DNS Results From Netcraft Search Engine

pentestlab.blog/category/coding/page/3

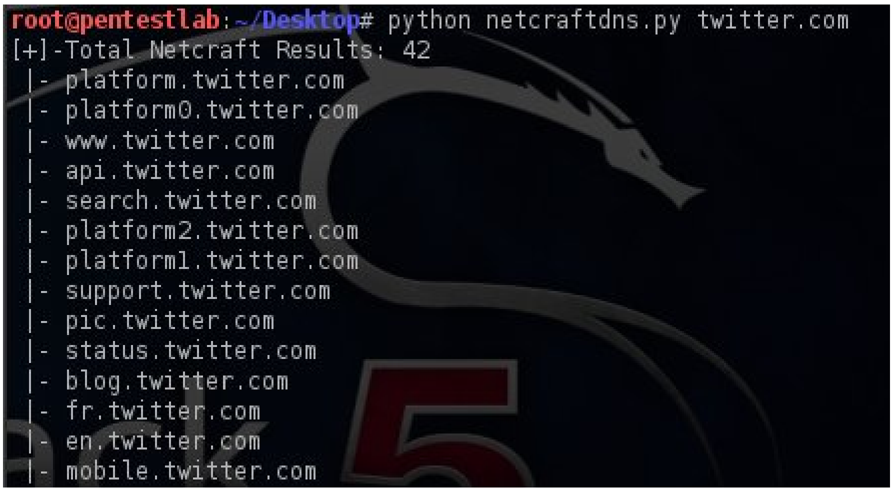
January 5, 2013

The following python script has developed by neuro from 0x0lab.org and it can obtain DNS results from netcraft search engine.This can be used in the information gathering stage of a penetration test.You can find the source code and a screenshot of the usage of this script below:

```
#!/usr/bin/python

import httplib
import re
import sys
import string

def help():
print "[netcraftdns v1.0] - by neuro [0x0lab.org]"
print "\nUsage: python netcraftdns.py <domain_name> \n"
sys.exit()

if len(sys.argv) < 1 or len(sys.argv) > 2:
help()
elif len(sys.argv) == 2:
domain_name =  sys.argv[1]
else:
help()

netcraftres=[]
totalnum=[]

def count(domain_name):
global nres
rg = httplib.HTTP('searchdns.netcraft.com')
rg.putrequest('GET', "/?restriction=site+ends+with&host=" + domain_name)
rg.putheader('Host', 'searchdns.netcraft.com')
rg.putheader('User-agent', 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5;
en-US; rv:1.9.0.4) Gecko/2008102920 Firefox/3.0.4')
rg.endheaders()
errcode, errmsg, headers = rg.getreply()

if errcode!=200:
print 'Error Sending Request', errcode, errmsg
else:
rgdata = rg.getfile().read()

searchres_pattern='Found [0-9]*'
sp = re.compile(searchres_pattern, re.I)
res=sp.findall(rgdata)
```

```
for total in res:
resclean=re.sub('Found ', '', total)
nres=resclean
print "[+]-Total Netcraft Results:", nres

def results(domain_name):
y=21
i=1
rg = httplib.HTTP('searchdns.netcraft.com')
rg.putrequest('GET', "/?restriction=site+ends+with&host=" + domain_name)
rg.putheader('Host', 'searchdns.netcraft.com')
rg.putheader('User-agent', 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5;
en-US; rv:1.9.0.4) Gecko/2008102920 Firefox/3.0.4')
rg.endheaders()
errcode, errmsg, headers = rg.getreply()

if errcode!=200:
print 'Error Sending Request', errcode, errmsg
else:
rgdata = rg.getfile().read()

pattern='[\w\.\-]+.'+domain_name
rgr = re.compile(pattern, re.I)
rgresults = rgr.findall(rgdata)

for netres in rgresults:
if netcraftres.count(netres) == 0:
netcraftres.append(netres)
print " |-", str(netres)
i=i+1

while y<nres:
if nres=="0":
break
rgi = httplib.HTTP('searchdns.netcraft.com')
rgi.putrequest('GET', "/?
host=*."+domain_name+"&last="+netcraftres[-1]+"&from="+str(y)+"&restriction
=site%20contains&position=")
rgi.putheader('Host', 'searchdns.netcraft.com')
rgi.putheader('User-agent', 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X
10.5; en-US; rv:1.9.0.4) Gecko/2008102920 Firefox/3.0.4')
rgi.endheaders()
errcode, errmsg, headers = rgi.getreply()

if errcode!=200:
print 'Error Sending Request', errcode, errmsg
else:
rgdata1 = rgi.getfile().read()

pattern2='[\w\.\-]+.'+domain_name
rgr1 = re.compile(pattern2, re.I)
rgresults1 = rgr.findall(rgdata1)
```

```
if y > int(nres):
break
else:
y = y + 20

for netres1 in rgresults1:
if netcraftres.count(netres1) == 0:
netcraftres.append(netres1)
print " |-", str(netres1)
i=i+1

count(domain_name)
results(domain_name)
```



```
root@pentestlab:~/Desktop# python netcraftdns.py twitter.com
[+]-Total Netcraft Results: 42
 |- platform.twitter.com
 |- platform0.twitter.com
 |- www.twitter.com
 |- api.twitter.com
 |- search.twitter.com
 |- platform2.twitter.com
 |- platform1.twitter.com
 |- support.twitter.com
 |- pic.twitter.com
 |- status.twitter.com
 |- blog.twitter.com
 |- fr.twitter.com
 |- en.twitter.com
 |- mobile.twitter.com
```

netcraftdns – Sample Results