# 1.1.4 – Exercises

1. Take some time to familiarize yourself with the Kali Linux menu

2. Determine the location of the file plink.exe in Kali

root@kali:~# updatedb

root@kali:~# locate plink.exe

/usr/share/windows-binaries/plink.exe

root@kali:~# find /usr -name plink.exe

/usr/share/windows-binaries/plink.exe

3. Find and read the documentation for the dnsenum tool

root@kali:~# locate dnsenum

/usr/bin/dnsenum

/usr/share/dnsenum

/usr/share/applications/kali-dnsenum.desktop

/usr/share/dnsenum/dns.txt

/usr/share/dnsrecon/lib/mdnsenum.py

/usr/share/doc/dnsenum

/usr/share/doc/dnsenum/README.md

/usr/share/doc/dnsenum/changelog.Debian.gz

/usr/share/doc/dnsenum/copyright

/usr/share/kali-menu/applications/kali-dnsenum.desktop

/usr/share/python-faraday/plugins/repo/dnsenum

/usr/share/python-faraday/plugins/repo/dnsenum/\_\_init\_\_.py

/usr/share/python-faraday/plugins/repo/dnsenum/plugin.py

/var/lib/dpkg/info/dnsenum.list

/var/lib/dpkg/info/dnsenum.md5sums

root@kali:~# cat /usr/share/doc/dnsenum/README.md

README - dnsenum.pl VERSION: 1.2.4

multithreaded perl script to enumerate DNS information of a domain

and to discover non-contiguous ip blocks.

OPERATIONS:

1) Get the host's addresse (A record).

2) Get the namservers (threaded).

3) Get the MX record (threaded).

4) Perform axfr queries on nameservers and get BIND VERSION (threaded).

5) Get extra names and subdomains via google scraping

(google query = "allinurl: -www site:domain").

6) Brute force subdomains from file, can also perform recursion

on subdomain that have NS records (all threaded).

7) Calculate C class domain network ranges and perform whois

queries on them (threaded).

8) Perform reverse lookups on netranges

( C class or/and whois netranges) (threaded).

9) Write to domain\_ips.txt file ip-blocks.

Changelog from version 1.2.2

- Fixed GoogleScraping

- Fixed wildcard issues

- Changed output function to get rid of errors with new Net::DNS version

- A bit of cleanup here and there

- Removed Bind Version detection

PREREQUISITES:

Modules that are included in perl 5.10.0:

Getopt::Long

IO::File

Thread::Queue

Other Necessary modules:

Must have:

Net::IP

Net::DNS

Net::Netmask

Optional:

Net::Whois::IP

HTML::Parser

WWW::Mechanize

XML::Writer

To install a module, simply run (as root):

perl -MCPAN -e shell

and then type: install <MODULE>

eg:

cpan[1]> install XML::Writer

Perl ithreads support:

perl version must be compliled with ithreads support.

threads

threads::shared

OPTIONS: run "perldoc dnsenum.pl".

Special thanks to all Perl developers.

Filip Waeytens <filip.waeytens[at]gmail.com>

tix tixxDZ <tixxdz[at]gmail.com>