实验 1 信息收集技术实验

1 实验目的

1.掌握两种以上查询目标DNS、IP地址信息的方法。

2 实验内容

1.使用nslookup实现DNS信息枚举。

2.使用whois查询DNS信息（枚举DNS信息）。

3.使用Dmitry进行DNS等信息收集。

3 实验前提

完成本实验，需要事先安装：

- kali 201902虚拟机，假设其IP地址为：10.10.10.130

如果使用kali完成实验内容1时中出现了下列类似信息：

- `xxx.com not found: 5(REFUSED)`
- `server can't find baidu.com: REFUSED`

那么可以考虑在vmware workstation菜单“编辑”-“虚拟网络编辑器”-“vmnet 8”-“NAT 设置”中，将“自动选择DNS”去掉，在下方手动添加DNS域名服务器IP地址：

- 8.8.8.8
- 9.9.9.9
- 114.114.114.114
- 114.114.115.115

4 实验步骤

4.1 使用nslookup实现DNS信息枚举

nslookup是一款交互式查询DNS服务器的软件。

1.打开kali中的命令行终端。

2.nslookup查询语法如下：

```
nslookup -qt=类型 目标域名 指定的DNS服务器IP或域名
```

`-qt=` 后面的类型可以选择：

- A 地址记录(Ipv4)
- AAAA 地址记录（Ipv6）
- CNAME 别名记录
- HINFO 硬件配置记录，包括CPU、操作系统信息
- ISDN 域名对应的ISDN号码
- MB 存放指定邮箱的服务器
- MG 邮件组记录
- MINFO 邮件组和邮箱的信息记录
- MR 改名的邮箱记录
- MX 邮件服务器记录
- NS 名字服务器记录
- PTR 反向记录
- RP 负责人记录
- SRV TCP服务器信息记录
- TXT 域名对应的文本信息

目标域名，是我们希望枚举的域名。

指定的DNS服务器IP或域名，可以是9.9.9.9，或8.8.8.8这些公知DNS server。

3.运行下列命令，并记录结果。

```
nslookup -qt=A xxx.com 9.9.9.9
```

4.2 使用whois查询DNS信息（枚举DNS信息）

WHOIS是一个基于TCP的查询和响应协议，通常用于为互联网用户提供信息服务。 它返回有关注册域名，IP地址块，Nameservers和更广泛的信息服务的信息。

1.尝试运行下列命令：

```
whois xxx.com
```

2.根据查询结果填写下列信息内容。

信息类型	信息内容
Registrar WHOIS Server	
Registrar URL	
Updated Date	
Creation Date	
Registry Expiry Date	
Registrar:	
Registrar IANA ID:	
Registrar Abuse Contact Email:	
Registrar Abuse Contact Phone:	
Name Server:	
Name Server:	
Name Server:	
Name Server:	
DNSSEC:	
Registrar Abuse Contact Email:	
Registrar Abuse Contact Phone:	

4.3 使用Dmitry进行DNS信息收集

Dmitry是Deepmagic Information Gathering Tool缩写，用于根据域名或其它信息进行网络信息收集。

它有以下功能：

- 根据IP（或域名）来查询目标主机的Whois信息
- 在Netcraft.com的网站上挖掘主机信息
- 查找目标域中用的子域

- 查找目标域的电子邮件地址
- 探测目标主机上打开的端口、被屏蔽的端口和关闭的端口

请先在kali2019终端下运行下列命令，查看dmitry帮助。

```
dmitry -h
```

4.3.1 使用 dmitry 根据域名收集信息

1.在Kali 201902中打开一个终端.

2.运行下列命令，记录命令结果，并回答该命令执行了哪些搜索功能。

```
dmitry -iwnse xxx.com
```

3.运行下列命令，记录命令结果，并回答该命令执行了哪些搜索功能。

```
dmitry -p example.com -f -b
```