第3章 黑客攻击机制

CHAPTER

3.1 知识要点

3.1.1 黑客攻击对象

网络由主机系统、转发结点和链路组成，将转发结点和实现转发结点互连的链路称为网络设施，因此，黑客攻击对象也分为主机系统和网络设施。

1. 主机系统

主机系统中存储了大量的信息资源，黑客攻击主机系统的主要目标是非法获取存储在主机系统中的信息资源，黑客非法获取主机系统中信息资源的过程称为非法访问，网络使得远程非法访问成为了可能。由于远程非法访问的隐蔽性和方便性，使得远程非法访问成为黑客攻击主机系统的主要手段。由于主机系统是网络的主要服务提供者，黑客攻击主机系统的另一个目的是使主机系统丧失服务功能。

2. 网络设施

转发结点中的配置信息、控制信息直接影响数据传输过程，因此，黑客攻击网络设施的重要目标是能够侵入转发结点，篡改配置信息和控制信息，使数据传输过程按照黑客预期的方向进行。传输过程中的信息资源是网络信息资源的重要组成部分，黑客攻击网络设施的另一个目标是嗅探、截获传输过程中的信息资源。实现正常的端到端数据传输是保障网络服务的基础，黑客攻击网络设施的又一个目标是破坏网络正常的端到端数据传输功能。

3.1.2 黑客攻击手段

1. 主机系统攻击手段

使主机系统感染病毒是最常见的主机系统攻击手段，病毒可以使主机系统按照黑客要求外泄信息，允许黑客随时登录主机系统，根据黑客指令对主机系统实施破坏。狭义病毒和蠕虫感染主机系统的方法已在第2章

做了详细讨论。利用主机系统漏洞非法登录主机系统，对主机系统资源实施非法访问，甚至上传病毒和木马，以此实现对该主机系统的长期控制仍然是黑客针对特定主机系统的主要攻击手段。黑客对特定主机系统的攻击过程分为侦查、扫描、获取访问权限、保持访问权限和消除入侵痕迹5个步骤。

(1) 侦查。

获取有关特定主机系统的信息，如域名、IP地址和所属单位的组织结构等。

(2) 扫描。

通过Ping操作确定主机系统是否在线，通过端口扫描确定主机系统打开的服务，通过探测过程确定主机操作系统类型及版本，通过漏洞扫描发现主机操作系统或应用程序存在的漏洞。

(3) 获取访问权限(缓冲器溢出和弱口令)。

通过猜测口令和字典文件破解弱口令。弱口令是指由一组关联性较强的字符组成的口令，如员工姓名全拼音、单位名称中每个汉字拼音的首个字符组合以及某个标准英语单词等。通过精心设计字典文件可以比较容易地破解弱口令。

通过利用操作系统或应用程序漏洞实施非法登录，最常见的操作系统或应用程序漏洞是缓冲器溢出，利用缓冲器溢出可以在主机上运行黑客的shellcode，并因此实现非法登录。

(4) 保持访问权限。

一旦实现非法登录，黑客或者创建具有管理员权限的账户，或者上传木马，在主机上保留后门，以便下次登录。

(5) 消除入侵痕迹。

为了隐藏入侵过程，往往需要在日志文件中删除和本次入侵过程相关的事件。

2. 网络设施攻击手段

网络设施攻击手段主要有信息嗅探攻击、信息拦截攻击、拒绝服务攻击、路由项欺骗攻击、DHCP欺骗攻击、DNS欺骗攻击、非法接入、重放攻击、分布式拒绝服务攻击和网络设备侵入等，大部分攻击手段已经在第1章的1.4节实验中作了详细讨论。

3.1.3 黑客攻击防御机制

1. 加密、完整性检测和鉴别

加密可以防止信息窃取，完整性检测可以防止信息篡改，源端鉴别可以防止源IP地址欺骗，身份鉴别可以防止非法访问。

2. 主机入侵防御系统

主机入侵防御系统是保护主机系统免遭攻击的主要手段，通过资源访问控制和行为监管，可以有效防御未知病毒实施的破坏操作和黑客对主机系统的攻击。

3. 网络入侵防御系统

无论是发生对主机系统的攻击行为，还是对网络设施的攻击行为，都会引发信息流异常，通过检测流经关键网段的信息流，可以发现正在实施的攻击，并加以干预。

4. 接入控制和交换机端口配置

安全端口使得每一个端口与一组 MAC 地址绑定，只有源 MAC 地址属于这组 MAC 地址的 MAC 帧才能通过该端口输入并转发。如图 3.1 所示，交换机端口之间或交换机端口与终端之间接入集线器，一方面使得黑客终端可以通过集线器嗅探两个交换机之间传输的信息，另一方面可以使得黑客终端通过假冒授权终端的 MAC 地址绕过安全端口的接入控制过程，非法接入网络。因此，必须通过配置，强迫交换机端口工作在全双工通信方式，保证交换机端口之间、交换机端口与终端之间无法接入集线器设备。

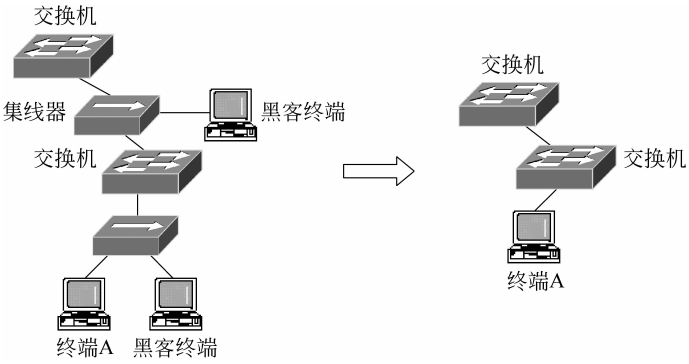

图 3.1　安全端口和全双工通信方式

5. 设备配置管理

图 3.2 中，二层交换机的设备配置管理地址属于 VLAN 1(默认 VLAN)对应的网络地址，如果三层交换机中 VLAN 1 对应的 IP 接口没有开启(down 状态)，三层交换机的路由表中没有目的网络为 VLAN 1 的路由项，其他网络中的终端就无法访问 VLAN 1，因此，只有属于 VLAN 1 的终端才能通过二层交换机的配置管理地址访问各个二层交换机并实施配置管理，这样就将二层交换机的配置管理网络与其他网络隔离，严格限制了允许管理配置二层交换机的终端。

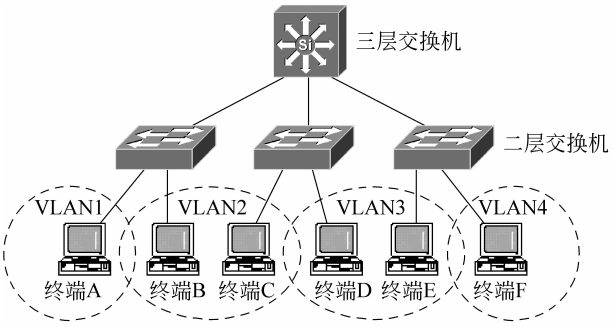

图 3.2　校园网简图

由于可以通过三层交换机的各个 IP 接口配置管理三层交换机，从网络设计上无法将三层交换机的配置管理网络和其他网络隔离，但可以通过配置管理端口的分组过滤器严格限制允许管理配置三层交换机的终端。同样可以通过配置管理端口的分组过滤器严格

限制允许管理配置二层交换机的终端。

对于图 3.3 所示的普通互连网络，可以通过任意路由器接口的 IP 地址对路由器进行配置管理。对于二层交换机，设备配置管理地址通常属于 VLAN 1(默认 VLAN)对应的网络地址。由于不存在跨路由器接口的 VLAN，因此路由器分隔的多个 VLAN 1 是独立的网络，需要分配不同的网络地址。除非每一个 VLAN 1 单独设置用于设备配置管理的终端，否则各个 VLAN 1 需要和其他网络相互通信。这种情况下，可以通过配置管理端口的分组过滤器严格限制允许管理配置二层交换机和路由器的终端。

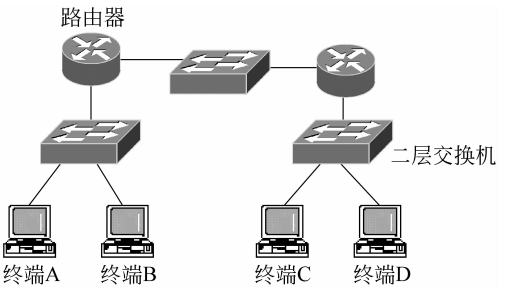

图 3.3 普通互连网络

6. 信息传输控制

简化的企业网如图 3.4 所示，分为内部网络、非军事区和外部网络三部分。为了有效抵御黑客攻击，一是通过 NAT 技术隐藏内部网络；二是通过设置访问控制策略严格控制网络之间的信息交换过程；三是通过严格控制未完成的 TCP 连接数量，防止 SYN 泛洪攻击发生。

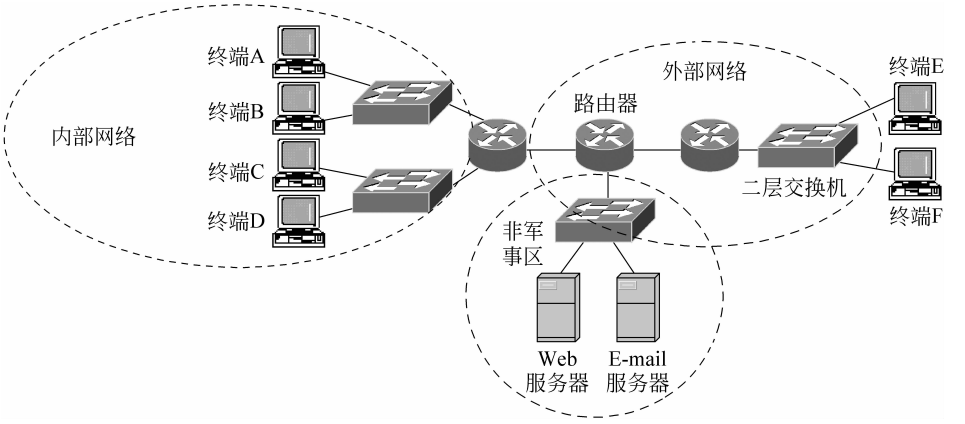

图 3.4 企业网简图

7. 流量管制

对于图 3.4 所示的企业网结构，为了防止外部网络中的黑客向内部网络传播邮件病毒，可以限制外部网络传输给非军事区中邮件服务器的 SMTP 报文的流量。

8. 安全路由

为了抵御图 3.5 所示的路由项欺骗攻击，要求对发送路由消息的路由器身份进行鉴

别，同时对接收到的路由消息的完整性进行检测，每一个路由器只处理授权路由器发送的、且传输过程中没有被篡改的路由消息。

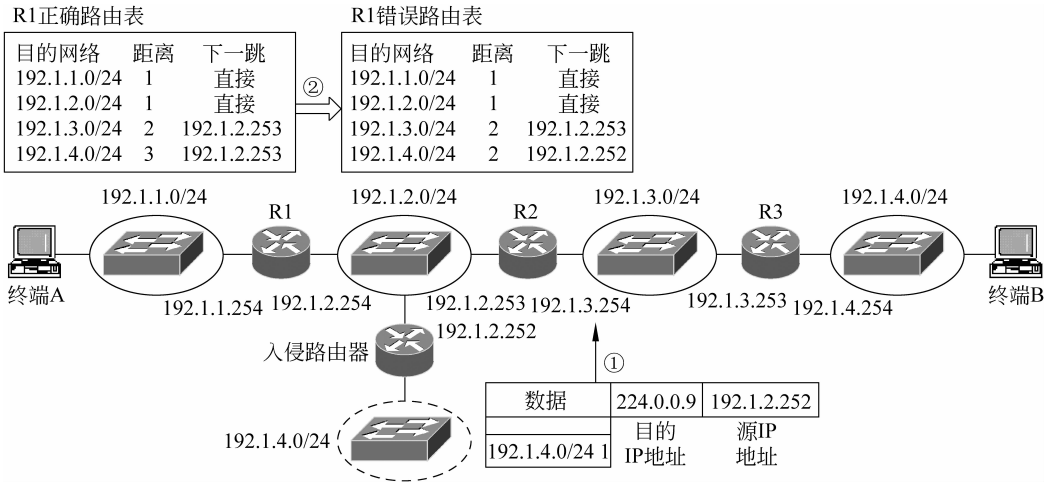

图 3.5　路由项欺骗攻击过程

9. 审计

实现审计一是建立记录网络操作过程的日志文件；二是对日志文件中的每一项记录进行分析，找出可能已经发生的网络攻击行为；三是改进网络安全策略，以应对网络面临的安全威胁。

10. DNS Sec 和应用层安全协议

如果用户得到的某个完全合格域名和 IP 地址之间的绑定关系是伪造的，用户可能被诱骗访问黑客精心设计的网站，并因此泄漏重要的私密信息。防止这种情况发生的措施有两个：一是通过 DNS Sec 对发送解析结果的 DNS 服务器的身份进行鉴别，并对接收到的解析结果进行完整性检测，防止使用黑客伪造或篡改的解析结果；二是通过应用层安全协议对访问的网站的身份进行鉴别，防止被诱骗访问黑客伪造的网站。

3.2　例 题 解 析

3.2.1　自测题

1. 选择题

(1) 下述_____不是黑客成功实施攻击的原因。

A. 主机系统漏洞　　B. 通信协议的安全缺陷

C. 用户警惕性不够　　D. 网络分层结构

(2) 下述_____不是黑客发现主机系统漏洞的步骤。

A. 通过主机扫描发现在线主机

B. 通过端口扫描发现开启的服务

C. 通过主动探测获得操作系统类型和版本号

D. 骗取用户口令

(3) 下述_____是最主要的主机系统漏洞。

A. 缓冲器溢出　　B. Unicode 漏洞　　C. Ping of Death　　D. Land

(4) 下述_____是解决主机系统漏洞的较好办法。

A. 消灭主机系统漏洞

B. 不让黑客知道已经发现的主机系统漏洞

C. 网络隔绝黑客扫描主机系统的途径

D. 将存在漏洞的主机系统和网络断开

(5) 下述_____不是网络中用于隔绝黑客扫描主机系统途径的机制。

A. 接入控制　　B. 网络间信息交换控制

C. 入侵防御系统的异常检测　　D. 主机系统用户登录控制

(6) 下述_____不是对主机系统实施的拒绝服务攻击。

A. Ping of Death　　B. SYN 泛洪

C. Smurf　　D. 穷举法猜测用户登录口令

(7) 缓冲器溢出的最大危害是_____。

A. 使系统崩溃　　B. 使系统运行出错

C. 管理员权限下运行黑客程序　　D. 侵占其他用户内存

(8) SYN 泛洪攻击利用_____。

A. 操作系统漏洞　　B. 通信协议缺陷

C. 缓冲区溢出　　D. 用户警惕性不够

(9) 下述_____是蠕虫病毒传播的主因。

A. 缓冲区溢出漏洞

B. 从服务器下载文件

C. 收发电子邮件

D. 通过移动媒介在主机系统间复制文件

(10) 下述_____不是以破坏信息保密性为目的的攻击行为。

A. 信息嗅探　　B. 信息截获　　C. 安装后门程序　　D. DDoS

(11) 下述_____不是以破坏信息完整性为目的的攻击行为。

A. 信息嗅探　　B. 信息截获

C. 路由项欺骗攻击　　D. ARP 欺骗攻击

(12) 下述_____不是以破坏信息可用性为目的的攻击行为。

A. Ping of Death　B. SYN 泛洪　　C. 安装后门程序　　D. DDoS

(13) 下述_____攻击行为与主机系统漏洞无关。

A. Ping of Death　B. Land　　C. 安装后门程序　　D. Smurf

(14) 安装主机入侵防御系统,对下述_____攻击行为作用不大。

A. 窃取信息资源　B. 篡改注册表　　C. 安装后门程序　　D. Smurf

(15) 安装网络入侵防御系统,对下述_____攻击行为作用不大。

A. 信息嗅探　　B. 利用缓冲区溢出运行黑客程序

C. 安装后门程序　　C. Smurf

(16) 防火墙实施的网络间信息交换控制，对下述_____攻击行为作用不大。

A. ARP 欺骗　　B. 木马外泄信息资源

C. Ping of Death　　D. SYN 泛洪

(17) 交换机提供的安全技术，对下述_____攻击行为作用不大。

A. ARP 欺骗　　B. 源 IP 地址欺骗

C. 伪造 DHCP 服务器　　D. Ping of Death

2. 填空题

(1) 主机系统漏洞是_____，黑客利用某个主机系统存在的漏洞实施攻击需要完成_____、_____、_____和_____ 4 个步骤。

(2) 缓冲器溢出是最严重的主机系统漏洞，黑客可以利用缓冲器溢出_____，这是蠕虫病毒快速传播的主因。

(3) _____、_____、_____和_____属于 DoS，其中，_____和_____是利用主机系统漏洞实现的。

(4) ARP 欺骗、DNS 欺骗、伪造 DHCP 服务器、源 IP 地址欺骗和路由项欺骗等攻击行为中交换机安全技术能够解决的有_____、_____和_____，路由器安全技术能够解决的有_____和_____。

(5) 网络中信息资源分为存储在主机系统中的信息资源和经过网络传输的信息资源两大类，_____、_____和_____等手段非法窃取存储在主机系统中的信息资源，_____、_____和_____等手段非法窃取经过网络传输的信息资源。

(6) 阻止黑客完成对主机系统实施攻击所需的 4 个步骤的网络安全技术有_____、_____和_____，其中_____阻止黑客终端接入网络，_____阻止黑客终端向主机系统传输与实施攻击有关的信息流，_____能够发现黑客正在进行的攻击行为并予以反制。

3. 名词解释

____ DoS　　____ DDoS

____伪造 DHCP 服务器　　____ DNS 欺骗

____ Smurf　　____ Ping of Death

____ SYN 泛洪　　____ Land

____ ARP 欺骗　　____源 IP 地址欺骗

____ Unicode 漏洞　　____路由项欺骗

____信息嗅探　　____信息截获

____缓冲器溢出　　____字典攻击

(a) 通过破坏，或者过度消耗主机系统和网络的资源，使得主机系统和网络无法提供正常服务的一种攻击行为。

(b) 从控制的多个主机系统同时向某个目标主机发起拒绝服务攻击的行为。

(c) 通过发送大量以网络中本不存在的 IP 地址为源地址的建立 TCP 连接请求，使得服务器 TCP 会话表被大量未完成的 TCP 连接占用，以至于无法响应正常的 TCP 连接

请求的攻击行为。

(d) 通过向目标主机发送大量以目标主机的 IP 地址为源地址的 TCP 连接请求,使得目标主机的 TCP 会话表被大量这样的 TCP 连接长期占用,以至于无法响应正常的 TCP 连接请求的攻击行为。

(e) 通过发送以目标主机 IP 地址为源地址、以某个大型网络的直接广播地址为目的地址的 ICMP ECHO 请求报文,使得大型网络中的每一个主机系统都向目标主机发送 ICMP ECHO 响应报文,并因此阻塞大型网络与目标主机之间的通路,使得目标主机无法接收发送正常报文的一种攻击行为。

(f) 一种因为分片后各段数据长度之和超过 64KB,使得接收端拼装数据时发生缓冲区溢出,并使接收端系统崩溃的攻击行为。

(g) 一种通过在 ARP 报文中给出错误的 IP 地址和 MAC 地址之间的绑定关系,使得路由器和主机系统错误地将主机系统 X 对应的 MAC 地址作为发送给主机系统 Y 的 MAC 帧的目的 MAC 地址的一种攻击行为。

(h) 一种不以发送者的 IP 地址,而以其他主机系统的 IP 地址,或者网络中不存在的 IP 地址作为 IP 分组源 IP 地址的攻击行为。

(i) 一种通过将配置错误的默认网关地址和 DNS 服务器地址的伪造的 DHCP 服务器接入网络,使得网络内的主机系统获得该伪造的 DHCP 服务器提供的错误的网络配置信息的攻击行为。

(j) 一种将错误的 IP 地址作为某个域名的解析结果的攻击行为。

(k) 一种虽然窃取经过网络传输的信息,但不影响信息传输过程的攻击行为。

(l) 一种截获经过网络传输的信息,使信息无法继续正常传输的攻击行为。

(m) 一种使得某个进程接收的信息超出分配给该进程的缓冲器容量,并使超出部分的信息覆盖分配给其他进程的缓冲器空间的攻击行为。

(n) 一种将一切可能成为口令的字符串集合作为字典文件,并用程序自动地逐个尝试字典文件中的字符串登录目标主机的攻击行为。

(o) 一种直接用 Unicode 输入禁止输入的字符串模式的攻击行为。

(p) 一种通过发送错误的路由消息或链路状态信息,使得路由器生成错误的通往某个目的网络的传输路径的攻击行为。

4. 判断题

(1) 操作系统和应用程序漏洞是可以消除的。

(2) 针对主机系统漏洞实施的攻击是无法防御的。

(3) 在被攻击前,通过补丁软件消除某个已经发现的漏洞是一种有效的抵御攻击的手段。

(4) 在无数漏洞中,缓冲器溢出漏洞是危害较大的一种漏洞。

(5) 缓冲器溢出漏洞是蠕虫得以快速传播的主因。

(6) Smurf 这样的拒绝服务攻击是无法防御的。

(7) 黑客攻击过程和正常访问过程是有所区别的,只是这种区别不是黑白那样分明。

(8) 网络设备本身也是黑客的攻击目标,需要重点保护。

(9) 黑客实施攻击需要具备多项条件,网络安全技术可以阻止这些条件成立。

(10) 只要目的 IP 地址正确,IP 分组能够到达目的终端。

(11) 单一网络安全技术的作用有限。

3.2.2　自测题答案

1. 选择题答案

(1) D,分层是复杂系统的有效设计方法,能够提高系统的可靠性和安全性。

(2) D,这一项和主机系统漏洞无关。

(3) A,黑客利用缓冲器溢出漏洞能够实现在管理员权限下运行自编程序,这一点对主机系统的危害极大。

(4) C,其他三项中,A 和 B 项做不到,D 项是笨办法。

(5) D,登录的前提是已经建立黑客和主机系统之间的传输通路。

(6) D,拒绝服务攻击是使主机系统丧失服务能力,D 项不会使主机系统崩溃。

(7) C,管理员权限下运行黑客程序,可以任意处理系统资源。

(8) B,TCP 连接建立过程存在缺陷。

(9) A,黑客利用缓冲器溢出漏洞实现在管理员权限下运行自编程序是蠕虫能够自动传播并激活的基础。

(10) D,拒绝服务攻击一般以破坏可用性为目的。

(11) A,破坏信息完整性首先需要截获信息,然后篡改信息。

(12) C,后门程序为了隐蔽,一般不会影响主机系统正常服务功能。

(13) D,这种拒绝服务攻击是任何主机系统自身无法抵御的。

(14) D,加强主机系统自身功能对抵御这种拒绝服务攻击是徒劳的。

(15) A,网络入侵防御系统需要发现异常信息流,然后才能对异常信息流实施干预,信息嗅探攻击不会导致信息流异常。

(16) A,ARP 欺骗攻击在网络内部进行,无需经过防火墙。

(17) D,这项攻击需要拼装完分片后产生的所有数据片才能发现,交换机一般不具有这项功能。

2. 填空题答案

(1) 无法消除的,信息收集,扫描,渗透,攻击。

(2) 在管理员权限下运行自编程序。

(3) Ping of Death,SYN 泛洪,Land,Smurf,Ping of Death,Land。

(4) ARP 欺骗,伪造 DHCP 服务器,源 IP 地址欺骗,源 IP 地址欺骗,路由项欺骗。

(5) 木马,非法登录主机系统,利用缓冲器溢出漏洞在管理员权限下运行黑客程序,ARP 欺骗,路由项欺骗,交换机间插入集线器嗅探信息。

(6) 交换机接入控制技术,防火墙,网络入侵防御系统,交换机接入控制技术,防火墙,网络入侵防御系统。

3. 名词解释答案

a DoS	b DDoS
i 伪造 DHCP 服务器	j DNS 欺骗
e Smurf	f Ping of Death
c SYN 泛洪	d Land
g ARP 欺骗	h 源 IP 地址欺骗
o Unicode 漏洞	p 路由项欺骗
k 信息嗅探	l 信息截获
m 缓冲器溢出	n 字典攻击

4. 判断题答案

(1) 错,目前软件设计方法下,消除漏洞是无法实现的。

(2) 错,黑客攻击某个主机系统首先需要建立与该主机系统之间的传输通路,然后发现该主机系统存在的漏洞,并针对该漏洞实施攻击,网络安全技术可以阻止黑客完成上述的每一个步骤。

(3) 对,这样可以防止黑客针对该漏洞实施的攻击。

(4) 对,黑客能够利用缓冲器溢出漏洞在管理员权限下运行自编程序。

(5) 对,利用缓冲器溢出漏洞在管理员权限下运行自编程序是蠕虫自动传播和激活的技术基础。

(6) 错,交换机和路由器防御源 IP 地址欺骗攻击的安全技术与最后一跳路由器过滤掉以直接广播地址为目的地址的 IP 分组的过滤技术都是有效防御手段。

(7) 对,这是网络入侵防御系统既是防御黑客攻击的有效手段,但又不能完全消除黑客攻击的原因。

(8) 对,被黑客控制网络设备的后果是无法想象的。

(9) 对,网络安全技术对防御黑客攻击是有所作为的。

(10) 错,有太多的原因不能使目的地址正确的 IP 分组到达正确的目的终端。

(11) 对,每一种网络安全技术有着适用范围和局限。

3.2.3 简答题解析

1. 黑客能够成功入侵主机系统的原因及应对策略。

回答:原因在于:一是基于当前的软件设计理论和方法,从根本上消除大型软件(操作系统和大型的应用程序)的漏洞是不可能的;二是随着时间的推移,使用的用户增多,漏洞终将被发现,还有一些组织和机构专门研究流行操作系统和应用程序的漏洞,并公开研究结果;三是一旦发现漏洞,就会出现针对该漏洞的攻击软件,并流行开来;四是只要某个主机系统还没有用补丁软件修补该漏洞,黑客就可通过针对该漏洞的攻击软件对该主机系统实施攻击。

应对策略分为以下三个方面:

一是黑客成功攻击某个主机系统的步骤包括:①建立与该主机系统之间的传输通路。②通过扫描发现该主机系统的操作系统或应用程序存在漏洞且没有用补丁软件修