kali linux渗透测试

第5课 Rencon-NG被动侦察，检测自己信息是否泄露

Recon-NG框架

Recon-NG的基本用法

使用 help 查看命令

add：向数据库添加一条记录

back：返回到上一级

delete：从数据库中删除一条记录

exit：退出Recon-NG

help:显示帮助信息

keys：管理API

load：载入指定模块

pdb：打开Python调试

query：查询数据库

record：将命令保存为资源文件

reload：重新载入所有模块

resource：执行一个资源文件

search：搜索可用的模块

set：设置参数

shell：执行操作系统命令

show：显示各种框架的条目

snapshots：创建一个快照

spool：将结果输出到一个文件

unset：重置参数值

use：载入指定模块

workspaces：管理工作区

Recon-NG是一个框架，包含非常多的模块

使用 show modules 命令 查看可以使用的模块

一共有5大分类，90个模块

由于模块数量非常多，为了便于快速学习掌握，Recon-NG在为模块命名的时候，采用了“分层式”的命名法

例如：recon/domains-hosts/bing-domain-Web

最前面的是模块类型，recon是用来侦察的模块

中间是给出模块工作的目标，domains-hosts，从命名上看是和域名有关的

最后给出的是使用的相关技术，bing-domain-Web就是借助微软的bing搜索对给出的域名进行侦察

实际应用案例

使用Recon-NG是侦察一个域名下的所有子域名

1.使用use命令选择要使用的模块

use recon/domains-hosts/brute_hosts

2.使用show options查看需要设置的参数有哪些

3.设置参数

4.使用run命令执行模块

使用recon/contacts-credentials/hibp_paste模块检测信息是否泄露

Haveibeenpwned网站

谢谢观赏