myLG

Information Security Inc.

Contents

- About myLG
- Demo Setup
- Features
- Required dependency
- Installing myLG
- Using myLG
- References

About myLG

- myLG is an open source software utility which combines the functions of the different network probes in one network diagnostic tool

myLG, Command line Network Diagnostic Tool

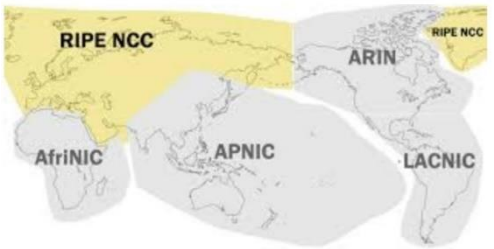
Demo Setup

- Setup
- Kali Linux 2017

```
root@LUCKY64:/opt3# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Features

- Popular looking glasses (ping/trace/bgp): Telia, Level3, NTT, Cogent, KPN
- More than 200 countries DNS Lookup information
- Local ping and real-time trace route
- Packet analyzer - TCP/IP and other packets
- Quick NMS (network management system)
- Local HTTP/HTTPS ping (GET, POST, HEAD)
- RIPE information (ASN, IP/CIDR)
- PeeringDB information



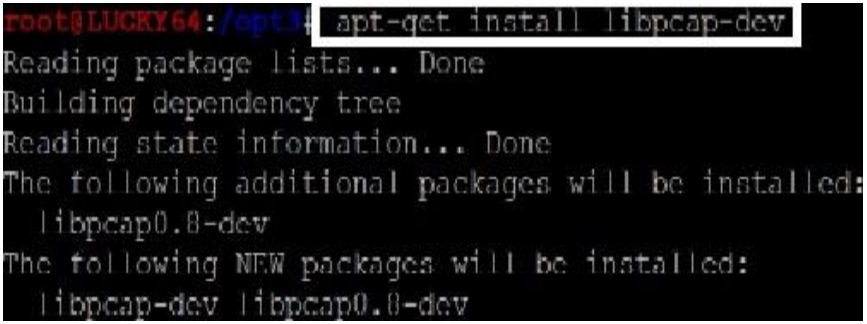
Features

- Port scanning
- Network LAN Discovery
- Internet Speed Test
- Web dashboard
- Configurable options
- Direct access to commands from shell
- Support vi and emacs mode, almost all basic features
- CLI auto complete and history features

Required dependency

• libpcap-dev

- LINUX
apt-get install libpcap-dev



Required dependency

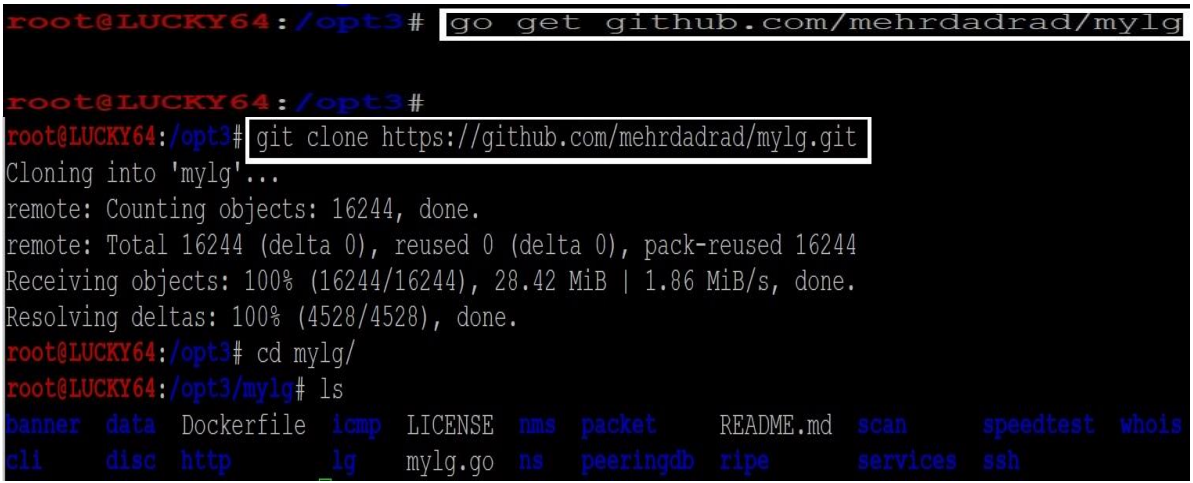
• golang

- LINUX
apt-get install golang

```
root@LUCKY64:~# apt-get install golang
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  golang-1.8 golang-1.8-doc golang-1.8-go golang-1.8-src golang-doc golang-go golang-src pkg-config
```

Installing myLG

- Clone GitHub repository



Installing myLG

- Build myLG

Using myLG

- Run myLG

Using myLG

- myLG help menu

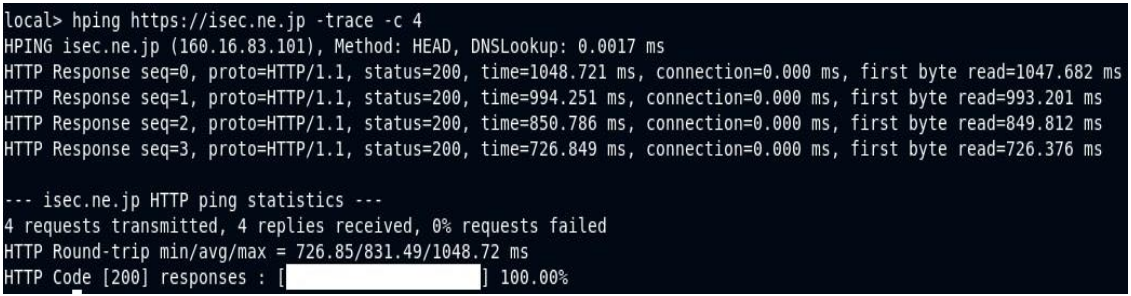
```
local> help
Usage:
        The myLG tool, developed to troubleshoot networking situations.
        The vi/emacs mode, almost all basic features are supported. Press tab to see which options are available.

        connect <provider name>     connects to external looking glass, press tab to see the menu
        node <city/country name>    connects to specific node at current looking glass, press tab to see the available nodes
        local                       back to local
        lg                          change mode to external looking glass
        ns                          change mode to name server looking up
        ping                        ping ip address or domain name
        trace                       trace ip address or domain name (real-time w/ -r option)
        dig                         nameserver look up
        nms                         quick NMS - monitor device/server ports real-time
        whois                       resolve AS number/IP/CIDR to holder (provided by ripe ncc)
        hping                       ping through HTTP/HTTPS w/ GET/POST/HEAD methods
        scan                        scan tcp ports (you can provide range >scan host minport maxport)
        dump                        prints out a description of the contents of packets on a network interface
        disc                        discover all the devices on a LAN
        peering                     peering information (provided by peeringdb.com)
        web                         web dashboard - opens dashboard at your default browser

        Please visit http://mylg.io/doc for more information
```

Using myLG

- myLG hping



Using myLG

- myLG port scanning

```
local> scan hackyourselffirst.troyhunt.com -p 1-1000
Scan hackyourselffirst.troyhunt.com (137.117.17.70) TCP ports 1-1000
please wait .
+----------+------+--------+
| PROTOCOL | PORT | STATUS |
+----------+------+--------+
| TCP      |   80 | Open   |
| TCP      |  443 | Open   |
| TCP      |  454 | Open   |
| TCP      |  455 | Open   |
+----------+------+--------+
Scan done: 4 opened port(s) found in 96.366 seconds
```

Using myLG

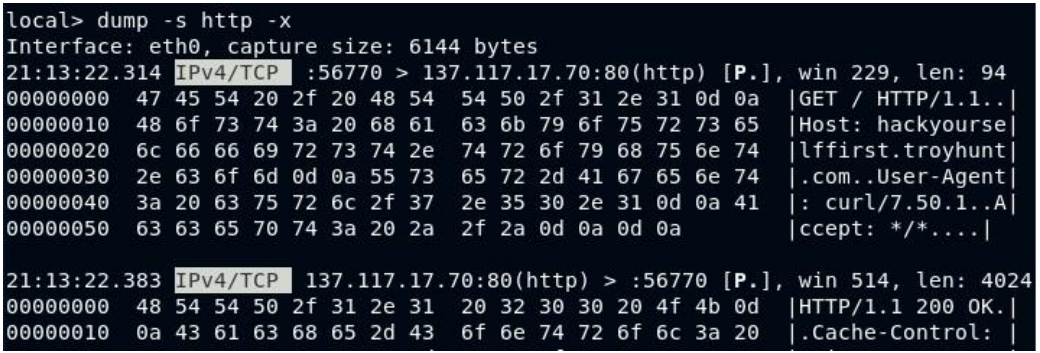
- myLG packet capture

```
local> dump help

    usage:
          dump [filter expression] [options]
          * The expression consists of one or more primitives (Berkeley Packet Filter (BPF) syntax)
    options:
          -c count       Stop after receiving count packets (default: 1M)
          -i interface   Listen on specified interface (default: first non-loopback)
          -w filename    Write packets to a pcap format file
          -d             Print list of available interfaces
          -t             Print without timestamp on each dump line.
          -x             Dump payload in hex format
          -s keyword     Search keyword at payload
          -n             Don't convert host addresses to names
          -nc            Shows dumps without color
    Example:
          dump tcp and port 443 -c 1000
          dump !udp
          dump -i eth0
          dump -w /tmp/mypcap
          dump tcp -s verisign -x
```

Using myLG

- myLG packet capture

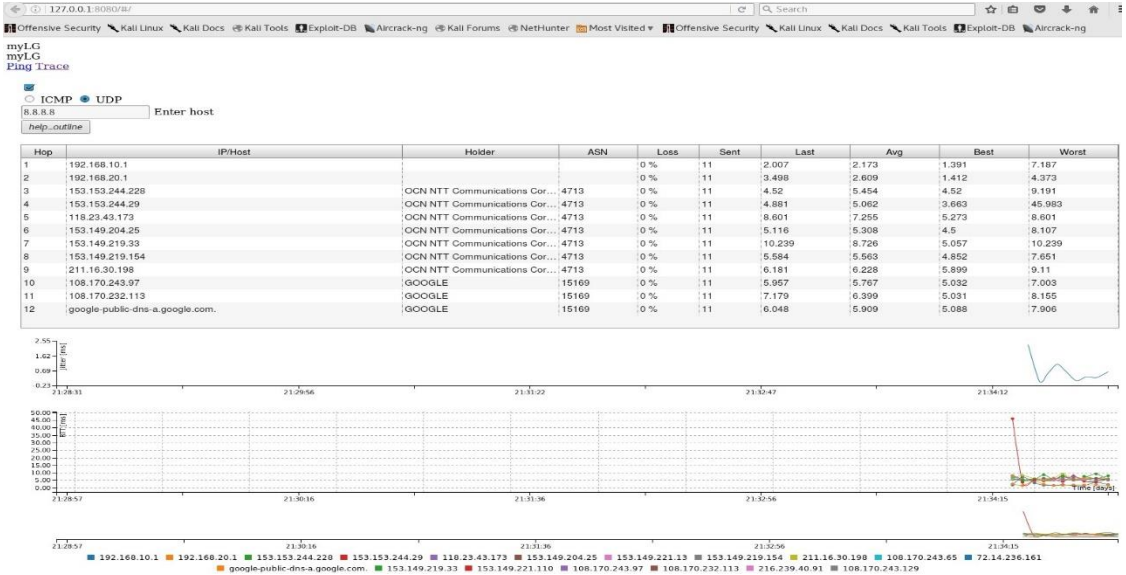


Using myLG

- myLG web dashboard

Using myLG

- myLG web dashboard



References

- Kitploit
http://www.kitploit.com/2016/11/mylg-network-diagnostic-tool.html

- Kali Linux
https://www.kali.org/

- Looking Glass server
https://en.wikipedia.org/wiki/Looking_Glass_server