SpeedPhish Framework

Information Security Inc.

iSEC
information security inc.

Contents

- About SPF (SpeedPhish Framework)
- Requirements
- Demo configuration
- Installation
- Usage
- References

About SPF

- SPF (SpeedPhish Framework) is a python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises

Requirements

- dnspython
- twisted
- PhantomJS

Demo configuration

- Kali Linux 2017 64 bit (https://www.kali.org/downloads/)

Installation

- Install dependencies

```
root@kali2017:~# pip install dnspython;pip install pycrypto
Requirement already satisfied: dnspython in /usr/lib/python2.7/dist-packages
Requirement already satisfied: pycrypto in /usr/lib/python2.7/dist-packages
root@kali2017:~# apt-get install python-twisted-web;apt-get install phantomjs
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python-automat python-hyperlink python-twisted-core
```

- GitHub recursive clone

```
git clone --recursive https://github.com/tatanus/SPF.git
```

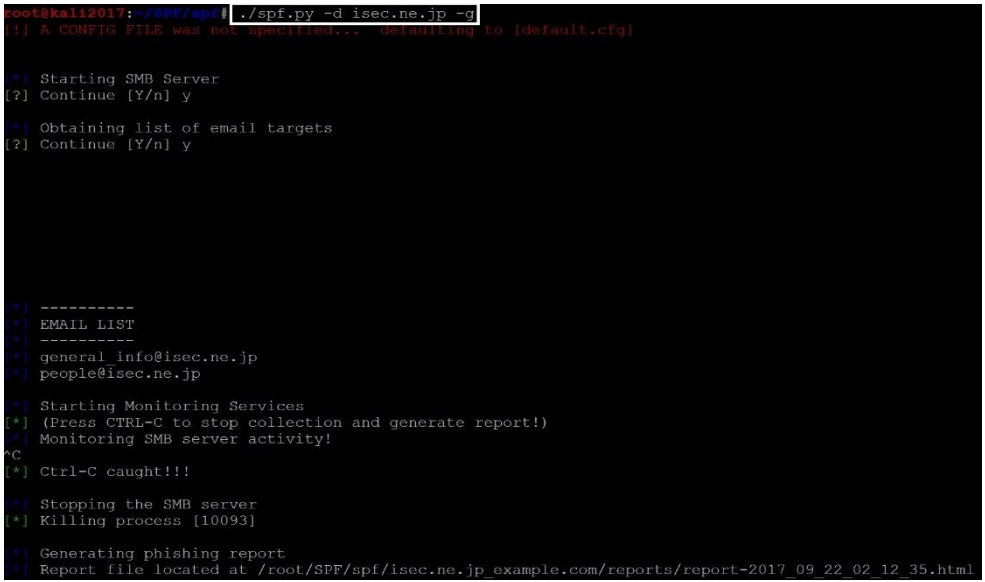
Usage

- ./spf.py –h

```
root@kali2017:~# cd SPF/spf/
root@kali2017:~/SPF/spf# pwd
/root/SPF/spf
root@kali2017:~/SPF/spf# ./spf.py -h
usage: spf.py [-h] [-f <list.txt>] [-C <config.txt>] [--all] [--test]
              [--recon] [--external] [--dns] [-g] [-s] [--simulate] [-w] [-W]
              [--adv] [--profile] [--pillage] [-d <domain>] [-p <domain>]
              [-c <company's name>] [--ip <IP address>] [-v] [-y]

optional arguments:
  -h, --help            show this help message and exit
  -d <domain>           domain name to phish
  -p <domain>           newly registered 'phish' domain name
  -c <company's name>   name of company to phish
  --ip <IP address>     IP of webserver defaults to [192.168.10.12]
  -v, --verbosity       increase output verbosity

input files:
  -f <list.txt>         file containing list of email addresses
  -C <config.txt>       config file

enable flags:
  --all                 enable ALL flags... same as (-g --external -s -w -v -v
                        -y)
  --test                enable all flags EXCEPT sending of emails... same as
                        (-g --external --simulate -w -y -v -v)
  --recon               gather info (i.e. email addresses, dns hosts, websites,
                        etc...) same as (-e --dns)
  --external            enable external tool utilization
  --dns                 enable automated gathering of dns hosts
  -g                    enable automated gathering of email targets
  -s                    enable automated sending of phishing emails to targets
  --simulate            simulate the sending of phishing emails to targets
  -w                    enable generation of phishing web sites
  -W                    leave web server running after termination of spf.py

ADVANCED:
  --adv                 perform all ADVANCED features same as (--dns --profile
                        --pillage)
  --profile             profile the target domain (requires the --dns flag)
  --pillage             auto pillage email accounts (requires the --dns flag)

misc:
  -y                    automatically answer yes to all questions
```

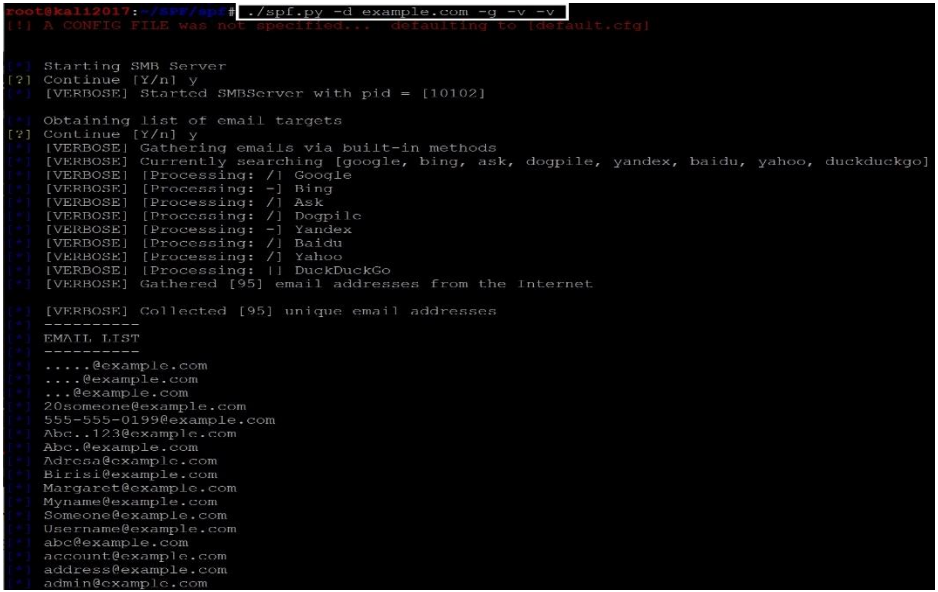
Usage

- Run it against an owned target



Usage

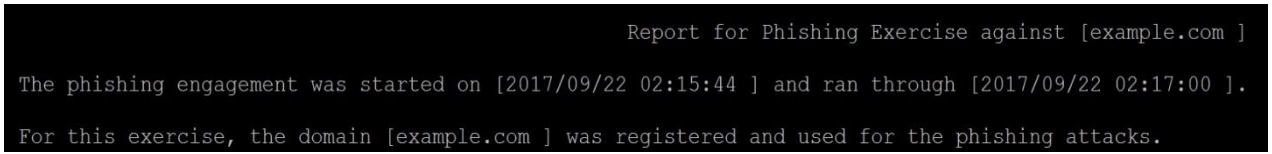
- Run it against an owned target



Usage

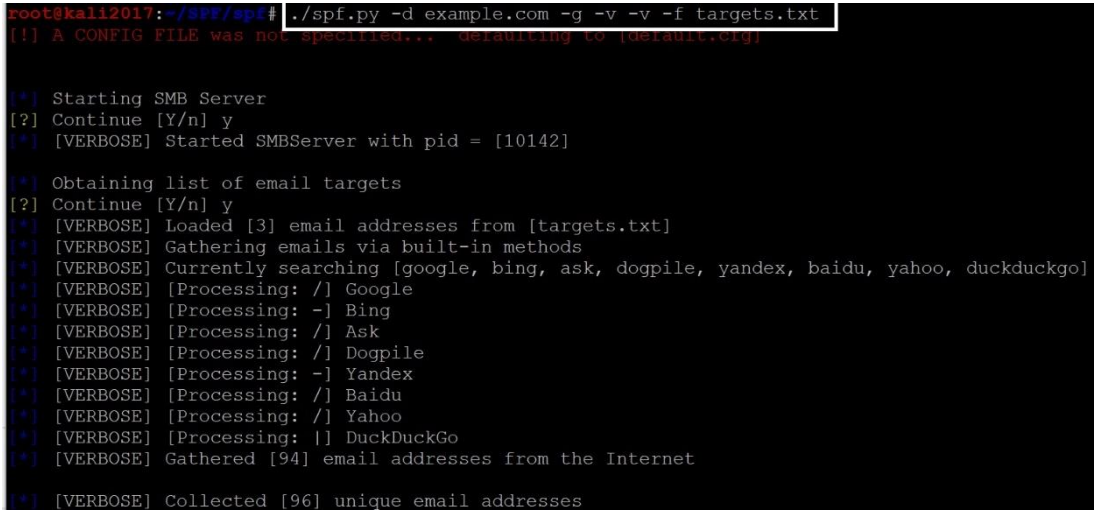
- Viewing the reports

```
root@kali2017:~/SPF/spf/example.com_example.com/reports# pwd
/root/SPF/spf/example.com_example.com/reports
root@kali2017:~/SPF/spf/example.com_example.com/reports# links2 report-2017_09_22_02_17_00.html
```



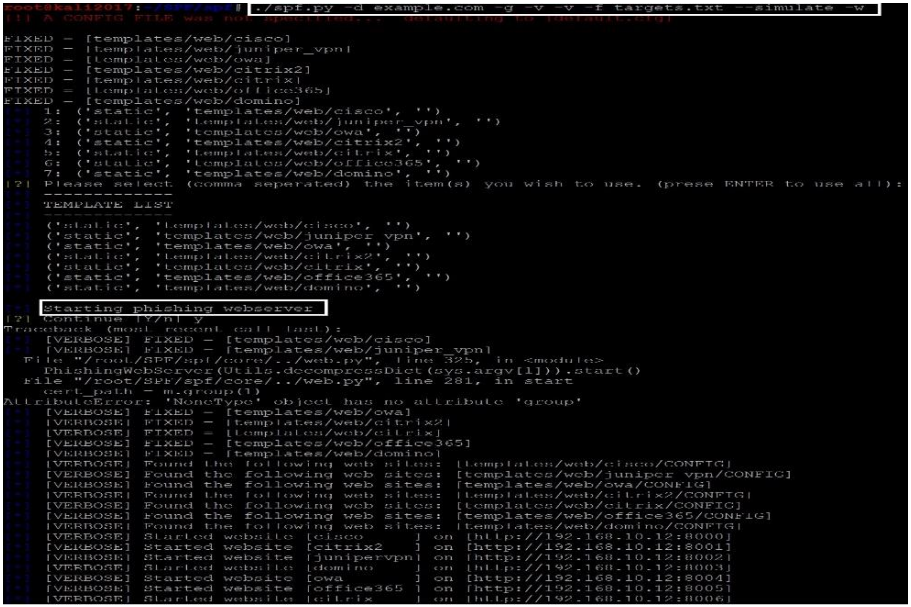
Usage

- Collecting emails



Usage

- Starting the phishing webserver



References

- Kitploit
http://www.kitploit.com/2015/08/spf-speedphish-framework.html

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