此文章已于 1:04:12 2015/12/25 发布到 Net | Linux | 安全

★Kali信息收集~ 5.The Harvester：邮箱挖掘器

* 1. 官网：**http://www.edge-security.com**
  2. 安装：**apt-get install theHarvester**
  3. 运行：终端输入 **theharvester** (小写)

计算机生成了可选文字:
FE(V) 
TheHarvester Ver. 2. 6 
* Coded by Christian Martorella 
* Edge- Security Research 
* cmartorella@dge- security. com 
Usage: 
theharvester opt Ions 
-d 
-d 
-d 
-d 
root@Kali: 
hosts 
0 50 
e 
resul t 
o 
-d: 
-b: 
-s: 
-v: 
-n: 
-e: 
1. 
h: 
Exampl es: 
Domain to search or company name 
data source: google, googleCS 
bing, bingapl 
pgp 
linkedin, google- profiles, people 123, 
J lgsaw, 
twitter, googleplus, all 
Start in result number X (default. 
0) 
Verify host name via dns resolution and search for virtual 
Save the results into an HTML and XML fil 
Perform a DNS reverse query on all ranges discovered 
Perform a DNS brute force for the domain name 
Perform a DNS T LD expansion discovery 
Use this DNS server 
Limit the number of results to work with( bing goes from 50 
use SHODAN database to query discovered hosts 
google 100 
0 100, and pgp doesn' t use this option) 
ft. 
ml c roso 
ml c roso 
ml c roso 
apple. com 
om -1 
500 -b google 
theharvester 
theharvester 
theharvester 
theharvester 
rootMati• 
ft com -b pgp 
200 -b linkedin 
-b googleCS 
500 
-s 300 

用法+参数：（返回邮箱+子域名）

计算机生成了可选文字:
Usage: 
theharvester options 
-d 
-d 
-d 
-d 
hosts 
0 50 
resul t 
-b: 
-s: 
-v: 
-n: 
-e: 
1. 
h. 
Exampl es: 
Domain to search or company name 
data source: google, googleCS 
bing, bingapl 
pgp 
linkedin, google- profiles, people 123, 
J lgsaw, 
twitter, googleplus, all 
Start in result number X (default. 
0) 
Verify host name via dns resolution and search for virtual 
Save the results into an HTML and XML fil 
Perform a DNS reverse query on all ranges discovered 
Perform a DNS brute force for the domain name 
Perform a DNS T LD expansion discovery 
Use this DNS server 
Limit the number of results to work with( bing goes from 50 
use SHODAN database to query discovered hosts 
google 100 
0 100, and pgp doesn' t use this option) 
ml c roso 
ml c roso 
ml c roso 
apple. com 
ft. com -1 
500 -b google 
theharvester 
theharvester 
theharvester 
theharvester 
ft com -b pgp 
200 -b linkedin 
-b googleCS 
500 
-s 300 

重要 最常见用法：**theharvester -d** 域名|公司名 **-b** 搜索来源（google，bing，pgp，linkedin等）

计算机生成了可选文字:
rootMat1: theharvester -d 58. com -b blng 
* 
* 
* 
2.6 
TheHarvester Ver. 
Coded by Christian Martorella 
dge- Security Research 
cma rtorella@dge- securit 
Y. com 
(-1 Searching in Bing: 
Searching 50 results. . 
Searching 100 result 

关键 不是每次都有结果的淡定点