Fierce Usage

Fierce sözlük saldırısı ile subdomain tespiti yapmaya yarar. Bu şekilde pentest için scope'umuzu belirleriz. Standart kullanımı şu şekildedir:

Syntax

> fierce -dns website-url

Examples

i) Varsayılan Sözlük ile Subdomain Tespiti

fierce'ın kendine ait varsayılan sözlüğü ile karabuk.edu.tr'de subdomain tespiti yapalım.

// Kali 2016'da fierce problemsiz çalışıyor.

Kali 2016 Console:

> fierce -dns karabuk.edu.tr // www kullanma. Yoksa fierce çalışmıyor.

Output:

```
DNS Servers for karabuk.edu.tr:
ns1.ulak.net.tr
ns1.karabuk.edu.tr

Trying zone transfer first...
        Testing ns1.ulak.net.tr
                Request timed out or transfer not allowed.
        Testing ns1.karabuk.edu.tr
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...

193.140.9.6     be.karabuk.edu.tr
193.140.9.1     gateway.karabuk.edu.tr
193.140.9.6     hotel.karabuk.edu.tr
127.0.0.1       localhost.karabuk.edu.tr
193.140.9.6     m.karabuk.edu.tr
193.140.9.6     maillist.karabuk.edu.tr
```

193.140.9.2 ns1.karabuk.edu.tr
193.140.9.6 technology.karabuk.edu.tr
193.140.9.19 test.karabuk.edu.tr
193.140.9.6 tv.karabuk.edu.tr
193.140.9.6 video.karabuk.edu.tr
193.140.9.6 web.karabuk.edu.tr
193.140.9.31 www.karabuk.edu.tr

Subnets found (may want to probe here using nmap or unicornscan):
127.0.0.0-255 : 1 hostnames found.
193.140.9.0-255 : 12 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 13 entries.

Have a nice day.

Görüldüğü üzere sözlük saldırısı ile belli sayıda subdomain tespiti yapılmıştır.

ii) Kendi Sözlüğümüz ile Subdomain Tespiti

Şimdi fierce'a kendi sözlüğümüzü verelim ve bu şekilde subdomain tespitinde bulunalım.

deneme.txt

sdfs
dfsd
fsd
dsf
sdfsd
f
technology
sd
fsd
dfds
sdfds
fgdf
f
sdf
ds
web
sdfsd
fsd
dsfsdf
fgfdd
f
sdfds

// Kali 2016'da fierce problemsiz çalışıyor.

Kali 2016 Console:

fierce -wordlist deneme.txt -dns karabuk.edu.tr // www kullanma. Yoksa // fierce çalışmıyor.

Output:

DNS Servers for karabuk.edu.tr:
ns1.ulak.net.tr
ns1.karabuk.edu.tr

Trying zone transfer first...
Testing ns1.ulak.net.tr
Request timed out or transfer not allowed.
Testing ns1.karabuk.edu.tr
Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 32 test(s)...
193.140.9.6 technology.karabuk.edu.tr
193.140.9.6 web.karabuk.edu.tr

Subnets found (may want to probe here using nmap or unicornscan):
193.140.9.0-255 : 2 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 2 entries.

Have a nice day.

iii) Kendi Sözlüğümüz ile Subdomain Tespiti (II)

fierce'a kendi sözlüğümüzü verelim ve bu sefer google'ın subdomainlerini tespit edelim.

deneme.txt

sdfs
dfsd
fsd
dsf
sdfsd
f
translate
sd
fsd
f
sdf
ds
mail
sdfsd
fsd
f
ds

// Kali 2016'da fierce problemsiz çalışıyor.

Kali 2016 Console:

fierce -wordlist deneme.txt -dns google.com.tr // www kullanma. Yoksa
// fierce çalışmıyor.

Output:

DNS Servers for google.com:
ns4.google.com
ns3.google.com
ns2.google.com
ns1.google.com

Trying zone transfer first...
Testing ns4.google.com
Request timed out or transfer not allowed.
Testing ns3.google.com
Request timed out or transfer not allowed.
Testing ns2.google.com
Request timed out or transfer not allowed.
Testing ns1.google.com
Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 29 test(s)...
216.58.206.165 mail.google.com
216.58.206.174 translate.google.com

Subnets found (may want to probe here using nmap or unicornscan):
216.58.206.0-255 : 2 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 2 entries.

Have a nice day.