Random Ramblings

Random Ramblings of a Network Security Engineer

Wednesday, August 3, 2011

Brute force Directory and Files on a Web server using dirb and Backtrack 4

One of the most commonly used web application directory/files brute force tool is dirbuster from OWASP ; which is a GUI based tool written using java. Dirb is also a directory/files bruter force tool but unlike owasp Dirbuster; it is a command line utility and can be run from a shell. It is available for download at : http://dirb.sourceforge.net/

In this post I will be showing you how to install and use dirb on a machine running Backtrack 4.

[1] Change Directory to /pentest/web/

```
root@bt:~# cd /pentest/web/
root@bt:~# cd /pentest/web/
```

[2] Download the dirb tarball from http://dirb.sourceforge.net/ and expand the tarball :

```
root@bt:/pentest/web# wget -c 'http://sourceforge.net/projects/dirb/files/dirb/2.03/dirb203.tar.gz/download' -O dirb203.tar.gz
root@bt:/pentest/web# tar -zxvf dirb203.tar.gz
root@bt:/pentest/web# cd dirb
```

```
root@bt:/pentest/web/dirb# ls
Makefile.am README.txt autoheader config.h.in configure.ac dirb.1 docs install-sh mkinstalldirs src utils win32
Makefile.in aclocal.m4 autom4te.cache configure depcomp dirb203.tar.gz gendict_src missing resume stamp-h.in
web2dic wordlists
```

```
root@bt:/pentest/web/dirb# cat README.txt
root@bt:/pentest/web/dirb# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking for libcurl >= 7.10.1... FAILED
configure: error: Curl-config was not found
```

[3] Install the dependencies :

```
root@bt:/pentest/web/dirb# aptitude install libcurl4-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading extended state information
Initializing package states... Done
Note: selecting "libcurl4-gnutls-dev" instead of the
virtual package "libcurl4-dev"
The following NEW packages will be installed:
libcurl4-gnutls-dev libgnutls-dev{a} libidn11-dev{a} libldap2-dev{a} libtasn1-3-dev{a}
0 packages upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 3057kB of archives. After unpacking 8106kB will be used.
Do you want to continue? [Y/n/?] y
Writing extended state information... Done
Get:1 http://archive.offensive-security.com pwnsauce/main libtasn1-3-dev 1.4-1 [358kB]
Get:2 http://archive.offensive-security.com pwnsauce/main libgnutls-dev 2.4.1-1ubuntu0.2 [402kB]
Get:3 http://archive.offensive-security.com pwnsauce/main libidn11-dev 1.8+20080606-1 [574kB]
```

Blog Archive
► 2014 (1)
► 2013 (3)
► 2012 (1)
▼ 2011 (7)
► December (1)
► October (1)
▼ August (2)
HOLYNIX VERSI SOLUTION
Brute force Direc Web server us
► July (1)
► March (2)
► 2010 (5)
► 2009 (1)

```
Get:4 http://archive.offensive-security.com pwnsauce/main libldap2-dev 2.4.11-0ubuntu6.1 [824kB]
Get:5 http://archive.offensive-security.com pwnsauce/main libcurl4-gnutls-dev 7.18.2-1ubuntu4.3 [900kB]
Fetched 3057kB in 39s (77.8kB/s)
Selecting previously deselected package libtasn1-3-dev.
(Reading database ... 229030 files and directories currently installed.)
Unpacking libtasn1-3-dev (from .../libtasn1-3-dev_1.4-1_i386.deb) ...
Selecting previously deselected package libgnutls-dev.
Unpacking libgnutls-dev (from .../libgnutls-dev_2.4.1-1ubuntu0.2_i386.deb) ...
Selecting previously deselected package libidn11-dev.
Unpacking libidn11-dev (from .../libidn11-dev_1.8+20080606-1_i386.deb) ...
Selecting previously deselected package libldap2-dev.
Unpacking libldap2-dev (from .../libldap2-dev_2.4.11-0ubuntu6.1_i386.deb) ...
Selecting previously deselected package libcurl4-gnutls-dev.
Unpacking libcurl4-gnutls-dev (from .../libcurl4-gnutls-dev_7.18.2-1ubuntu4.3_i386.deb) ...
Processing triggers for man-db ...
Setting up libtasn1-3-dev (1.4-1) ...

Setting up libgnutls-dev (2.4.1-1ubuntu0.2) ...
Setting up libidn11-dev (1.8+20080606-1) ...

Setting up libldap2-dev (2.4.11-0ubuntu6.1) ...
Setting up libcurl4-gnutls-dev (7.18.2-1ubuntu4.3) ...

Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading extended state information
Initializing package states... Done
Writing extended state information... Done
```

[4] Configure and compile dirb:

```
root@bt:/pentest/web/dirb# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking for libcurl >= 7.10.1... 7.18.2
checking for style of include used by make... GNU
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking dependency style of gcc... gcc3
checking for curl_easy_init in -lcurl... yes
configure: creating ./config.status
config.status: creating Makefile
config.status: creating src/Makefile
config.status: creating gendict_src/Makefile
config.status: creating web2dic/Makefile
config.status: creating config.h
config.status: executing depfiles commands

DIRB 2.03 build configuration.

Now you must execute: "make"


root@bt:/pentest/web/dirb# make

make all-recursive
make[1]: Entering directory `/pentest/web/dirb'
Making all in src
make[2]: Entering directory `/pentest/web/dirb/src'
if gcc -DHAVE_CONFIG_H -I. -I. -I.. -Wall -g -O2 -MT crea_wordlist.o -MD -MP -MF ".deps/crea_wordlist.Tpo" -c -o crea_wordlist.o crea_wordlist.c; \
then mv -f ".deps/crea_wordlist.Tpo" ".deps/crea_wordlist.Po"; else rm -f ".deps/crea_wordlist.Tpo"; exit 1; fi
if gcc -DHAVE_CONFIG_H -I. -I. -I.. -Wall -g -O2 -MT dirb.o -MD -MP -MF ".deps/dirb.Tpo" -c -o dirb.o dirb.c; \
then mv -f ".deps/dirb.Tpo" ".deps/dirb.Po"; else rm -f ".deps/dirb.Tpo"; exit 1; fi
if gcc -DHAVE_CONFIG_H -I. -I. -I.. -Wall -g -O2 -MT get_url.o -MD -MP -MF ".deps/get_url.Tpo" -c -o get_url.o get_url.c; \
then mv -f ".deps/get_url.Tpo" ".deps/get_url.Po"; else rm -f ".deps/get_url.Tpo"; exit 1; fi
get_url.c: In function 'get_url':
get_url.c:95: warning: call to '_curl_easy_getinfo_err_long' declared with attribute warning: curl_easy_getinfo expects a pointer to long for this info
if gcc -DHAVE_CONFIG_H -I. -I. -I.. -Wall -g -O2 -MT lanza_ataque.o -MD -MP -MF ".deps/lanza_ataque.Tpo" -c -o lanza_ataque.o lanza_ataque.c; \
then mv -f ".deps/lanza_ataque.Tpo" ".deps/lanza_ataque.Po"; else rm -f ".deps/lanza_ataque.Tpo"; exit 1; fi
if gcc -DHAVE_CONFIG_H -I. -I. -I.. -Wall -g -O2 -MT calculanec.o -MD -MP -MF ".deps/calculanec.Tpo" -c -o calculanec.o calculanec.c; \
then mv -f ".deps/calculanec.Tpo" ".deps/calculanec.Po"; else rm -f ".deps/calculanec.Tpo"; exit 1; fi
```

```
if gcc -DHAVE_CONFIG_H -I. -I.. -I.. -Wall -g -O2 -MT utils.o -MD -MP -MF ".deps/utils.Tpo" -c -o utils.o utils.c; \
then mv -f ".deps/utils.Tpo" ".deps/utils.Po"; else rm -f ".deps/utils.Tpo"; exit 1; fi
utils.c: In function 'kbhit':
utils.c:273: warning: ignoring return value of 'read', declared with attribute warn_unused_result
if gcc -DHAVE_CONFIG_H -I. -I.. -I.. -Wall -g -O2 -MT options.o -MD -MP -MF ".deps/options.Tpo" -c -o options.o options.c; \
then mv -f ".deps/options.Tpo" ".deps/options.Po"; else rm -f ".deps/options.Tpo"; exit 1; fi
if gcc -DHAVE_CONFIG_H -I. -I.. -I.. -Wall -g -O2 -MT resume.o -MD -MP -MF ".deps/resume.Tpo" -c -o resume.o resume.c; \
then mv -f ".deps/resume.Tpo" ".deps/resume.Po"; else rm -f ".deps/resume.Tpo"; exit 1; fi
resume.c: In function 'dump':
resume.c:47: warning: ignoring return value of 'fwrite', declared with attribute warn_unused_result
resume.c:61: warning: ignoring return value of 'fwrite', declared with attribute warn_unused_result
resume.c:62: warning: ignoring return value of 'fwrite', declared with attribute warn_unused_result
resume.c:78: warning: ignoring return value of 'fwrite', declared with attribute warn_unused_result
resume.c:79: warning: ignoring return value of 'fwrite', declared with attribute warn_unused_result
resume.c: In function 'resume':
resume.c:107: warning: ignoring return value of 'fread', declared with attribute warn_unused_result
gcc -Wall -g -O2 -o dirb -lcurl -Wl,-Bsymbolic-functions -lidn -lldap -lrt -L/usr/lib -g -O2 -Wl,-Bsymbolic-functions -lgssapi_krb5 -lkrb5 -lk5crypto -lcom_err -
lgssapi_krb5 -lz -lgnutls crea_wordlist.o dirb.o get_url.o lanza_ataque.o calculanec.o utils.o options.o resume.o -lcurl
cp dirb ../
make[2]: Leaving directory `/pentest/web/dirb/src'
Making all in gendict_src
make[2]: Entering directory `/pentest/web/dirb/gendict_src'
if gcc -DHAVE_CONFIG_H -I. -I.. -I.. -Wall -g -g -O2 -MT gendict.o -MD -MP -MF ".deps/gendict.Tpo" -c -o gendict.o gendict.c; \
then mv -f ".deps/gendict.Tpo" ".deps/gendict.Po"; else rm -f ".deps/gendict.Tpo"; exit 1; fi
gcc -Wall -g -g -O2 -o gendict gendict.o -lcurl
cp gendict ../
make[2]: Leaving directory `/pentest/web/dirb/gendict_src'
Making all in web2dic
make[2]: Entering directory `/pentest/web/dirb/web2dic'
if gcc -DHAVE_CONFIG_H -I. -I.. -I.. -Wall -g -g -O2 -MT html2dic.o -MD -MP -MF ".deps/html2dic.Tpo" -c -o html2dic.o html2dic.c; \
then mv -f ".deps/html2dic.Tpo" ".deps/html2dic.Po"; else rm -f ".deps/html2dic.Tpo"; exit 1; fi
gcc -Wall -g -g -O2 -o html2dic html2dic.o -lcurl
make[2]: Leaving directory `/pentest/web/dirb/web2dic'
make[2]: Entering directory `/pentest/web/dirb'
make[2]: Nothing to be done for `all-am'.
make[2]: Leaving directory `/pentest/web/dirb'
make[1]: Leaving directory `/pentest/web/dirb'
```

```
root@bt:/pentest/web/dirb# make install
Making install in src
make[1]: Entering directory `/pentest/web/dirb/src'
make[2]: Entering directory `/pentest/web/dirb/src'
test -z "/usr/local/bin" || mkdir -p -- "/usr/local/bin"
/usr/bin/install -c 'dirb' '/usr/local/bin/dirb'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/pentest/web/dirb/src'
make[1]: Leaving directory `/pentest/web/dirb/src'
Making install in gendict_src
make[1]: Entering directory `/pentest/web/dirb/gendict_src'
make[2]: Entering directory `/pentest/web/dirb/gendict_src'
test -z "/usr/local/bin" || mkdir -p -- "/usr/local/bin"
/usr/bin/install -c 'gendict' '/usr/local/bin/gendict'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/pentest/web/dirb/gendict_src'
make[1]: Leaving directory `/pentest/web/dirb/gendict_src'
Making install in web2dic
make[1]: Entering directory `/pentest/web/dirb/web2dic'
make[2]: Entering directory `/pentest/web/dirb/web2dic'
test -z "/usr/local/bin" || mkdir -p -- "/usr/local/bin"
/usr/bin/install -c 'html2dic' '/usr/local/bin/html2dic'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/pentest/web/dirb/web2dic'
make[1]: Leaving directory `/pentest/web/dirb/web2dic'
make[1]: Entering directory `/pentest/web/dirb'
make[2]: Entering directory `/pentest/web/dirb'
make[2]: Nothing to be done for `install-exec-am'.
test -z "/usr/local/share/man/man1" || mkdir -p -- "/usr/local/share/man/man1"
/usr/bin/install -c -m 644 './dirb.1' '/usr/local/share/man/man1/dirb.1'
make[2]: Leaving directory `/pentest/web/dirb'
make[1]: Leaving directory `/pentest/web/dirb'
root@bt:/pentest/web/dirb# /usr/local/bin/dirb
Makefile aclocal.m4 config.h.in configure.ac dirb203.tar.gz install-sh src/ web2dic/
Makefile.am autoheader config.log depcomp docs/ missing stamp-h.in win32/
Makefile.in autom4te.cache/ config.status dirb gendict mkinstalldirs stamp-h1 wordlists/
README.txt config.h configure dirb.1 gendict_src/ resume/ utils/
```

[6] Test the installed binary :

```
root@bt:/pentest/web/dirb# /usr/local/bin/dirb


-----------------
DIRB v2.03
By The Dark Raver
-----------------

./dirb [] [options]

========================= NOTES ========================= : Base URL to scan. (Use -resume for session resuming) :
List of wordfiles. (wordfile1,wordfile2,wordfile3...)

======================== HOTKEYS ========================
'n' -> Go to next directory.
'q' -> Stop scan. (Saving state for resume)

======================== OPTIONS ========================
-a : Specify your custom USER_AGENT.
-c : Set a cookie for the HTTP request.
-f : Fine tunning of NOT_FOUND (404) detection.
-H : Add a custom header to the HTTP request.
-i : Use case-insensitive search.
-l : Print "Location" header when found.
-N : Ignore responses with this HTTP code.
-o : Save output to disk.
-p : Use this proxy. (Default port is 1080)
-P : Proxy Authentication.
-r : Don't search recursively.
-R : Interactive recursion. (Asks for each directory)
-S : Silent Mode. Don't show tested words. (For dumb terminals)
-t : Don't force an ending '/' on URLs.
-u : HTTP Authentication.
-v : Show also NOT_FOUND pages.
-w : Don't stop on WARNING messages.
-X / -x : Append each word with this extensions.
-z : Add a miliseconds delay to not cause excessive Flood.

======================== EXAMPLES ========================
./dirb http://url/directory/ (Simple Test)
./dirb http://url/ -X .html (Test files with '.html' extension)
./dirb http://url/ wordlists/vulns/apache.txt (Test with apache.txt wordlist)
./dirb https://secure_url/ (Simple Test with SSL)
```

root@bt:/pentest/web/dirb#

[6] Take dirb for a test ride using the common wordlist file that comes with its installation. It is also possible to use dirbuster wordlist with dirb :

```
root@bt:/pentest/web/dirb# /usr/local/bin/dirb http://orangehrm.example.com wordlists/common.txt

-----------------
DIRB v2.03
By The Dark Raver
-----------------

START_TIME: Thu Aug 4 07:09:53 2011
URL_BASE: http://orangehrm.example.com/
WORDLIST_FILES: wordlists/common.txt

-----------------

GENERATED WORDS: 1942

---- Scanning URL: http://orangehrm.example.com/ ----
+ http://orangehrm.example.com/build/
==> DIRECTORY
+ http://orangehrm.example.com/favicon.ico
(FOUND: 200 [Ok] - Size: 564)
+ http://orangehrm.example.com/javascript
(FOUND: 403 [Forbidden] - Size: 416)
+ http://orangehrm.example.com/language/
==> DIRECTORY
+ http://orangehrm.example.com/lib/
==> DIRECTORY
+ http://orangehrm.example.com/license/
==> DIRECTORY
```

```
+ http://orangehrm.example.com/manual/
==> DIRECTORY
+ http://orangehrm.example.com/phpmyadmin/
==> DIRECTORY
+ http://orangehrm.example.com/plugins/
==> DIRECTORY
+ http://orangehrm.example.com/resources/
==> DIRECTORY
+ http://orangehrm.example.com/scripts/
==> DIRECTORY
+ http://orangehrm.example.com/stats
(FOUND: 401 [Auth Required] - Size: 605)
+ http://orangehrm.example.com/templates/
==> DIRECTORY
+ http://orangehrm.example.com/themes/
==> DIRECTORY

---- Entering directory: http://orangehrm.example.com/build/ ----

---- Entering directory: http://orangehrm.example.com/language/ ----
+ http://orangehrm.example.com/language/default/
==> DIRECTORY
+ http://orangehrm.example.com/language/en/
==> DIRECTORY
+ http://orangehrm.example.com/language/es/
==> DIRECTORY
+ http://orangehrm.example.com/language/ja/
==> DIRECTORY
+ http://orangehrm.example.com/language/nl/
==> DIRECTORY
+ http://orangehrm.example.com/language/ru/
==> DIRECTORY
```

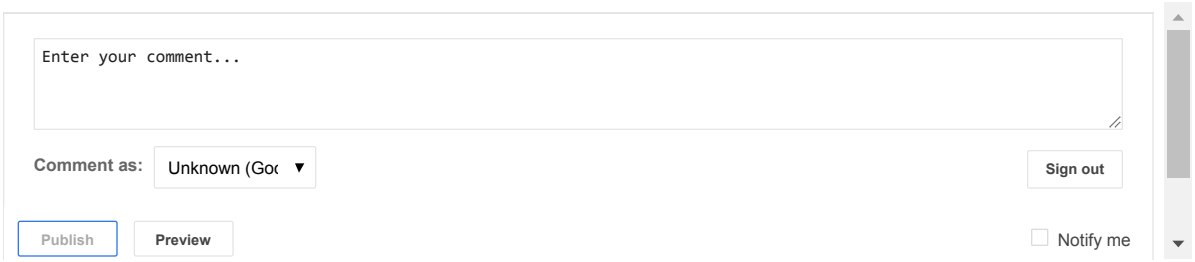
Posted by Prithak at 10:50 PM

Reactions: funny (2) interesting (1) cool (2)

No comments:

Post a Comment

Note: Only a member of this blog may post a comment.



Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)