

# **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



### • ./spf.py --h

root@kal12017: # cd SPF/spf/	
root@kal12017:-/spf# pwd	
/root/SPF/spf	
root@kal12017:-/SPF/sp	# ./spl.py -h
usage: spf.py [-h] [-f [recon [adv]	<pre><li><list.txt>] [-C <config.txt>] [all] [test] ] [external] [dns] [-g] [-s] [simulate] [-w] [-W] [profile] [pillage] [-d <domain>] [-p <domain>] [pany's name&gt;] [ip &lt;1P address&gt;] [-v] [-y]</domain></domain></config.txt></list.txt></li></pre>
optional arguments:	
-h,help	show this help message and exit
-d <domain></domain>	domain name to phish
-p <domain></domain>	newly registered 'phish' domain name
-c <company's name=""></company's>	name of company to phish
ip <ip address=""></ip>	IP of webserver defaults to [192.168.10.12]
-v,verbosity	increase output verbosity
input files:	
-f <list.txt></list.txt>	file containing list of email addresses
-C <config.txt></config.txt>	
enable flags:	
all	enable ALL flags same as $(-gexternal -s -w -v -v -v)$
test	enable all flags EXCEPT sending of emails same as (-qexternalsimulate -w -y -v -v)
recon	gather info (i.e. email addresses, dns hosts, websites, etc) same as (-edns)
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	<pre>perform all ADVANCED features same as (dnsprofile pillage)</pre>
profile	profile the target domain (requires thedns flag)
pillage	auto pillage email accounts (requires thedns flag)
misc:	
-y	automatically answer yes to all questions

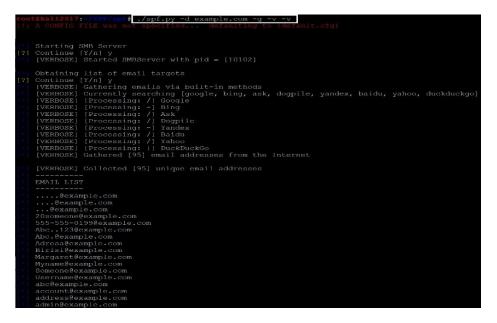


#### • Run it against an owned target





#### Run it against an owned target





#### • Viewing the reports

root@kal12017:-/SPF/spf/example.com/example.com/reports# pwd
/root/SPF/spf/example.com\_example.com/reports
root@kal12017:-/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.

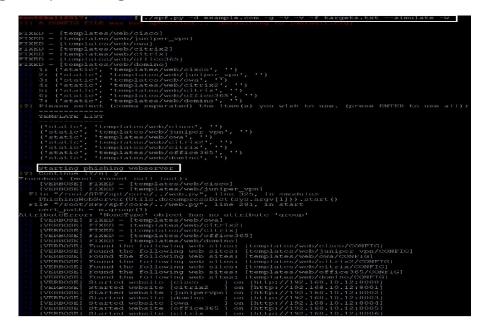


### Collecting emails

	<pre>@kali2017: /spf.pu# ./spf.py -d example.com -g -v -v -f targets.txt</pre>
[1] #	A CONFIG FILE was not specified defaulting to [default.crg]
[*] \$	Starting SMB Server
[?] (	Continue [Y/n] y
1*1	[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]
1*1	[VERBOSE] [Processing: /] Google
[*]	[VERBOSE] [Processing: -] Bing
1 * 1	[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



#### Starting the phishing webserver





### References

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

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

