第5章 网络攻防技术

5.1 网络信息收集

孙子兵法云："知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼，每战必殆。"网络攻防也是如此。

在现实世界中，只要不是太蠢的窃贼，都懂得在实施盗窃计划之前，必须观察和收集目标房屋的相关信息，如主人作息时间、门锁类型、是否安装远程报警系统等安防设备，甚至邻里关系、物业管理水平、小区安保措施、得手后的逃跑路线等。

对于网络攻击者而言，如果想要不留痕迹地入侵远程目标系统，那么在入侵系统之前，他们也必须了解目标系统可能存在的漏洞与缺陷信息，这些信息包括但不限于：系统在管理上的安全缺陷和漏洞、使用的网络协议安全缺陷与漏洞、使用的操作系统安全缺陷与漏洞、部署的数据库管理系统的安全缺陷和漏洞；而且在入侵实施过程中，攻击者还需要进一步掌握更多信息，如目标网络内部拓扑结构、目标网络与外部网络的连接方式与链路路径、防火墙的端口过滤与访问控制配置、使用的身份认证与访问控制机制等。一旦攻击者完全掌握了这些信息，目标系统就彻底暴露在攻击者面前了。

实际上，攻击者只要有足够的耐心和灵活的思路，结合各种黑客工具和技巧，他们可以从公开渠道收集到目标系统的各类信息，绝对会让人大吃一惊。

对于防御者而言，如果防御者能从攻击者的视觉了解到他们想要看到什么，他们能看到什么，他们能利用这些情报做到什么，那防御者就会知道自己所维护的系统可能存在哪些潜在的安全威胁，以及如何去解决和防范这些安全威胁。

应该指出的是，网络信息收集和入侵并不具有明显界限的先后次序关系，信息收集是融入整个入侵过程中，攻击者收集的信息越全面细致，就越有利于入侵攻击的实施，而随着入侵攻击的深入，攻击者就能获得更多目标系统的安全细节。

本节将从网络踩点、网络扫描、网络查点这3方面介绍对网络攻防双方都适用的最为基础的网络信息收集技术，并给出防范这些攻击技术的简单而有效的防御措施。

5.1.1 网络踩点

网络踩点是指黑客通过因特网有计划有步骤地信息收集，了解攻击目标的隐私信息、网络环境和信息安全状况，根据踩点结果，攻击者将寻找出攻击目标可能存在的薄弱环节，为进一步的攻击行动提供指引。

下面，我们对最为流行与常见的网络踩点手段 Google Hacking、Whois 服务和 DNS 查询进行介绍。

Google Hacking 是指通过 Web 搜索引擎查找特定安全漏洞或私密信息的方法，其会利用各个常用的搜索引擎，以及流行的 Google Hacking 客户端软件 Athena、Wikto、SiteDigger。

能否利用搜索引擎在 Web 中找到所需要的信息，关键在于能否合理地提取搜索的关键字。我们可以利用表 5.1 列出的这些常见的搜索引擎高级搜索语法和表 5.2 的搜索引擎操作符结合，生成搜索关键字。

表 5.1　搜索引擎高级搜索语法

搜索引擎高级搜索语法	说　　明
intext	把网页中的正文内容中的某个字符作为搜索条件。例如在搜索引擎里输入“intext：网络空间安全概论”，将返回所有在网页正文部分包含“网络空间安全概论”的网页，allintext 使用方法和 intext 类似
intitle	搜索网页标题中是否有我们所要找的字符。例如搜索“intitle：网络空间安全”，将返回所有网页标题中包含“网络空间安全”的网页，同理，allintitle 也同 intitle 类似
cache	搜索搜索引擎里关于某些内容的缓存
define	搜索某个词语的定义，搜索“define:hacker”，将返回关于 hacker 的定义
filetype	搜索指定类型的文件。例如输入“filetype:doc”，将返回所有以 doc 结尾的文件 URL
info	查找指定站点的一些基本信息
inurl	搜索我们指定的字符是否存在于 URL 中。例如输入“inurl：admin”，将返回 N 个类似于这样的链接：http://www.xxx.com/xxx/admin，用来找管理员登录的 URL。allinurl 也同 inurl 类似，可指定多个字符
link	搜索与给定网页存在链接的页面，例如搜索“link：www.zhihuishu.com”，可以返回所有和 www.zhihuishu.com 做了链接的 URL
site	仅搜索特定网站或域名范围，例如搜索“site:www.zhihuishu.com”，将返回所有与 www.zhihuishu.com 这个网址相关的 URL

表 5.2　搜索引擎操作符

搜索引擎操作符	说　　明
＋	把搜索引擎可能忽略的关键字列入查询范围
－	查询结果中排除含有这个检索关键字的页面
“”	查询结果精确匹配双引号部分包含完整搜索关键字
|	查询结果包含输入的多个关键字中任意一个即可匹配
·	单一的通配符
*	通配符，代表多个字母

例如，使用“site:org　filetype:xls 身份证号”这样的关键字，可能搜索到如图 5.1 所示

的包含个人身份信息的数据表，而类似“site:org inurl:login”的关键字，能找到如图 5.2 所示的网站登录页面，以使得攻击者得以进行进一步攻击测试。

分中心	个人编号	IC卡编号	单位编号	姓名	性别	人员类别	出生日期	公民身份号码
[redacted]中心	[redacted]86	03[redacted]	[redacted]4	[redacted]	男	[redacted]城镇居民	[redacted]26	[redacted]6181
[redacted]中心	[redacted]91	03[redacted]	[redacted]4	[redacted]	女	[redacted]城镇居民	[redacted]23	[redacted]3094
[redacted]中心	[redacted]20	03[redacted]	[redacted]4	[redacted]	女	[redacted]城镇居民	[redacted]18	[redacted]8332
[redacted]中心	[redacted]50	03[redacted]	[redacted]4	[redacted]	男	[redacted]城镇居民	[redacted]12	[redacted]2121
[redacted]中心	[redacted]87	86[redacted]	[redacted]4	[redacted]	女	[redacted]城镇居民	[redacted]28	[redacted]8012
[redacted]中心	[redacted]01	86[redacted]	[redacted]4	[redacted]	女	[redacted]城镇居民	[redacted]03	[redacted]3098
[redacted]中心	[redacted]03	86[redacted]	[redacted]4	[redacted]	男	[redacted]城镇居民	[redacted]10	[redacted]0361
[redacted]中心	[redacted]04	86[redacted]	[redacted]4	[redacted]	女	[redacted]城镇居民	[redacted]02	[redacted]2974

图 5.1　搜索引擎搜索到的包含身份证号的文档

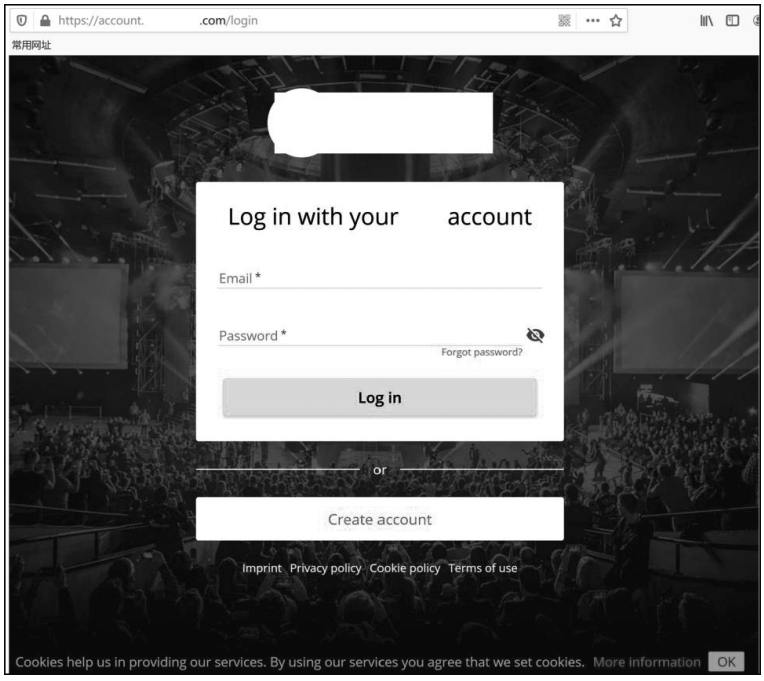

图 5.2　搜索引擎搜索到的网站登录页面

如果说使用搜索引擎还需要手工设置搜索关键字，而且从成百上千个搜索结果中找到目标网站也需要具备一定的专业知识，这对攻击者而言多少有点效率低下。那么诸如 Katana(https://github.com/adnane-X-tebbaa/Katana)、能快速识别系统弱点和敏感数据的工具集项目 Google Hacking Diggity Project (https://resources.bishopfox.com/resources/tools/google-hacking-diggity/)等较为知名的自动化工具，可以自动执行 Google Hacking 搜索出大量的安全漏洞、错误、配置缺陷、应用程序独有的旗标信息等安防细节，即使是一位初出茅庐的黑客小子，也能很轻易地使用这些工具从世界各地的 Web 网站中找到目标。

那么，如何避免让我们成为网络攻击者的目标呢？防范 Google Hacking 应该做到以下几点。

(1) 将不希望被别人搜索到的敏感信息从论坛、微博、微信等公共媒体上删除干净。

(2) 发现存在非预期泄露的敏感信息后,应采取行动进行清除。

(3) 发布信息时,尽量不要出现真实个人信息。例如,不要轻易相信各种微店、拼团、网络抽奖活动,因为这些活动往往要求提供个人电话号码、社交媒体账号甚至身份证号码等个人隐私信息。

(4) 作为网络管理员,不要轻易在讨论组或技术论坛上发布求助技术帖,因为那样往往会将单位内部网络拓扑结构或路由器配置信息泄露给他人。

(5) 关注中国国家漏洞库 CNNVD 等安全漏洞信息库发布的技术信息,及时更新软件或操作系统补丁。

网络踩点的第二个技巧是使用 WHOIS 查询。WHOIS 查询包括 DNS 注册信息查询服务和 IP WHOIS 查询。什么是 DNS 和 IP 呢?

在真实世界中,有多种方式来标识一个人类。例如,身份证号码、户口本或出生证书上的名字、学生证上的学号或者工作证上的工号等,但在某些特定环境下,某种识别方法可能比别的方法更合适些。例如,在日常生活中,我们更愿意以户口本上的姓名而非身份证号码来记忆某个特定的人,因为前者更容易被记住。

Internet 上的主机和人类一样,也使用多种方式进行标识。例如,使用 www.fzu.edu.cn 这种域名形式来标识一部提供 Web 服务的服务器,使用 EA-F8-D7-AC-49-2E 以太网硬件地址,或 220.181.38.148 这种 IPv4 地址,或 FE80:A00:20FF:FE01:C782 这类 IPv6 地址对主机进行标识,这些不同的主机标识形式,是互联网中联络特定网络或主机所必需的关键信息。对人类而言,更喜欢域名这种便于记忆的主机标识,而作为通信枢纽的路由器,使用定长且有着层次结构的 IP 地址标识目标主机,显然更便于快速寻址。

为了折中上述这些标识的不同应用场景,Internet 需要能提供一种域名到 IP 地址转换的服务,这就是域名系统(Domain Name System,DNS)的主要任务,如图 5.3 所示。DNS 包括:①一个由分层的 DNS 服务器实现的分布式数据库;②一个使得主机能够查询分布式数据库的应用层协议。

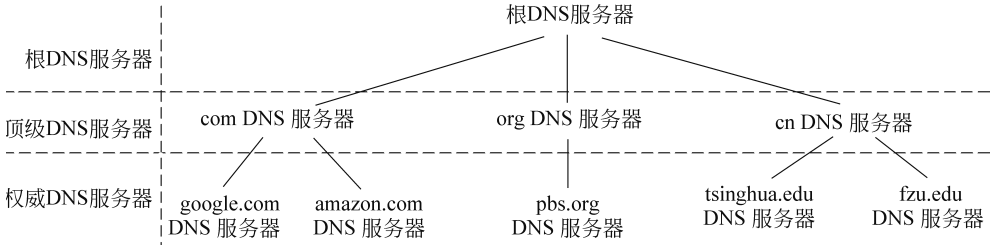

图 5.3 DNS 服务器的部分层次结构

一个组织或个人申请 DNS 域名时,会以注册人身份,通过商业运营的注册商,例如国内比较知名的万网,确认所选择的域名是否未被他人注册;接着,注册商向官方注册局申请分配此域名。域名注册成功后,官方注册局(Registry)信息、注册商(Registrar)信息、注册人(Registrant)的详细域名注册信息(域名登记人信息、联系方式、域名注册时间和更新时间、权威域名服务器的 IP 地址等),会进入官方注册局或注册商维护的公开数据库中,并向公众提供 DNS 注册信息的 WHOIS 查询。

因此,垃圾邮件制造者和其他类型的网络攻击者,通常会利用这些公开资源,查询他们

所感兴趣的目标组织或个人的 DNS 注册信息、网络位置(IP 地址)及真实地理位置等信息。

那么,当今的 Internet 是谁在负责维护如此庞大的 DNS/IP 信息库呢? 答案是 ICANN (Internet Corporation for Assigned Names and Numbers,互联网名称与数字地址分配机构)。该机构位于 DNS/IP 层次化管理结构的顶层,目前主要负责协调以下几类标识符的分配工作。

(1) Internet 域名。

(2) IP 地址。

(3) 网络通信协议的参数和端口号码。

ICANN 有很多下属分支机构,但与 DNS/IP 注册和分配相关的机构主要有 3 个:ASO、GNSO、CNNSO,如图 5.4 所示。

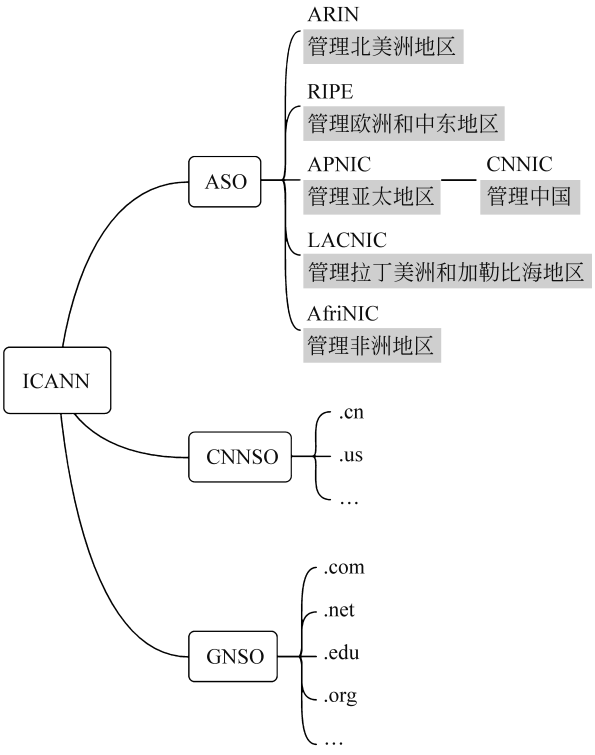

图 5.4 ICANN 与 DNS/IP 管理分支机构的层次结构图

(1) ASO(Address Supporting Organization,地址支持组织),主要听取、审查与 IP 地址分配政策有关的意见,并向 ICANN 董事会提出建议,负责把 IP 地址块统一分配给负责各自辖区内公共 Internet 号码资源管理、分配和注册事务的五大洲际 Internet 注册管理机构(Regional Internet Registry,RIR)。这些 RIR 再把 IP 地址分配给企事业单位、Internet 接入服务提供商(Internet Service Provider,ISP)或者国家 Internet 注册机构(National Internet Registry,NIR)或者本地 Internet 注册机构(Local Internet Registry,LIR):http://www.aso.icann.org。

(2) GNSO(Generic Name Supporting Organization,通用名称支持组织),负责听取、审查与通用顶级域域名(如.com、.net、.edu、.org、.info 等)分配政策有关的各种意见,并向

ICANN 董事会提出建议：http://www.gnso.icann.org。

(3) CNNSO(Country Code Domain Name Supporting Organization，国家代码域名支持组织)，负责听取、审查与国家代码顶级域域名(如.cn、.jp、.us、.uk 等)分配有关的各种意见，并向 ICANN 董事会提出建议：http://www.cnnso.icann.org。

因此，ICANN 是所有 WHOIS 查询的最佳出发点。例如，如图 5.5 所示为 ICANN 官网查询得到的 www.baidu.com 的域名注册信息。

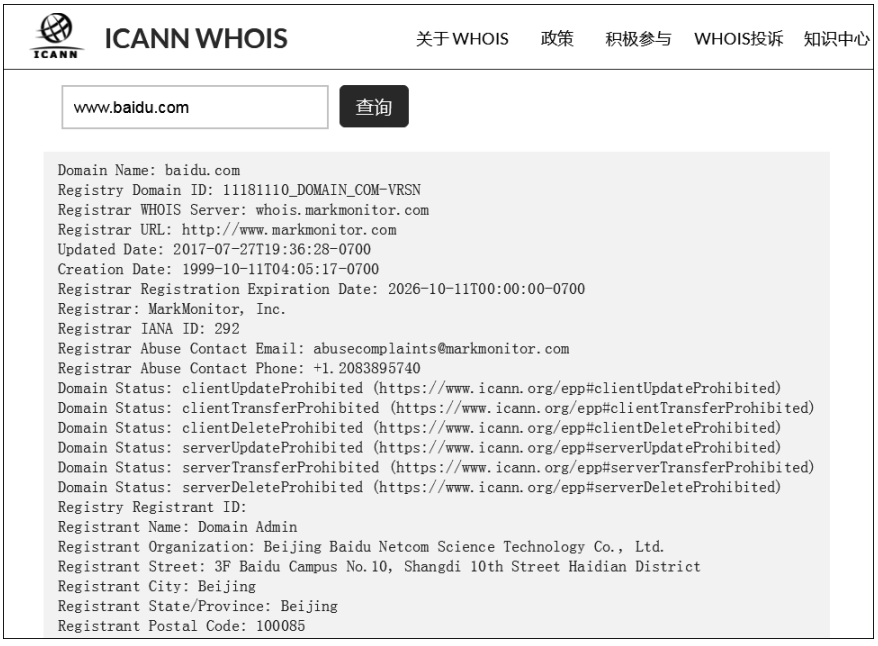

图 5.5　www.baidu.com WHOIS 查询结果部分截图

综上所述，DNS WHOIS 查询的一般思路是：在 www.iana.org 得到某个提供 WHOIS 查询服务的权威机构，进一步查询得到目标组织的域名注册商，再从域名注册商查询得到目标组织的域名注册细节。

此外，以下这些一站式 WHOIS 信息查询机构也能提供 DNS 查询服务。

- http://whois.iana.org 或 http://www.internic.net。
- http://www.allwhois.com 或 http://www.uwhois.com。
- http://www.internic.net/whois.html。
- 站长之家：whois.chinaz.com。

那么，IP 注册信息的 WHOIS 查询如何实现呢？现在已经知道 IP 分配事务是由 ICANN 的地址管理组织 ASO 总体负责，而具体 IP 网段分配记录和注册者信息都存储于各个洲际互联网管理局 RIR 的数据库中。因此，任意一个 RIR 都可以作为 IP 注册信息查询的出发点。

以下是 59.77.231.60 这个 IP 地址通过 APNIC 的 WHOIS 查询得知该 IP 地址为福州大学所有及其他详细注册信息，查询结果如图 5.6 所示(由于 IP WHOIS 查询有时效性，图例仅供参考)。

```
% Information related to '59.77.224.0 - 59.77.255.255'

% Abuse contact for '59.77.224.0 - 59.77.255.255' is 'abuse@net.edu.cn'

inetnum:        59.77.224.0 - 59.77.255.255
netname:        FZU-CN
descr:          ~{8#V]4sQ'~}
descr:          Fuzhou University
descr:          Fuzhou, Fujian 350002, China
country:        CN
remarks:        conn-id SH000873
admin-c:        SZ35-AP
tech-c:         SZ35-AP
tech-c:         CER-AP
remarks:        origin AS4538
mnt-by:         MAINT-CERNET-AP
status:         ASSIGNED NON-PORTABLE
last-modified:  2008-09-04T07:07:09Z
source:         APNIC

role:           CERNET Helpdesk
address:        Room 224, Main Building
address:        Tsinghua University
address:        Beijing 100084, China
country:        CN
phone:          +86-10-6278-4049
fax-no:         +86-10-6278-5933
e-mail:         cernet-helpdesk-ip@net.edu.cn
remarks:        abuse@net.edu.cn
admin-c:        XL1-CN
tech-c:         SZ2-AP
nic-hdl:        CER-AP
remarks:        Point of Contact for admin-c
mnt-by:         MAINT-CERNET-AP
last-modified:  2011-12-06T00:10:30Z
source:         APNIC

person:         Song Zhigang
address:        Netwok Center
address:        Fuzhou University
address:        Fuzhou, Fujian 350002, China
country:        CN
phone:          +86-591-3703142 ext. 116
fax-no:         +86-591-3703142 ext. 104
e-mail:         zgsong@fzu.edu.cn
nic-hdl:        SZ35-AP
mnt-by:         MAINT-CERNET-AP
last-modified:  2011-12-22T05:27:11Z
source:         APNIC
```

图 5.6　APNIC 对 IP 地址 59.77.231.60 的查询结果

虽然管理联系人、已注册的网络地址块、正式的名字服务器等这些信息都必须向注册机构提供，且允许互联网上的其他用户公开获得。但用户还是可以采取一些安防措施不让攻击者轻易得手。

(1) 及时更新负责管理、技术和缴费等事务的联系人信息，并及时通知域名注册机构。

(2) 为了防止社会工程学攻击，最好使用不在本单位电话交换机范围内的号码作为联系电话，还可以使用虚构的人名来作为管理性事务的联系人，这样，一旦某位员工受到了来自这个虚构联系人的电子邮件或电话，该单位的信息安全部门就能很快发现黑客对本单位的攻击企图。

(3) 可以使用域名注册商提供的私密注册服务，确保敏感信息如组织的实际物理地址、电话号码、电子邮箱等信息不被公开。

除了 DNS/IP WHOIS 查询可能导致信息泄露，如果 DNS 配置得不够安全，同样有可能泄露组织的敏感信息。由于 DNS 是一个能把主机名映射为 IP 地址或者把 IP 地址映射

为主机名的分布式数据库系统，所以对于一名网络管理员来说，允许不受信任的 Internet 用户执行 DNS 区域传送是后果极为严重的错误配置。

DNS 区域传送是指一台辅助 DNS 服务器使用来自主服务器的数据刷新自己的 ZONE 数据库，原本目的是为了实现 DNS 服务的冗余备份。本来 DNS 区域传送的操作请求只能来自于辅助 DNS 服务器，但现在许多 DNS 服务器被错误配置成只要有人发出请求，就会向对方提供一个区域数据库的拷贝。设想一下，如果一个组织没有使用公用/私用 DNS 机制来分割外部公用 DNS 信息和内部私用 DNS 信息，则区域传送将把一个组织内部网络的完整导航图全都暴露在攻击者面前。这将使得攻击者可以：

(1) 搜集到目标的重要信息。

(2) 作为跳板，攻击那些仅通过 DNS 传送才暴露的目标。

尽管令人难以置信，现实是仍然有不少网络管理员允许不受限制的 DNS 区域传送。一个简单而粗暴的解决方案是：对外的 DNS 服务器配置为禁止 DNS 区域传送，且该服务器不能包含内部网络相关主机的敏感信息。

5.1.2 网络扫描

如果说网络踩点相当于实施盗窃之前侦查外围环境以确定目标大楼，那么网络扫描就是从中寻找有人居住的房间，并找出所有可供潜入的门窗。网络攻击者可以通过网络扫描技术和自动化扫描工具，确定目标网络内活跃的主机列表，以及这些主机开放的通信端口、操作系统类型等敏感信息。

常见的网络扫描类型包括主机扫描、端口扫描、操作系统/网络服务辨识、漏洞扫描，见表 5.3。

表 5.3 网络扫描类型和目的

网络扫描类型	网络扫描目的	对比的入室盗窃
主机扫描	找出网段内活跃主机	确定目标：找出大楼中有人居住的房间
端口扫描	找出主机上所开放的网络服务	寻找门窗：找出可进入房间的门窗位置
操作系统/网络服务辨识	识别主机安装的操作系统类型与开放网络服务类型，以选择不同渗透攻击代码及配置	识别房间、门窗等差值的类型，针对不同材质结构选择不同破解工具
漏洞扫描	找出主机/网络服务上存在的安全漏洞，作为破解通道	缝隙/漏洞搜索：进一步发现门窗中可撬开的缝隙、锁眼

1. 主机扫描

主机扫描是指向目标系统发出特定的数据包，并分析目标系统返回的响应结果(或者没有任何结果)的行为。

典型的主机扫描常常使用 ICMP(RFC 792)实现。ICMP 可提供与 IP 协议层配置和 IP 数据包处置相关的诊断和控制信息的通信协议。因其能提供丰富的网络诊断信息，所以可被用于实现主机扫描。常用于主机扫描的 ICMP 报文如表 5.4 所示。

表 5.4 常用于主机扫描的 ICMP 报文

名　　称	类　　型
ICMP Destination Unreachable(目标不可达)	3
ICMP Source Quench (源抑制)	4
ICMP Redirection(重定向)	5
ICMP Timestamp Request/Reply(时间戳)	13/14
ICMP Address Mask Request/Reply(子网掩码)	17/18
ICMP Time Exceeded(超时)	11
ICMP Parameter Problem(参数有错)	12
ICMP Echo Request/Reply(响应请求/应答)	8/0

例如,经典的 PING 程序(操作系统自带)使用 ICMP Echo Request/Reply(响应请求/响应)报文,攻击者可用 ping 来确认目标主机是否在线。而使用 ICMP 地址掩码请求/答复(ICMP Address Mask Request/Reply)消息,攻击者可以获得目标设备的子网掩码,据此,攻击者还能进一步找出目标网络的各个子网,并获得默认网关和广播地址信息,进而攻击默认网关或对目标网络发起"拒绝式"服务攻击。

所以有安全意识的网络管理员,往往会在他们的网络边界路由器或防火墙设置规则阻塞 ICMP 报文,因为从上面的两个例子不难看出,如果允许 ICMP 通信不受限制地进入网络边界路由器,会给网络攻击者们留下发动攻击的可乘之机。

由于 ICMP 报文可能被防火墙过滤,所以除了 ICMP Ping 扫描,网络攻击者也经常使用 TCP 或 UDP,结合端口扫描技术来发现活动主机。例如,大多数网络都允许 80 端口的通信穿过自己的网络边界路由器到达内部非军事区,甚至大多数无状态防火墙产品如 Cisco IOS 系列,通常还会放行 80 端口的 TCP ACK 数据包;同理,选择 SMTP 的 25 端口、POP 的 110 端口、IMAP 的 143 端口等知名的网络服务支持端口进行 ping 扫描,通常也都能获得满意的扫描结果。

较为常见的基于开放端口的主机扫描如图 5.7 所示,从上到下分别是 TCP ACK ping 扫描、TCP SYN ping 扫描、UDP ping 扫描。

常见的主机扫描工具包括 ping 扫描和 Namp 扫描,前者通过向目标网络发出 IMCP Echo Request 数据包,并分析目标网络返回的响应结果来判断目标网络内的主机是否存活,UNIX 典型的 ping 工具为 fping,Windows 典型的 ping 工具是 SuperScan。Nmap 工具则集合了 ICMP/SYN/ACK/UDP ping 功能,是一个功能强大的跨平台扫描工具。

如何防范主机扫描呢? 首先利用诸如 snort 之类的入侵检测系统,监测主机扫描活动。其次,根据业务需求,对允许放行哪些 ICMP 通信报文进入网络或特定系统做出细致评估。例如,使用访问控制列表将外来 ICMP 通信限制在外部网络,以及在不妨碍正常通信的前提下,只允许指定的 ICMP 数据包到达特定主机等措施,如只允许 ECHO_REPLY、TIME_EXCEEDED、HOST_UNREACHABE 进入 DMZ 网络,而限制 TIMESTAMP、ADDRESS MASK 的进入。

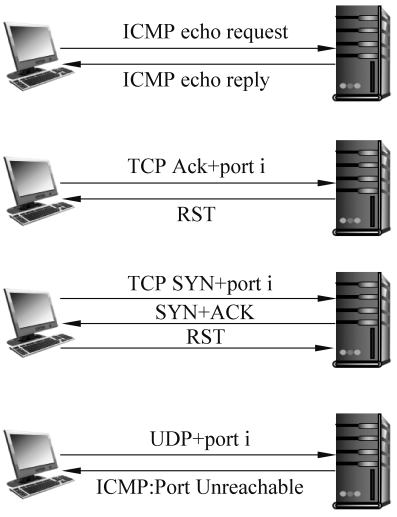

图 5.7　基于 ICMP/TCP/UDP 的主机扫描

2. 端口扫描

Internet 上主机间的通信总是通过端口发生的，因此当网络攻击者通过主机扫描确定活跃主机之后，活跃主机的开放端口就是他们入侵目标系统的绝佳通道。端口扫描是指网络攻击者通过连接到远程目标系统的 TCP/UDP 端口，以确定哪些服务正在运行，或者正处于监听状态。打个比方，处于监听状态的活跃服务相当于你家的大门和窗户，它们都是外人窥探你私人领地的通道，这些通道或者可以使外人窥探你的私密信息，或者当通道损坏时（网络服务存在安全漏洞），外人可以在非授权情况下侵入你家。表 5.5 列出了常见的网络服务及对应的默认开放端口。

表 5.5　常见的网络服务及默认开放端口

默 认 端 口	对应的网络服务
21	FTP 文件传输服务
22	SSH 安全登录服务
23	Telnet 远程登录服务
25	SMTP 简单邮件传输服务
53	DNS 域名解析服务
67	BooTP/DHCP(Bootstrap Protocol Server，引导程序协议服务器端)
68	BooTP/DHCP(Bootstrap Protocol Client，引导程序协议客户端)
69	TFTP 简单文件传输服务(UDP)
79	Finger 服务开放，用于查询远程主机在线用户、操作系统类型以及是否缓冲区溢出等用户详细信息
80/8080	HTTP 超文本传输服务
110	POP3 邮件服务