第3章 网络攻击技术

【本章学习目标】

- 了解黑客概念和黑客分类
- 掌握网络攻击的定义
- 理解黑客攻击步骤
- 掌握代理跳板的原理和方法
- 了解信息搜集的种类
- 掌握网络扫描的步骤
- 掌握操作系统探测技术原理
- 了解各种网络攻击方法
- 掌握 DDoS 攻击原理与防御方法

3.1 黑　　客

3.1.1 黑客概念

黑客是 Hacker 的音译，源于动词 Hack，其引申意义是“干了一件非常漂亮的事”。在这里我们所说的黑客是指那些精于某方面技术的人。对于计算机而言，黑客就是精通网络、系统、外设以及软硬件技术的人。

黑客最早出现于 20 世纪 50 年代，最早的计算机于 1946 年在宾夕法尼亚大学诞生，而最早的黑客出现于麻省理工学院。最初的黑客是一些高级技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。但到了今天，黑客一词已被泛指那些专门利用计算机搞破坏或恶作剧的家伙，对这些人的正确叫法是 Cracker，有人也翻译成骇客或是入侵者。

3.1.2 黑客分类

第一种分类是将黑客分为破坏者、红客和间谍，如图 3-1 所示。

(1) 破坏者：以破坏为主的黑客。

(2) 红客：红客一词比较容易理解，有很强的政治性，红客的行为旨在抗击外来网络入侵，维护国内网络安全，有很强的爱国色彩。

(3) 间谍：专门为了利益而去做一些破坏或窃取一些信息。

第二种分类是将黑客分为白帽子、黑帽子和灰帽子。

(1) 白帽子：是创新者。研究漏洞，追求先进技术并与大家共享的黑客称为“白帽子”。

(2) 黑帽子：是破坏者。以破坏和入侵为目的的黑客称为“黑帽子”。

(3) 灰帽子：是破解者。介于以上二者之间的叫作“灰帽子”，这是一个追求网上信息公开的群体，他们不破坏，但要进入别人的网站读取信息。

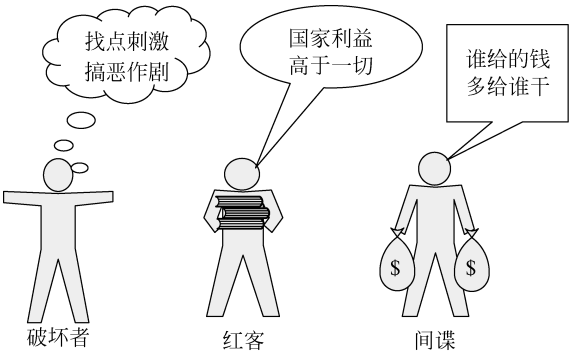


图 3-1　黑客分类

3.1.3　黑客行为发展趋势

黑客行为有以下 7 个方面的发展趋势。

(1) 手段高明化：综合各种流行的攻击方法，技巧性更强，更容易得手。例如，guest 账户显示为禁用状态，但能用其登录而且拥有管理员权限，这就用到了留后门的方法，如果管理员不知道这种黑客手段，就很难发现已被入侵。

(2) 活动频繁化：黑客行为将越来越频繁，查看一台刚刚启动几分钟的服务器，就可在它的各种日志中发现黑客攻击的痕迹。

(3) 动机复杂化：黑客行为的动机也更加复杂，有政治目的、个人目的和商业目的等。

(4) 黑客年轻化：由于互联网的普及，形成全球一体化，甚至很多偏远地区也可以从网络上接触到世界各地的信息资源，所以越来越多对黑客攻击感兴趣的中学生也已经踏足到这个领域。

(5) 破坏力扩大化：因互联网的普及，电子商务也在蓬勃发展，全社会对互联网的依赖性日益增强，黑客的破坏力也日益扩大化。仅在美国，黑客每年造成的经济损失就超过 100 亿美元。

(6) 黑客技术普及化：黑客组织的形成和黑客傻瓜式工具的大量出现导致的一个直接后果就是黑客技术的普及。在互联网上，传授黑客技术的站点比比皆是，这些黑客站点提供黑客工具，公布系统漏洞，公开传授黑客技术，进行黑客教学，甚至还提供网上论坛、网上聊天工具以相互交流黑客技术经验，协调黑客行动。黑客事件的剧增，黑客组织规模的扩大，黑客站点的大量涌现，也说明了黑客技术开始普及，甚至很多十几岁的年轻人也有了自己的黑客站点，从很多论坛上可以看到学习探讨黑客技术的人也越来越多。

(7) 黑客组织化：因为利益的驱使，黑客开始由原来的独立个体变成有组织的黑客群体，在黑客组织内部，成员之间相互交流技术经验，共同采取黑客行动，行动的成功率增高，影响力也更大。

3.2 网络攻击概述

3.2.1 网络攻击定义

网络攻击是对网络系统的机密性、完整性、可用性等产生危害的行为。实际上，网络攻击是黑客利用被攻击方网络系统自身存在的漏洞，通过使用网络命令和专用软件侵入其网络系统实施的攻击。

3.2.2 网络攻击分类

X.800 和 RFC 2828 对网络攻击进行了分类。它们把攻击分为两类：被动攻击和主动攻击。被动攻击试图获得或利用系统的信息，但不会对系统的资源造成破坏。而主动攻击则不同，它试图破坏系统的资源，影响系统的正常工作。

1. 被动攻击

被动攻击的特性是对所传输的信息进行窃听和监测，攻击者的目标是获得线路上所传输的信息。窃听攻击和流量分析就是两种被动攻击的例子。

(1) 窃听攻击。如图 3-2 所示，电子邮件和传输的文件中都可能包含敏感或秘密信息，攻击者通过窃听，可以截获这些敏感或秘密信息，网络管理人员的工作就是阻止攻击者获得这些信息。

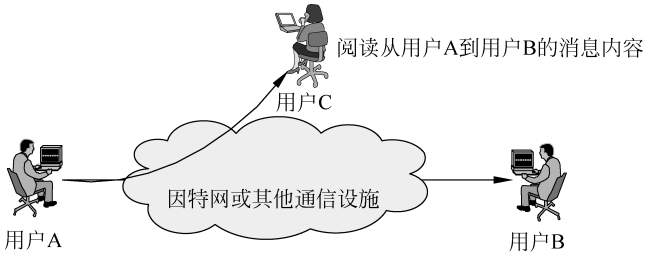


图 3-2 窃听攻击

(2) 流量分析。如图 3-3 所示，假设已经采取了某种措施来隐藏消息内容或其他信息的流量，使攻击者即使捕获了消息也不能从中发现有价值的信息。加密是隐藏消息的常用方法，即使对消息进行了合理的加密保护，攻击者仍然可以通过流量分析获得这些消息的模式。攻击者可以通过确定主机的身份及其所处的位置，观察传输消息的频率和长度，然后根据所获得的信息推断本次通信的性质。

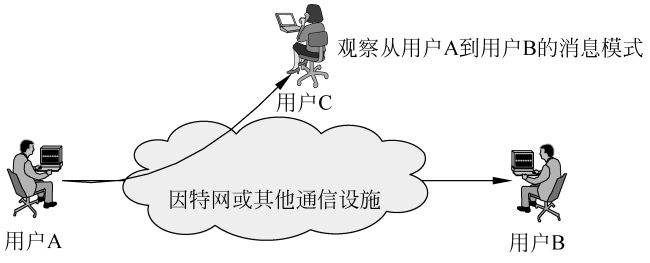


图 3-3 流量分析

由于被动攻击不涉及对数据的更改，所以很难被察觉。通过采用加密措施，完全有可能阻止这种攻击。因此，处理被动攻击的重点是预防，而不是检测。

2. 主动攻击

主动攻击是指恶意篡改数据流或伪造数据流等攻击行为，它一般分为以下 4 类。

(1) 伪装攻击。伪装攻击是指某个实体假装成其他实体，对目标发起攻击，如图 3-4 所示。例如，攻击者捕获认证信息，然后将其重发，这样攻击者就有可能获得其他实体所拥有的访问权限。

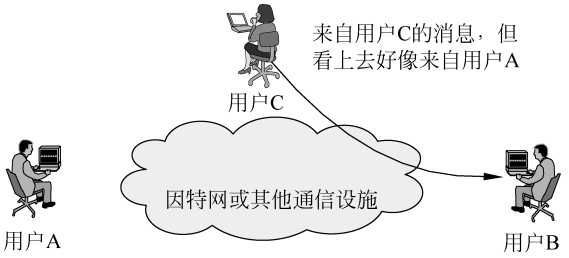


图 3-4　伪装攻击

(2) 重放攻击。重放攻击是指攻击者为了达到某种目的，将获得的消息再次发送，以在非授权的情况下进行传输，如图 3-5 所示。

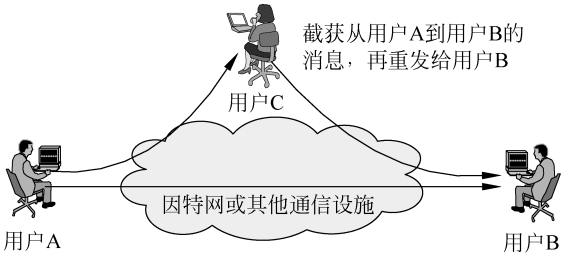


图 3-5　重放攻击

(3) 消息篡改。消息篡改是指攻击者对所获得的合法消息中的一部分进行修改或延迟消息的传输，以达到其非授权的目的，如图 3-6 所示。

图 3-6　消息篡改

(4) 拒绝服务攻击。拒绝服务攻击是指阻止或禁止人们正常使用网络服务或管理通信设备，如图 3-7 所示。

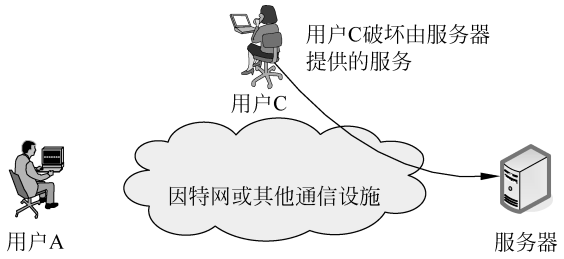


图 3-7　拒绝服务攻击

主动攻击与被动攻击相反，被动攻击虽然难以检测，但采取某些安全防护措施就可以有效阻止；主动攻击虽然易于检测，但却难以阻止。所以对付主动攻击的重点应当放在如何检测并发现它们上，并采取相应的应急响应措施，使系统从故障状态恢复到正常运行。

3.2.3　网络攻击五部曲

一次成功的入侵攻击，可以归纳成基本的 5 个步骤，即人们常说的“网络攻击五部曲”，如图 3-8 所示，具体步骤和顺序可根据攻击时的实际情况随时进行调整。

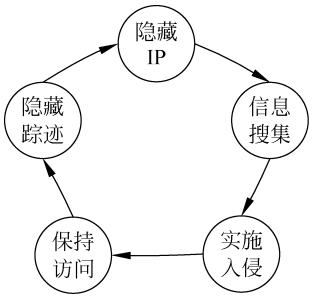


图 3-8　网络攻击五部曲

1. 隐藏 IP

当入侵者找到远程主机/服务器的系统缺陷后，会对其进行试探性的入侵，此时，入侵者将要面对的可能是缺乏经验的个人计算机用户，也可能是网络安全专家，或是对方布下的一个网络陷阱。所以，对于有经验的入侵者，他们会在入侵时步步小心，使用各种方法来隐藏自己，尽量不去直接与目标接触，以免暴露给远程主机/服务器。

2. 信息搜集

信息搜集俗称踩点，就是通过各种途径对所要攻击的目标进行多方面的了解。

3. 实施入侵

入侵者得到管理员权限，连接到远程计算机，对其进行控制，达到自己攻击的目的。

4. 保持访问

入侵者为了保持长期对胜利果实的访问权，在已经攻破的计算机上种植一些供自己访问的后门。

5. 隐藏踪迹

一次成功的入侵，一般会在对方的计算机上存储相关的登录日志，这样就容易被管理员发现。在入侵完毕后需要清除登录日志及其他相关的日志。

3.3　隐 藏 IP

任何攻击者都不希望自己的攻击行为被暴露，所以在实施攻击之前的首要任务是隐藏自己的 IP 地址。

通常有以下两种方式可以实现隐藏 IP 地址的效果。

(1) IP 欺骗。利用别人的主机(俗称“肉鸡”)进行攻击,也就是说黑客首先登录到一个第三方的主机,然后再对目标进行攻击,这样一旦被发现,被攻击者也只能得到那台“肉鸡”的 IP。

(2) 网络代理跳板。做多级跳板代理,这样在被攻击者的主机上留下的将是代理跳板主机的 IP 地址。

3.3.1 IP 欺骗

1. IP 欺骗概述

所谓 IP 欺骗,就是伪造某台主机的 IP 地址的技术,其实质是让一台主机扮演另一台主机,以达到隐藏自己的目的。IP 欺骗通常要通过编写程序来实现,IP 欺骗者通过使用 RAW Socket 编程,发送带有假冒的源 IP 地址的 IP 数据报,来达到自己的目的。另外,网络上也有大量可以发送伪造的 IP 地址的工具,使用这些工具可以任意指定源 IP 地址,以免留下自己的痕迹。

IP 是网络层的一个面向无连接的协议,IP 数据报的主要内容由源 IP 地址、目的 IP 地址和所传数据构成,IP 的任务就是根据每个数据报文的目的地址,路由完成报文从源地址到目的地址的传送。至于报文在传送过程中是否丢失或出现差错,IP 不会考虑,对 IP 来讲,源设备与目的设备没有什么关系,它们是相互独立的。IP 包只是根据数据报文中的目的地址发送,因此借助高层协议的应用程序来伪造 IP 地址是比较容易实现的。

在 IP 欺骗的状态下,三次握手的情况如下。

第一步:黑客假冒主机 A 的 IP 向服务方主机 B 发送 SYN,告诉主机 B 是它所信任的主机 A 想发起一次 TCP 连接,序列号为数值 X,这一步实现比较简单,黑客将 IP 包的源地址伪造成主机 A 的 IP 地址即可。

要注意的是,在攻击的整个过程中,必须使主机 A 与网络的正常连接中断。因为 SYN 请求中 IP 包源地址是主机 A 的,当主机 B 收到 SYN 请求时,将根据 IP 包中源地址反馈 ACK SYN 给主机 A,但事实上主机 A 并未向主机 B 发送 SYN 请求,所以主机 A 收到后会认为这是一次错误的连接,从而向主机 B 回送 RST,中断连接。为了解决这个问题,在整个攻击过程中需要设法停止主机 A 的网络功能,使之拒绝服务即可。

第二步:服务方主机 B 产生 SYN ACK 响应,并向请求方主机 A(注意:是主机 A,不是黑客,因为主机 B 收到的 IP 包的源地址是主机 A)发送 ACK,ACK 的值为 X+1,表示数据成功接收到,且告知下一次接收到字节的 SEQ 是 X+1,同时,主机 B 向请求方主机 A 发送自己的 SEQ,注意这个数值对黑客是不可见的。

第三步:黑客再次向服务方发送 ACK,表示接收到服务方的回应。虽然实际上它并没有收到服务方主机 B 的 SYN ACK 响应,这次它的 SEQ 值为 X+1,同时它必须猜出 ACK 的值,并加 1 后回馈给主机 B。

如果黑客能成功地猜出主机 B 的 ACK 的值,那么 TCP 的三次握手就宣告成功,主机 B 会将黑客看作主机 A。黑客主机这种连接是“盲人”式的,黑客永远不会收到来自主机 B 的包,因为这些反馈包都被路由到主机 A 那里了。

由三次握手我们可以看出,IP 欺骗的关键在于猜出在第二步服务方所回应的 SEQ 值,有了这个值,TCP 连接方可成功地建立。在早期,这是个令人头疼的问题,但随着 IP 欺骗攻击手段的研究日益深入,一些专用的算法得到应用,并产生了一些专用的 C 程序,如

SEQ-Scan 等，当黑客使用这些 C 程序时，一切问题均可迎刃而解。

2. IP 欺骗的防备

1）防备网络外部的欺骗

对于来自网络外部的欺骗，阻止这种攻击的方法是很简单的。在局部网络的对外路由器上加一个限制条件，设置不允许声称来自于内部网络的外来包通过即可。尽管路由器可以通过分析测试源地址来解决 IP 欺骗中的一般问题，但是如果网络还存在外部的可信任主机，那么路由器就无法防止别人冒充这些主机而进行 IP 欺骗。

2）监视网络

通过对信息包的监控来检查 IP 欺骗这种攻击将是非常有效的方法。使用 NETLOG 等信息包检查工具对信息的源地址和目的地址进行检查，如果发现了信息包来自两个以上不同的地址，即说明系统有可能受到 IP 欺骗，防火墙外面正有黑客试图入侵系统。

3）安装过滤路由器

检测和保护站点免受 IP 欺骗的最好方法是安装一个过滤路由器，来限制对外部接口的访问，禁止带有内部网络资源地址包的通过。当然也应禁止（过滤）带有不同内部资源地址的内部包通过路由器到外部网络上去，这样即可防止内部用户对别的站点进行 IP 欺骗。

3.3.2 网络代理跳板

当从本地入侵其他主机时，自己的 IP 会暴露给对方，通过将某一台主机设置为代理，通过该主机再入侵其他主机，就会留下代理的 IP 地址，这样可以有效地保护自己的安全。这种二级代理的基本结构如图 3-9 所示。

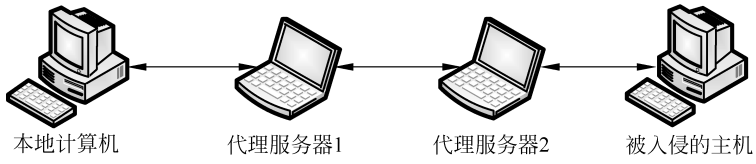


图 3-9　二级代理的基本结构

本地计算机通过两级代理入侵某一台主机，这样在被入侵的主机上，不会留下自己的信息。可以选择更多的代理级别，但是考虑到网络带宽的问题，一般选择两级或三级代理比较合适。能否被选择做代理主机有一个首要条件，即必须先安装相关的代理软件，一般是将已经入侵的主机作为代理服务器。

3.4 网络扫描

3.4.1 网络扫描概述

在攻击者对特定的网络资源进行攻击之前，他们需要了解将要攻击的环境，这需要搜集、汇总各种和目标系统相关的信息，包括主机数目、类型、操作系统等。

网络扫描技术是一种重要的网络安全技术。扫描本身不算一种攻击行为，但是它常常可以作为攻击发起前的准备工作。扫描器能够自动检测远程或本地主机的安全性弱点，发现远程服务器各种 TCP 端口的分配、提供的服务及相应的软件版本，记录目标给予的回答，

搜集关于目标主机的各种有用信息。扫描器可以帮助发现目标主机存在的一些问题，而这些问题可能恰恰就是黑客攻击的关键点。

反之，网络管理员同样可以利用安全扫描技术与防火墙、入侵检测系统互相配合，有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评价网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说防火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，可以有效避免黑客攻击行为，做到防患于未然。

3.4.2 网络扫描步骤

一次完整的网络扫描分为以下三个阶段。

(1) 第一阶段：发现目标主机或网络。

(2) 第二阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

(3) 第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

网络扫描技术包括：Ping 扫射、操作系统探测、端口扫描及漏洞扫描等。这些技术在网络扫描的三个阶段中各有体现。

1. Ping 扫射技术

Ping 扫射技术用于网络安全扫描的第一阶段，可以帮助我们识别系统是否处于活动状态。在公司里，一天中的不同时间有不同的主机在活动，攻击者想知道哪些主机是活动的，哪些不是，他们一般在白天寻找活动的主机，然后在深夜再次查找，这样就能区分工作站和服务器。

2. 操作系统探测技术

操作系统探测技术用于网络安全扫描的第二阶段，攻击者已知哪些主机是活动的，下一步要识别每台主机运行哪种操作系统。因为对于不同类型的操作系统，其上的系统漏洞有很大区别，甚至同一种操作系统的不同版本的系统漏洞也是不一样的，所以攻击的方法也完全不同。

操作系统探测技术的原理是不同的操作系统在网络底层协议的各种实现细节上略有不同，扫描程序通过向远程主机发送不平常的或者没有意义的数据包来进行探测，因为这些数据包 RFC 在互联网标准中没有列出，每个操作系统对它们的处理方法不同，扫描程序通过解析输出，能够弄清自己正在访问的设备运行的是何种操作系统。

3. 端口扫描技术

端口扫描技术同样用于网络安全扫描的第二阶段，端口扫描是通过与目标系统的 TCP/IP 端口连接，查看该系统处于监听或运行状态的服务。

端口扫描也是一种获取主机信息的有效方法。在 UNIX/Linux 系统中，任何用户均可使用端口扫描程序而不需要 root 权限。从扫描的端口数目和端口号可以判断出目标主机运行的操作系统，通过收集扫描的信息，能够轻松地掌握局域网络的构造。表 3-1 所示为一些常用端口号和对应服务的对照表，不过应该认识到，这种对应仅仅是约定，并没有严格的规范进行约束，特别是对于高于 1024 的端口。

1）端口分类

（1）熟知端口号：由因特网指派名字和号码，公司负责分配给一些常用的应用层程序固定使用，其数值一般为0～1023。

（2）一般端口号：用来随时分配给请求通信的客户进程。

表3-1　常用服务端口对照表

服　务	端　口	服　务	端　口
socks	1080/tcp	wins	1512/tcp
socks	1080/udp	nfs	2049/tcp 2049/udp
mysql	3306/tcp 3306/udp	gopher	70/tcp 70/udp
netstat	15/tcp	finger	79/tcp 79/udp
linuxconf	98/tcp	http	80/tcp 80/udp
rndc	953/tcp 953/udp	pop3	110/tcp 110/udp
squid	3128/tcp	imap	143/tcp 143/udp
ftp	21/tcp 21/udp	ldap	389/tcp 389/udp
ssh	22/tcp 22/udp	rtsp	544/udp
telnet	23/tcp 23/udp	shell	514/tcp
smtp	25/tcp 25/udp	syslog	514/udp
nameserver	42/tcp 42/udp	uucp	540/tcp

2）端口扫描原理

入侵者如果想要探测目标计算机开放了哪些端口，提供了哪些服务，就需要先与目标端口建立TCP连接，这也就是扫描的出发点。尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复（即三次握手中的第二次），则说明该端口开放，即为“活动端口”。

3）端口扫描原理分类

端口扫描原理分为三类，如图3-10所示，分别为全连接扫描、半连接扫描以及无连接扫描。

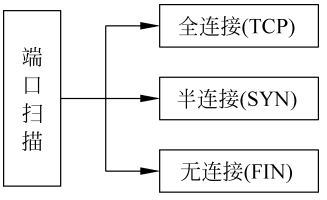


图3-10　端口扫描原理分类

（1）全连接扫描（TCP扫描）：这种扫描方法使用三次握手与目标主机建立标准的TCP连接，即向对方发送一个正常的TCP连接请求，如果存在三次握手，则连接建立。

（2）半连接扫描（SYN扫描）：若端口扫描没有完成一个完整的TCP连接，扫描主机向

目标主机的指定端口发送 SYN 数据段，表示发送建立连接请求。

① 如果目标主机的回应 TCP 报文中 SYN＝1，ACK＝1，说明该端口是活动的，接着扫描主机传送一个 RST 给目标主机拒绝建立 TCP 连接，从而导致三次握手过程的失败。即建立连接时只完成了前两次握手。

② 如果目标主机回应的是 RST，则表示该端口为“死端口”，这种情况下，扫描主机不用做任何回应。

(3) 无连接扫描(FIN 扫描)：依靠发送 FIN 来判断目标主机的指定端口是否活动。发送一个 FIN＝1 的 TCP 报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，当发送 FIN 报文到一个活动的端口时，该报文只是简单的丢掉，不会返回任何回应。从 FIN 扫描可以看出，这种扫描没有涉及任何 TCP 连接部分，因此，这种扫描比前两种都安全，可以称为秘密扫描。

4. 漏洞扫描技术

网络扫描的第三阶段采用的漏洞扫描通常是在端口扫描的基础上，对得到的信息进行相关处理，进而检测出目标系统存在的安全漏洞。

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：

(1) 在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否存在满足匹配条件的漏洞。

(2) 通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱口令等，若模拟攻击成功，则表明目标主机系统存在安全漏洞。

3.5 网络攻击

任何以干扰、破坏网络系统为目的的非授权行为都称为网络攻击。黑客进行网络攻击通常分为三大类型：社会工程学攻击、利用型攻击和拒绝服务型攻击。

1. 社会工程学攻击

社会工程学攻击，是一种利用“社会工程学”来实施的网络攻击行为。社会工程学是利用人的本能反应、好奇心、信任、贪便宜等弱点，使用诸如欺骗、伤害等危害手段，获取自身利益的手法。

2. 利用型攻击

利用型攻击是一类试图直接对用户的主机进行控制的攻击，最常见的利用型攻击有物理攻击、暴力攻击、漏洞攻击、缓冲区溢出攻击和木马攻击。

3. 拒绝服务型攻击

拒绝服务型攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看，拒绝服务型攻击算是一种很简单，但又很有效的攻击方式。它的目的就是拒绝服务访问，破坏系统的正常运行，最终使网络连接堵塞，或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽。

3.5.1 社会工程学攻击

社会工程学攻击是利用人们的心理特征骗取用户的信任，获取机密信息、系统设置等不公开的资料，为黑客攻击和病毒感染创造有利条件。

社会工程学攻击与黑客使用的其他技术具有很大的差别，它所研究的对象不是严谨的计算机技术，而是目标网络的人员。社会工程学主要是利用说服或欺骗的方法来获得对信息系统的访问，这种说服和欺骗通常是通过与人交流或其他互动方式实现的。

近年来，更多的黑客转向利用人的弱点即社会工程学方法来实施网络攻击。利用社会工程学手段突破信息安全防御措施的事件，已经呈现出上升甚至泛滥的趋势。

目前社会工程学攻击主要包括两种方式：打电话和伪造 E-mail。

1. 打电话

在社会工程学攻击中有些黑客冒充失去密码的合法雇员，通过这种简单的方法重新获得密码。

2. 伪造 E-mail

使用 telnet，一个黑客可以截获任何一个身份所发送 E-mail 的全部信息，这样的 E-mail 信息是真的，因为它发自于一个合法的用户。一个冒充系统管理员或经理的黑客可以伪造这些信息显得绝对真实的 E-mail，从而较为轻松地获得大量的信息，实施他们的恶意阴谋。

3.5.2 物理攻击

物理攻击是指通过接触到的设备进行攻击。物理攻击有两种方法。

(1) 管理员离开计算机时，没有加密计算机或者直接把管理员登录的计算机借给他人使用时，别人就可以通过工具软件来获得用户名和密码。

(2) 普通用户通过提升权限，获得与管理员相同的权限，达到长期占有计算机的目的，或通过命令进入到某个计算机后，使用命令新建用户名及密码，并提升权限。

到目前为止，任何操作系统都没有本地安全性可言，当本地接触一台计算机时，不管是什么类型的操作系统，都可以轻易地利用一些工具或者系统的一些特性来登录系统。对物理攻击的防范措施主要有：设定计算机屏保和开机密码；计算机需要借出时应该在监督下使用；以及在其他用户使用完后对系统做详细的检查。

3.5.3 暴力攻击

暴力攻击采用字典穷举法(也称暴力法)来破解用户的密码。字典就是一个文本文件，里面包含了所有可能的密码列表。攻击者可以通过一些工具软件，自动地从字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；如果口令错误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程是由计算机程序来自动完成的，所以几个小时就可以把记录在字典里的数十万单词都尝试一遍。也就是说，只有被破解用户的密码存在于字典中，才会被这种方式所找到。千万不要小看这个看上去守株待兔的方法，由于网络上经常有不同的黑客彼此交换字典，因此一份网上流传的字典通常包含了很多黑客累积的经验，对于安全意识不强的用户，破解率是很高的。

1. 暴力攻击类型

目前常用的暴力破解主要包含以下 4 种类型。

1) 词典攻击

因为多数人使用普通词典中的单词作为口令，发起词典攻击通常是较好的开端。词典

攻击使用一个包含大多数词典单词的文件，用这些单词猜测用户口令。

2）强行攻击

许多人认为如果使用足够长的口令，或者使用足够完善的加密模式，就能有一个攻不破的口令。事实上没有攻不破的口令，这只是个时间问题。如果有速度足够快的计算机能尝试字母、数字、特殊字符等所有的组合，将最终能破解所有的口令。这种类型的攻击方法叫作强行攻击。使用强行攻击，先从字母 a 开始，尝试 aa、ab、ac 等，然后再尝试 aaa、aab……以此类推下去。

3）组合攻击

词典攻击只能发现词典单词口令，但是速度快。强行攻击能发现所有的口令，但是破解时间很长。在公司里，很多管理员要求员工设置口令时使用字母和数字组合，一些员工的对策是在口令后面添加几个数字。如把口令 computer 变成 computer123，实际上这样的口令很弱。有一种攻击使用词典单词，但是在单词尾部串接几个字母和数字，这就是组合攻击。它基本上介于词典攻击和强行攻击之间。图 3-11 是一个简单的组合攻击字典文件。

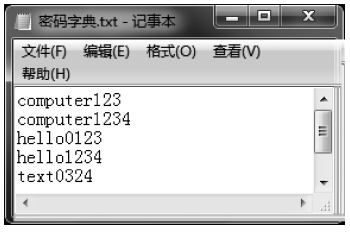


图 3-11　字典文件

4）社会工程学字典攻击

如果黑客从侧面了解到该服务器所属单位的电话号码范围、街道号、门牌号、网络管理员的手机号、生日等，就会以这些数据为基准参数制造黑客字典。因为很多人为了记忆简便，都会利用自己的一些常用信息作为密码，所以就导致了字典攻击的可能性。利用对目标用户本人的了解，可以使用社会工程学来生成字典，再利用该字典进行攻击，这个字典的成功率会比盲目地使用一个字典的成功率高。图 3-12 是一个社会工程学字典生成器主界面。

图 3-12　社会工程学字典生成器主界面

2. 暴力攻击的防御

暴力攻击的防御方法如下：

(1) 不管是服务器还是客户计算机，尽量减少账户的数量；

(2) 所有账户的密码必须足够复杂，一般约定普通客户计算机上的账户密码最小长度为 6 位，服务器上的账户密码最小长度为 8 位；

(3) 密码不要使用与单位或个人有关的信息构成；

(4) 根据现在通用的密码暴力猜测算法，可以反向思考，加大黑客的破解难度，如可以用大写字母开头构造密码，或者以特殊字符开头构造密码；

(5) 密码中不要包含英文单词，英文单词是字典攻击的猜测范围，破解成功率很高；

(6) 密码中不要使用连续的字符或者字母；

(7) 密码必须强行设置策略实现至少 40 天更新一次，更新后的密码与更新前的密码不要类似，更加不要使用曾经使用过的密码；

(8) 设置服务器或者客户计算机的操作系统密码尝试次数。

3.5.4 漏洞攻击

漏洞一词是从英文单词 vulnerability 翻译而来的，原词应译为“脆弱性”，但是中国的技术人员已经更愿意接受“漏洞”这一通俗化的解释。从众多报刊杂志或者网络资源中，人们或许已经对计算机系统的“漏洞”这个概念有了一个感性的理解。确实，这里的“漏洞”并不是一个物理上的概念，它是指计算机系统具有的某种可能被入侵者恶意利用的属性。

简单地说，计算机漏洞是系统的一组特性。恶意的入侵者能够利用这组特性，通过已授权的手段和方式获取对资源的未授权访问，或者对系统造成损害。这里的漏洞既包括单个计算机系统的漏洞，也包括计算机网络系统的漏洞。当系统的某个漏洞被入侵者渗透而造成泄密时，其结果就称为一次安全事件。

1. 存在漏洞的原因

从技术角度而言，漏洞的来源主要有以下几个方面：

(1) 软件或协议设计时的瑕疵。协议定义了网络上计算机会话和通信的规则，如果在协议设计时存在瑕疵，那么无论实现该协议的方法多么完美，它都存在漏洞。

(2) 软件或协议实现中的弱点。即使协议设计得很完美，实现协议的方式仍然可能引入漏洞。

(3) 软件本身的瑕疵。例如，没有进行数据内容和大小的检查，不能正常处理资源耗尽的情况等，攻击者通过渗透这些漏洞，即使不具有特权账号，也可能获得额外的、未授权的访问。

(4) 系统和网络的错误配置。这一类漏洞并不是由协议或软件本身的问题造成的，而是由服务和软件的不正确部署和配置造成的。

2. 公开的计算机漏洞信息

公开漏洞可以促使提供软件或硬件的厂商更快地解决问题，也可以让系统管理员更有针对性地对自己管理的系统进行配置和管理。多年的实践也使人们逐渐认识到，建立在漏洞公开基础之上的安全才是更可靠的安全。因特网上已经有许多关于各种漏洞的描述和与此相关的数据库。下面是一些比较权威的漏洞信息资源。

(1) 通用漏洞和曝光。通用漏洞和曝光(CVE)是一个公共安全漏洞和曝光信息的标准

化名字列表，它致力于为所有公开的漏洞和安全曝光名称制定标准化的工作。CVE是一个字典而不是数据库，它的目标是使不同的漏洞数据库共享数据和搜索信息变得更加容易。目前已经有200多个组织、产品和安全警告提供服务实现了“CVE兼容”。

(2) CERT/CC漏洞信息数据库。CERT/CC漏洞数据库也是一个CVE兼容的数据库。它可以通过名字、ID号、CVE名字、发布日期、严重性等字段检索漏洞信息。

3.5.5 缓冲区溢出攻击

目前最流行的一种攻击技术就是缓冲区溢出攻击。当目标操作系统收到了超过它能接收的最大信息量时，将发生缓冲区溢出。这项攻击对技术要求比较高，但是攻击的过程却非常简单。

1. 缓冲区溢出

缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的空间时，溢出的数据覆盖在合法数据上。理想情况是，程序检查数据长度并且不允许输入超过缓冲区长度的字符串。大多数程序都会假设数据长度总是与所分配的存储空间相匹配，这就为缓冲区溢出埋下了隐患。操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈中，堆栈也会出现缓冲区溢出。

缓冲区溢出的原理很简单，如下所示。

```
void function (char * str)
{
    char buff[16];
    strcpy(buff,str);
}
```

程序中利用strcpy()函数将str中的内容复制到buff中，只要str的长度大于16，就会造成缓冲区溢出，存在类似strcpy()函数这种问题的C语言函数还有很多。

当一个超长的数据进入到缓冲区时，超出部分就会被写入其他缓冲区，其他缓冲区存放的可能是数据、下一条指令的指针或者是其他程序的输出内容，这些内容都被覆盖或者破坏掉了。可见一小部分数据或者一套指令的溢出就可能导致一个程序或者操作系统崩溃。

缓冲区溢出是由编程错误引出的。如果缓冲区被写满，而程序没有去检查缓冲区边界，也没有停止接收数据，这时缓冲区溢出就会发生。缓冲区溢出之所以泛滥，是由于开放源代码程序的本质决定的。标准C语言具有许多复制和添加字符串的函数，这使得标准C语言很难进行边界检查。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误，但是，如果输入的数据是经过黑客精心设计的，覆盖缓冲区的数据恰恰是黑客或者病毒的攻击程序代码，一旦多余字节被编译执行，黑客或者病毒就有可能为所欲为，获取系统的控制权。

2. 缓冲区溢出的防御

缓冲区溢出是目前导致“黑客”型病毒横行的主要原因。从“红色代码”到Slammer，再到“冲击波”，都是利用缓冲区溢出漏洞的典型病毒案例。缓冲区溢出是一个编程问题，防止利用缓冲区溢出发起的攻击，关键在于程序开发者在开发程序时仔细检查溢出情况，不允许数据溢出缓冲区。此外，用户需要经常登录操作系统和应用程序提供商的网站，跟踪公布的

系统漏洞，及时下载补丁程序，弥补系统漏洞。因此，缓冲区溢出的防御方法大致可以划分为以下两类。

(1) 编译时防御，目标是加固程序来抵抗在新程序中的攻击。

编译时防御，是指在进行编译时通过检测程序防止或侦测缓冲区溢出。完成该防御的可能性关键在于选择一种不允许缓冲区溢出的高级语言，鼓励使用安全的编码技术，使用安全的标准库，或者包含用来检测栈帧是否被破坏的附加代码。

(2) 运行时防御，目标是在现有的程序中检测和终止攻击。

就像我们已经注意到的那样，大多数编译时防御的方法需要对现有的程序重新编译。因此，人们有了对运行时防御的兴趣，像操作系统通过更新来对存在漏洞的程序提供保护一样，运行时防御也能如此配置。

3.5.6 木马攻击

木马攻击是黑客最常用的攻击方法，木马的危害性在于它对计算机系统强大的控制和破坏能力，如窃取密码、控制系统操作、进行文件操作等，一台计算机一旦被一个功能强大的木马植入，攻击者就可以像操作自己的计算机一样控制这台计算机，远程监控这台计算机上的所有操作。

木马全称“特洛伊木马”，英文为 Trojan Horse，它来源于古希腊故事。有一次，古希腊大军围攻特洛伊城，久攻不下。于是古希腊谋士献计制造一只高二丈的大木马假装作战神马，随后在攻击数天后假装兵败，留下木马拔营而去。城中得到解围的消息，举城欢庆，并把这个奇异的战利品搬入城内，当全城军民尽入梦乡时，藏于木马中的将士从木马中打开密门而下，打开城门引入外兵，攻下特洛伊城。这就是“特洛伊木马”的来历。计算机界把伪装成良性程序的文件形象地称为“木马”。

木马主要有以下特点。

(1) 伪装性，木马总是伪装成其他程序来迷惑管理员。

(2) 潜伏性，木马能够毫无声响地打开端口等待外部连接。

(3) 隐蔽性，木马的运行隐蔽，甚至使用进程查看器都看不出。

(4) 不易删除，计算机一旦中了木马，最省事的方法就是重装系统。

(5) 通用性，即使远程主机是 Windows 98 系统，入侵者也可以实现远程控制。

木马与后门的区别：本质上，木马和后门都有提供网络后门的功能，但是木马的功能稍微强大一些，一般还有远程控制的功能，而后门程序的功能比较单一，只是方便客户端能够登录对方的主机。

1. 木马分类

常见的木马主要可以分为以下 8 种类型。

1) 破坏型木马

破坏型木马唯一的功能就是破坏并且删除文件，它能自动删除目标计算机上的 DLL、EXE 文件，所以非常危险，一旦被感染就会严重威胁计算机的安全。

2) 密码发送型木马

密码发送型木马是专门为了盗取被感染的计算机上的密码编写的，木马一旦执行，就会自动搜索内存、临时文件夹及各种敏感文件，一旦搜索到有用的密码，木马就会利用免费的

电子邮件服务将密码发送到指定的邮箱，达到获取密码的目的。这类木马大多使用 25 号端口发送 E-mail，它们大多会在每次 Windows 重启时重新运行，其目的是找到所有隐藏密码并且在受害者不知道的情况下把密码发送到指定的邮箱。如果目标计算机有隐藏密码，这些木马是很危险的。

3）远程访问型木马

最有代表性的远程访问型木马是特洛伊木马，如果客户知道了服务端的 IP 地址，只需运行服务端程序就可以实现远程控制。

4）键盘记录木马

这种特洛伊木马是非常简单的，它只做一件事情，就是记录被攻击者的键盘敲击并且在 LOG 文件里查找密码，这种特洛伊木马随着 Windows 的启动而启动。它们分为在线记录和离线记录，分别记录在线和离线状态下敲击键盘时的按键情况。从这些按键中很容易就会得到密码等有用信息，当然对于这种类型的木马，邮件发送功能也是必不可少的。

5）DoS 攻击木马

随着 DoS 攻击应用得越来越广泛，被用作 DoS 攻击的木马也越来越流行起来。当一台计算机被入侵并被种上了 DoS 攻击木马，那么日后这台计算机就成为 DoS 攻击者的最得力的助手了。攻击者控制的“肉鸡”数量越多，发动 DoS 攻击取得成功的概率就越大。所以，这种木马的危害不是体现在被感染的计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

还有一种类似 DoS 攻击的木马称为邮件炸弹木马，一旦计算机被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方瘫痪，不能接受邮件为止。

6）代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的“肉鸡”种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用 Telnet 等程序，从而隐藏自己踪迹。

7）FTP 木马

这种木马可能是最简单和最古老的木马，它的唯一功能就是打开 21 端口，等待用户连接。现在新 FTP 木马还加上了密码功能，因此只有攻击者本人才知道正确的密码，从而进入对方计算机。

8）程序杀手木马

上面的木马功能虽然形形色色，不过要到对方计算机上发挥自己的作用，还要通过防木马软件这一关才行。常见的防木马软件有 ZoneAlarm、Norton Anti-Virus 等。程序杀手木马的功能就是关闭对方计算机上运行的这类程序，让其他的木马更好地发挥作用。

2. 木马连接方式

1）传统连接方式

传统连接方式即 C/S 连接方式，在这种连接方式下，远程主机开放监听端口等待外部连接，成为服务端。当入侵者需要与远程主机建立连接的时候，便主动发出连接请求，从而建立连接，建立过程如图 3-13 所示。

这种连接需要服务端开放端口等待连接，需要客户端知道服务端的 IP 地址与服务端口号。因此，传统连接不适合与动态 IP 地址或局域网内主机建立连接。

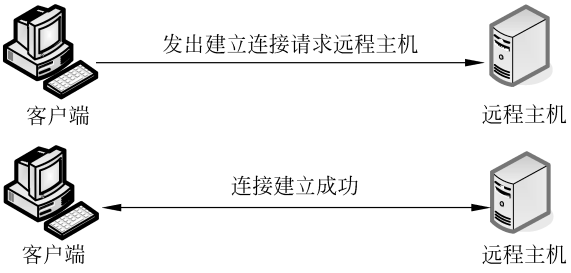


图 3-13　传统连接方式

2）反弹端口连接方式

反弹端口连接方式中连接的建立不再由客户端主动要求连接，而是由服务端来完成，这种连接过程恰恰与传统连接方式相反。当远程主机安装木马后，由远程主机主动寻找客户端建立连接，客户端则开放端口等待连接，具体建立过程如图 3-14 所示。

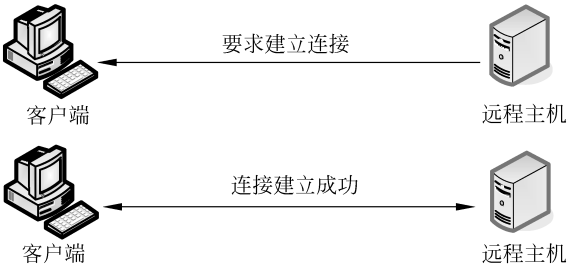


图 3-14　反弹端口连接方式

3. 木马防御

使用以下方法进行防御，基本上可以阻止基于木马的入侵。

1）显示文件扩展名

文件扩展名是文件格式和功能的代表，通过文件扩展名，管理员一眼就能认出文件的真正身份，例如，.exe 代表可执行文件，.jpg 代表图形文件、.txt 代表文本文件，.htm 代表网页文件等。知道了文件的扩展名，再看文件的图标，如果它们之间的对应不一致，如文件扩展名是.exe，但却使用了.jpg 的图标，那么就说明这个文件被修改过，这样的文件大多是木马。

2）不打开任何可疑文件、文件夹、网页

不只是执行扩展名为.exe、.bat 的文件名有被攻击的危险，打开网页和文件夹也都有危险，因此，只有尽量不打开任何可疑文件、文件夹、网页，才能避免被种植木马。

3）升级 IE

很多木马是利用了 IE 的漏洞，所以要经常升级 IE。

4）常开病毒防火墙

由于病毒防火墙比较占系统资源，容易造成系统运行缓慢，因此许多管理员不喜欢开病毒防火墙，而是认为新下载的文件进行病毒扫描就足够了。但是需要注意的是，仅仅使用杀毒软件对文件进行扫描是远远不能实现安全目的的，病毒防火墙能够对系统进行实时监控，及时发现活动的木马并把它杀死。

5）常开网络防火墙

使用网络防火墙并进行相应的设置，这样一来，即使计算机真的中了木马程序，防火墙也可以拦截大多数木马的连接。

3.5.7 拒绝服务攻击

1. DoS 攻击

拒绝服务(Denial-of-Service，DoS)攻击是一种针对某些服务可用性的攻击。从计算机和通信安全的角度讲，DoS 攻击一般攻击目标系统的网络服务，通过攻击其网络连接来实现。这种针对服务可用性的攻击不同于其他传统意义上的不可抗力产生的攻击，它是通过造成 IT 基础设备的损害或毁坏而导致服务能力的丧失。

NIST 计算机安全事故处理指南(NIST Computer Security Incident Handling Guide)中对 DoS 攻击给出的定义如下：拒绝服务是一种通过耗尽 CPU、内存、带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为。

由上述定义可知，可作为 DoS 攻击对象的资源有下面几类。

1）网络带宽

网络带宽与连接服务器和因特网的网络链路的容量相关。对于大部分机构来说，网络带宽指的是连接到其网络服务提供商的链路容量，如图 3-15 给出的网络实例所示。通常这个连接的容量低于 ISP 路由器内部以及 ISP 路由器之间的链路容量，这就意味着可能会发生这样的情况：经过具有更高容量的链路而到达 ISP 路由器的通信量要高于到机构的链路的通信量。在这种情况下，ISP 路由器只能发送链路所能承载的最大流量，对于超出的流量

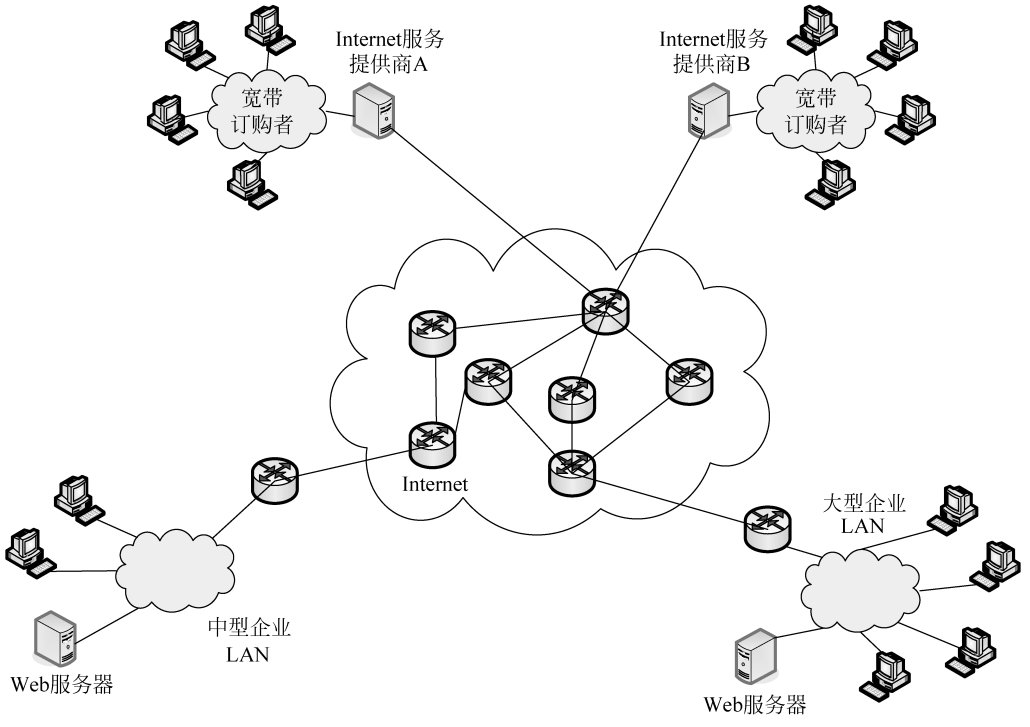


图 3-15　说明 DoS 攻击的网络实例

必须丢弃。在正常网络运行环境下，正常用户的超负荷访问同样会使得服务器网络繁忙。那么这些正常用户当中就会随机地有一部分不能得到服务器的响应，对于一个已经超负荷的 TCP/IP 网络连接来说，服务器不可用也是预料之中的。但在 DoS 攻击的情况下，攻击者直接地或间接地制造出大量的恶意流量发往目标服务器。这种攻击流量相比任何的合法流量来说是压倒性的，从而有效地拒绝了合法用户对服务器的访问。

2）系统资源

针对系统资源的 DoS 攻击，是通过使用某些特殊数据包来触发系统的网络处理软件的缺陷，从而导致系统崩溃。如果受到这种 DoS 攻击，除非管理员重新启动网络处理程序，否则服务器将无法再通过网络处理程序来提供网络服务。例如，经典的死亡之 ping 和泪滴攻击都是这种类型的攻击，它们主要是针对早期的 Windows 9x 操作系统。

3）应用资源

针对特定应用服务程序的攻击一般使用一定数量的合法请求，而每个合法请求都会明显地消耗掉服务器上的系统资源，从而达到限制服务器响应其他合法用户请求的目的。例如，某 Web 服务器可能会提供数据库查询服务，如果能够构造出一个巨大的、高代价的查询请求，那么攻击者就能够向服务器提出大量的这类查询请求。这样就会限制 Web 服务器响应其他合法用户的查询请求。

2. DoS 攻击原理

DoS 攻击的基本原理是使被攻击服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪，而停止提供正常的网络服务。

要对服务器实施拒绝服务攻击，有两种方式：

（1）迫使服务器的缓冲区满载，不接收新的请求；

（2）使用 IP 欺骗，迫使服务器把合法用户的连接复位。影响合法用户的连接，这也是 DoS 攻击实施的基本思想。

为便于理解，介绍一个简单的 DoS 攻击基本过程，如图 3-16 所示。

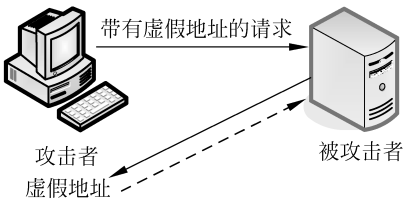


图 3-16　一个简单的 DoS 攻击的基本过程

攻击者先向被攻击者发送众多带有虚假地址的请求，被攻击者发送回复信息后等待回传信息，由于是伪造地址，所以被攻击者一直等不到回传信息，分配给这次请求的资源就始终不被释放。当被攻击者等待一段时间后，连接会因超时被切断，攻击者会再度传送一批伪地址的新请求，这样反复进行，被攻击者的资源将被耗尽，最终导致被攻击者主机瘫痪。

3. DoS 攻击类型

DoS 攻击从攻击目的和手段上主要分为以下一些类型，它们以不同的方式对目标网络造成破坏。

1）带宽耗用 DoS 攻击

最阴险的 DoS 攻击是带宽耗用攻击。它的本质就是攻击者消耗掉通达某个网络的所有可用的带宽。这种攻击可以发生在局域网上，不过更常见的是攻击者远程消耗资源。为了达到这一目的，一种方法是攻击者通过使用更多的带宽造成受害者网络的拥塞，另一种方

法是攻击者通过征用多个站点，集中拥塞受害者的网络连接来达到 DoS 攻击效果。

2）资源衰竭 DoS 攻击

资源衰竭攻击与带宽耗用攻击的差异在于前者集中于系统资源的消耗而不是网络资源的消耗。一般来说，它涉及诸如 CPU 利用率、内存、文件系统和系统进程总数之类系统资源的消耗。攻击者往往拥有一定数量系统资源的合法访问权，然后，攻击者会滥用这种访问权消耗额外的资源，这样，系统或合法用户被剥夺了原来享有的资源，造成系统崩溃或可利用资源耗尽。

3）编程缺陷 DoS 攻击

部分 DoS 攻击并不需要发送大量的数据包来进行攻击。编程缺陷攻击就是利用应用程序、操作系统等在处理异常条件时的逻辑错误实施的 DoS 攻击。攻击者通常向目标系统发送精心设计的畸形分组来试图导致服务的失效和系统的崩溃。

4）基于路由的 DoS 攻击

在基于路由的 DoS 攻击中，攻击者操纵路由表项以拒绝向合法系统或网络提供服务。诸如路由信息协议和边界网关协议之类较早版本的路由协议没有或只有很弱的认证机制，这就给攻击者变换合法路径提供了良好的前提，它们往往通过假冒源 IP 地址就能创建 DoS 攻击。这种攻击的后果是受害者网络的分组经由攻击者的网络路由，或者被路由到不存在的黑洞网络上。

5）基于 DNS 的 DoS 攻击

基于 DNS 的攻击与基于路由的 DoS 攻击类似。大多数的 DNS 攻击会将虚假的地址信息发送给受害者的域名服务器高速缓存，这样，当用户请求某 DNS 服务器执行查找请求的时候，攻击者就达到了把它们重定向到自己喜欢的站点上的效果。

4. 分布式拒绝服务攻击

DDoS 全名是 Distributed Denial of Service（分布式拒绝服务攻击），很多 DoS 攻击源一起攻击某台服务器就组成了 DDoS 攻击，DDoS 最早可追溯到 1996 年最初，在中国开始频繁出现于 2002 年，2003 年已经初具规模。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这种攻击来势迅猛，令人难以防备，且具有较大的破坏性。

一个比较完善的 DDoS 攻击体系分成 4 大部分，如图 3-17 所示。

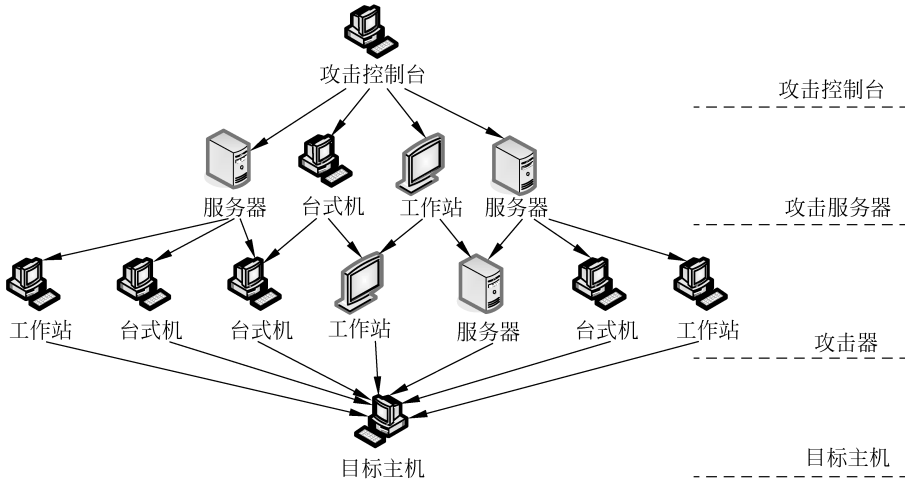


图 3-17　DDoS 攻击体系

(1) 攻击控制台：黑客所用的主机，也称为攻击者。它操纵整个攻击过程，向攻击服务器发送攻击命令。

(2) 攻击服务器：是攻击者非法侵入并控制的一些主机，这些主机分别控制大量的代理攻击主机。其上面安装特定的程序，可以接收攻击者发来的特殊指令，并且可以把这些指令发送到攻击器上。

(3) 攻击器：也是攻击者侵入并控制的一批主机，其上面运行攻击程序，接收和运行攻击服务器发来的命令。

(4) 目标主机：被攻击的受害者。

先来看一下最重要的攻击服务器和攻击器，它们分别用作控制和实际发起攻击。请注意攻击服务器与攻击器的区别，对目标主机来说，DDoS 的实际攻击包是从攻击器傀儡机上发出的，攻击服务器只发布命令而不参与实际的攻击。对于攻击服务器和攻击器，攻击控制台有控制权或者部分控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些攻击服务器并没有什么异常，只是一旦黑客连接到它们进行控制并发出指令，攻击服务器就成为害人者去发起攻击了。

为什么黑客不直接去控制攻击器，而要从攻击服务器上转一下呢？从攻击者的角度来说，他肯定不愿意被发现，而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台计算机后，高水平的攻击者会首先做两件事：第一，考虑如何留好后门；第二，考虑如何清理日志。但是在攻击器上清理日志实在是一项庞大的工程，即使在很好的日志清理工具的帮助下，黑客想完全清除日志也是比较困难的。这就导致了有些攻击器清除日志不是很干净，通过它上面的线索能找到控制它的上一级计算机，上级计算机如果是黑客自己的机器，那么他就会被查找出来。但如果这是攻击服务器的话，黑客自身还是安全的。攻击服务器的数目很少，一般一台就可以控制几十台攻击器，清理一台攻击服务器的日志对黑客来讲就容易多了，这样从攻击服务器再找到黑客的可能性也大大降低。

5. DDoS 攻击过程

DDoS 攻击的过程可以描述如下：

(1) 搜集了解目标的情况。了解被攻击目标主机的数据、地址情况，目标主机的配置、性能，以及目标主机的带宽，从目标主机中找到可能成为傀儡机的主机。

(2) 占领傀儡机。傀儡机选择链路状态好、性能好、安全管理水平差的主机。首先采用扫描手段，随机或者是有针对性地利用扫描器去发现互联网上那些有漏洞的主机，如程序的溢出漏洞、数据库漏洞等；随后尝试入侵，一旦入侵成功，把 DDoS 攻击用的程序上传过去，一般是利用 FTP。在攻击器上，会有一个 DDoS 的发包程序，攻击者就是利用它来向目标主机发送恶意攻击包。

(3) 实际攻击。经过前两个阶段的精心准备，就可以瞄准目标准备攻击了。攻击者登录到作为攻击服务器的傀儡机，向所有的攻击器发出 DDoS 攻击命令，这时候埋伏在攻击器中的 DDoS 攻击程序就会响应攻击服务器的命令，一起向目标主机或设备高速发送大量的数据包，导致服务停止、死机或连接线路拥塞中断。

6. DDoS 防御方法

1) 定期扫描

要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行清

理。骨干节点的计算机因为具有较高的带宽，是黑客利用的最佳位置，因此对这些计算机本身加强安全配置是非常重要的。而且连接到网络主节点的都是服务器级别的计算机，所以定期扫描漏洞就变得更加重要了。

2）采用高性能的网络设备

首先要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好的产品。假如和网络提供商有特殊关系或协议的话，当大量攻击发生时请他们在网络接点处做一下流量限制来对抗某些种类的 DDoS 攻击是非常有效的。

3）尽量避免 NAT 的使用

无论是路由器还是硬件防护墙设备要尽量避免采用网络地址转换 NAT 的使用，因为采用此技术会大幅降低网络通信能力。原因是 NAT 需要对地址来回转换，转换过程中需要对网络包校验和进行计算，因此浪费了很多 CPU 的时间，但在必须使用 NAT 时，那就只能如此了。

4）充足的网络带宽保证

网络带宽直接决定了能抵抗攻击的能力，假若仅仅有 10M 带宽的话，无论采取什么措施都很难对抗现在的 SYNFlood 攻击，目前至少要选择 100M 的共享带宽，最佳选择是使用 1000M 的共享带宽。但需要注意的是，主机上的网卡是 1000M 的并不意味着它的网络带宽就是千兆的，若把它接在 100M 的交换机上，它的实际带宽不会超过 100M，而且接在 100M 的带宽上也不等于就有了百兆的带宽，因为网络服务商很可能会在交换机上限制实际带宽为 10M。

5）在骨干节点配置防火墙

防火墙本身能抵御 DDoS 攻击和其他一些攻击。在发现受到攻击的时候，可以将攻击导向一些牺牲主机，这样可以保护真正的主机不被攻击。

6）过滤不必要的服务和端口

过滤不必要的服务和端口，只开放服务端口成为目前很多服务器的流行做法，如 WWW 服务器只开放 80 端口而将其他所有端口关闭或在防火墙上做阻止策略。

7）检查访问者的来源

使用 Unicast Reverse Path Forwarding 等通过反向路由器查询的方法检查访问者的 IP 地址是否是真，如果是假的，将予以屏蔽。许多黑客在攻击时常采用假 IP 地址的方式迷惑用户，很难查出它来自何处。因此，利用 Unicast Reverse Path Forwarding 可减少假 IP 地址的出现，有助于提高网络安全性。

8）限制 SYN/ICMP 流量

用户应在路由器上配置 SYN/ICMP 的最大流量来限制 SYN/ICMP 包所能占有的最高带宽，当出现的较大流量超过 SYN/ICMP 的限定时，说明不是正常的网络访问，而是有黑客入侵。早期限制 SYN/ICMP 流量是最好的防范 DoS 的方法，虽然目前该方法对于 DDoS 效果不太明显了，不过仍然能够起到一定的作用。

7. DDoS 防护部署

1）串行部署防御 DDoS 攻击

串行部署防御模式主要应用在企业网络中，在网络的出口或要保护的目标地址前进行部署，提供串行的保护形式，如图 3-18 所示。

此种部署模式不需要 DDoS 攻击检测器，而是直接将防护设备部署在需要保护的设备前面，利用设备的识别能力，直接过滤攻击流量。

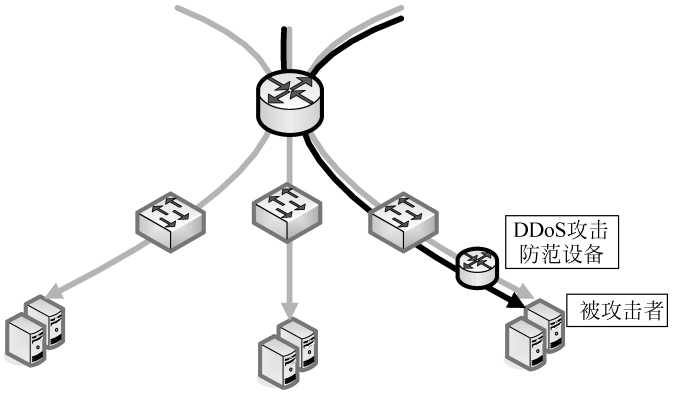


图 3-18　串行部署防御模式

此种部署模式实施起来比较简单，但有以下几个较为明显的弱点，例如，任何时候流量都经过防范设备，可能会成为性能瓶颈；在需要保护的目标设备比较多时，投资较高；对来自上游的基于带宽的 DDoS 攻击无法提供有效保护。

2）旁路部署防御 DDoS 攻击

完整的 DDoS 保护围绕以下 4 个关键主题建立：

（1）要缓解攻击，而不只是检测；

（2）从恶意业务中精确辨认出正常的业务，维持业务继续进行，而不只是检测攻击的存在；

（3）内含性能和体系结构能对上游进行配置，保护所有易受损点；

（4）维持可靠性和成本效益可升级性。

旁路式部署防御模式可以完全围绕这几个关键主题进行，没有串行模式的几大弱点，可以应用在各种网络中，对网络设备和服务器等提供保护，如图 3-19 所示。

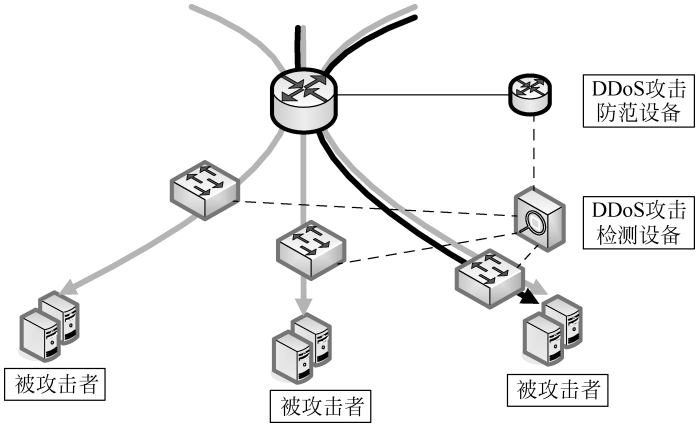


图 3-19　旁路部署防御模式

此种部署模式在原有网络的基础上实施，对原有网络没有任何改变。此方式需要 DDoS 攻击检测器和流量异常检测手段，当检测器发现 DDoS 攻击后，直接通知 DDoS 防范器将流量引导到 DDoS 防范器进行过滤，然后将过滤后正常的流量继续传送到目标地址。

这种模式在检测、转移、验证和转发的基础上实施一个完整 DDoS 保护解决方案来提供完全保护。

3.6 网络后门

简单地说,后门是攻击者再次进入网络或者是系统而不被发现的隐蔽通道。

有人说,留后门是一种艺术。留后门并不是一项简单的工作,入侵者不但要留下下次进入的通道,而且还要对自己所做的一切加以隐藏,如果建立起的后门马上就被管理员发现就没有任何用处了。所以,只要是不容易被发现的后门都是好后门。

1. 留后门的目的

(1) 保持对目标系统的长期控制;

(2) 监听目标系统的行动或记录目标系统的敏感信息,随时报告入侵者。

2. 后门的分类

留后门的方法多不胜数,可以利用不同后门的特点对后门进行分类。

按后门的整体特点可分为主动后门和被动后门。主动后门是后门程序主动监听某个端口或进程,随时等待连接,后门的特征非常明显。被动后门不会做任何工作,只有连接者去连接的时候才能表现出后门的特征。

按开放端口情况可分为开放端口的后门、不开放端口的后门、利用系统已经开放的端口的后门。

按工作模式可分为命令模式的后门、图形界面的后门、B/S 结构基于浏览器的后门。

按连接模式可分为正向连接后门、反向连接后门。

3.7 清除日志

清除日志是黑客入侵的最后的一步,黑客能做到来无影去无踪,这一步起到决定性的作用。大多数系统都是通过记录日志文件来检测是谁进入过系统并且停留了多长时间,根据日志文件所设置的级别不同,还可以发现入侵者做了些什么,对哪些文件进行了操作。

1. 清除 IIS 日志

当用户访问某个 IIS 服务器后,无论是正常的访问还是非正常的访问,IIS 都会记录访问者的 IP 地址以及访问时间等信息。这些信息记录在 Winnt\System32\logFiles 目录下,打开任一文件夹下的任一文件,可以看到 IIS 日志的基本格式,记录了用户访问的服务器文件、用户登录时间、用户的 IP 地址,以及用户浏览器和操作系统的版本号。

清除 IIS 日志的最简单的方法是直接到该目录下删除这些文件夹,但是全部删除文件后,一定会引起管理员的怀疑。一般入侵的过程是短暂的,只会保存到一个 LOG 文件中,只要在该 LOG 文件中删除所有自己的记录即可。也可以使用工具软件 CleanIISLog.exe 等清除指定的 IIS 日志记录。

2. 清除主机日志

主机日志包括三类日志:应用程序日志、安全日志和系统日志。可以在计算机上通过控制面板下的管理工具下的“事件查看器”查看日志信息。当非法入侵对方的计算机后,这些日志同样会记载一些入侵者的信息,为了防止被发现,也需要清除这些日志。清除主机日志可以使用 clearlogs.exe 等工具软件实现。

3.8 本章小结

网络攻击技术
定义
网络系统的机密性、完整性、可用性等产生危害的行为
分类
被动攻击
窃听攻击
流量分析
主动攻击
伪装攻击
重放攻击
消息篡改
拒绝服务攻击
隐藏IP
IP欺骗
网络代理跳板
步骤
信息搜集
发现目标主机或网络
ping扫射技术
发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务及服务软件的版本等
操作系统探测技术
端口扫描技术
全连接扫描
半连接扫描
无连接扫描
根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞
漏洞扫描技术
实施入侵
社会工程学攻击
物理攻击
暴力攻击
词典攻击
强行攻击
组合攻击
社会工程学典攻击
漏洞攻击
缓冲区溢出攻击
木马攻击
传统连接方式
反弹端口连接方式
拒绝服务攻击
DoS攻击
DDoS攻击
攻击控制台
攻击服务器
攻击器
目标主机
保持访问
网络后门
隐藏踪迹
清除日志
清除IIS日志
清除主机日志
网络攻击
网络攻击技术
黑客
专门利用计算机搞破坏或恶作剧的家伙
定义
分类
红客
破坏者
间谍
行为发展趋势
手段高明化
活动频繁化
动机复杂化
黑客年轻化
破坏力扩大化
黑客技术普及化
黑客组织化

3.9 习　　题

一、填空题

1. X.800 和 RFC 2828 对网络攻击进行了分类，分为被动攻击和主动攻击。(　　)试图获得或利用系统的信息，但不会对系统的资源造成破坏。

2. 主动攻击一般分为伪装攻击、(　　)、消息篡改和拒绝服务攻击 4 类。

3. 网络攻击五部曲包括(　　)、信息搜集、实施入侵、保持访问和隐藏踪迹。

4. (　　)是伪造某台主机的 IP 地址的技术，其实质就是让一台主机来扮演另一台主机，以达到隐藏自己的目的。

5. (　　)是依靠发送 FIN 来判断目标计算机的指定端口是否活动，也称为秘密扫描。

6. 网卡的工作模式包括广播模式、组播模式、直接模式和(　　)。

7. (　　)就是利用人们的心理特征骗取用户的信任，获取机密信息、系统设置等不公开的资料。

8. (　　)是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的空间，溢出的数据覆盖在合法数据上。

9. 木马的连接方式包括传统连接方式和(　　)连接方式。

10. 一个比较完善的 DDoS 攻击体系分成(　　)、攻击服务器、攻击器和目标主机 4 个部分。

二、选择题

1. 在黑客攻击技术中，(　　)是黑客发现获得主机信息的一种最佳途径。

A. 端口扫描　　B. 缓冲区溢出　　C. 网络监听　　D. 口令破解

2. 字典攻击被用于(　　)。

A. 用户欺骗　　B. 远程登录　　C. 网络嗅探　　D. 破解密码

3. 一次字典攻击能否成功，主要决定于(　　)。

A. 字典文件　　B. 计算机性能　　C. 网络速度　　D. 黑客经验

4. 为了防御网络监听，最常用的方法是(　　)。

A. 采用物理传输(非网络)　　B. 信息加密

C. 无线网　　D. 使用专线传输

5. 向有限的空间输入超长的字符串是(　　)攻击。

A. 缓冲区溢出　　B. 网络监听　　C. 端口扫描　　D. IP 欺骗

6. 使用服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统信息无法正常服务，这属于(　　)攻击。

A. 拒绝服务　　B. 文件共享

C. BIND 漏洞　　D. 远程过程调用

7. 拒绝服务攻击是对计算机网络的(　　)安全属性的破坏。

A. 保密性　　B. 完整性

C. 可用性　　D. 不可否认性

8. 假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包，这是(　　)攻击手段。

A. 缓冲区溢出　　B. 地址欺骗　　C. 拒绝服务　　D. 暴力攻击

9. 小李在使用 super scan 对网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是(　　)。

A. 文件服务器　　B. 邮件服务器　　C. Web 服务器　　D. DNS 服务器

10. 在 DDoS 攻击中，通过非法入侵并被控制，但并不向被攻击者直接发起攻击的计算机称为(　　)。

A. 攻击控制台　　B. 攻击服务器　　C. 攻击器　　D. 目标主机

11. 对利用软件缺陷进行的网络攻击，最有效的防范方法是(　　)。

A. 及时更新补丁程序　　B. 安装防病毒软件

C. 安装防火墙　　D. 安装漏洞扫描软件

12. 缓冲区溢出的最大危害是(　　)。

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

13. (　　)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

14. 端口扫描技术(　　)。

A. 只能作为攻击工具

B. 只能作为防御工具

C. 只能作为检查系统漏洞的工具

D. 既可以作为攻击工具，也可以作为防御工具

15. 采用模拟攻击漏洞探测技术的好处是(　　)。

A. 可以探测到所有漏洞　　B. 完全没有破坏性

C. 对目标系统没有负面影响　　D. 探测结果准确率高

16. 半连接端口扫描技术显著的特点是(　　)。

A. 不需要特殊权限

B. 不会在日志中留下任何记录

C. 不建立完整的 TCP 连接

D. 可以扫描到 UDP 端口

17. 以下对 DoS 攻击的描述，正确的是(　　)。

A. 不需要侵入受攻击的系统

B. 以窃取目标系统上的机密信息为目的

C. 导致目标系统无法正常处理用户的请求

D. 若目标系统没有漏洞，远程攻击不会成功

18. Windows 系统能设置在几次无效登录后锁定账号，可以防止(　　)。

A. 木马　　B. 暴力破解　　C. IP 欺骗　　D. 缓冲区溢出

19. TCP SYN 泛洪攻击的原理是利用了(　　)。

A. TCP 三次握手过程　　B. TCP 面向流的工作机制

C. TCP 数据传输中的窗口技术　　D. TCP 连接终止时的 FIN 报文

20. 木马与病毒的最大区别是(　　)。

A. 木马不破坏文件,而病毒会破坏文件

B. 木马无法自我复制,而病毒能够自我复制

C. 木马无法使数据丢失,而病毒会使数据丢失

D. 木马不具有潜伏性,而病毒有潜伏性

21. 木马无法通过(　　)隐藏自己。

A. 任务栏　　B. 任务管理器

C. 邮件服务器　　D. 修改系统配置文件

22. 计算机感染木马后的典型现象是(　　)。

A. 程序异常退出　　B. 有未知程序试图建立网络连接

C. 邮箱被垃圾邮件填满　　D. Windows 系统黑屏

23. 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

24. 以下(　　)不属于防止口令猜测的措施。

A. 严格限定从一个给定的终端进行非法认证的次数

B. 确保口令不在终端上再现

C. 防止用户使用太短的口令

D. 使用机器产生的口令

25. (　　)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

26. 属于操作系统中日志记录功能的是(　　)。

A. 控制用户的作业排序和运行

B. 以合理的方式处理错误事件,而不至于影响其他程序的正常运行

C. 保护系统程序和作业,禁止不合要求的对程序和数据的访问

D. 对计算机用户访问系统和资源的情况进行记录

27. (　　)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

28. (　　)是最主要的主机系统漏洞。

A. 缓冲区溢出　　B. Unicode 漏洞

C. Ping of Death　　D. Land

29. (　　)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

30.（　　）无法破坏网络的可用性。

A. 病毒　　B. 拒绝服务攻击

C. 非法访问　　D. 线缆遭受破坏

31.（　　）和信息保密性无关。

A. 加密/解密算法　　B. 终端接入控制

C. 病毒　　D. 拒绝服务攻击

32.（　　）不属于主动攻击。

A. 流量分析　　B. 重放　　C. IP 地址欺骗　　D. 拒绝服务

33.（　　）属于主动攻击。

A. 篡改和破坏数据　　B. 嗅探数据　　C. 数据流分析　　D. 非法访问

34. 关于 MAC 表溢出攻击，以下选项中描述错误的是（　　）。

A. MAC 表能够存储的转发项是有限的

B. 交换机无法鉴别 MAC 帧的源 MAC 地址和接收端口之间的绑定关系

C. 交换机广播没有转发项与之匹配的 MAC 帧

D. 不允许存在多项 MAC 地址不同但转发端口相同的转发项

35. 关于 MAC 地址欺骗攻击，以下选项中描述错误的是（　　）。

A. 交换机无法鉴别 MAC 帧的源 MAC 地址和接收端口之间的绑定关系

B. 交换机根据最新的 MAC 帧的源 MAC 地址和接收端口之间的绑定关系更新转发项

C. 终端可以伪造自己的 MAC 地址

D. 允许存在多项 MAC 地址相同但转发端口不同的转发项

36. 关于 ARP 欺骗攻击，以下选项中描述正确的是（　　）。

A. 广播的 ARP 请求报文中给出黑客终端的 MAC 地址与攻击目标的 IP 地址之间的绑定关系

B. 广播的 ARP 请求报文中给出攻击目标的 MAC 地址与黑客终端的 IP 地址之间的绑定关系

C. 广播的 ARP 请求报文中给出黑客终端的 MAC 地址与黑客终端的 IP 地址之间的绑定关系

D. 广播的 ARP 请求报告中给出攻击目标的 MAC 地址与攻击目标的 IP 地址之间的绑定关系

37. 关于 SYN 泛洪攻击，以下选项中描述错误的是（　　）。

A. TCP 会话表中的连接项是有限的

B. 未完成建立过程的 TCP 连接占用连接项

C. 用伪造的、网络中本不存在的 IP 地址发起 TCP 连接建立过程

D. 未完成建立过程的 TCP 连接永久占用连接项

38. 关于 Smurf 攻击，以下选项中描述错误的是（　　）。

A. 封装 ICMP ECHO 请求报文的 IP 分组的源 IP 地址是攻击目标的 IP 地址

B. 封装 ICMP ECHO 请求报文的 IP 分组的目的 IP 地址是广播地址

C. 接收 ICMP ECHO 请求报文的终端回送 ICMP ECHO 响应报文

D. 单个 ICMP ECHO 请求报文只能引发单个 ICMP ECHO 响应报文

39. 关于间接 DDoS 攻击，以下选项中描述错误的是(　　)。

A. 傀儡机随机生成有效 IP 地址集

B. 正常主机系统发送对应的响应报文

C. 正常主机系统不对接收到的请求报文进行源端鉴别

D. 傀儡机发送的请求报文以随机生成的有效 IP 地址为源 IP 地址

40. 以下关于网络钓鱼的说法中，不正确的是(　　)。

A. 网络钓鱼融合了伪装、欺骗等多种攻击方式

B. 网络钓鱼与 Web 服务没有关系

C. 典型的网络钓鱼攻击是将被攻击者引诱到一个精心设计的钓鱼网站上

D. 网络钓鱼是“社会工程攻击”的一种形式

41. 关于钓鱼网站，以下选项中描述错误的是(　　)。

A. 黑客构建模仿某个著名网站的假网站

B. 假网站的 IP 地址与著名网站的 IP 地址相同

C. 正确的域名得到错误的解析结果

D. 用户不对访问的网站的身份进行鉴别

42. 利用 ICMP 进行扫描时，(　　)是可以扫描的目标主机信息。

A. IP 地址　　B. 操作系统版本　　C. 漏洞　　D. 弱口令

43. 关于黑客入侵，以下选项中描述错误的是(　　)。

A. 存在黑客终端与攻击目标之间的传输路径

B. 攻击目标存在漏洞

C. 黑客通过扫描发现攻击目标存在的漏洞

D. 黑客必须已经获取攻击目标的管理员账户信息

44. (　　)攻击与操作系统漏洞无关。

A. 非法登录主机系统

B. 向主机系统植入病毒

C. 缓冲区溢出

D. 消耗掉主机系统连接网络的链路的带宽

45. (　　)不是 ARP 欺骗攻击的技术原理。

A. 终端接收到 ARP 报文，记录 ARP 报文中的 IP 地址与 MAC 地址对

B. 如果 ARP 缓冲区中已经存在 IP 地址与 MAC 地址对，以该 MAC 地址作为该 IP 地址的解析结果

C. 可以在 ARP 报文中伪造 IP 地址与 MAC 地址对

D. ARP 缓存区中的 IP 地址与 MAC 地址对存在寿命

三、判断题

1. TCP SYN 泛洪攻击属于一种典型的 DoS 攻击。

2. 木马有时称为木马病毒，但却不具有计算机病毒的主要特征。

3. 要实现 DDoS 攻击，攻击者必须能够控制大量的计算机为其服务。

4. 在 LAND 攻击中，LAND 攻击报文的源 IP 地址和目的 IP 地址是相同的。

5. 拒绝服务攻击就是利用更多的傀儡机对目标发起进攻，使目标系统资源耗尽无法处理正常用户的请求。

四、简答题

1. 黑客攻击5个步骤是什么？

2. DDoS攻击由哪4部分组成？

3. 端口扫描的基本原理是什么？

4. 什么是计算机网络安全漏洞？

5. 什么是DoS？

6. 什么是字典攻击？

7. 什么是Unicode漏洞？

8. 简述网络扫描的步骤。

五、综合题

1. 阅读下面程序，回答问题(1)～(2)。

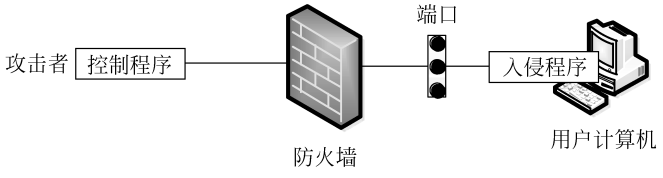
```
void function(char * str)
{
  char buffer[16];
  strcopy(buffer,str);
}
void main()
{
  int t;
  char buffer[128];
  for(i = 0;i < 127;i++)
      buffer[i] = 'A';
      buffer[127] = 0;
  function(buffer);
  print("This is a test\n");
}
```

(1) 上述代码存在什么类型的安全隐患？

(2) 造成上述隐患的两个原因是什么？

2. 阅读以下说明，回答问题(1)～(4)。

说明：特洛伊木马是一种基于客户机/服务器模式的远程控制程序，黑客可以利用木马程序入侵用户的计算机系统。木马的工作模式如下图所示。



(1) 对于传统的木马程序，侵入被攻击主机的入侵程序属于__①__。攻击者一旦获取入侵程序的__②__，便与它连接起来。

① A. 客户程序　　B. 服务器程序　　C. 代理程序　　D. 系统程序

② A. 用户名和口令　　B. 密钥

C. 访问权限　　D. 地址和端口号

(2) 以下 ③ 和 ④ 属于计算机感染特洛伊木马后的典型现象。

③、④ A. 程序堆栈溢出　　B. 有未知程序试图建立网络连接

C. 邮箱被莫名邮件填满　　D. 系统中有可疑的进程在运行

(3) 安装了防火墙软件的主机可以利用防火墙的 ⑤ 功能,有效地防止外部非法连接来拦截木马。

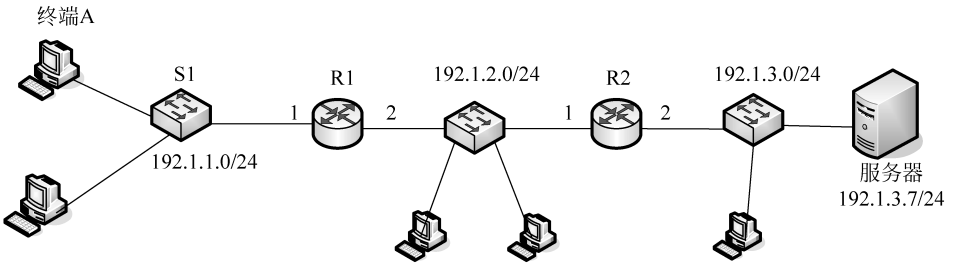
⑤ A. 身份认证　　B. 地址转换　　C. 日志记录　　D. 包过滤

(4) 以下措施中能有效防治木马入侵的有 ⑥ 和 ⑦ 。

⑥、⑦ A. 不随意下载来历不明的软件　　B. 仅开放非系统端口

C. 实行加密数据传输　　D. 实行实时网络连接监控程序

3. 网络结构如下图所示,回答以下问题。



(1) 如果终端 A 想要通过 Smurf 攻击服务器,给出终端 A 发送的三种类型的 ICMP ECHO 请求报文的源 IP 和目的 IP。

(2) 如果要求网络能够阻止终端 A 发起对服务器的 Smurf 攻击,给出在交换机 S1、路由器 R1 和路由器 R2 上采取的措施。