

Forum: [Hack Forums](#)

Thread: [\[Tutorial\] 01 - Information Gathering.](#)

Mr. Robot - November 14, 2018, 9:39 am

This is the first part continuing from installation and setup of a Virtual Machine for beginners. Getting comfortable with the tools inside Kali Linux.

Here we will be covering 01 - Information Gathering. Linked at the bottom when complete, will be 02 - Vulnerability Analysis.

At any time if you wish to find more information about a tool you can type
Code man toolnameman is short for manual.

dmitry - Information about websites/servers/subdomains/website emails
Spoiler ([Click to View](#)) To run dmitry you can click "Applications", Mouse over "Information Gathering" and choose dmitry. You may also open a terminal and type
Code dmitry which will give you the output:

dmitry is used to gather information from a hostname or IP address, it can try find email addresses, subdomains and will do port scans of the host.

There are better ways of gather data than dmitry however we will still cover it as it was one of the best tools of its time.

The options fall into 2 categories. Passive and active (with of course -o being output to save to a text file as an output option)

We will be covering the passive options:

- i: Whois lookup on the IP address of a host.
- w: Whois lookup on the domain name of a host.
- n: Retrieve NetCraft.com information on a host.
- s: Search for subdomains.
- e: Search for email addresses.

An example command to look up the whois information on the IP of the website.

Code dmitry -i imgur.com

Whereas this example would do a lookup on the hostname imgur.com instead.

Code dmitry -w imgur.com

If we wish to check NetCraft.com - don't bother using the -n switch as you can simply go to their website and it's much easier.

If we wish to find subdomains such as prefix.imgur.com

Code dmitry -s imgur.com The output shows us: stack.imgur.com

apidocs.imgur.com

i.imgur.com

store.imgur.com

api.imgur.com

status.imgur.com

munity.imgur.com

community.imgur.com

help.imgur.com

If we wish to look for emails using @imgur.com however dmitry doesn't like this command as much as other tools so we wont be using it.

Code dmitry -e imgur.com

A good way to combine these commands would be something like

Code dmitry -wnseo imgur.com This will create a text file called imgur.com.txt while also scanning the URL and outputting all the results to it.

That's pretty much all we will cover with dmitry.

dnmap-client + dnmap-server

Spoiler ([Click to View](#))[spoiler]To run either dnmap-client or dnmap-server you can click "Applications", Mouse over "Information Gathering" and choose each. You may also open a terminal and type

Code dnmap_client which will give you the output:

```
Code +-----+
| dnmap Client Version 0.6                               |
| This program 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 2 of the License, or    |
| (at your option) any later version.                               |
|                               |                             |
| Author: Garcia Sebastian, eldraco@gmail.com                 |
| www.mateslab.com.ar                                           |
+-----+
```

usage: /usr/bin/dnmap_client <options>

options:

- s, --server-ip IP address of dnmap server.
- p, --server-port Port of dnmap server. Dnmap port defaults to 46001
- a, --alias Your name alias so we can give credit to you for your help. Optional
- d, --debug Debugging.
- m, --max-rate Force nmaps commands to use at most this rate. Useful to slow nmap down.

Adds the --max-rate parameter.

Or

Code dnmap_server which will give you the output:

```
Code +-----+
| dnmap_server Version 0.6                               |
| This program 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 2 of the License, or |
| (at your option) any later version. |
| |
| Author: Garcia Sebastian, eldraco@gmail.com |
| www.mateslab.com.ar |
+-----+

usage: /usr/bin/dnmap_server <options>

options:

- f, --nmap-commands Nmap commands file
- p, --port TCP port where we listen for connections.
- L, --log-file Log file. Defaults to /var/log/dnmap_server.conf.
- l, --log-level Log level. Defaults to info.
- v, --verbose_level Verbose level. Give a number between 1 and 5. Defaults to 1. Level 0 means be quiet.
- t, --client-timeout How many time should we wait before marking a client Offline. We still remember its values just in case it comes back.
- s, --sort Field to sort the statical value. You can choose from: Alias, #Commands, UpTime, RunCmdXMin, AvrCmdXMin, Status
- P, --pem-file pem file to use for TLS connection. By default we use the server.pem file provided with the server in the current directory.

dnmap_server uses a '<nmap-commands-file-name>.dnmaptrace' file to know where it must continue reading the nmap commands file. If you want to start over again, just delete the '<nmap-commands-file-name>.dnmaptrace' file

For now I will be leaving this as is as there is so much to cover in this section. You can read these commands and figure out how to work it by trial and error + reading the manual in the mean time.

ike-scan - Discover and fingerprint IKE hosts (IPsec VPN servers)

Spoiler ([Click to View](#)) To run ike-scan you can click "Applications", Mouse over "Information Gathering" and choose ike-scan. You may also open a terminal and type
Code ike-scan which will give you the output:
Code Usage: ike-scan [options] [hosts...]

Target hosts must be specified on the command line unless the --file option is given, in which case the targets are read from the specified file instead.

The target hosts can be specified as IP addresses or hostnames. You can also specify the target as IPnetwork/bits (e.g. 192.168.1.0/24) to specify all hosts in the given network (network and broadcast addresses included), or IPstart-IPend (e.g. 192.168.1.3-192.168.1.27) to specify all hosts in the inclusive range, or IPnetwork:NetMask (e.g. 192.168.1.0:255.255.255.0) to specify all hosts in the given network and mask.

These different options for specifying target hosts may be used both on the command line, and also in the file specified with the --file option.

use "ike-scan --help" for detailed information on the available options.

Report bugs or send suggestions to ike-scan@nta-monitor.com

See the ike-scan homepage at <http://www.nta-monitor.com/tools/ike-scan/>

maltego

Spoiler ([Click to View](#)) To run maltego you can click "Applications", Mouse over "Information Gathering" and choose maltego. You may also open a terminal and type
Code maltego

netdiscover - an active/passive arp reconnaissance tool.

Spoiler ([Click to View](#)) To run netdiscover you can click "Applications", Mouse over "Information Gathering" and choose netdiscover. You may also open a terminal and type

Code netdiscoverCode Netdiscover 0.3-pre-beta7 [Active/passive arp reconnaissance tool]

Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-s time] [-n node] [-c count] [-f] [-d] [-S] [-P] [-c]

- i device: your network device
- r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
- l file: scan the list of ranges contained into the given file
- p passive mode: do not send anything, only sniff
- m file: scan the list of known MACs and host names
- F filter: Customize pcap filter expression (default: "arp")
- s time: time to sleep between each arp request (milliseconds)
- n node: last ip octet used for scanning (from 2 to 253)
- c count: number of times to send each arp request (for nets with packet loss)
- f enable fastmode scan, saves a lot of time, recommended for auto
- d ignore home config files for autoscan and fast mode
- S enable sleep time suppression between each request (hardcore mode)
- P print results in a format suitable for parsing by another program
- N Do not print header. Only valid when -P is enabled.
- L in parsable output mode (-P), continue listening after the active scan is completed

If -r, -l or -p are not enabled, netdiscover will scan for common lan addresses.

nmap - Network exploration tool and security / port scanner

Spoiler ([Click to View](#)) To run nmap you can click "Applications", Mouse over "Information Gathering" and choose nmap. You may also open a terminal and type

Code nmapThere is so much to cover here so I will simply edit this later with more information

p0f - identify remote systems passively

Spoiler ([Click to View](#)) To run p0f you can click "Applications", Mouse over "Information Gathering" and choose p0f. You may also open a terminal and type

Code p0f

recon-ng - Web Reconnaissance framework

Spoiler ([Click to View](#)) To run recon-ng you can click "Applications", Mouse over "Information

Gathering" and choose recon-ng. You may also open a terminal and type
Code recon-ng

sparta - Find and attack devices locally and over the net/Bruteforce xmpp/ssh/teamspeak and more
Spoiler ([Click to View](#))To run sparta you can click "Applications", Mouse over "Information
Gathering" and choose sparta. You may also open a terminal and type
Code sparta

zenmap - Graphical Nmap frontend and results viewer
Spoiler ([Click to View](#))To run zenmap you can click "Applications", Mouse over "Information
Gathering" and choose zenmap. You may also open a terminal and type
Code zenmap

Serty - March 2, 2019, 4:02 pm

i have downloaded Kali Linux but i dont seem to have any of theses applictaions. Do i need to install them?

TouchMe - March 2, 2019, 5:45 pm

(Mar 2, 2019 05:02 PM)Serty Wrote: ([CITE](#)) i have downloaded Kali Linux but i dont seem to have any of theses applictaions. Do i need to install them?

Nigga they come default with kali, you might've installed kali light

You can probably do apt-get install AppName

Daxer - March 2, 2019, 5:48 pm

(Mar 2, 2019 06:45 PM)TouchMe Wrote: ([CITE](#)) Nigga they come default with kali, you might've installed kali light

You can probably do apt-get install AppName
Had to google that didn't you?

TouchMe - March 2, 2019, 6:01 pm

(Mar 2, 2019 06:48 PM)Daxer Wrote: ([CITE](#)) Had to google that didn't you?
Had to get another -3 didn't you?

And nah, about 30 seconds after commenting I was like, man I should probably tell him how or people will criticize my post

You should probably practice this concept ^

hacker1 - March 5, 2019, 1:55 am

thanks.but can you put some passive in fo gathering techniques,like using shodan,google hacking database.,,,?

Night_Zero - September 7, 2019, 5:30 pm

Thanks ! but someone can send me the 2nd tutorial link? I did not find