此文章已于 1:05:44 2015/12/25 发布到 Net | Linux | 安全

★Kali信息收集~★6.Dmitry:汇总收集

* 1. 概述：

DMitry（Deepmagic Information Gathering Tool）是一个一体化的信息收集工具。它可以用来收集以下信息：

**1. 端口扫描**

**2. whois主机IP和域名信息**

**3. 从Netcraft.com获取主机信息**

**4. 子域名**

**5. 域名中包含的邮件地址**

尽管这些信息可以在Kali中通过多种工具获取，但是使用DMitry可以将收集的信息保存在一个文件中，方便查看。

* 1. 参数：

计算机生成了可选文字:
dmit ry 
Deepmagic Information Gathering Tool 
There be some deep magic going on" 
Usage: dmitry ( -winsepfbl ( - 
O- 91 fro %ost. txt I host 
Save output to %ost txt or to 
fil 
ified by -o 
file 
e spec 
Perform a whois lookup on the IP address of a host 
Perform a whois lookup on the domain name of a host 
Retrieve Netcraft. 
om information on a host 
-p 
pe rfo rm 
pe rfo rm 
pe rfo rm 
pe rfo rm 
Read in 
a search for possible subdomains 
a search for possible email addresses 
a TCP port 
scan on a host 
a TCP port 
scan on a host showing output reporting filtered por 
the banner received from the scanned port 
TTL in seconds when scanning a TCP port ( Default 
2) 
flagged to be passed 
0-9 Se 
t the 
*Requi res 
the -p 

* 1. 常用：
  + 重要 **获取 whois ，ip，主机信息，子域名，电子邮件**

**子域名和电子邮箱依赖谷歌搜索，没有翻墙的可能比较蛋疼一点，可以只用 -win参数**

dnt@Kali:~$ **dmitry -winse cnblogs.com**

Deepmagic Information Gathering Tool

"There be some deep magic going on"

ERROR: Unable to locate Host IP addr. for cnblogs.com

Continuing with limited modules

HostIP:

HostName:cnblogs.com

Gathered Inic-whois information for cnblogs.com

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

Domain Name: CNBLOGS.COM

Registrar: 35 TECHNOLOGY CO., LTD

Sponsoring Registrar IANA ID: 1316

Whois Server: whois.35.com

**Referral URL:** [**http://www.35.com**](http://www.35.com)

**Name Server: NS3.DNSV4.COM**

**Name Server: NS4.DNSV4.COM**

Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>

Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>

Updated Date: 12-nov-2014

Creation Date: 12-nov-2003

Expiration Date: 12-nov-2021

>>> Last update of whois database: Thu, 24 Dec 2015 15:40:29 GMT <<<

For more information on Whois status codes, please visit

<https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>.

NOTICE: The expiration date displayed in this record is the date the

regi in

ist Z L Dry ris l

currently set to expire. This date does not necessarily reflect the expiration

date of the domain name registrant's agreement with the sponsoring

registrar. Users may consult the sponsoring registrar's Whois database to

view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois

database through the use of electronic processes that are high-volume and

gis ter dom Z ai Z N n names or

modify existing registrations; the Data in VeriSign Global Registry

Services' ("VeriSign") Whois database is provided by VeriSign for

information purposes only, and to assist persons in obtaining information

about or related to a domain name registration record. VeriSign does not

guarantee its accuracy. By submitting a Whois query, you agree to abide

by the following terms of use: You agree that you may use this Data only

wi ll you Z us Z N e th

is cesData

to: (1) allow, enable, or otherwise support the transmission of mass

unsolicited, commercial advertising or solicitations via e-mail, telephone,

or facsimile; or (2) enable high volume, automated, electronic processes

that apply to VeriSign (or its computer systems). The compilation,

repackaging, dissemination or other use of this Data is expressly

prohibited without the prior written consent of VeriSign. You agree not to

to acce Z N ss or

query the Whois database except as reasonably necessary to register

domain names or modify existing registrations. VeriSign reserves the right

to restrict your access to the Whois database in its sole discretion to ensure

operational stability. VeriSign may restrict or terminate your access to the

Whois database for failure to abide by these terms of use. VeriSign

reserves the right to modify these terms at any time.

Theoma

ins and

Registrars.

Gathered Netcraft information for cnblogs.com

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

Retrieving Netcraft.com information for cnblogs.com

Netcraft.com Information gathered

Gathered Subdomain information for cnblogs.com

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

Searching Google.com:80...

**…………………………………**

* + **扫描网站端口（这个建议使用Nmap）**

dnt@Kali:~$ **dmitry -p cnblogs.com -f -b**

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:42.121.252.58

HostName:cnblogs.com

Gathered TCP Port information for 42.121.252.58

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

Port                State

1/tcp                filtered

2/tcp                filtered

3/tcp                filtered

4/tcp                filtered

5/tcp                filtered

6/tcp                filtered

7/tcp                filtered

8/tcp                filtered

9/tcp                filtered

10/tcp                filtered

11/tcp                filtered

12/tcp                filtered

13/tcp                filtered

14/tcp                filtered

15/tcp                filtered

16/tcp                filtered

17/tcp                filtered

18/tcp                filtered

19/tcp                filtered

20/tcp                filtered

21/tcp                filtered

22/tcp                filtered

23/tcp                filtered

24/tcp                filtered

25/tcp                filtered

26/tcp                filtered

27/tcp                filtered

28/tcp                filtered

29/tcp                filtered

30/tcp                filtered

31/tcp                filtered

32/tcp                filtered

33/tcp                filtered

34/tcp                filtered

35/tcp                filtered

36/tcp                filtered

37/tcp                filtered

38/tcp                filtered

39/tcp                filtered

40/tcp                filtered

41/tcp                filtered

42/tcp                filtered

43/tcp                filtered

**…………………………**