项目 3

利用 Kali Linux 收集及利用信息

Project 3

3.1 用户需求与分析

黑客为了发动攻击需要收集关于目标主机的基本信息，黑客得到的信息越多，攻击成功的概率也就越高。Kali Linux 操作系统上提供了很多工具，可以协助整理和组织目标主机的数据。

3.2 预 备 知 识

3.2.1 枚举服务

枚举是一类程序，它允许用户从一个网络中收集某一类的所有相关信息。DNS 枚举可以收集本地所有 DNS 服务和相关条目，可以帮助黑客收集目标组织的关键信息，如用户名、计算机名和 IP 地址等，为了获得这些信息，黑客可以使用 DNSenum 工具。

1. DNS 枚举工具 DNSenum

DNSenum 是一款非常强大的域名信息收集工具，它能够通过谷歌或者字典文件猜测可能存在的域名，并对一个网段进行反向查询。它不仅可以查询网站的主机地址信息、域名服务器和邮件交换记录，还可以在域名服务器上执行 AXFR 请求，然后通过谷歌脚本得到扩展域名信息，提取子域名并查询，最后计算 C 类地址并执行 WHOIS 查询，执行反向查询，把地址段写入文件。

2. DNS 枚举工具 Fierce

Fierce 工具和 DNSenum 工具性质差不多，主要是对子域名进行扫描和收集信息的。使用 Fierce 工具获取一个目标主机上所有 IP 地址和主机信息。

3.2.2 测试网络范围

测量网络范围内的 IP 地址或域名也是黑客信息收集的重要组成部分，通过测量网络

范围内的IP地址或域名，可以确定是否存在入侵网络并损害系统。通常情况下，黑客只要在一个领域找到漏洞就可以利用这个漏洞攻击另外一个领域。在Kali中提供了DMitry和Scapy工具，其中DMitry工具用来查询目标网络中IP地址或域名信息，而Scapy工具用来扫描网络及嗅探数据包。

1. 域名查询工具DMitry

DMitry工具是用来查询IP或域名WHOIS信息的，WHOIS是用来查询域名是否已经被注册及注册域名详细信息的数据库，例如域名所有人和域名注册商。使用该工具可以查到域名的注册商和过期时间等。

虽然使用DMitry工具可以查到IP或域名信息，但还是不能判断出网络范围，因为一般的路由器和防火墙并不支持IP地址范围的方式，所以现实中经常要把IP地址转换成子网掩码的格式、CIDR格式和思科反向子网掩码格式等。在Linux中，Netmask工具可以在IP范围、子网掩码、CIDR和Cisco等格式中互相转换，并且提供了IP地址的点分十进制、二进制、八进制和十六进制之间的相互转换。

2. 路由跟踪工具Scapy

Scapy是一款功能强大的交互式数据包处理工具、数据包生成器、网络扫描器、网络发现工具和包嗅探工具。它提供多种类别的交互式生成数据包或数据包集合、对数据包进行操作、发送数据包、包嗅探、应答和反馈匹配等功能。

3.2.3 系统指纹识别和服务指纹识别

现在一些便携式计算机操作系统使用指纹识别来验证密码进行登录，例如苹果手机。指纹识别是识别系统的一个典型模式，包括指纹图形获取、处理、特征提取和对等模块。目标系统中服务的指纹信息包括服务端口、服务名和版本等，在Kali中可以使用Nmap和Amap工具识别指纹信息。使用Nmap工具可以查看目标主机正在运行的端口号，还可以获取各个端口对应的服务及版本信息。服务枚举工具Amap能够识别正运行在一个指定端口或一个范围端口上的应用程序。

3.2.4 网络映射器Nmap简介

Nmap号称“扫描之王”，提供了大量基于DOS命令行的选项。它是一个免费开放的网络扫描和嗅探工具，也叫作网络映射器(Network Mapper)。该工具有3个基本功能：①探测一组主机是否在线；②扫描主机端口，嗅探所提供的网络服务；③可以推断主机所用的操作系统。通常，网络管理员利用Nmap来进行网络系统安全的评估，而黑客可以使用该软件扫描，通过向远程主机发送探测数据包来获取主机的响应，并根据主机的端口开放情况得到网络的安全状态，从中寻找存在漏洞的目标主机，从而实施下一步的攻击。

Nmap使用TCP/IP协议栈指纹准确地判断目标主机的操作系统类型。首先，Nmap通过对目标主机进行端口扫描，找出有哪些端口正在目标主机上监听。当侦测到目标主机有多于一个开放的TCP端口、一个关闭的TCP端口和一个关闭的UDP端口时，Nmap

的探测能力是最好的。其次，Nmap 对目标主机进行一系列测试，利用得出的测试结果建立响应目标主机的 Nmap 指纹。最后，将此 Nmap 指纹与指纹库中的指纹进行查找匹配，从而得出操作系统的类型。Nmap 支持 4 种扫描方式：ping 扫描、TCP connect()扫描、TCP SYN 扫描、UDP 扫描。该工具既有 Windows 版本也有 Linux 版本，可以在 http://www.insecure.org/nmap 上免费下载，下载后直接运行进行安装即可。

3.3　方 案设 计

方案设计如表 3-1 所示。

表 3-1　方案设计

任务名称	利用 Kali Linux 收集及利用信息
任务分解	1. 利用枚举工具收集关键信息 2. 利用域名查询工具测量网络范围 3. 利用路由跟踪工具测量网络范围 4. 使用工具进行系统指纹识别 5. 使用工具进行服务指纹识别
能力目标	1. 使用 DNS 枚举工具收集目标主机的关键信息 2. 利用域名查询工具查询目标网络中 IP 地址或域名信息 3. 能利用路由跟踪工具来扫描网络及嗅探数据包 4. 能使用 Nmap 工具识别正在运行的目标主机的系统指纹信息 5. 能使用 Amap 工具识别正在运行的目标主机的服务指纹信息
知识目标	1. 了解枚举服务的定义 2. 熟悉 DNS 枚举工具 3. 熟悉域名查询工具和路由跟踪工具 4. 了解系统指纹识别和服务指纹识别的概念 5. 了解网络映射器 Nmap 工具
素质目标	1. 培养良好的职业道德 2. 树立较强的安全意识 3. 掌握网络安全行业的基本情况 4. 树立较强的安全、节约、环保意识

3.4　项 目 实 施

3.4.1　任务 1：利用枚举工具收集关键信息

1. 任务目标

使用 DNS 枚举工具收集目标主机的关键信息，如用户名、计算机名和 IP 地址等。

2. 工作任务

（1）DNS 枚举工具 DNSenum 的使用。
（2）DNS 枚举工具 Fierce 的使用。

3. 工作环境

一台预装 Kali Linux 系统的主机。

4. 实施过程

（1）DNS 枚举工具 DNSenum 的使用。

① 在终端执行如图 3-1 所示的命令，输出信息显示了 DNS 服务的详细信息，其中包括顺德职业技术学院 Web 服务器的 IP 地址、域名服务地址。

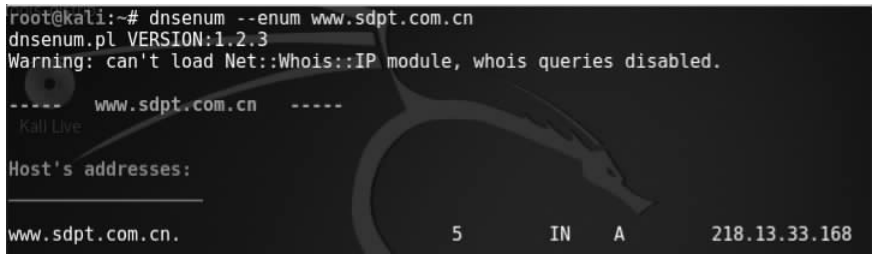

图 3-1 显示服务的详细信息

② 在终端执行如图 3-2 所示的命令，输出信息显示了 DNS 服务的详细信息，其中包括百度网站 Web 服务器的 IP 地址、域名服务地址。

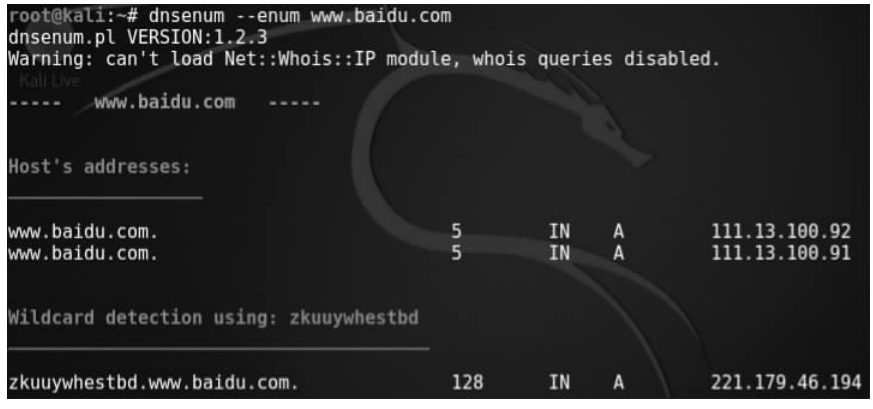

图 3-2 查看百度 Web 服务器的详细信息

③ 使用 DNSenum 工具检查 DNS 枚举时，还可以使用 dnsenum 命令的一些附加选项，如使用--threads [number]设置用户同时运行多个进程数；使用-r 允许用户启用递归查询；使用-d 允许用户设置 WHOIS 请求之间时间延迟数（单位为秒）；使用-O 允许用户指定输出位置；使用-w 允许用户启用 WHOIS 请求。

(2) DNS 枚举工具 Fierce 的使用。

① 在终端执行如图 3-3 所示的命令。

② 输出信息显示了 baidu.com 下所有的子域，如图 3-4 所示。

图 3-3　Fierce 工具的使用

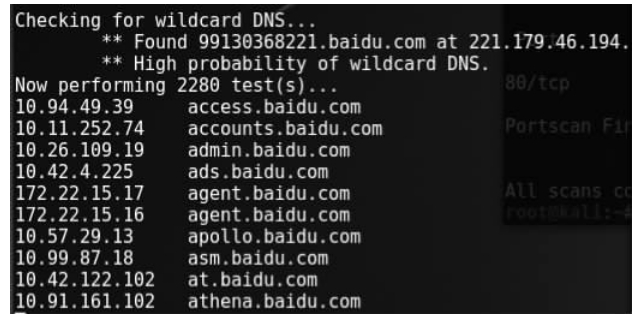

图 3-4　baidu.com 下所有的子域

3.4.2　任务 2：利用域名查询工具和路由跟踪工具测量网络范围

1. 任务目标

利用域名查询工具查询目标网络中 IP 地址或域名信息，利用路由跟踪工具来扫描网络及嗅探数据包。

2. 工作任务

(1) 域名查询工具 DMitry 的使用。

(2) 路由跟踪工具 Scapy 的使用。

3. 工作环境

一台预装 Kali Linux 系统的主机。

4. 实施过程

(1) 域名查询工具 DMitry 的使用。

① 查看 DMitry 工具的帮助信息，如图 3-5 所示。信息显示了 dmitry 命令的语法格式和所有可用参数。

② 使用 DMitry 工具收集 sdpt.com.cn 域名的信息，如图 3-6 所示。

③ 以上输出信息显示了 sdpt.com.cn 域名的 IP 地址、WHOIS 信息及开放的端口号。

④ 使用 dmitry 命令的-s 选项，可以查询可能的子域，如图 3-7 所示。从输出的信息中，可以看到搜索到了一个子域，该子域名为 Google.com，IP 地址为 111.13.101.208。由于不能连接 Google.com 网站，因此出现 Unable to connect：Socket Connect Error 错误信息。

```
root@kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

图 3-5　DMitry 工具的帮助信息

```
root@kali:~# dmitry -wnpb sdpt.com.cn
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:218.13.33.168
HostName:sdpt.com.cn

Gathered Inic-whois information for sdpt.com.cn
---------------------------------
Error: Unable to connect - Invalid Host
ERROR: Connection to InicWhois Server cn.whois-servers.net failed

Gathered Netcraft information for sdpt.com.cn

Retrieving Netcraft.com information for sdpt.com.cn
Netcraft.com Information gathered
Gathered TCP Port information for 218.13.33.168
---------------------------------
 Port            State
80/tcp           open
Portscan Finished: Scanned 150 ports, 69 ports were in state closed

All scans completed, exiting
```

图 3-6　sdpt. com. cn 域名的信息

```
root@kali:~# dmitry -s baidu.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:111.13.101.208
HostName:baidu.com

Gathered Subdomain information for baidu.com
---------------------------------
Searching Google.com:80...
Unable to connect: Socket Connect Error
```

图 3-7　查询合理的子域

⑤ 用 netmask 命令将域名 sdpt. com. cn 转换成标准的子网掩码格式，如图 3-8 所示。

```
root@kali:~# netmask -s sdpt.com.cn
218.13.33.168/255.255.255.255
```

图 3-8　将域名转换为子网掩码格式

(2) 路由跟踪工具 Scapy 的使用。

① 启动 Scapy 工具，如图 3-9 所示。

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.3.2)
>>>
```

图 3-9　启动 Scapy 工具

② 使用 sr()函数实现发送和接收数据包，执行命令如下所示，执行以上命令后，会自动与 www. sdpt. com. cn 建立连接，执行几分钟后，使用 Ctrl＋C 组合键终止接收数据包，如图 3-10 所示。从输出的信息中可以看到收到 25 个数据包，得到 11 个响应包及保留了 13 个包。

```
>>> ans,unans=sr(IP(dst="www.baidu.com/30",ttl=(1,6))/TCP())
Begin emission:
.****Finished to send 24 packets.
.....***.....****^C
Received 25 packets, got 11 answers, remaining 13 packets
```

图 3-10　使用 sr()函数发送和接收数据包

③ 以表的形式查看数据包的发送情况，如图 3-11 所示，输出的信息显示了该网络中的所有 IP 地址。

```
>>> ans.make_table(lambda(s,r):(s.dst,s.ttl,r.src))
   111.13.100.88 111.13.100.89 111.13.100.90 111.13.100.91
1 192.168.232.2 192.168.232.2 192.168.232.2 192.168.232.2
2 -             111.13.100.89 111.13.100.90 111.13.100.91
3 -             111.13.100.89 111.13.100.90 111.13.100.91
4 -             111.13.100.89 -             -
```

图 3-11　以表的形式查看数据包的发送情况

④ 使用 scapy 命令查看 TCP 路由跟踪信息，如图 3-12 所示。输出信息显示了与 www. baidu. com、www. kali. org、www. sdpt. com. cn 三个网站连接后所经过的地址。

```
res,unans = traceroute(["www.baidu.com","www.kali.org","www.sdpt.com.cn"],dport = [80,
443],maxttl = 20,retry = -2)
```

输出信息中，RA 标识路由区，SA 表示服务区。其中路由区是指当前系统中移动台当前的位置，RA 的标识符是 RAI，RA 是包含在 LA 内的。服务区是指移动台可获得服务的区域，即不同通信网用户无须知道移动台的实际位置，而可与之通信的区域。

⑤ 执行下列命令退出 Scapy，也可以按 Ctrl＋D 组合键退出 Scapy。

```
>>> res,unans=traceroute(["www.baidu.com","www.kali.org","www.sdpt.com.cn"],dport=[80,443],maxttl=20,retry=-2)
Begin emission:
**************************************Finished to send 120 packets.
************************************************************Begin emission:
Finished to send 19 packets.
Begin emission:
Finished to send 19 packets.

Received 101 packets, got 101 answers, remaining 19 packets
   111.13.100.91:tcp443 111.13.100.91:tcp80 192.124.249.10:tcp443 192.124.249.10:tcp80 218.13.33.168:tcp443 218.13.33.168:tcp80
1  192.168.232.2   11    192.168.232.2   11  192.168.232.2   11    192.168.232.2   11   192.168.232.2   11   192.168.232.2   11
2  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
3  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
4  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
5  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
6  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
7  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
8  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
9  111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
10 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
11 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
12 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
13 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
14 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
15 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
16 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
17 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
18 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
19 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
20 111.13.100.91   SA    111.13.100.91   SA  192.124.249.10  SA    192.124.249.10  SA   -                    218.13.33.168   SA
```

图 3-12　查看 TCP 路由跟踪信息

```
>>> exit()
```

3.4.3　任务 3：使用工具进行系统指纹识别和服务指纹识别

1. 任务目标

使用工具测试正在运行的目标主机的操作系统以及服务的指纹信息，包括服务端口、服务器名和版本等。

2. 工作任务

（1）使用 Nmap 工具识别系统指纹信息。
（2）使用 Nmap 工具识别服务指纹信息。
（3）使用 Amap 工具识别服务指纹信息。

3. 工作环境

一台预装 Kali Linux 系统的主机。

4. 实施过程

（1）使用 Nmap 工具识别系统指纹信息。

① 使用 nmap 命令的-O 选项启用操作系统测试功能，如图 3-13 所示。

② 输出的信息显示了主机 192.168.232.129 的指纹信息，包括目标主机打开的端口、MAC 地址、操作系统类型和内核版本等。

（2）使用 Nmap 工具识别服务指纹信息。

① 使用 nmap 命令的-sV 选项查看 192.168.232.129 服务器上正在运行的端口，如图 3-14 所示。

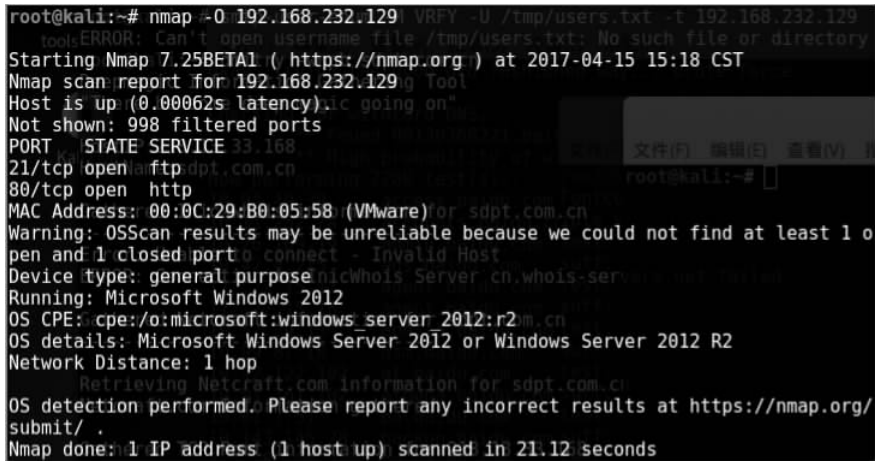

图 3-13　启用操作系统测试功能

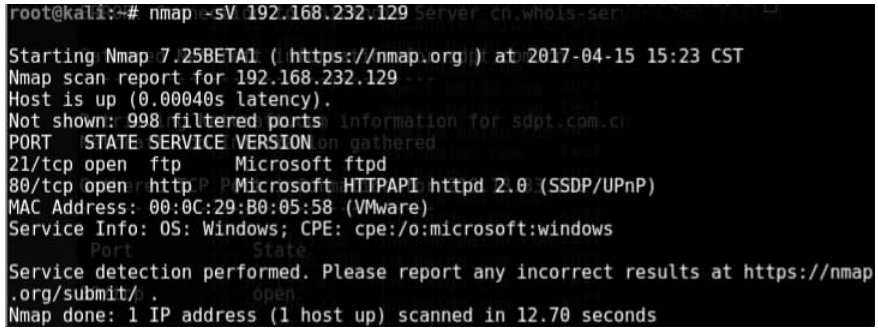

图 3-14　查看服务器上正在运行的端口

② 输出的信息显示了目标服务器 192.168.232.129 上运行的端口号有 21 和 80，同时还获取各个端口对应的服务及版本信息。

(3) 使用 Amap 工具识别服务指纹信息。

① 使用 Amap 工具在指定的 50～100 端口范围内测试目标主机 192.168.232.129 上正在运行的应用程序，如图 3-15 所示。

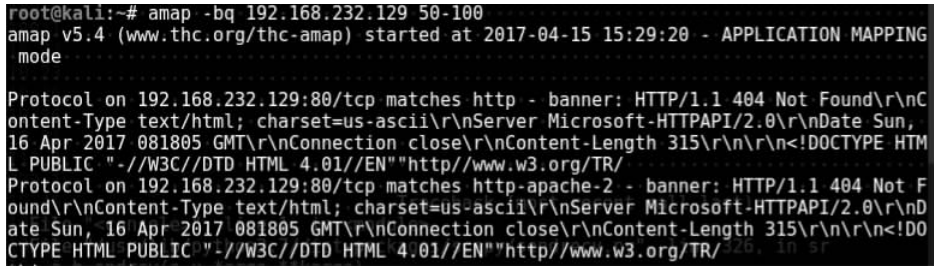

图 3-15　在指定的端口范围内测试目标主机上正在运行的应用程序

② 输出的信息显示了目标主机 192.168.232.129 在 50～100 端口范围内正在运行的端口，从输出结果的第二段内容中可以了解到主机 192.168.232.129 使用时的 Windows Server 操作系统。

3.5 常见问题解答

为什么要测试网络范围？

答：测试网络范围内的 IP 地址或域名是网络攻击的重要组成部分，通过查询目标网络中 IP 地址或域名信息，扫描网络即嗅探数据包，可以确定是否有黑客入侵自己的网络并损害系统。

3.6 认 证 试 题

简答题

1. 简述什么是枚举服务。
2. 简述什么是系统指纹信息和服务指纹信息。