

hostmap User Guide

by Alessandro ‘jekil‘ Tanasi

release 0.2

Abstract

“It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.” – Sun Tzu, The Art of War

This paper is the hostmap user guide. Get the latest version in the project homepage: <http://hostmap.sourceforge.net>

Contents

1	Introduction	4
1.1	Requirements	4
1.2	Use case	4
1.3	How to get hostmap	4
2	Installation	5
2.1	Zip and tar.gz archive	5
3	Quick start guide	6
3.1	Your first discovery	6
3.2	Fast and furious	8
4	Features and techniques	11
4.1	Features	11
4.2	Techniques	11
4.2.1	DNS enumeration techniques	11
4.2.2	SSL/TLS Protocol enumeration techniques	12
4.2.3	Passive web enumeration techniques	12
5	Usage	14
5.1	Show help	14
5.2	Show version	15
5.3	Target	15
5.4	Show debug messages	15
5.5	Use a user defined DNS server	15
5.6	DNS Zone Transfer check	15
5.7	Without host name brute-forcing	15
5.8	Brute-force aggressivity	16
5.9	Only passive discovery	16
5.10	Without paranoid check	16
5.11	Using the configuration file	17
6	Feedback and bug reports	18
7	Copyright and license	19
8	Disclaimer	20
9	FAQ	21
9.1	General questions	21
9.1.1	Can i redistribute hostmap?	21
9.1.2	Can i include hostmap in my closed source commercial product?	21
9.1.3	I want to help hostmap, what can i do?	21
9.2	Usage questions	21
9.2.1	How can i improve hostmap performances?	21
9.2.2	Some alias and virtual hosts weren't enumerated or there was a difference between two hostmap runs	21
9.3	Feedback questions	22

9.3.1	I found a bug or i want to suggest some features . . .	22
9.3.2	I want to help but i haven't time	22
9.3.3	This software is shit and you are an idiot	22

1 Introduction

This is the official user guide for version 0.2 of the hostmap host name discovery tool. This guide is designed to explain what hostmap is, how it works, and what you can do with it.

The latest version of this document can be found on the hostmap web site: <http://hostmap.sourceforge.net>.

The hostmap host name discovery tool is an utility designed to discover the host names related to a given IP address.

The primary users of hostmap are professionals performing vulnerability assessments and penetration tests.

1.1 Requirements

hostmap is fully implemented using Ruby, an object oriented programming language. The Ruby interpreter is freely downloadable from its official site: <http://ruby-lang.org/>. It's installable in GNU/Linux, Apple OSX and Microsoft Windows.

hostmap is fully portable in GNU/Linux, Apple OSX and Microsoft Windows.

1.2 Use case

In the real world an IP address can be registered in a DNS server with multiple host names, because it can have some aliases or it is hosting a bunch of websites.

For example the IP address 1.2.3.4 can has the following names registered, as you can see from a piece of the BIND zone configuration file:

```
www.foo.com      CNAME foo.com
foo.com          A        1.2.3.4
mail.foo.com     A        1.2.3.4
```

An user, or a penetration tester, that needs to test the security of the 1.2.3.4 machine needs to know all his host names.

The purpose of hostmap is to discover all this registered DNS names, also called host names or virtual hosts, to provide a better knowledge of the target and an extended attack surface to the user.

1.3 How to get hostmap

You can get the latest hostmap version from the official website <http://hostmap.sourceforge.net>.

hostmap is available in several packaging formats to fit your own requirements.

2 Installation

There are several ways and package to use or install hostmap, choose one of the following.

If you don't know what you need, use the zip archive so you don't need to install it, simply download, unpack and run.

2.1 Zip and tar.gz archive

Operating system independent host compressed sources.

You need only to unzip the archive and run hostmap as explained in the Quick Start Guide. See Section 3.

3 Quick start guide

A ten seconds guide to use hostmap! Now the scenario is: you have an IP address and you want to know all the host names related.

3.1 Your first discovery

To start a discovery with hostmap using the default options you need only to use the -t options followed by the target IP address, see an example:

```
$ ruby hostmap.rb -t 94.23.200.187
hostmap 0.2 codename prematurata
Coded by Alessandro 'jekil' Tanasi <alessandro@tanasi.it>

[2009-12-16 19:08] Found new hostname rps9072.ovh.net
[2009-12-16 19:08] Found new domain ovh.net
[2009-12-16 19:08] Found new hostname www.tanasi.it
[2009-12-16 19:08] Found new domain tanasi.it
[2009-12-16 19:08] Found new hostname www.lonerunners.net
[2009-12-16 19:08] Found new domain lonerunners.net
[2009-12-16 19:08] Found new hostname lonerunners.net
[2009-12-16 19:08] Found new hostname angelo.lonerunners.net
[2009-12-16 19:08] Found new hostname lab.lonerunners.net
[2009-12-16 19:09] Found new hostname secdocs.lonerunners.net
[2009-12-16 19:12] Skipping DNS Zone transfer because it is disabled
by default, you must enable it from from command line.
[2009-12-16 19:12] Found new mail server 2.kmx.ovh.net
[2009-12-16 19:12] Skipping DNS Zone transfer because it is disabled
by default, you must enable it from from command line.
[2009-12-16 19:12] Found new nameserver dns13.ovh.net
[2009-12-16 19:12] Found new mail server 1.kmx.ovh.net
[2009-12-16 19:12] Found new nameserver ns1.th.seeweb.it
[2009-12-16 19:12] Skipping DNS Zone transfer because it is disabled
by default, you must enable it from from command line.
[2009-12-16 19:12] Found new mail server aspmx3.googlemail.com
[2009-12-16 19:12] Found new nameserver ns13.ovh.net
[2009-12-16 19:12] Found new nameserver ns2.th.seeweb.it
[2009-12-16 19:12] Found new mail server aspmx5.googlemail.com
[2009-12-16 19:12] Found new nameserver dns10.ovh.net
[2009-12-16 19:12] Found new mail server alt2.aspmx.l.google.com
[2009-12-16 19:12] Found new nameserver ns38.domaincontrol.com
[2009-12-16 19:12] Found new mail server aspmx2.googlemail.com
[2009-12-16 19:12] Found new mail server aspmx4.googlemail.com
[2009-12-16 19:12] Found new nameserver ns12.ovh.net
[2009-12-16 19:12] Found new nameserver ns37.domaincontrol.com
[2009-12-16 19:12] Found new mail server alt1.aspmx.l.google.com
```

[2009-12-16 19:12] Found new mail server aspmx.l.google.com
[2009-12-16 19:12] Found new nameserver dns15.ovh.net
[2009-12-16 19:12] Found new nameserver ns15.ovh.net
[2009-12-16 19:12] Found new nameserver ns11.ovh.net
[2009-12-16 19:12] Found new nameserver ns10.ovh.net
[2009-12-16 19:12] Found new nameserver dns12.ovh.net
[2009-12-16 19:12] Found new nameserver dns11.ovh.net
[2009-12-16 19:15] Found new hostname ww.tanasi.it
[2009-12-16 19:15] Found new hostname www.tanasi.it
[2009-12-16 19:15] Found new hostname www.lonerunners.net
[2009-12-16 19:15] Found new hostname ww.lonerunners.net

Results for 94.23.200.187

Served by name server (probably)

ns37.domaincontrol.com

ns2.th.seeweb.it

ns13.ovh.net

dns10.ovh.net

dns11.ovh.net

dns13.ovh.net

dns12.ovh.net

ns15.ovh.net

ns1.th.seeweb.it

dns15.ovh.net

ns38.domaincontrol.com

ns11.ovh.net

ns10.ovh.net

ns12.ovh.net

Served by mail exchange (probably)

aspmx.l.google.com

aspmx2.googlemail.com

alt2.aspmx.l.google.com

aspmx3.googlemail.com

aspmx4.googlemail.com

2.kmx.ovh.net

alt1.aspmx.l.google.com

aspmx5.googlemail.com

1.kmx.ovh.net

Hostnames:

ww.lonerunners.net

secdocs.lonerunners.net

angelo.lonerunners.net

rps9072.ovh.net

www.lonerunners.net

lab.lonerunners.net

www.lonerunners.net

```
www.tanasi.it
lonerunners.net
www.tanasi.it
ww.tanasi.it
```

3.2 Fast and furious

To speed up your discovery you can disable the brute forcing enumeration check, so you can miss some results but you can get the best performances.

```
$ ruby hostmap.rb -t 94.23.200.187 --without-bruteforce
hostmap 0.2 codename prematurata
Coded by Alessandro 'jekil' Tanasi <alessandro@tanasi.it>
```

```
[2009-12-16 12:52] Found new hostname www.lonerunners.net
[2009-12-16 12:52] Found new hostname www.tanasi.it
[2009-12-16 12:52] Found new domain lonerunners.net
[2009-12-16 12:52] Found new domain tanasi.it
[2009-12-16 12:52] Found new hostname lonerunners.net
[2009-12-16 12:52] Found new hostname rps9072.ovh.net
[2009-12-16 12:52] Found new hostname angelo.lonerunners.net
[2009-12-16 12:52] Found new domain ovh.net
[2009-12-16 12:53] Found new hostname secdocs.lonerunners.net
[2009-12-16 12:53] Found new hostname lab.lonerunners.net
[2009-12-16 12:55] Skipping DNS Zone transfer because it is disabled
by default, you must enable it from from command line.
[2009-12-16 12:55] Skipping DNS bruteforce because it is disabled from
command line
[2009-12-16 12:55] Found new nameserver ns1.th.seeweb.it
[2009-12-16 12:55] Skipping DNS Zone transfer because it is disabled
by default, you must enable it from from command line.
[2009-12-16 12:55] Found new mail server aspmx3.googlemail.com
[2009-12-16 12:55] Found new nameserver ns2.th.seeweb.it
[2009-12-16 12:55] Skipping DNS bruteforce because it is disabled from
command line
[2009-12-16 12:55] Skipping DNS Zone transfer because it is disabled
by default, you must enable it from from command line.
[2009-12-16 12:55] Found new mail server aspmx5.googlemail.com
[2009-12-16 12:55] Found new mail server alt2.aspmx.l.google.com
[2009-12-16 12:55] Found new nameserver ns38.domaincontrol.com
[2009-12-16 12:55] Found new nameserver ns13.ovh.net
[2009-12-16 12:55] Skipping DNS bruteforce because it is disabled from
command line
[2009-12-16 12:55] Found new mail server aspmx4.googlemail.com
[2009-12-16 12:55] Found new mail server 2.kmx.ovh.net
[2009-12-16 12:55] Found new nameserver dns13.ovh.net
```

[2009-12-16 12:55] Found new mail server aspmx2.googlemail.com
[2009-12-16 12:55] Found new nameserver ns37.domaincontrol.com
[2009-12-16 12:55] Found new mail server 1.kmx.ovh.net
[2009-12-16 12:55] Found new nameserver dns10.ovh.net
[2009-12-16 12:55] Found new mail server alt1.aspmx.l.google.com
[2009-12-16 12:55] Found new mail server aspmx.l.google.com
[2009-12-16 12:55] Found new nameserver dns15.ovh.net
[2009-12-16 12:55] Found new nameserver ns12.ovh.net
[2009-12-16 12:55] Found new nameserver ns15.ovh.net
[2009-12-16 12:55] Found new nameserver ns10.ovh.net
[2009-12-16 12:55] Found new nameserver ns11.ovh.net
[2009-12-16 12:55] Found new nameserver dns12.ovh.net
[2009-12-16 12:55] Found new nameserver dns11.ovh.net

Results for 94.23.200.187

Served by name server (probably)

ns37.domaincontrol.com

ns13.ovh.net

ns2.th.seeweb.it

dns10.ovh.net

dns11.ovh.net

dns13.ovh.net

dns12.ovh.net

ns15.ovh.net

ns1.th.seeweb.it

dns15.ovh.net

ns38.domaincontrol.com

ns11.ovh.net

ns10.ovh.net

ns12.ovh.net

Served by mail exchange (probably)

aspmx.l.google.com

aspmx2.googlemail.com

alt2.aspmx.l.google.com

aspmx3.googlemail.com

2.kmx.ovh.net

aspmx4.googlemail.com

alt1.aspmx.l.google.com

1.kmx.ovh.net

aspmx5.googlemail.com

Hostnames:

secdocs.lonerunners.net

angelo.lonerunners.net

rps9072.ovh.net

lab.lonerunners.net

www.tanasi.it

www.lonerunners.net
lonerunners.net

4 Features and techniques

The aim of hostmap is to enumerate all the virtual hosts and DNS names of an IP address, and do this in the fastest and detailed way.

To achieve this hostmap uses a lot of techniques, some never used by any other tool, combined with development technologies to get the best performances.

4.1 Features

- DNS names and virtual host enumeration
- Multiple discovery techniques
- Results correlation, aggregation and normalization
- Multithread and event based engine
- Platform independent: hostmap can run on GNU/Linux, Microsoft Windows, Apple OSX and in each system where Ruby works.

4.2 Techniques

To enumerate all the alias of a target machine hostmap uses a lot of techniques based on protocols, exposed services, target weakness, target vulnerabilities, brute-forcing, public databases and search engines that can reveal a target's alias.

The data are fetched at run time from this data sources using multi thread engine to speed up the fetching phase.

All data fetched being aggregated, normalized, correlated and the results are checked at run time to avoid false positives.

The hostmap engine is based on the knowledge of event, each enumeration action can get results, based on type of enumeration action and the type of the results hostmap dynamically choose the next action to take and the next enumeration check to launch. hostmap uses an adaptive engine written to get much more results possible.

The techniques used by hostmap are the following.

4.2.1 DNS enumeration techniques

The following enumeration techniques are based on the DNS protocol and are:

- Reverse DNS lookup
Performs a PTR request to get the host name from IP address.
- Name servers record lookup
Get the authoritative name server for the target host.

- Mail exchange record lookup
Get the MX records for the target host domain.
- DNS AXFR zone transfer
The name server that serve the target machine's domain zone can be prone to a zone transfer vulnerability. This allow an attacker to perform a AXFR zone transfer and get a dump of all DNS records served by this name server.
- Host name brute-forcing
Using a brute-forcing tries to guess an host name on the enumerated domain that resolve as the target IP address.

4.2.2 SSL/TLS Protocol enumeration techniques

The following enumeration techniques are based on the SSL/TLS protocol and are:

- X.509 Certificate
Usually the target machine can publish some HTTP services. A connection is tried to the common HTTP service ports and is tried to negotiate an SSL/TLS connection, if the remote server supply a X.509 certificate the host name is taken from the issuer and subject Common Name (CN) field and from alternate subject extension field.

4.2.3 Passive web enumeration techniques

The following enumeration techniques are based on third party web sites and are:

- Search engines
The following search engines are used:
 - Microsoft Bing (with and without search API): <http://search.msn.com>
- GPG/PGP key databases
The following public databases are used:
 - MIT GPG key server: <http://pgp.mit.edu:11371>
- DNS/WHOIS databases
Public WHOIS information database, like RIPE, or DNS snapshot database are used to passively enumerate host name and track his history.
The following public databases are used:
 - DNShistory: <http://dnshistory.org>

- Domainsdb: <http://www.domainsdb.net/>
- Fbk.de: <http://www.bfk.de/>
- Gigablast: <http://www.gigablast.com>
- Netcraft: <http://searchdns.netcraft.com>
- Robtex: <http://www.robtex.com>
- Tomdns: <http://www.tomdns.net>
- Web-max: <http://www.web-max.ca>

5 Usage

You can use hostmap from command line interface with following:

```
ruby hostmap.rb OPTIONS -t TARGET
```

Where TARGET is the IP address of the host against you want a host discovery and OPTIONS is a list of hostmap's options.

Available options are explained here.

5.1 Show help

Option: -h or -help

Show the help screen with all options available.

```
$ ruby hostmap.rb -h
hostmap 0.2 codename prematurata
Coded by Alessandro 'jekil' Tanasi <alessandro@tanasi.it>

Usage: hostmap.rb [options] -t [target]

Target options:
  -t, --target [STRING]          set target domain

Discovery options:
  --with-zonetransfer            enable DNS zone transfer check
  --without-bruteforce          disable DNS bruteforcing
  --bruteforce-level [STRING]   set bruteforce aggressivity,
values are lite, custom or full (default is lite)
  --without-be-paranoid         don't check the results
consistency
  --http-ports [STRING]         set a comma separated list of
custom HTTP ports to check
  --only-passive                passive discovery, don't make
network activity to the target network

Common options:
  -d, --dns [STRING]           set a comma separated list of DNS
servers IP addresses to use instead of system defaults
```

<code>-v, --verbose</code>	<code>set verbose mode</code>
<code>-h, --help</code>	<code>show this help message</code>

5.2 Show version

Option: `-version`

Show the hostmap version.

5.3 Target

Option: `-t` or `-target`

The host IP address that will be scanned for host names.
A target must be always set.

5.4 Show debug messages

Option: `-v` or `-verbose`

Show all debug messages, this can give a more detailed view of hostmap work.

5.5 Use a user defined DNS server

Option: `-d` or `-dns`

Use a user specified DNS server for all DNS queries. You use this option with a comma separated list of DNS server IP addresses to as parameters.

5.6 DNS Zone Transfer check

Option: `-with-zone-transfer`

Performs a DNS AXFR zone transfer check against name servers that handle the target host.

This option can discover a misconfigured DNS server that allow a full zone transfer, an attacker that use this type of vulnerability can get the full list of the names handled by the vulnerable DNS server.

Some system administrators can see this type of check as an attack against his systems, so this option is disabled by default and use it carefully at your own risk.

5.7 Without host name brute-forcing

Option: `-without-brute-force`

Disable the host name brute forcing check.

Disabling brute forcing you get a fastest scan but you can miss some results that are enumerated only with brute forcing.

5.8 Brute-force aggressivity

Option: `-brute-force-level`

With this option you can choose the aggressivity of the DNS host name brute-forcing.

Accepted values are *lite*, *custom* or *full*. The default value is *lite*.

You can see the dictionary used by each level in the `dictionaries` folder of `hostmap`.

If you need to edit default dictionaries or edit you own we suggest to use *custom.txt* under the *dictionaries* directory.

5.9 Only passive discovery

Option: `-only-passive`

Runs only the enumeration checks that don't performs any activity with the target.

Use this if you want to run a stealth discovery.

5.10 Without paranoid check

Option: `-without-be-paranoid`

By defaults for each enumerated alias `hostmap` performs a paranoid check to assure that the enumerated DNS name resolves with the target IP address.

With this check `hostmap` confirms the enumerated alias and assure the quality of his results.

In same cases, this can be prone to false positives, because an alias can be discarded if it doesn't resolve with the target IP address but some services on the target host are still configured to serve that alias.

An example can be a web server, that is configured for virtual hosting, and is configured to serve `antani.gov` website. After an year of activity `antani.gov` is moved to another hosting company, so the DNS records are changed to point to the new company web servers, but the system administrator of the old hosting company miss to delete the virtual host from the web server configuration. So we have a virtual host that is alive in a service (HTTP) but his DNS record point to a IP address that isn't the target IP address.

This strange behavior can't be detected by `hostmap`, but using the `-without-be-paranoid` option you can skip the paranoid check and get the list of all enumerated alias for your target.

The use of `-without-be-paranoid` slows `hostmap` execution and is useful only when the `hostmap` results are post processed by user.

5.11 Using the configuration file

The file `hostmap.conf` is used to store some common user settings. You need to simply edit and save it to change the settings automatically loaded at each `hostmap` run.

The options in the configuration file are overridden by the supplied command line options.

6 Feedback and bug reports

Any kind of feedback is very appreciated!

If you have feature requests, ideas, bug reports or simply you want to give your feedback about hostmap write to alessandro@tanasi.it `mailto:alessandro@tanasi.it`. I am happy to read your opinion.

7 Copyright and license

hostmap is copyrighted by Alessandro Tanasi and is licensed under GNU General Public License version 3.

hostmap is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

See the GNU General Public License for more details, the full software license is available in the LICENSE.txt file.

8 Disclaimer

hostmap is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

hostmap is a PoC (Proof of Concept) it's not written to real use because if you use it you can violate the policy of some search engines ;)

Whatever you do with this tool is uniquely your responsibility.

9 FAQ

9.1 General questions

9.1.1 Can i redistribute hostmap?

Yes, you can. hostmap is licensed under the GNU General Public License version 3. See Section 7.

9.1.2 Can i include hostmap in my closed source commercial product?

Generally no, you can't. hostmap is licensed under the GNU General Public License version 3. See Section 7.

9.1.3 I want to help hostmap, what can i do?

Your help is very appreciated, you can help hostmap in several ways, from coding to send bug reports. See 9.3

9.2 Usage questions

9.2.1 How can i improve hostmap performances?

hostmap try to get the best performances available with your connection speed, if you want to speed up hostmap you can try to run it without DNS brute-force using the option `-without-brute-force` documented in 5.7.

If this is not enough for you, try to use only active checks and skip all requests to web services with `-only-passive` documented in 5.9.

Remember that this restrict the number on analysis and you can get less results.

9.2.2 Some alias and virtual hosts weren't enumerated or there was a difference between two hostmap runs

Some alias or virtual hosts cannot be enumerated for one or more times for the following reasons:

- Network connectivity issue: DNS traffic use the UDP protocol that is a best effort not reliable protocol, so sometimes if there is a network issue packets can be lost.
- Plugin trace back: A plugin can get a trace back if there is a bug or in most cases if the service used (like a remote web site) is offline. hostmap use third party services as data mining sources so hostmap results depends on the data sources availability.
- Application level virtual hosts that have a wrong DNS record: if hostmap detect an alias or virtual host that doesn't resolve with the target IP address drops this result. To read more about this see 5.10.

hostmap try to do the best to limit this strange behavior but sometimes there is situations (like network congestion) that can be influenced by hostmap.

9.3 Feedback questions

9.3.1 I found a bug or i want to suggest some features

Any feedback is welcome, write an e-mail to Alessandro Tanasi at alessandro@tanasi.it and you will get an answer to your questions. See the Section 6.

9.3.2 I want to help but i haven't time

There are many ways to help hostmap: coding, testing, donating money, reviewing code and documentation or submitting bug reports and feedback. To do this you don't need to spend a lot of time. Simply reading this user guide and submitting bug reports related to English errors is a great help.

9.3.3 This software is shit and you are an idiot

Yeah, can be true. Write an e-mail to Alessandro Tanasi at alessandro@tanasi.it if you need to talk about idiots, we can have fun together.