



# SpeedPhish Framework

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 (-c --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

```
root@kali2017:~/SPF/spf# ./spf.py -d isec.ne.jp -g
[!] A CONFIG FILE was not specified... defaulting to [default.cfg]

[?] Starting SMB Server
[?] Continue [Y/n] y

[?] Obtaining list of email targets
[?] Continue [Y/n] y

[?] -----
[?] EMAIL LIST
[?] -----
[?] general_info@isec.ne.jp
[?] people@isec.ne.jp

[?] Starting Monitoring Services
[*] (Press CTRL-C to stop collection and generate report!)
[?] Monitoring SMB server activity!
^C
[*] Ctrl-C caught!!!

[?] Stopping the SMB server
[*] Killing process [10093]

[?] Generating phishing report
[?] Report file located at /root/SPF/spf/isec.ne.jp_example.com/reports/report-2017_09_22_02_12_35.html
```



# Usage

- Run it against an owned target

```
root@kali2017:~/sp/sgs# ./spf.py -d example.com -g -v -v
[!] A CONFIG FILE was not specified... defaulting to (rabbit.cfg)

[*] Starting SMB Server
[?] Continue [Y/n] y
[*] [VERBOSE] Started SMBServer with pid = [10102]

[*] Obtaining list of email targets
[?] Continue [Y/n] y
[*] [VERBOSE] Gathering emails via built-in methods
[*] [VERBOSE] Currently searching [google, bing, ask, dogpile, yandex, baidu, yahoo, duckduckgo]
[*] [VERBOSE] [Processing: /] Google
[*] [VERBOSE] [Processing: -] Bing
[*] [VERBOSE] [Processing: /] Ask
[*] [VERBOSE] [Processing: /] Dogpile
[*] [VERBOSE] [Processing: -] Yandex
[*] [VERBOSE] [Processing: /] Baidu
[*] [VERBOSE] [Processing: /] Yahoo
[*] [VERBOSE] [Processing: /] DuckDuckGo
[*] [VERBOSE] Gathered [95] email addresses from the Internet

[*] [VERBOSE] Collected [95] unique email addresses
[*] -----
[*] EMAIL LIST
[*] -----
[*] ....@example.com
[*] ...@example.com
[*] ..@example.com
[*] 20someone@example.com
[*] 555-555-0199@example.com
[*] Abc.123@example.com
[*] Abc@example.com
[*] Adress@example.com
[*] Birisi@example.com
[*] Margaret@example.com
[*] Myname@example.com
[*] Someone@example.com
[*] Username@example.com
[*] abc@example.com
[*] account@example.com
[*] address@example.com
[*] admin@example.com
```

# 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
```

```
Report for Phishing Exercise against [example.com ]
The phishing engagement was started on [2017/09/22 02:15:44 ] and ran through [2017/09/22 02:17:00 ].
For this exercise, the domain [example.com ] was registered and used for the phishing attacks.
```

# Usage

- Collecting emails

```
root@kali2017:~/SPF/spf# ./spf.py -d example.com -g -v -v -f targets.txt
[!] A CONFIG FILE was not specified... defaulting to [default.cfg]

[*] Starting SMB Server
[?] Continue [Y/n] y
[*] [VERBOSE] Started SMBServer with pid = [10142]

[*] Obtaining list of email targets
[?] Continue [Y/n] y
[*] [VERBOSE] Loaded [3] email addresses from [targets.txt]
[*] [VERBOSE] Gathering emails via built-in methods
[*] [VERBOSE] Currently searching [google, bing, ask, dogpile, yandex, baidu, yahoo, duckduckgo]
[*] [VERBOSE] [Processing: /] Google
[*] [VERBOSE] [Processing: -] Bing
[*] [VERBOSE] [Processing: /] Ask
[*] [VERBOSE] [Processing: /] Dogpile
[*] [VERBOSE] [Processing: -] Yandex
[*] [VERBOSE] [Processing: /] Baidu
[*] [VERBOSE] [Processing: /] Yahoo
[*] [VERBOSE] [Processing: |] DuckDuckGo
[*] [VERBOSE] Gathered [94] email addresses from the Internet

[*] [VERBOSE] Collected [96] unique email addresses
```

# Usage

- Starting the phishing webserver

```
root@kali:~# ./sp.py -d example.com -g -v -v -i targets.txt -simulate -w
[!] A CONFIG FILE was not found
FIXED - [templates/web/cisco]
FIXED - [templates/web/juniper_vpn]
FIXED - [templates/web/owa]
FIXED - [templates/web/citrix2]
FIXED - [templates/web/citrix]
FIXED - [templates/web/office365]
FIXED - [templates/web/domino]
1: ('static', 'templates/web/cisco', '')
2: ('static', 'templates/web/juniper_vpn', '')
3: ('static', 'templates/web/owa', '')
4: ('static', 'templates/web/citrix2', '')
5: ('static', 'templates/web/citrix', '')
6: ('static', 'templates/web/office365', '')
7: ('static', 'templates/web/domino', '')
[?] Please select (comma separated) the item(s) you wish to use. (press ENTER to use all):
-----
TEMPLATE LIST
('static', 'templates/web/cisco', '')
('static', 'templates/web/juniper_vpn', '')
('static', 'templates/web/owa', '')
('static', 'templates/web/citrix2', '')
('static', 'templates/web/citrix', '')
('static', 'templates/web/office365', '')
('static', 'templates/web/domino', '')
Starting phishing webserver
[?] Continue [Y/N] Y
Traceback (most recent call last):
  File "root/SPE/spe/core/..web.py", line 32, in <module>
    PhishingWebServer(Utils.decompressDict(sys.argv[1])).start()
  File "root/SPE/spe/core/..web.py", line 281, in start
    curl_path = pg.group()
AttributeError: 'NoneType' object has no attribute 'group'
[VERBOSE] FIXED - [templates/web/owa]
[VERBOSE] FIXED - [templates/web/citrix2]
[VERBOSE] FIXED - [templates/web/citrix]
[VERBOSE] FIXED - [templates/web/office365]
[VERBOSE] FIXED - [templates/web/domino]
[VERBOSE] Found the following web sites: [templates/web/cisco/CONFPG]
[VERBOSE] Found the following web sites: [templates/web/juniper_vpn/CONFPG]
[VERBOSE] Found the following web sites: [templates/web/owa/CONFPG]
[VERBOSE] Found the following web sites: [templates/web/citrix2/CONFPG]
[VERBOSE] Found the following web sites: [templates/web/citrix/CONFPG]
[VERBOSE] Found the following web sites: [templates/web/office365/CONFPG]
[VERBOSE] Found the following web sites: [templates/web/domino/CONFPG]
[VERBOSE] Started website [cisco] on [http://192.168.10.12:8000]
[VERBOSE] Started website [citrix2] on [http://192.168.10.12:8001]
[VERBOSE] Started website [juniper_vpn] on [http://192.168.10.12:8002]
[VERBOSE] Started website [domino] on [http://192.168.10.12:8003]
[VERBOSE] Started website [owa] on [http://192.168.10.12:8004]
[VERBOSE] Started website [office365] on [http://192.168.10.12:8005]
[VERBOSE] Started website [citrix] on [http://192.168.10.12:8006]
```

# References

- Kitploit  
<http://www.kitploit.com/2015/08/spf-speedphish-framework.html>
- Kali Linux  
<https://www.kali.org/downloads/>