# Profiling Passwords

pentestlab.blog/category/tools

February 2, 2015


Before we begin an infrastructure penetration test it is important before we go onsite to have a customized password wordlist that will apply only to the client that we are conducting the job. A good password list can play major role in the success of a penetration test as the timeframe is most of the time limited and we don't want to spend hours of trying to brute force a system with a public and more generic password list that contain passwords which are not relevant when can focus more on passwords that might apply to the customer and to the systems that we are targeting.

In order to achieve that we will use Wyd. The idea behind this tool is to analyze files in various formats (plain, html, php, doc, ppt, mp3, pdf, jpeg) and to extract words and strings.

The first step is to download the web content of the site of our client with wget.

```
root@kali:~# cd Desktop/wyd-0.2/
root@kali:~/Desktop/wyd-0.2# mkdir victim-site
root@kali:~/Desktop/wyd-0.2# cd victim-site/
root@kali:~/Desktop/wyd-0.2/victim-site# wget -r https://www.obrela.com/
--2015-02-01 15:52:58--  https://www.obrela.com/
Resolving www.obrela.com (www.obrela.com)... 193.242.245.70
Connecting to www.obrela.com (www.obrela.com)|193.242.245.70|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: /Home/ [following]
--2015-02-01 15:53:01--  https://www.obrela.com/Home/
Reusing existing connection to www.obrela.com:443.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: /home/ [following]
--2015-02-01 15:53:01--  https://www.obrela.com/home/
Reusing existing connection to www.obrela.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `www.obrela.com/index.html'

    [  <=>                                  ] 61,558      229K/s   in 0.3s

2015-02-01 15:53:02 (229 KB/s) - `www.obrela.com/index.html' saved [61558]
```

Downloading Web Content of the Target Site

Then we run Wyd and we write the output into an txt file.

```
root@kali:~/Desktop/wyd-0.2# perl wyd.pl -o victim-site-wordlist.txt -t -b -e /r
oot/Desktop/wyd-0.2/victim-site/www.obrela.com

*
* wyd.pl 0.2 by Max Moser and Martin J. Muench
*


* Error initializing some modules:

wlgmod::doc: Cannot find 'catdoc' (http://www.45.free.net/~vitus/software/catdoc
/)
wlgmod::odt: Canont find module OpenOffice::OODoc (http://www.cpan.org/modules/i
ndex.html)
wlgmod::mp3: Cannot find 'mp3info' (http://www.ibiblio.org/mp3info/)
wlgmod::jpeg: Cannot find 'jhead' (http://www.sentex.net/~mwandel/jhead/)
wlgmod::ppt: Cannot find 'catppt' (http://www.45.free.net/~vitus/software/catdoc
/)

* Press enter to disable them and continue or STRG+C to abort

Ignoring file '/root/Desktop/wyd-0.2/victim-site/www.obrela.com/Contact-US.aspx'
Ignoring file '/root/Desktop/wyd-0.2/victim-site/www.obrela.com/Home.aspx'
```

Running Wyd tool to generate passwords

We used the -t parameter in order to separate wordlist files by type and the -b and -e for disabling the removal of non-alpha characters at the beginning and at the end of the word.

Afterwards we can view the contents of the wordlist and we can choose the most relevant keywords for our custom password list.

```
root@kali:~/Desktop/wyd-0.2# ls
BUGS     docs    testfiles  victim-site                 wlgmod
CHANGES  README  TODO       victim-site-wordlist.txt.html  wyd.pl
root@kali:~/Desktop/wyd-0.2# cat victim-site-wordlist.txt.html
```

View the contents of the Password List

```
Continuity
PKI
Consulting
managed
MSS
Level
1
Managed
Compliance
2
Operations
Assurance
3
Intelligence
Event
(SEM)
Log
(SIM)
Fraud
(FMS)
Incident
Emergency
Support
```

Contents of Password List

Generation of custom password lists can be done as well with Crunch and CUPP.

https://pentestlab.wordpress.com/2012/03/06/common-user-passwords-profiler/

https://pentestlab.wordpress.com/2012/07/12/creating-wordlists-with-crunch/