# 渗透测试实践

## 第一章 渗透测试概要

### 1.1黑客专用linux系统

<https://www.kali.org/downloads/>

### 1.2黑客实验环境的搭建和使用

### 1.3渗透测试的步骤

1.侦察

2.扫描

3.漏洞利用

4.维持访问

5.隐藏

## 第二章侦察

### 2.1简介

### 2.2HttpTrack

复制一个网站的副本，网页，连接，图片，代码

[http://www.httrack.com](http://www.httrack.com/)

在linux下载，apt-get install webhttrack

### 2.3Google 指令——善用搜索

**Site** 定位搜索网站 site:域名+空格+搜索内容

Allintile 标题中有全部关键字才出现在搜索结果里 allintitle index of

Intitle 标题中只要有一个关键字就出现在搜索结果里 intitle index of

Inurl url中有关键字才出现在搜过结果里 url:admin

Cache 让网页只显示快照里的结果 cache:域名

Filetype 搜索某个类型的文件 filetype:pdf 搜索pdf文件

指令可以组合

### 2.4The Harvester——挖掘并利用邮箱地址

Blacktrack linux 已经内置了该软件

使用步骤：

1.单机屏幕左下角的K-Start龙图标

2.将鼠标只想菜单顶端的Backtrack

3.进入Informatioin Gathering (信息收集)

4进入all

5.单击The Harvester

也可以直接打开终端 The Harvester的目录

/pentest/enumeraion/google/theharvester

然后运行

。/theHarvester .py syngress.com -l 10 -b google

-l 小写的L 表示限定返回的搜索结果的条数

-b 用来指定将要搜索的公共只是库 可以选择Google Bing PGP LinkedIn

### 2.5 whois

whois + 域名

如果返回dns服务器只有名字，可以使用host命令，将名字翻译成IP

### ２.６　Netcraft　是否有漏网之鱼

登陆news.netcraft.com 搜索sybgress，会搜索出相应的报告

### 2.7 host 查看ip

Host 主机名

### 2.8 dns获取信息

#### 2.8.1 NS LookUp，查看dns信息

使用：

1.输入命令nslookup 进入程序中

2.Servcer 8.8.8.8 进入该dns中

3.set type =any 显示该dns中所有信息

4.set type 5 mx 查询公司的邮箱服务器

#### 2.8.2 dig 从dns服务器提取大量信息

Dig @targeIp domain -t AXFR

2.9

社会工程学

慈善黑客协会

以工换粮计划

渗透人员应该懂的黑客技术 第二版

Kali 也有面向 WiFi 的工具，像 Aircrack-ng、Kismet、以及 Pixie。

对于破解密码，它也有像 Hydra、Crunch、Hashcat、以及 John the Ripper 这样的工具

NMap 和 Wireskark 这样的经典信息采集工具