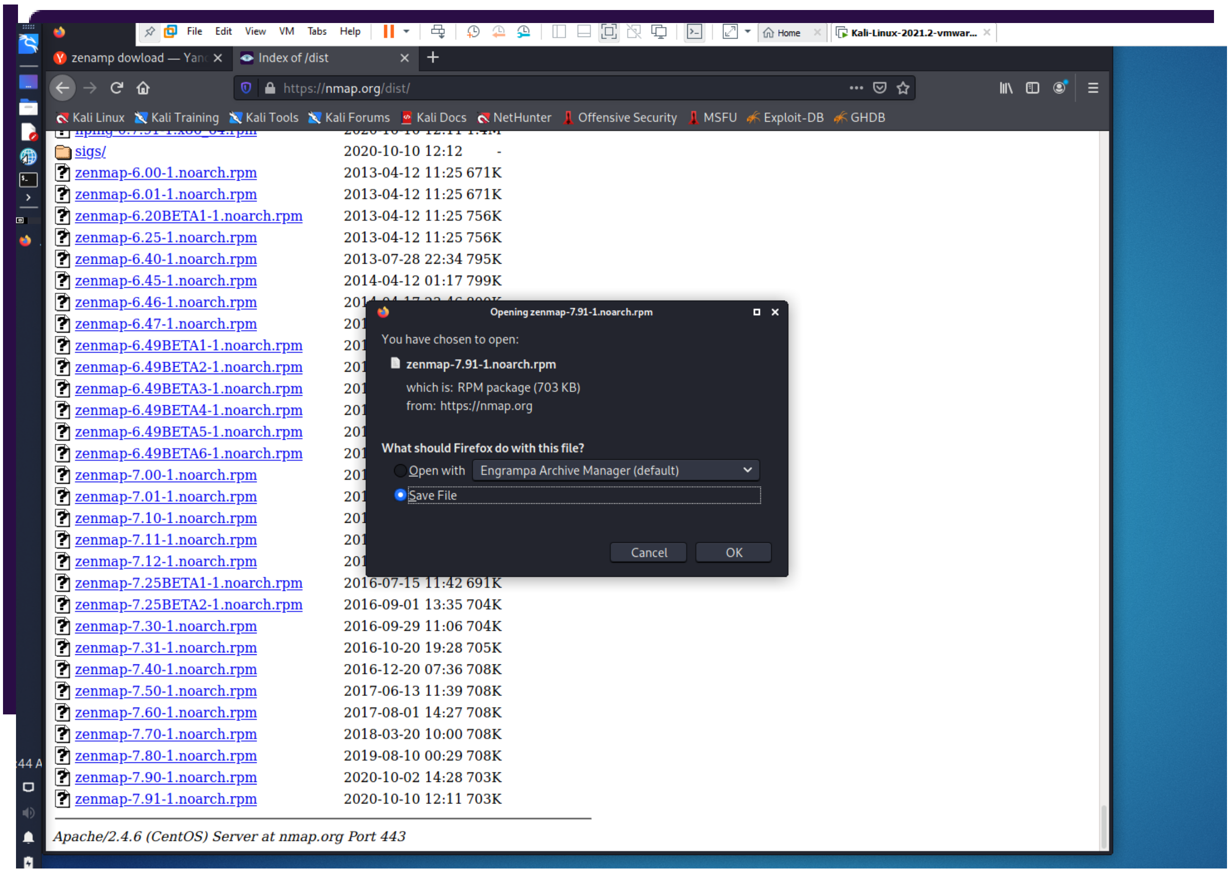
Code:

```
1. wget
   http://archive.ubuntu.com/ubuntu/pool/universe/n/nmap/zenmap_7.60-
   1ubuntu5_all.deb


2. sudo apt install ./zenmap_7.60-1ubuntu5_all.deb
```

3. Now run as a root user

From web page + terminal

1. Nmap.org/dist
2. apt-get install alien dpkg-dev debhelper build-essential
3. alien-zenmap (write as a same file name .rpm type)
4. dpkg-i zenmap (write as a same file name .deb type)
5. zenmap (run as a root user)



https://nmap.org/dist/

```
sigs/                              2020-10-10 12:12    -
zenmap-6.00-1.noarch.rpm           2013-04-12 11:25 671K
zenmap-6.01-1.noarch.rpm           2013-04-12 11:25 671K
zenmap-6.20BETA1-1.noarch.rpm      2013-04-12 11:25 756K
zenmap-6.25-1.noarch.rpm           2013-04-12 11:25 756K
zenmap-6.40-1.noarch.rpm           2013-07-28 22:34 795K
zenmap-6.45-1.noarch.rpm           2014-04-12 01:17 799K
zenmap-6.46-1.noarch.rpm           2014-04-17 22:46 800K
zenmap-6.47-1.noarch.rpm           201
zenmap-6.49BETA1-1.noarch.rpm      201
zenmap-6.49BETA2-1.noarch.rpm      201
zenmap-6.49BETA3-1.noarch.rpm      201
zenmap-6.49BETA4-1.noarch.rpm      201
zenmap-6.49BETA5-1.noarch.rpm      201
zenmap-6.49BETA6-1.noarch.rpm      201
zenmap-7.00-1.noarch.rpm           201
zenmap-7.01-1.noarch.rpm           201
zenmap-7.10-1.noarch.rpm           201
zenmap-7.11-1.noarch.rpm           201
zenmap-7.12-1.noarch.rpm           201
zenmap-7.25BETA1-1.noarch.rpm      2016-07-15 11:42 691K
zenmap-7.25BETA2-1.noarch.rpm      2016-09-01 13:35 704K
zenmap-7.30-1.noarch.rpm           2016-09-29 11:06 704K
zenmap-7.31-1.noarch.rpm           2016-10-20 19:28 705K
zenmap-7.40-1.noarch.rpm           2016-12-20 07:36 708K
zenmap-7.50-1.noarch.rpm           2017-06-13 11:39 708K
zenmap-7.60-1.noarch.rpm           2017-08-01 14:27 708K
zenmap-7.70-1.noarch.rpm           2018-03-20 10:00 708K
zenmap-7.80-1.noarch.rpm           2019-08-10 00:29 708K
zenmap-7.90-1.noarch.rpm           2020-10-02 14:28 703K
zenmap-7.91-1.noarch.rpm           2020-10-10 12:11 703K
```

Apache/2.4.6 (CentOS) Server at nmap.org Port 443

Opening zenmap-7.91-1.noarch.rpm

You have chosen to open:

zenmap-7.91-1.noarch.rpm

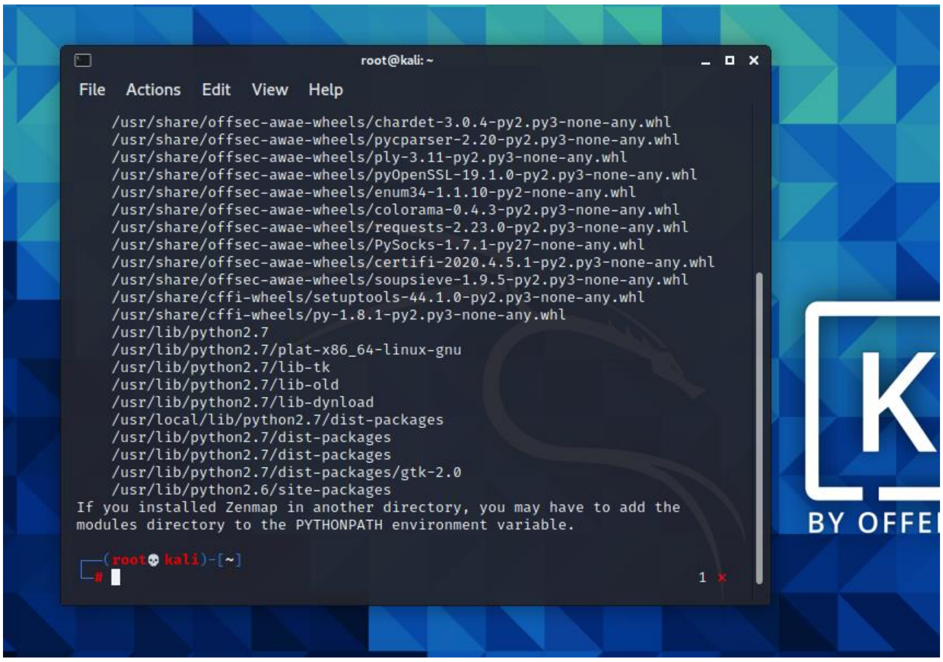
which is: RPM package (703 KB)
from: https://nmap.org

What should Firefox do with this file?

○ Open with Engrampa Archive Manager (default)
● Save File

Cancel OK

Some Erors



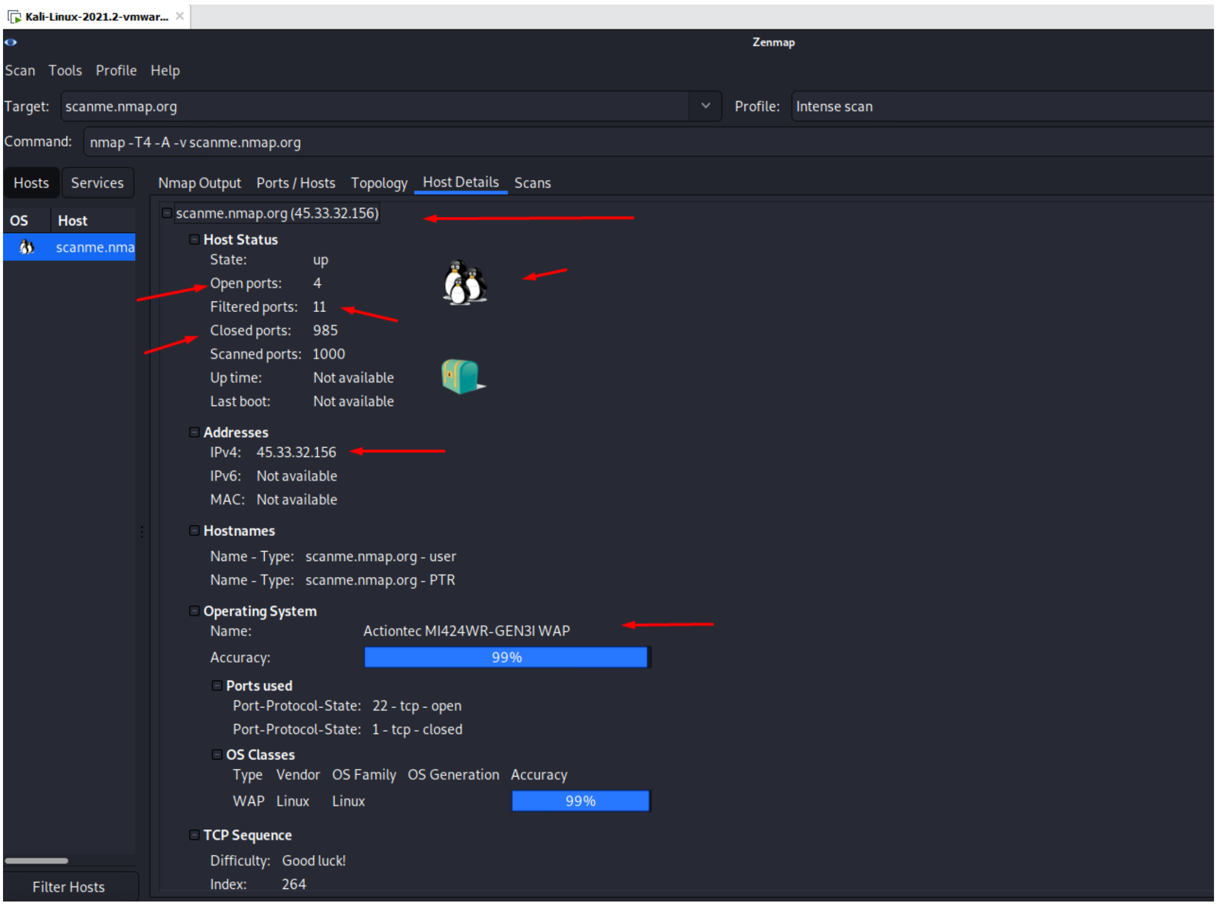
```
    /usr/share/offsec-awae-wheels/chardet-3.0.4-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/pycparser-2.20-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/ply-3.11-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/enum34-1.1.10-py2-none-any.whl
    /usr/share/offsec-awae-wheels/colorama-0.4.3-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/PySocks-1.7.1-py27-none-any.whl
    /usr/share/offsec-awae-wheels/certifi-2020.4.5.1-py2.py3-none-any.whl
    /usr/share/offsec-awae-wheels/soupsieve-1.9.5-py2.py3-none-any.whl
    /usr/share/cffi-wheels/setuptools-44.1.0-py2.py3-none-any.whl
    /usr/share/cffi-wheels/py-1.8.1-py2.py3-none-any.whl
    /usr/lib/python2.7
    /usr/lib/python2.7/plat-x86_64-linux-gnu
    /usr/lib/python2.7/lib-tk
    /usr/lib/python2.7/lib-old
    /usr/lib/python2.7/lib-dynload
    /usr/local/lib/python2.7/dist-packages
    /usr/lib/python2.7/dist-packages
    /usr/lib/python2.7/dist-packages
    /usr/lib/python2.7/dist-packages/gtk-2.0
    /usr/lib/python2.6/site-packages
If you installed Zenmap in another directory, you may have to add the
modules directory to the PYTHONPATH environment variable.

┌──(root💀kali)-[~]
└─#                                                                1 ×
```

Solving

```
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pygtk/python-gtk2_2.24.0-5.1ubuntu2_amd64.deb

wget http://azure.archive.ubuntu.com/ubuntu/pool/universe/p/pygobject-2/python-gobject-2_2.28.6-14ubuntu1_amd64.deb

wget http://security.ubuntu.com/ubuntu/pool/universe/p/pycairo/python-cairo_1.16.2-2ubuntu2_amd64.deb

dpkg -i python-gobject-2_2.28.6-14ubuntu1_amd64.deb

dpkg -i python-cairo_1.16.2-2ubuntu2_amd64.deb

dpkg -i python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
```

https://stackoverflow.com/questions/66345837/converting-rpm-files-to-debian-error-package-build-failed

Result screen of zenmap after scenning



Target: scanme.nmap.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.nmap.org

scanme.nmap.org (45.33.32.156)

Host Status

State: up

Open ports: 4

Filtered ports: 11

Closed ports: 985

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 45.33.32.156

IPv6: Not available

MAC: Not available

Hostnames

Name - Type: scanme.nmap.org - user

Name - Type: scanme.nmap.org - PTR

Operating System

Name: Actiontec MI424WR-GEN3I WAP

Accuracy: 99%

Ports used

Port-Protocol-State: 22 - tcp - open

Port-Protocol-State: 1 - tcp - closed

OS Classes

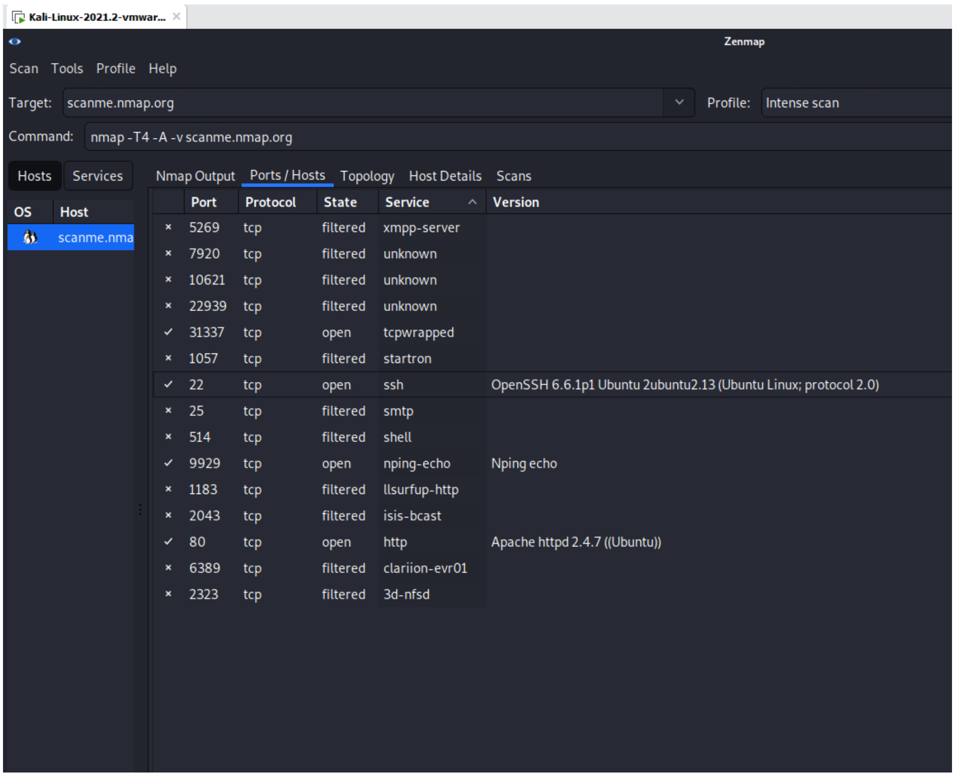
Type	Vendor	OS Family	OS Generation	Accuracy
WAP	Linux	Linux		99%

TCP Sequence

Difficulty: Good luck!

Index: 264

Ports and services



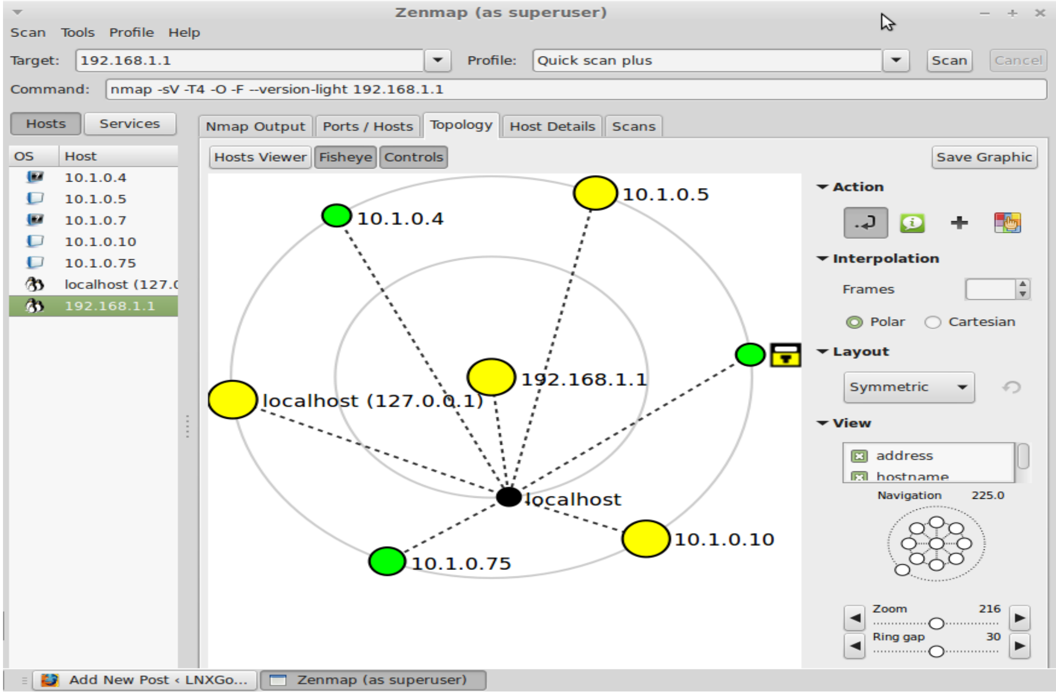
Target: scanme.nmap.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.nmap.org

	Port	Protocol	State	Service	Version
×	5269	tcp	filtered	xmpp-server	
×	7920	tcp	filtered	unknown	
×	10621	tcp	filtered	unknown	
×	22939	tcp	filtered	unknown	
✓	31337	tcp	open	tcpwrapped	
×	1057	tcp	filtered	startron	
✓	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
×	25	tcp	filtered	smtp	
×	514	tcp	filtered	shell	
✓	9929	tcp	open	nping-echo	Nping echo
×	1183	tcp	filtered	llsurfup-http	
×	2043	tcp	filtered	isis-bcast	
✓	80	tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
×	6389	tcp	filtered	clariion-evr01	
×	2323	tcp	filtered	3d-nfsd	

Topology part



Zenmap (as superuser)

Target: 192.168.1.1

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 192.168.1.1

OS	Host
	10.1.0.4
	10.1.0.5
	10.1.0.7
	10.1.0.10
	10.1.0.75
	localhost (127.(
	192.168.1.1

Frames: ◉ Polar ○ Cartesian

Layout: Symmetric

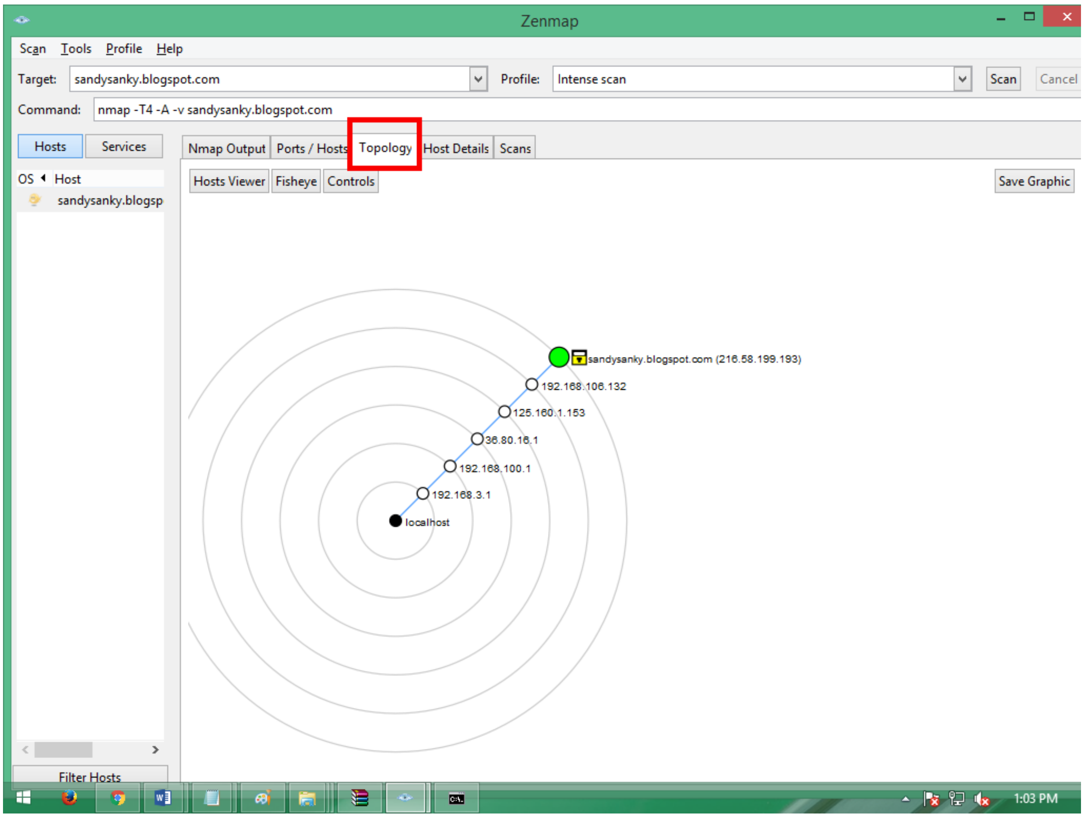
View: ☒ address ☒ hostname

Navigation 225.0

Zoom 216

Ring gap 30

Inside of the network



Zenmap

Target: sandysanky.blogspot.com

Profile: Intense scan

Command: nmap -T4 -A -v sandysanky.blogspot.com

OS	Host
	sandysanky.blogsp

Outside of the network