第 5 章

拒绝服务攻击

CHAPTER 5


视频讲解

5.1　概述

拒绝服务(Denial of Service,DoS)攻击是一种使系统无法正常地向用户提供服务的攻击。攻击者对系统进行干扰或控制,导致系统崩溃或者无法提供足够的带宽、处理能力、存储空间等资源,使得系统提供的服务质量很差甚至完全停止,在正常用户看来系统好像拒绝为其提供服务一样。

近年来,拒绝服务攻击引起了人们的广泛关注。早期的拒绝服务攻击主要通过向受害者发送大量网络数据包实现。随着技术的演变,攻击手段变得越来越复杂,防御也变得越来越困难。拒绝服务攻击可以使受害者主机无法正常工作,从而造成直接的经济损失,还会降低公司信誉,造成间接经济损失,甚至直接威胁社会的正常运行、威胁公共安全。

攻击者发动拒绝服务攻击的一般目的是获得经济利益,此外还有一些其他目的。

1) 获取经济利益

攻击者可能因为间接或者直接的经济利益而攻击特定的系统。假设存在两家相互竞争的互联网公司,用户通常愿意去服务质量更好的公司。若其中一家公司会向其竞争对手发动 DoS 攻击,从而降低了竞争对手的服务质量,则这家公司有可能获得对手流失的用户。另一类攻击利用 DoS 攻击对受害者进行勒索。例如,在 2004 年欧洲杯足球赛期间,发生了一起针对博彩公司的敲诈案件。攻击者宣称,若该公司不支付高额费用就会发动 DoS 攻击,使用户无法访问公司网站。

2) 辅助网络攻击

拒绝服务攻击可以作为其他攻击的辅助手段。例如,攻击者仅用 DoS 攻击不能破坏系统的机密性和完整性,但 DoS 攻击可以作为间接手段使系统无法正常工作,从而降低系统的防御能力。攻击者然后结合其他攻击手段,就有可能达到非法访问或篡改信息的目的。

3) 其他目的

与其他攻击技术相比,DoS 攻击的原理相对简单,可以利用工具开展大规模自动化攻击。因此一些技术不熟练的攻击者会利用 DoS 攻击达成各种目的,如练习网络攻击技术、向同伴炫耀、对他人进行报复。某些机构或组织可能出于宣传目的,利用 DoS 攻击对特定网络资源发起攻击。当发生军事冲突时,拒绝服务攻击可以使敌国的重要基础设施(如电力系统、金融系统)发生瘫痪,影响其政府职能和民众生活,进而威胁其国家安全与社会稳定。


视频讲解

5.2　拒绝服务攻击的分类

5.2.1　根据攻击原理分类

根据攻击原理的不同,拒绝服务攻击可分为基于流量的攻击和基于漏洞的攻击两大类别。

1. 基于流量的攻击

基于流量的攻击方式通过向受害者发送大量数据消耗其系统资源,导致系统不能回应

合法用户的请求，因此无法提供正常服务。例如，UDP 洪水攻击就是通过发送大量的 UDP 报文占满受害者主机的带宽，导致受害者主机无法同其他主机通信。

2. 基于漏洞的攻击

网络协议可能存在安全漏洞。基于漏洞的攻击利用网络协议中的缺陷，通过发送少量精心设计的报文触发漏洞，使受害者主机系统崩溃或资源耗尽，因此无法提供正常的服务。例如，在 Ping of Death 攻击中，攻击者向目标机器发送超长的 ICMP 报文，如果目标机存在漏洞，不知道如何处理此类报文，则可能引发操作系统崩溃。

5.2.2　根据攻击目标分类

根据攻击目标的不同，拒绝服务攻击可以分为 7 类：面向应用的攻击、面向操作系统的攻击、面向路由器的攻击、面向通信连接的攻击、面向链路的攻击、面向基础设施的攻击以及面向防火墙的攻击。

1. 面向应用的攻击

攻击者利用某些方法耗尽应用的资源，使其无法提供正常的服务。例如，攻击者攻击 XML 分析器时，向其发送一个特别构造的小型 XML 文档，该文档可以扩张为一个很大的 XML 文档，从而导致 XML 分析器因内存资源耗尽而停止工作。

2. 面向操作系统的攻击

面向操作系统的攻击与面向应用的攻击类似，攻击者通过某些方法来耗尽操作系统的资源，使其无法提供服务。例如，在 TCP 的 SYN 洪水攻击中，攻击者向受害者主机发送大量的 TCP SYN 请求，导致受害者主机一直处于半连接状态。过多的半连接可以耗尽操作系统的内存资源，从而使整个系统因内存不足而无法正常工作。

3. 面向路由器的攻击

针对 IP 路由器的拒绝服务攻击一般利用路由协议进行攻击。这类攻击影响的往往不只是路由器，而是路由器所在的网络。例如用大量的路由信息使路由表过载，从而耗尽路由器的 CPU 和内存资源。当路由器停止响应时，整个网络都会受其影响。

4. 面向通信连接的攻击

面向通信连接的拒绝服务攻击旨在中断或破坏网络通信。如果攻击者已知通信的发起方或接收方以及 TCP 信息，则可以发送伪装的报文使连接双方失去同步或者使 TCP 连接被重置，从而中断通信。

5. 面向链路的攻击

面向链路的攻击旨在使网络链路无法正常传输数据。例如，向链路发送大量的 UDP 报文。由于 UDP 没有拥塞控制机制，该攻击可能造成链路拥塞。

6. 面向基础设施的攻击

网络应用的正常运行离不开网络基础设施的支撑。典型的互联网基础设施包括全球性的域名服务(DNS)和公钥基础设施(PKI)等。对网络基础设施的拒绝服务攻击可以造成网络服务的中断。例如,2002 年,13 个顶级域名服务器受到拒绝服务攻击,导致多个国家无法访问互联网。在局域网内,DHCP 服务也是一种基础设施。如果攻击者耗尽了 DHCP 服务器的 IP 地址池,用户不能获得 IP 地址,则无法访问互联网。

7. 面向防火墙的攻击

作为一种保护内部网络的安全设备,防火墙也可能受到拒绝服务攻击。攻击者通过发送大量的流量,可以耗尽防火墙的带宽和 CPU 资源。对于状态防火墙,则可以利用过量的状态记录耗尽防火墙的内存资源。当防火墙资源不足时,一般会断开内部网络的对外连接,从而使内网中的主机无法访问外部网络,也无法对外提供服务。

5.2.3 根据网络协议层次分类

根据攻击目标的分类可被看作一种水平分类法,而根据网络层次对拒绝服务攻击进行分类则可被看作一种垂直分类法。TCP/IP 协议族可以分为 5 层。理论上,攻击者可以在其中任何一层中发起拒绝服务攻击。这里介绍面向网络层、传输层和应用层的拒绝服务攻击。

1. 面向网络层的拒绝服务攻击

IP 协议是网络层最重要的协议。IP 是基于分组的无连接协议,存在一些安全缺陷。例如,许多拒绝服务攻击就是基于 IP 地址欺骗实施的。

在网络层的重要协议还包括 ICMP 和 IGMP,其中,ICMP 常常用于拒绝服务攻击。例如,在 Ping 洪水攻击中,攻击者以极高的速率向目标主机发送 ICMP 请求报文,从而占用其带宽或系统资源。在 Smurf 攻击中,攻击者向网络广播地址发送 ICMP 响应请求数据包,并将请求数据包的源地址篡改为受害者主机的 IP 地址,从而导致广播地址对应的所有主机向受害者发送 ICMP 应答数据包。

2. 面向传输层的拒绝服务攻击

互联网上的传输层协议主要是 TCP 和 UDP。

TCP 是面向连接的协议,在建立连接时需要三次握手过程。SYN 洪水攻击就是利用三次握手过程开展的拒绝服务攻击。攻击者向受害者主机发送大量的 TCP 连接请求,让主机长时间处于 TCP 半连接状态,最终耗尽系统的内存资源。在 Land 攻击中,攻击者向受害者发送大量 TCP 连接请求,其中源地址和目的地址均设置为受害者主机的 IP 地址。受害者主机需要长期维持大量自己到自己的 TCP 连接,导致内存资源被无效占用。

UDP 是无连接的传输层协议,没有拥塞避免机制。UDP 洪水攻击正是基于该特点开展拒绝服务攻击。攻击者向受害者主机发送大量的 UDP 报文,从而造成受害者主机所在网络的拥塞。

3. 面向应用层的拒绝服务攻击

理论上，任何一种应用协议都可能成为拒绝服务攻击的目标。应用协议一般以客户端/服务器的方式工作，即客户端向服务器发送请求，服务器进行响应。因此攻击者可以利用多个客户端向服务器连续地发出服务请求。为了响应这些请求，服务器可能需要消耗大量的带宽、计算或内存资源，导致服务器无法向其他用户提供正常的服务。例如，用户向 FTP 服务器上传大量文件，或者利用 HTTP 同时下载多个视频文件，从而消耗服务器的全部带宽。典型的面向应用层拒绝服务攻击还包括 HTTP 慢速攻击、DNS 洪水攻击、邮件炸弹等。

5.2.4　根据攻击流量速率分类

1. 恒定速率攻击

恒定速率攻击在短时间内达到攻击速率的最大值并维护不变。当收到攻击命令后，被控制的主机立即以其可以发送的最大流量向受害者进攻，且在整个攻击过程中一直保持峰值流量。这种攻击可以在极短的时间内让受害者承受巨大的流量，从而失去服务能力。恒定速率攻击方式简单，但特征明显，容易被防火墙等安全设备检测出来。

2. 脉冲攻击

在脉冲攻击中，攻击主机周期性地向受害者发送攻击流量，但每次攻击持续时间很短，在发起下一次攻击之前会静默一段时间。脉冲攻击的瞬时攻击流量可以很大，但在一个攻击周期内的平均攻击速率并不高，因此又被称为低速率拒绝服务攻击，它相比恒定速率攻击更难被检测出来。脉冲攻击可以有效地利用 TCP 的拥塞控制机制。脉冲攻击在短时间内发送攻击流量，使链路瞬时产生拥塞，导致大量的 TCP 报文丢失，从而引发 TCP 的拥塞控制，主动降低网络的传输速率。如果周期性地持续攻击，就会严重地影响网络的服务质量。

3. 变速率攻击

变速率攻击在整个攻击过程中会调整其攻击速率，以保持较好的隐蔽性。例如，攻击者刚开始以较低的速率向受害者主机发出网络请求，然后逐渐增加攻击速率。由于初始速率不高，安全设备将其识别为正常，从而成功建立网络连接。攻击者还可采取更加智能的方式控制攻击流量，例如根据攻击目标的受害情况猜测其采取的防御措施，进而改进其攻击模式，以造成更严重的攻击伤害。因此变速率攻击具有较高的隐蔽性和灵活性。

5.2.5　根据攻击源分布模式分类

早期的 DoS 攻击采用一对一的攻击方式，攻击者控制单个主机向目标主机发起攻击。随着网络安全技术的发展，利用包过滤技术或 IP 封锁技术能有效地防范这种攻击。攻击者为实现其攻击目的，开始采用多对一的攻击方式，这种采用多个攻击源的方式又称为分布式拒绝服务(Distributed Denial of Service，DDoS)攻击。因此，按照攻击源的分布模式可以将攻击分为单源拒绝服务攻击和分布式拒绝服务攻击。

1. 单源拒绝服务攻击

单源拒绝服务攻击是指攻击报文是由单个主机产生的攻击方式。前文已经提到许多单源拒绝服务攻击的实例,例如基于漏洞的 Land 攻击,以及利用基于流量的 UDP Flood 攻击等。其中基于流量的拒绝服务攻击更为常见。早期的计算机系统在带宽大小、CPU 频率和内存空间等方面性能不高,单源拒绝服务攻击已经能造成显著的攻击效果。随着计算机性能的快速提高,如今仅使用单源拒绝服务攻击已经很难消耗攻击目标的全部资源。且单源拒绝服务攻击容易暴露攻击者的源地址,进而被安全设备发现并禁用。因此,单源拒绝服务攻击的威胁已大大降低。如今,分布式拒绝服务攻击是更常见的攻击方式。

2. 分布式拒绝服务攻击

分布式拒绝服务攻击是指攻击报文是由多个主机产生的攻击方式。DoS 和 DDoS 可以采用同一种攻击技术,它们的主要区别在于攻击源数量和攻击流量。DDoS 对计算资源的占用远远超过一般的 DoS 攻击,它可以控制成千上万的主机同时开展拒绝服务攻击,这使得 DDoS 成为如今网络最大的威胁之一。在进行攻击之前,攻击者一般先利用主机漏洞控制网络中的大量主机,然后发送指令操纵这些主机同时向目标网络或主机发起 DoS 攻击。

与一般的 DoS 攻击相比,除了拥有更多的资源外,DDoS 攻击也更加灵活。由于控制了多台主机,攻击者可在不同主机上采用不同的攻击方式。当受到特定类型的攻击时,受害者主机会对该类攻击着重防御,多种类型的攻击则增加了防御的难度。此外,攻击者可将攻击主机分成多组,在不同的时间段进行攻击,从而提高隐蔽性。

5.2.6 根据攻击技术分类

在拒绝服务攻击中,攻击者希望以较小的成本取得较好的攻击效果,并尽量隐藏攻击主机的 IP 地址。除了 IP 地址欺骗外,攻击还会使用其他攻击技术增强攻击强度。根据采用的攻击技术,拒绝服务攻击可分为以下三类。

1. IP 源地址欺骗

攻击者在对受害主机发起攻击时,可以修改数据报文里的源 IP 地址,造成数据包是从另一台主机发来的假象,这就是 IP 源地址欺骗技术。因为一旦 IP 地址暴露,安全设备就会禁用 IP,使拒绝服务攻击失效。一般情况下,攻击者只是为了占用连接资源而不需要接收回复的信息,因此攻击者会修改攻击数据包的源 IP 地址,从而用虚假的 IP 地址发动拒绝服务攻击。

2. 反射攻击

反射攻击是指攻击者开展攻击时不直接将攻击报文发送给受害主机,而是发送给中间主机,该主机又称为反射器。图 5.1 所示为反射攻击的原理。攻击者通常将攻击报文的源地址修改为受害主机的 IP 地址。当反射器收到攻击报文后如果向源地址发送消息,则受害主机将收到大量数据包,从而影响其正常工作。理论上,任何对接收到的消息作出响应的主机都可以作为反射器,如常见的 DNS 服务器、Web 服务器等。攻击者发动反射攻击消耗的

自身资源较少。

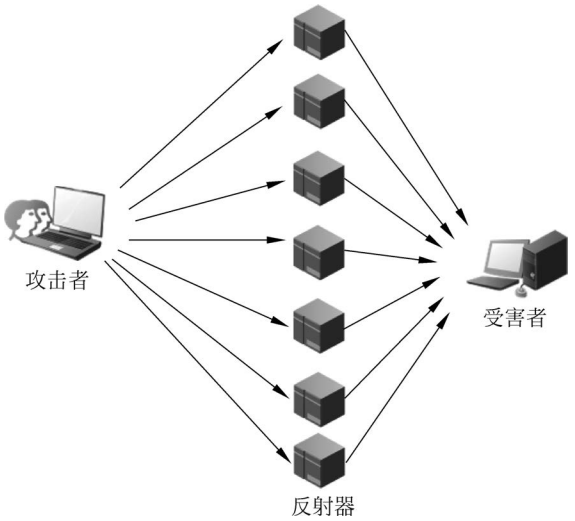

图 5.1　反射攻击示意图

Smurf 攻击是一种典型的反射攻击。攻击者向网络广播地址发送 ICMP 响应请求，并将请求数据包的源地址篡改为受害者地址，从而导致广播地址对应的所有主机向受害者发送 ICMP 应答包。

有的反射攻击不需要篡改源地址，例如 HTTP 代理攻击。Web 服务器在响应动态页面请求时，通常需要频繁地访问数据库，从服务器响应时间较长。而 HTTP 代理攻击就是利用这一特点。攻击者利用代理服务器向 Web 服务器发出请求，使其频繁地访问动态页面。Web 服务器将大量的计算资源用于响应这些恶意的动态页面请求，因此无法为正常用户提供服务。

3. 放大攻击

放大攻击是指攻击者利用一些服务放大对目标主机的攻击流量。例如前文所提到的 ICMP Smurf 攻击中，攻击者向网络广播地址发送 ICMP 响应请求。假设广播地址对应的网络包含 n 台主机，这 n 台主机在接收这些数据包后都作出回复，则攻击者发出一次请求将产生 n 个响应报文，因此攻击被放大了 n 倍。

除了利用网络广播的方式外，还可利用其他方式放大攻击流量。例如，在利用 DNS 服务器发动反射攻击的方式中，假设 DNS 请求消息的长度为 40 字节，响应消息则可能达到 4000 字节的长度，利用这一方式放大了 100 倍，从而轻易地使目标主机瘫痪。

5.3　典型的拒绝服务攻击

本节介绍五种典型的拒绝服务攻击。

5.3.1　Land 攻击

Land 攻击是一种利用了 TCP 漏洞的攻击手段，主要针对建立 TCP 连接的三次握手过

程。Land 攻击的原理比较简单,它将 SYN 包中的源 IP 地址修改为攻击目标的 IP 地址,并发送给攻击目标,使得攻击目标与自身完成握手并建立一个空的 TCP 连接。早期的系统不会检测源 IP 地址,因此攻击目标会建立相应的连接并维持连接直到超时释放。当这类连接数目过多时,就会耗尽系统资源。

由于攻击原理比较简单,因此对此类攻击的检测方法相对容易。只需要过滤掉源 IP 和目的 IP 相同的数据包即可,可以通过配置防火墙或路由器包过滤规则有效防御。

5.3.2　Teardrop 攻击

Teardrop 攻击又称碎片攻击,是一种利用网络层协议漏洞发起的拒绝服务攻击,通过发送畸形报文实现。当数据包的长度超过数据链路层规定的最大长度时,就需要对数据包进行分片传输。如果攻击者恶意篡改了分片数据的偏移地址,当攻击目标接收到数据包后,由于无法正常解析出数据包内容,可能导致系统崩溃。已发现 Teardrop 攻击对早期 Windows 操作系统(如 Windows 95、Windows 98、Windows 3.1 等)和低版本的 Linux 系统有效。

图 5.2 为 Teardrop 攻击的示意图。对于一个 150 字节的原始 IP 数据包(如图 5.2(a)),假设接收方主机先收到一个 120 字节的分片数据包,并知道这是第一个分片数据包,然后接收到一个偏移地址为 120、长度为 30 字节的分片数据包,并知道这是最后一个分片数据包,此时接收方系统能够按照偏移地址正确重组数据包(如图 5.2(b))。但是,如果攻击者将第二个数据包的偏移地址修改为 80,那么接收方就会将 80+30=110 作为总长度,从而导致数据产生重叠和丢失(如图 5.2(c))。由于早期的操作系统不能正确处理这一意外情况,就会导致系统因出现异常而崩溃。

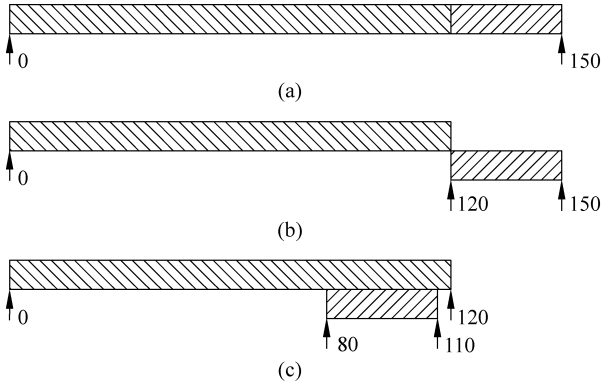

图 5.2　碎片攻击图示

5.3.3　Ping of Death 攻击

Ping of Death 攻击是一种利用 ICMP 的漏洞开展的拒绝服务攻击。ICMP 规定数据包长度不能超过 65 507 字节。当长度超过此上限时,接收方主机的操作系统可能出现内存分配错误的问题,并导致主机崩溃。

TCP/IP 规定,IP 数据包的长度不超过 65 535 字节,除去固定长度 20 字节的 IP 头,IP

数据包的数据段长度最高不得超过 65 515 字节。由于 ICMP 包是封装在 IP 数据包中的，除去 8 字节的 ICMP 包首部，一个 ICMP 包最多可以传输 65 507 字节的数据。这个长度超过了数据链路层规定的最大长度，因此会进行分片传输。当接收方收到的分片数据进行重组时，如果传输的数据长度过大，重组后的 IP 数据包大小超过了预先设置的 65 535 字节的缓冲区大小，就会引发系统崩溃。

5.3.4　洪水型拒绝服务攻击

洪水型拒绝服务攻击，它不依赖于协议设计中的漏洞，而是通过发送大量数据占用受害者的资源，因此洪水型拒绝服务攻击是基于流量的攻击。因特网的特点及缺陷为洪水型拒绝服务攻击的实施提供了便利。首先，因特网采用包交换机制，不同用户共享公共传输信道，当公共资源被占用时，正常用户的服务就会受到影响。洪水型攻击正是通过大量占用公共资源来妨碍正常用户的服务。其次，TCP/IP 缺少 IP 地址认证机制，数据包中 IP 地址的真实性无法保证。因此攻击者可以使用伪造的 IP 地址发动拒绝服务攻击。最后，因特网上存在大量不安全的系统，攻击者可以控制这些系统发动洪水型攻击。常见的洪水型攻击方式有 SYN 洪水攻击、UDP 洪水攻击、Ping 洪水攻击、HTTP 洪水攻击以及针对电子邮件系统的拒绝服务攻击等。

下面以 SYN 洪水攻击为例进行介绍。在建立 TCP 连接的三次握手过程中（如图 5.3 所示），客户端首先向服务器发送 SYN 包，服务器收到后向客户端发出 SYN ACK 包，并等待客户端返回的 ACK 包。此时，服务器处于监听状态（又称为半连接状态），它将保持此状态直到接收到 ACK 包或者等待超时。不同系统的超时参数不同，一般为几十秒，也可能长达十几分钟。

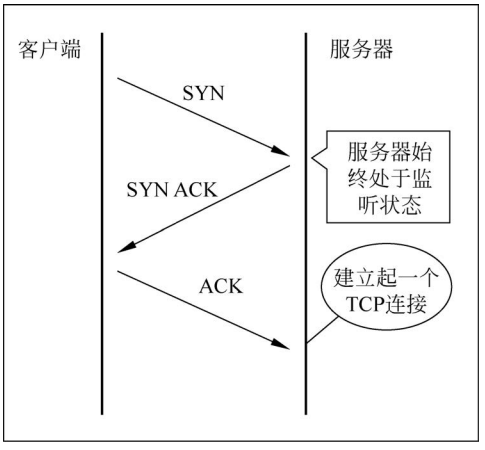

图 5.3　建立 TCP 连接的三次握手过程

在 SYN 攻击中，攻击者不会对 SYN ACK 消息进行响应。因此服务器将一直保持半连接状态。在此状态下，服务器需要维护一个半开连接栈，用于保存与连接相关的信息。如果半开连接栈维持的连接数量没有限制，则攻击者不断发出的 SYN 请求将耗尽系统的内存资源。如果系统对连接数据有限制，则超过上限值后，系统不再接受正常用户的 TCP 连接请求。在两种情况下都会造成系统拒绝服务。

5.3.5　Smurf 攻击

Smurf 是以最初发动该攻击的程序命名的。图 5.4 所示为 Smurf 攻击的原理。攻击者向网络广播地址发送 ICMP 响应请求数据包,并将请求数据包的源地址篡改为受害者主机的 IP 地址。当广播地址对应网络中的主机收到响应请求数据包时,会向数据包的源地址即受害者主机发出响应数据包。因此受害者主机会在短时间内接收到大量数据包,从而导致系统异常。

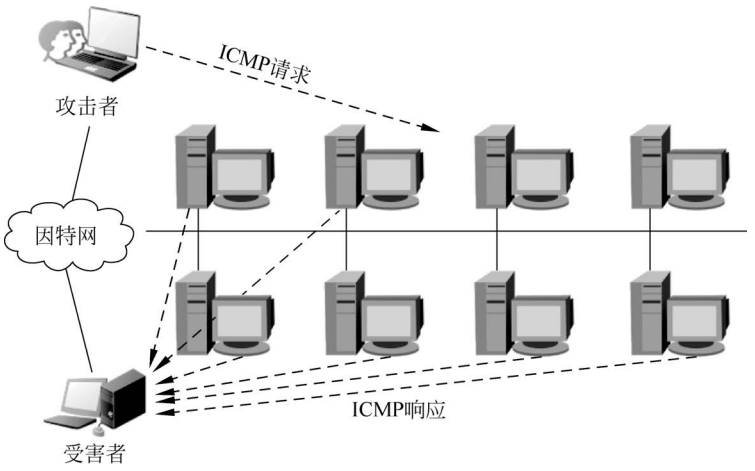

图 5.4　Smurf 攻击示意图

5.4　僵尸网络与 DDoS 攻击

5.4.1　基本概念

DDoS(Distributed Denial of Service,分布式拒绝服务)攻击是指利用分布在网络各处的大量主机对目标发起的拒绝服务攻击。相比一般的 DoS 攻击,参与 DDoS 攻击的主机数量更庞大,物理位置更分散。攻击者一般利用僵尸网络实施 DDoS 攻击。

僵尸网络是通过在大量主机中植入恶意程序,进而形成的一个受攻击者控制的计算机网络。由于僵尸网络具有充足的带宽和系统资源,攻击者可利用僵尸网络开展多种破坏行为,特别是 DDoS 攻击。

图 5.5 所示为利用僵尸网络开展 DDoS 攻击的一个示意图,涉及以下四种角色。

(1) 攻击者:攻击者是发起 DDoS 攻击的主体。在发动攻击前,攻击者首先在大量计算机中植入僵尸程序以获得对这些计算机的控制权。

(2) 僵尸网络控制器:僵尸网络控制器即命令和控制(Command & Control)服务器,它是僵尸网络实现控制和通信的中心服务器,用于向僵尸主机发送命令,或者接收来自僵尸主机的消息。

(3) 僵尸主机:当一台主机被植入了僵尸程序后,它就成为僵尸网络的一个节点,即僵

尸主机。僵尸主机是向受害者开展实质性攻击的主机。

(4) 受害者：受害者是 DDoS 攻击的目标主机。如果受害者主机受到来自大量僵尸主机的拒绝服务攻击，则可能无法正常工作。

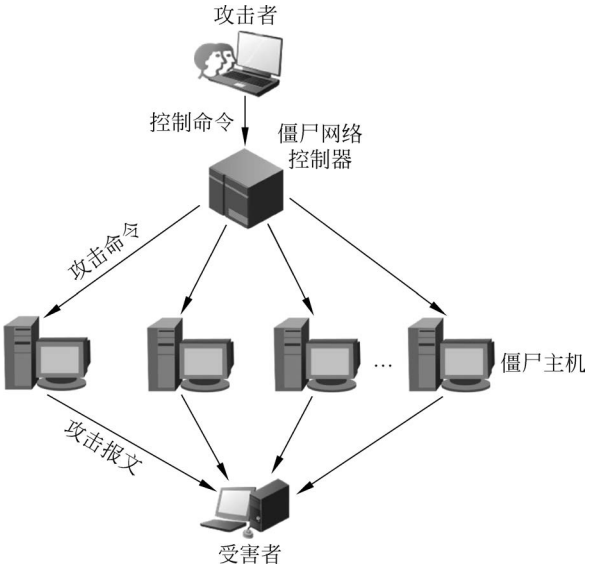

图 5.5　利用僵尸网络开展 DDoS 攻击的示意图

5.4.2　利用僵尸网络发动 DDoS 攻击的一般过程

利用僵尸网络发动 DDoS 攻击的过程一般可分为信息搜集、感染目标主机和实施攻击三个阶段。

1. 信息搜集

信息搜集阶段的主要目标是给出一个可供感染的主机列表。这些主机通常存在特定的安全漏洞，攻击者利用这些漏洞可以植入僵尸程序。攻击者也可能搜集关于主机更详细的信息，如主机名、IP 地址、主机所在网络的带宽和拓扑结构以及主机用户的个人信息等。利用网络扫描技术可以发现潜在的目标主机及其信息，利用漏洞扫描技术则可以发现主机的安全漏洞。关于网络扫描和漏洞扫描更详细的介绍请参见第 3 章。

2. 感染目标主机

为了构建僵尸网络，需要在大量目标主机中植入僵尸程序，使它们成为僵尸主机。僵尸程序包括两个主要功能，一是接受控制器的指令，二是对受害者发动攻击。但是僵尸程序通常不具备自我传播的能力，需要借助其他方式感染目标主机。一种典型的方式是利用蠕虫，它是一种可以独立运行的计算机程序，能够通过网络快速感染其他主机(关于蠕虫更详细的介绍可参见 8.1 节)。其他可能的感染方式还包括计算机病毒、系统漏洞利用、移动代码、口令猜测等。实施这些感染方式可能需要第一阶段搜集到的各种信息。当一台主机被植入僵尸程序后，该主机就被感染。此时，它可以接收攻击者的命令并成为感染更多主机的一个源头。

当一部分主机被感染后,攻击者可以利用已感染的主机更高效地寻找潜在的僵尸主机。例如,扫描已感染主机局域网中的其他主机,或者扫描已感染主机通信列表中主机。刚开始或许只有少数主机被感染,但是被感染的主机数可能会快速增加,当足够多的主机被感染,就完成了僵尸网络的构建。在这一过程中,攻击者可能会控制主机感染的速度。如果感染速度太慢,则需要很长时间才能获得足够多的僵尸主机;如果感染速度太快,又容易引起安全管理人员的注意,导致僵尸网络被过早发现。

3. 实施攻击

僵尸网络构建完成后,攻击者可向分布在互联网中的大量僵尸主机发布命令,让它们同时向受害者发起 DoS 攻击,从而实现 DDoS 攻击。攻击者也可以设定触发时间,让僵尸主机在特定的时间开展攻击。若攻击者改变了攻击目标,只需发布新的命令,而不需要重新构建僵尸网络。

5.4.3 僵尸网络模型

根据僵尸网络采用的工作机制的不同,可以将僵尸网络模型划分为 IRC 僵尸网络模型、P2P 僵尸网络模型和 HTTP 僵尸网络模型。

1. IRC 僵尸网络模型

IRC(Internet Relay Chat,因特网中继聊天)是一个互联网应用层协议,对应标准为 RFC 1459。该协议可实现在互联网上进行实时通信。例如,常见的聊天室功能可基于 IRC 协议实现。IRC 协议采用客户机/服务器模式工作,基于 TCP,默认端口号为 6667。频道(channel)是 IRC 的一个重要概念,它代表一个或多个客户端的集合。当第一个客户端加入频道时,频道自动创建,当最后一个客户端离开信道时,频道停止使用。用户可在 IRC 服务器上创建和加入感兴趣的频道,将消息发送给频道内的所有用户。IRC 也支持一对一通信,即一个用户将消息发送给另一个特定的用户。

IRC 的另一个特点是允许多个服务器进行消息中继传递。假设多台 IRC 服务器有不同的 IP 地址,但共享同一个域名,则这些 IRC 服务器构成 IRC 网络。当两个客户端连接到 IRC 网络中不同的服务器时,它们可通过 IRC 网络中服务器之间的消息中继进行通信。

IRC 协议的这些特点客观上为攻击者构造僵尸网络提供了便利。攻击者可利用动态域名服务将域名映射到其所控制的多台 IRC 服务器上,从而组成一个 IRC 网络。即使某台服务器被摧毁后,网络中的其他 IRC 服务器仍能正常工作,从而避免整个僵尸网络瘫痪。图 5.6 所示为基于 IRC 协议的僵尸网络的例子。

攻击者使用 IRC 协议构建僵尸网络的典型过程如下。

(1) 攻击者在多台主机上植入僵尸程序,使其成为僵尸主机;

(2) 攻击者组建 IRC 服务器网络;

(3) 僵尸主机以随机产生的用户名在 IRC 服务器上注册;

(4) 僵尸主机加入攻击者控制的 IRC 频道;

(5) 僵尸主机监听攻击者发出的消息;

(6) 攻击者利用 IRC 频道向僵尸程序发出攻击指令。

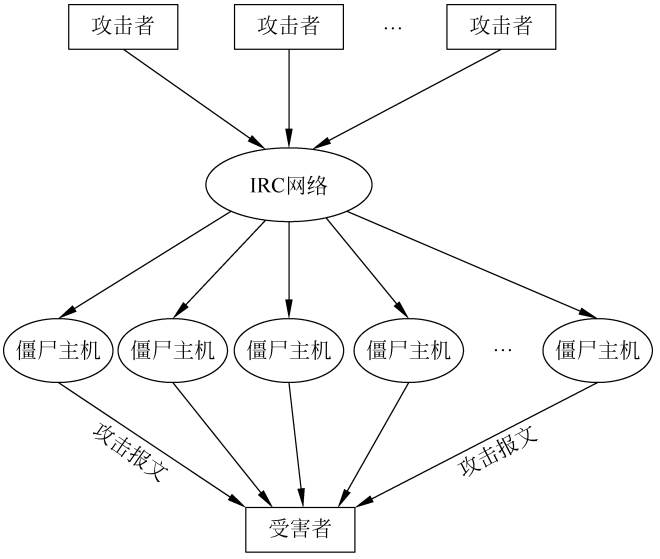

图 5.6　基于 IRC 协议的僵尸网络模型

2. P2P 僵尸网络模型

P2P 网络(Peer-to-peer networking,点对点网络/对等网络)是一种网络组织形式。P2P 网络中的各台计算机拥有相同的网络功能,在地位上没有主从之分。在 P2P 网络中,用户可以不通过中间服务器而直接与其他主机相连,使用户可方便地实现信息交流和各种信息资源的共享。

P2P 僵尸网络是指在网络中按照 P2P 通信方式进行组织的僵尸网络。由于 IRC 僵尸网络是一种集中式网络,当全部 IRC 服务器被摧毁后,攻击者不能利用僵尸主机发动攻击,而 P2P 僵尸网络的分布性则使它具有更强的存活能力。图 5.7 所示为一个基于 P2P 的僵尸网络的例子,其中每一个僵尸节点既担任控制器的角色,也可以发起实质的攻击。

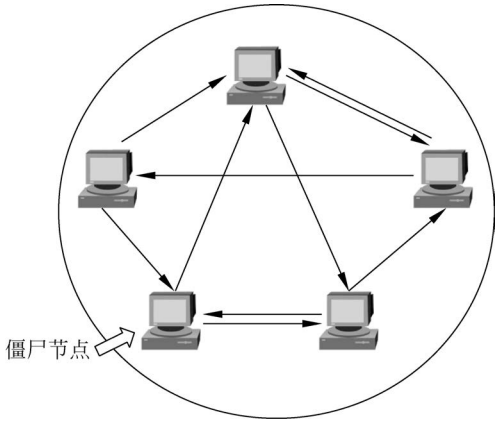

图 5.7　基于 P2P 的僵尸网络模型

P2P 僵尸网络的典型工作流程包括三个阶段。

(1) 招募僵尸成员:攻击者网络上查找存在安全漏洞的主机,向其植入僵尸程序,使其

感染为僵尸主机。

(2) 加入僵尸网络：僵尸程序中包含一个 P2P 网络初始节点列表。僵尸主机被感染之后，会向这些节点发出连接请求，从而加入僵尸网络中。

(3) 接收攻击指令：加入到僵尸网络之后，僵尸节点将等待并接收攻击者通过僵尸网络发送的攻击命令。

3. HTTP 僵尸网络模型

随着 Web 应用的广泛使用，基于 HTTP 的僵尸网络开始成为最常见的僵尸网络之一。HTTP 僵尸网络与 IRC 僵尸网络均属于集中式僵尸网络，两者在结构和功能方面有许多相似之处。不同之处在于 IRC 僵尸网络采用 IRC 服务器作为控制器，而 HTTP 僵尸网络采用 Web 服务器作为控制器，如图 5.8 所示。僵尸网络利用 HTTP 实现控制器与僵尸主机的通信和控制功能。

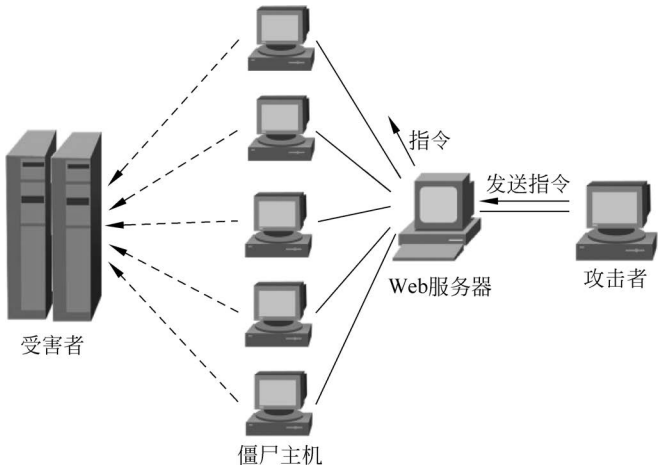

图 5.8　基于 HTTP 的僵尸网络模型

与基于 IRC 协议的僵尸网络相比，基于 HTTP 的僵尸网络具有以下优势：

(1) Web 服务是最常见的互联网服务之一，利用 HTTP 进行通信有较好的隐蔽性，使安全设备难以发现和过滤 HTTP 僵尸网络发动的攻击。

(2) Web 服务器接口友好，便于攻击者对控制器进行配置。

(3) Web 具有丰富的报告工具，便于攻击者方便地了解僵尸网络的情况。

5.5　拒绝服务攻击的检测与防御

5.5.1　拒绝服务攻击的检测

拒绝服务攻击的检测是对抗拒绝服务攻击中的一个重要环节。如果能够较早检测出拒绝服务攻击，而不是等到受害者系统无法工作时才发现攻击，系统用户会获得更多益处。例如，受害者可以提前部署防御措施以减缓攻击的危害，或者提醒其用户对其数据资产进行保护。

根据拒绝服务攻击检测的位置，可以将拒绝服务攻击检测分为目的端检测，源端检测和中间网络检测。本小节介绍在受害者位置上开展的检测，即目的端检测，包括主机异常现象检测和伪造数据包检测。

1. 主机异常现象检测

若主机出现以下异常现象，说明有可能发生了拒绝服务攻击。

现象 1：网络通信流量超过其正常范围，特别地，某一特定源地址的通信流量显著超过平时的统计值。

现象 2：网络通信中出现特别大的 UDP 和 ICMP 包。UDP 载荷一般不超过 10 字节，ICMP 消息一般不超过 128 字节，过大的数据包说明很可能出现拒绝服务攻击。

现象 3：数据包载荷没有空格、标点符号和换行符等文本信息中常见的字符，只存在数字和字母等字符。例如，由 BASE64 编码生成的字段带有上述特征。

现象 4：数据包内字段出现大量二进制数据流。这种情况可能是正常用户在传输二进制文件，也可能是攻击者在传输加密数据流。

现象 5：出现大量 ICMP 目标不可达信息，即接收到的数据包其目的地址无主机或主机没有活动。

现象 6：出现大量 SYN 包，但 SYN 包与 ACK 包的数量差距很大。例如，当主机受到 SYN 洪水攻击时，主机可能收到大量的 SYN 包，但收到的 ACK 包数量却很少，如图 5.9 所示。

C:\netstat -n - TCP

Activate Connections

Proto	Local Address	Foreign Address	State
TCP	10.170.0.120:10	127.160.7.110:203	SYN_RECV
TCP	10.170.0.120:10	243.12.204.155:2206	SYN_RECV
TCP	10.170.0.120:10	235.116.17.22:3980	SYN_RECV
TCP	10.170.0.120:10	220.200.90.43:4402	SYN_RECV
TCP	10.170.0.120:10	126.20.7.25:52	SYN_RECV
TCP	10.170.0.120:10	238.115.7.18:29	SYN_RECV
TCP	10.170.0.120:10	117.100.7.69:22	SYN_RECV
TCP	10.170.0.120:10	225.10.7.226:75	SYN_RECV

图 5.9　受到 SYN 攻击时主机的连接状态

2. 伪造数据包检测

在 DoS 攻击中，攻击者可能使用伪造的数据包，即发送虚假 IP 地址的数据包。这里列出一些常用的伪造数据包检测方法，分为主动检测和被动检测两类。

1）主动检测方法

基于主机的主动检测是一种向接收到的数据包的源 IP 地址主动发出探测数据包，以判断 IP 地址是否被伪造的检测方法，包括利用 TTL（Time To Live，生存时间）值检测、利用 IP 识别号探测，以及利用 TCP 检测等方法。

（1）利用 TTL 值检测。

根据 IP 协议，每经过一个网段，数据包的 TTL 值会减 1，因此到达目标节点时数据包的 TTL 值与其初始 TTL 值之间的差正好等于数据包经过的跳数（即网段数）。一般而言，

在两个节点间传输数据包时经过的路径是相对稳定的,因此数据包从源节点到目标节点经过的跳数应基本不变。对于同一种网络协议(如 ICMP、UDP 或 TCP),发送者的初始 TTL 值是相同的,因此到达目标节点时数据包的 TTL 值也应基本不变。基于这一原理,当收到一个数据包后,接收者可记录其 TTL 值,然后向数据包的源地址发送相同协议的测试数据包,若其返回的数据包的 TTL 值与记录的 TTL 值相差较大,则发送者的 IP 地址可能是伪造的。

如果攻击者到接收者的跳数与伪造地址到接收者的跳数相同,或者攻击者知道伪造地址到接收者的跳数并据此修改数据包的初始 TTL 值,则该方法不能检测出伪造的地址。

(2) 利用 IP 识别号检测。

通常,一个系统发送的数据包的识别号(identifier number)是按规律递增的。大多数操作系统设置的识别号等于上一个数据包识别号加 1。基于这一原理,当收到一个数据包后,接收者可记录其识别号,然后向该数据包的源地址发送一个探测数据包,若返回的数据包的识别号比记录的识别号小,或者两者的差值较大,则该数据包的地址可能是伪造的。如果数据包发送者通信繁忙,则该探测包应及早发出。否则发送者可能与第三方主机发生大量通信,使返回数据包的识别号与记录的识别号有较大差值,从而导致误判。

(3) 利用 TCP 检测。

前面两种方法利用 IP 协议的字段进行伪造检测,还有一些方法利用 TCP 检测伪造数据包。TCP 具有的数据重传和流量控制机制可用于这一目的。TCP 的数据重传机制是指在发送 TCP 数据包之后,若长时间内未收到确认消息,则对该数据包进行重传。TCP 的流量控制机制是指接收方可要求发送方调整其发送速度。

数据接收方通过 ACK 数据包中的确认号向发送方确认目前已收到的数据包。如果该确认号不在发送方所期望的确认号区间内,则发送方将发送一个确认号为最小期望值的数据包以重新建立同步。根据这一原理,主机可以向源 IP 地址发送一个确认号小于最小期望值的 ACK 探测数据包。正常情况下,源 IP 地址应回复一个 ACK 包以重新建立同步,否则判定该 IP 地址是攻击者伪造的。

在 TCP 连接过程中,接收方会通知发送方自己的接收窗口大小,发送方根据窗口大小调整数据包的发送速率。因此,主机可将接收窗口大小设置得很小,若收到了超过接收窗口大小的数据包,则认为收到的数据包是伪造的。特别地,可以将窗口大小设置为 0,若发送方发送的数据包带有数据载荷,则可判定发送方的数组包是伪造的。

2) 被动检测方法

主动检测方法需要主机向发送者主动发送检测数据包,并等待返回数据包以进行检测,因此主动检测法需要耗费主机较多资源。被动检测法只需要对接收到的数据包进行分析,若发现异常,则认为数据包伪造的。常见方法有基于 TTL 的被动检测和基于操作系统特征的被动检测。

(1) 基于 TTL 的被动检测。

如前所述,对主机而言,来自同一 IP 地址的数据包的 TTL 值相对稳定。事实上,来自同一子网的数据包,其 TTL 值也应相对稳定。因此,可以将收到的数据包的 TTL 值同来自同一子网的历史数据包的 TTL 值进行比较。如果接收到的数据包 TTL 值与历史数据包的 TTL 平均值相比,误差超过一个合理的范围,则认为该数据包是伪造数据包。

（2）基于操作系统特征的被动检测。

不同操作系统实现 TCP/IP 时对于某些参数值的设置上有一些微小的差别，如 TCP 中的初始窗口的大小，这些参数可以看作操作系统在网络通信中表现出的部分特征。另一方面，同一 IP 地址采用的操作系统则相对稳定，因此可观察接收到的数据包反映出的操作系统特征，是否与同一 IP 地址过去的操作系统特征相同。如果不同，则可能是伪造数据包。

5.5.2　拒绝服务攻击的防御

DoS 攻击特别是 DDoS 攻击，通常利用分布网络中的大量主机向受害者发起攻击。攻击流量从攻击者或僵尸主机出发，经过中间网络，最终到达受害者的主机或所在的网络。将数据的发送位置称为源端，数据在传输过程中经过的路径称为中间网络，数据的接收位置称为目的端。当攻击者直接发送攻击数据时，源端包含攻击者本机和攻击者所在的网络；当攻击者利用其他的僵尸主机发送攻击数据时，源端包含僵尸主机及其所在的网络。如果攻击者针对受害者的主机，目的端指受害者主机及其所在的网络；如果攻击者的目标是受害者的带宽，则目的端指受害者所在的网络。

DoS 攻击的防御是极具挑战性的任务。目前并没有一劳永逸的防御方法可以应对 DoS 攻击，特别是高强度的 DDoS 攻击。但是防御者仍然可以利用监控、溯源、过滤、控制等多种措施发现并限制攻击造成的危害。这些措施可以在发起攻击的源端、中间网络或目的端进行。在不同位置进行防御具有不同的优缺点。在目的端更容易检测到 DoS 攻击，因为目的端能够观察到所有的攻击，而且作为受害者，目的端愿意尽最大努力防御 DoS 攻击。但是当目的端检测到攻击时，大量网络资源可能已被浪费，甚至目的端可能已经失去正常服务的能力。在尽量接近攻击者的源端阻断攻击似乎是更好的方法，可以缓解攻击造成的网络资源浪费。然而，源端的攻击流量往往分散在各地，不容易观察到明显的模式，而且源端不是防御的直接受益者，防御 DoS 攻击的意愿没有目的端强烈。中间网络防御的优缺点则介于这二者之间。因此理想的方案是构建一个纵深的防御体系，在源端、中间网络和目的端三个位置均实施 DoS 防御。

1. 目的端防御

目的端防御包含对受害者的主机、受害者所在的网络开展的防御措施，有时也需要受害者的网络服务商提供协助。拒绝服务攻击的目的端防御包括增强主机容忍性、提高网络与主机的安全性、入口过滤和 IP 追踪技术等方法。

1）增强容忍性

增强容忍性旨在提高被攻击者承受攻击的能力。这是一种简单有效的防御方式，也是使用最广泛的目的端防御方法之一。对于轻量级的 DoS 攻击，该方法对服务的影响较小。下面介绍一些增强容忍性的方法。

（1）增加资源。这是比较直接的解决方案。若拒绝服务攻击使主机的资源不够时，可以增加相应的带宽、计算和存储资源。该方法需要增加运营成本。

（2）使用代理服务器。该方法避免客户端与主机直接通信，而是使用一台代理服务器作为客户端与主机之间的中介，即客户端与代理服务器直接通信，代理服务器与主机通信。

由于代理服务器可以为拒绝服务攻击进行特殊的设置,因此有可能缓解主机面临的压力。

(3) 随机释放连接。对于面向连接的服务,当连接数达到上限时,系统无法建立新的网络连接,因此不能响应新的服务请求。此时系统可随机释放一部分正在建立或已经建立的连接,以便响应新的服务请求。该方法是以牺牲服务质量为代价实现的,因为它可能中断正常用户的连接。例如,SYN 洪水攻击会快速填满半开连接栈,导致新的 TCP 连接请求失败。此时系统可随机选择一部分半开连接,释放其占用的资源,使系统恢复一部分资源以响应新的 TCP 连接请求。在这一过程中,一些正常用户的连接请求可能无法得到响应,但至少有机会响应新的 TCP 连接请求。

(4) 推迟提供资源。该方法仅当确认对方不是攻击者时才提供资源。例如,对于 SYN 洪水攻击,SYN Cookie 技术就采用了这一思路。当主机接收到一个 SYN 包时,SYN Cookie 并不立刻为其分配内存空间,而是计算一个 cookie 值,并将发给对方的 SYN/ACK 数据包的序列号设置为此 cookie 值。仅当对方响应的 ACK 数据包的序列号等于此 cookie 值+1 时,才为此 TCP 连接分配资源。另一个例子是 Web 服务器在用户通过验证码识别后,才检查其登录密码是否正确,从而节省了主机的计算资源。

2) 提高安全性

除了增强被攻击者的容忍性,还可以通过提高网络或者主机的安全性以防御拒绝服务攻击。

(1) 流量控制。流量控制是提高网络或主机安全性的一种简单有效的方法。对于一些容易受到攻击者利用的网络协议(如 ICMP 协议),可以制定特别的流量控制规则。即使这些协议被攻击者利用,其占用的网络带宽不会超过预先设置的上限,对整个网络的威胁是有限的。流量控制可在网络的边界设备如防火墙、网关等处实施。

(2) 关闭不需要的服务。系统运行时,对外提供的服务可包含潜在的安全漏洞。开放的服务越多,受到的威胁也越多。关闭不需要的服务和端口可以使系统保持更加安全的状态。

(3) 实行严格的补丁管理。系统管理者应关注系统漏洞的发布情况,及时为系统打好补丁。

(4) 安全测试与加固。对系统进行主动的漏洞扫描和安全测试。利用测试中发现的问题修补系统漏洞,改进防御措施和工具。通过防火墙、入侵检测系统等安全设施加固系统安全。

(5) 恶意程序检测。僵尸程序、蠕虫、木马、病毒是拒绝服务攻击常用的恶意程序,通过检测恶意程序可以有效地减少拒绝服务攻击。

3) 入口过滤

入口过滤是指当数据包进入网络时对其进行检查,如果数据包不满足安全要求,则禁止其进入。入口过滤一般通过防火墙实现。有的路由器也可以实现部分的入口过滤功能。以下介绍几个常见的入口过滤方法。

(1) 端口与协议过滤。对于不再使用的服务和一些容易被拒绝服务攻击者利用的协议进行限制和禁止,可以有效降低被 DoS 攻击利用的风险。

(2) 静态地址过滤。地址过滤是指禁止包含特殊 IP 地址的数据包进入网络。例如不应该出现在互联网上的私网地址、保留的 IP 地址、由外部网络发出但却属于内部网络的 IP

地址等。有的攻击数据包直接向内部网络的广播地址发出，根据需要也可以禁止这类数据包进入网络。

（3）自适应地址过滤。该方法并不事先设定被禁止入网的 IP 地址，而是学习一个模型以生成过滤规则。该模型根据以往的通信记录构建，可以计算一个给定地址为正常 IP 地址的概率。例如，以适当频率出现在历史访问记录中的 IP 地址一般是正常的。当目的端疑似遭受 DoS 攻击、面临较大流量压力时，根据该模型可以得出总体丢包率最低时的过滤规则，并在防火墙等设备上实施此规则，以禁止最有可能为攻击流量的数据包进入网络。与随机地阻止数据包进入网络相比，该方法能更好地保证正常用户的服务质量。

4）IP 追踪技术

在 DoS 攻击中，攻击者常利用僵尸网络发送伪造 IP 地址的攻击数据包。IP 追踪技术旨在找出这些数据包的真实源地址。常见的 IP 追踪技术包括链路检测法、包标记法、路由日志法和 ICMP 追踪法等。

（1）链路测试法。

链路测试法（Link Testing）通过检查潜在的网络链路发现攻击链路，然后重复此过程逐级回溯到离攻击者最近的路由器。常用的链路测试机制有输入调试法和受控洪泛法。

输入调试法（Input Debugging）利用路由器的输入调试机制找到攻击源端。在输入调试法中，工程师首先确定攻击报文的特征，然后在上游路由器的输出端口加载该特征进行流量过滤，由此确定输入该攻击流量的路由器。这个过程重复执行直到找到离攻击者最近的路由器。该工作需要获得攻击路径上各个路由器管理者的允许，并由熟练的网络工程师参与调试。

受控洪泛法（Controlled Flooding）通过向网络中的路由器发送大量数据包来定位攻击源。受害者首先选择它相邻链路的上游路由器，分别向其发送大量数据包。由于数据包经过超载链路时会出现很高的丢包率，据此可以确定攻击链路。该过程重复执行直到确定攻击源。该方法要求受害者掌握网络拓扑结构。此外，该检测方法本身类似于一种拒绝服务攻击，因此会加重网络拥塞。

（2）包标记法。

包标记法通过在数据包中记录其经过的路径，帮助受害者追踪攻击源。虽然攻击数据包的源 IP 地址是虚假的，但是数据包途经的网络路径很难造假。路由器对它转发的数据包进行采样，将路由器信息添加到采样的数据包中。当 DoS 攻击发生时，受害者从标记数据包提取路由器信息，然后重构出攻击路径，从而确定攻击源。当数据包经过路径过长时，添加的路由器信息可能超过数据包允许的长度，这是包标记法需要克服的一个难题。

（3）路由日志法。

路由日志法利用记录在路由器记录的信息发现攻击路径。网络中的路由器将所有经过它的数据包的特征保存在日志文件中。当受害者检测到 DoS 攻击时，将其收集到的攻击数据包的特征，与路由器日志中的数据流的特征进行对比，综合多个路由器的信息确定攻击路径。路由日志法需要巨大的存储空间来存储日志文件，而且该方法存在侵犯用户隐私的风险。

（4）ICMP 追踪法。

ICMP 追踪法利用 ICMP 数据包向受害者发送攻击相关信息，帮助受害者确定攻击路

径。路由器对它所转发的报文以很低的概率采样,并生成一个与采样的报文相关的 ICMP iTrace 消息,并将此消息发送给采样报文的接收者。ICMP iTrace 消息包含了报文的特征信息、路由器的 IP 地址信息及其上下游路由器 IP 地址信息。ICMP 追踪法即不需要路由器存储海量数据,也不会出现包标记法面临的数据包长度限制问题,因此该方法具有较大的灵活性。

2. 源端防御

源端防御是在攻击者发起攻击时采取一定的措施,避免攻击数据包进入网络中,从而在源头上遏制拒绝服务攻击。源端防御机制部署在接近攻击源的位置,如攻击者所在网络的路由器。目的端防御中提到的增强主机或网络安全性的各种方法也适用于源端防御。其他常用的源端防御方法包括源地址验证机制和出口过滤。

1) 源地址验证机制

RFC5210 定义了源地址验证的体系结构 SAVA (Source Address Validation Architecture)。SAVA 包括三个层次的源地址验证技术,如图 5.10 所示。第一层的验证技术是接入源地址验证,旨在防止主机粒度的源地址伪造,即一个主机不能伪造成为另外一个主机的 IP 地址,从而确保主机源地址的真实性。第二层验证技术是域内源地址验证,旨在防止子网粒度的源地址伪造,即位于某一子网的主机不能伪造成其他子网主机的 IP 地址。第三层验证技术是过滤假冒报文,保证由某自治系统(Autonomous System,AS)发送的报文源地址属于该自治系统,从而保证在自治系统粒度的源地址的真实性。

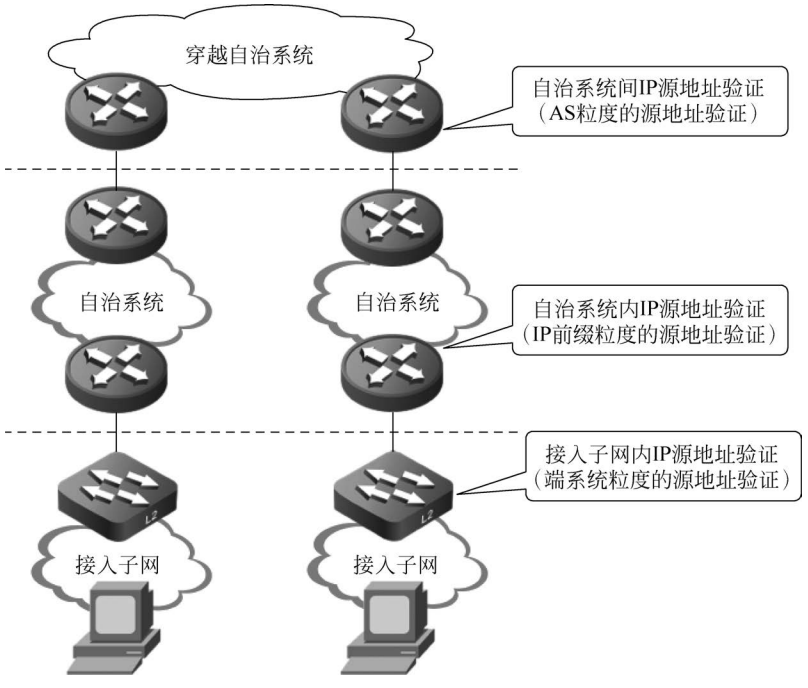

图 5.10　源地址验证体验结构 SAVA

2) 出口过滤

出口过滤的目的是禁止攻击数据包流出到外网中。一种情况是当发现伪造数据包时,

例如来自内部网络的数据包其 IP 地址不属于内部网络，此时网络的边界路由器在转发时将这些数据包丢弃。

源端防御也可以利用流量的统计分析实现异常流量的出口过滤。D-WARD 是一种基于实时流量监控的源端防御方法。它部署在源端网络的边界路由器上，监视源网络的出入流量，并将流量信息与正常的流量模型进行比较。如果网络流量与正常流量模型不符合，则对该流量进行过滤。例如，在 TCP 协议中，发送的数据包需要接收者进行确认，如果发送的数据包与确认的数据包数量之比超过了某个阈值，则认为对外发送的流量可能是攻击流量。

源端防御机制旨在从源头上缓解 DoS 攻击，但是该机制的防御效果受到多个因素的影响。首先，攻击源通常分布网络各处，要求每个源端都能检测并过滤攻击流量比较困难；其次，由于源端处的攻击特征不像目的端那样明显，导致系统要么误检率较高，要么漏检率较高；最后，由于源端需要为防御措施付出成本，而自身受益却不明显，可能缺少防御的意愿。

3. 中间网络防御

中间网络防御可以通过禁止转发广播包、基于路由的包过滤和拥塞控制等方法缓解 DoS 攻击。基于路由的包过滤方法要求路由器已知网络的拓扑结构和网络的连接特征。例如，自治系统的边界路由器根据这些已知信息，结合数据包的源地址和目标地址判断该数据包是否是伪造的。

路由器也可以通过拥塞控制机制减轻 DDoS 攻击的影响。例如通过在边界路由器部署拥塞处理机制，利用队列管理保证每个流获得公平的带宽，或者根据数据流的拥塞程度调整路由器缓存，识别并丢弃攻击数据包以降低 DoS 攻击的危害。

5.6　拒绝服务攻击中的对抗

1996 年 9 月，针对 Panix 的 SYN 洪水攻击被许多人认为是第一个针对互联网服务的拒绝服务攻击。Panix 是美国当时一个规模较大的互联网服务提供商。攻击者每秒向服务器发送超过 100 次的 TCP SYN 请求，使服务器无法响应正常用户的请求。Panix 被攻击后，计算机紧急响应小组(CERT)在攻击出现两周内提出了针对 SYN 洪水攻击的防御和缓解方法。

Trinoo 攻击被认为是第一次真正意义上的 DDoS 攻击。1999 年 8 月，该攻击使用超过 200 台主机对美国明尼苏达大学的某台服务器进行分布式攻击，使其在两天内无法提供正常服务。

2002 年 10 月，13 台根 DNS 服务器遭到大规模的拒绝服务攻击，这是针对 DNS 服务器的较早攻击。受到攻击的服务器接收到数据超过平时的 30 倍，攻击时间持续 1 小时左右，造成 13 台根服务器中的 9 台无法正常工作。如今，DNS 服务器采用的负载均衡技术和 anycast 技术可以较好地防御此类攻击。

大多数的 DDoS 攻击利用了僵尸网络。1998 年出现的 GTBot 可能是最早出现的恶意僵尸网络，它使用 IRC 协议构建命令控制频道。自 GTBot 被攻击者广泛使用后，许多僵尸网络，如 PrettyPark、Sdbot、Spybot 等均基于 IRC 协议。然而这类基于 IRC 协议的僵尸网

络容易被防御人员检测出来。为了提高僵尸网络的隐蔽性和健壮性,控制者开始转向 P2P 协议和 HTTP 协议。第一个 P2P 僵尸网络是 2002 年出现的 Slapper,之后出现了 Sinit、Phatbot 和 Storm 等网络。早期的 P2P 僵尸网络存在许多缺陷,例如 Slapper 并没有认证机制,它容易被防御人员劫持。第一个 HTTP 僵尸网络是 2004 年出现的 Bobax。僵尸程序利用 HTTP 协议对控制服务器进行轮询,从而获取控制命令,具有较强的隐蔽性。以 Storm 和 Bobax 为代表的僵尸网络的流行,促使各种防御方法的提出。基于 HTTP 和 P2P 协议的僵尸网络,其控制频道容易被阻断。2008 年出现的 Conficker 僵尸网络同时使用 Domain Flux 和 Random P2P 两种寻址方法,使其控制频道更难被阻断。对僵尸网络的防御技术包括检测、追踪、劫持等。

近年来,信息技术的不断发展使许多新型拒绝攻击不断出现,为网络安全带来新的挑战。从攻击对象来看,软件定义网络、物联网、云服务、无人机等平台和服务已成为拒绝服务攻击的重要受害者;从攻击手段来看,工业控制网络、物联网、智能手机、人工智能技术常被作为拒绝服务攻击的载体和关键技术。另一方面,深度学习和大数据等新技术也成为防御拒绝服务攻击的有力手段。

5.7 拒绝服务攻击对抗项目

1. 项目概述

本项目要求对抗双方模拟针对 Web 服务器的拒绝服务攻击及防御的过程。对抗分为三轮。在第一轮,双方搭建模拟环境,利用工具开展简单的拒绝服务攻击和防御活动;在第二轮,双方针对第一轮演示结果,对攻击和防御进行改进;在第三轮,双方根据第二轮的对抗结果,查阅参考资料、提出新想法,利用多种资源开展攻击和防御活动。

2. 能力目标

(1) 熟悉多个拒绝服务攻击的方法和工具。
(2) 能够识别拒绝服务攻击的具体类型并开展针对性的防御。
(3) 能够检索和学习参考资料并据此设计新的攻击或防御方法。
(4) 能够编写程序将设计的方法用于实践。
(5) 能够撰写项目报告详细正确地描述对抗过程和技术细节。

3. 项目背景

A 公司是一家以经营网页游戏为主营业务的小型游戏公司。他们最近推出的战棋类游戏受到玩家喜爱,访问人数直线上升。今天上午,他们收到一封来自 B 组织的勒索邮件,要求他们支付一定数量的数字货币,否则将在当天晚上对他们实施拒绝服务攻击,使玩家无法访问他们的网站。

4. 评分标准

学生的项目成绩由三部分构成:

（1）对抗得分。由每一轮的对抗结果决定。

（2）能力得分。根据学生在对抗过程中展现的专业能力决定。

（3）报告得分。由项目报告的质量决定。

5. 小组分工

项目由两个小组进行对抗，各组人数应大体相当，每组可包含 1～4 人。分工应确保每个组员达到至少 3 项能力目标。

两个小组可分别扮演 A、B 双方，或者同时扮演 A、B 双方。

6. 基础知识

项目需要的基础知识包括：

（1）操作系统、网络与防火墙的基本知识。

（2）拒绝服务攻击的基本知识。

（3）防御拒绝服务的基本方法。

（4）常见的拒绝服务攻击 SYN flood、UDP flood、HTTP flood、Slowloris、RUDY、LOIC、HOIC。

（5）程序编写知识。

7. 工具准备

（1）虚拟机软件，用于搭建靶机，推荐使用 VMWare。

（2）操作系统，用于搭建靶机，推荐使用 Linux。

（3）Web 服务器，用于提供 Web 服务，推荐使用 Apache。

（4）防御工具，用于防御拒绝服务攻击。例如 Fail2Ban。

（5）抓包软件，用于查看网络攻击流量，例如 Tcpdump、Wireshark。

（6）编程语言，用于开发攻击或防御程序，常用的有 Python、C++、Java 等。

8. 实验环境

本项目需要至少两台计算机，一台用于 A 方，安装 Web 服务器，可放置在互联网上；另一台用于 B 方，可通过互联网访问 A 方的 Web 服务器。

9. 第一轮对抗

第一轮的任务是搭建模拟环境，并开展指定的攻击和防御活动。

1）对抗准备

A 方应搭建 Web 服务器，可提供网页登录功能。A 方具有抓包能力，并安装有软件防火墙。

B 方可访问 A 方的服务器，并以用户的身份登录网站。B 方可利用 Hping3 等工具实施 ICMP flood 攻击。

双方可在同一局域网中。也可 A 方在互联网上，B 方远程访问 A 方服务器。若 A 方服务器由服务商提供，应确保已关闭拒绝服务攻击防护。

2) 对抗过程

(1) B 方访问 A 方网站。

(2) B 方利用工具对 A 方进行 ICMP flood 攻击。

(3) A 方对访问流量进行抓包,确认攻击流量到达网站。

(4) A 方展示其网站能否正常访问。

(5) A 方设置防火墙阻止 ICMP flood 攻击。

(6) A 方再次展示其网站能否正常访问。

3) 对抗得分

达到以下要求,对应方可获得积分:

(1) 环境配置正确。

(2) A 方攻击流量可到达 B 方。

(3) A 方攻击流量可达到预定速率。

(4) A 方攻击使 B 方网站不能正常访问。

(5) B 方防御成功。

以上各项的具体分值可由双方在对抗前商议确定。

10. 第二轮对抗

在第二轮对抗中,双方应发挥主动性,利用多个已知方法开展拒绝服务攻击和防御活动。

1) 对抗准备

A 方的 Web 服务器应放置在互联网上,B 方远程访问 A 方服务器。A 方应关闭服务商提供的拒绝服务攻击防护。

A 方利用工具或编写程序实现 SYN flood、UDP flood、HTTP flood、Slowloris、RUDY、LOIC、HOIC 中的至少三种攻击。

B 方应利用工具或编写程序识别和防御以上攻击。

2) 对抗过程

A 方开展三次不同类型的攻击。对于每次攻击,B 应检查服务器能否正常访问,A 方的攻击速率,识别 A 方的攻击类型,实施防御措施,检查防御效果。

3) 对抗得分

对抗得分由以下部分构成:

(1) A 方攻击流量的速率可达到预定值。

(2) A 方攻击使 B 方网站不能正常访问。

(3) B 方正确识别 A 方攻击类型。

(4) B 方防御成功。

以上各部分的具体分值可由双方在对抗前商议确定。第二轮的总分值应高于第一轮。

11. 第三轮对抗

在第三轮对抗中,双方应发挥创造性,查阅、学习和实践新的方法,努力在对抗中取胜。

1）对抗准备

A 方的 Web 服务器应放置在互联网上，B 方远程访问 A 方服务器。A 方应关闭服务商提供的拒绝服务攻击防护。

双方通过查阅资料、学习并设计新的方法、编写程序、利用多种资源为对抗作准备。

2）对抗过程

（1）A 方开展一次攻击。

（2）B 方检查攻击并进行防御。

（3）A 方再开展一次攻击。

（4）B 方检查攻击并进行防御。

3）对抗得分

对抗得分由以下部分构成：

（1）A 方第一次攻击成功。

（2）B 方第一次防御成功。

（3）A 方第二次攻击成功。

（4）B 方第二次防御成功。

以上各部分的具体分值可由双方在对抗前商议确定。第三轮的总分值应高于第二轮。

5.8　参考文献

[1] 鲍旭华，洪海，曹志华. 破坏之王：DDoS 攻击与防范深度剖析[M]. 北京：机械工业出版社，2014.

[2] 杨家海，安常青. 网络空间安全：拒绝服务攻击检测与防御[M]. 北京：人民邮电出版社，2018.

[3] 林沛满. Wireshark 网络分析的艺术[M]. 北京：人民邮电出版社，2016.

[4] 李禾，王述洋. 拒绝服务攻击/分布式拒绝服务攻击防范技术的研究[J]. 中国安全科学学报，2009，19(01)：132-136.

[5] 文坤，杨家海，张宾. 低速率拒绝服务攻击研究与进展综述[J]. 软件学报，2014，25(03)：591-605.

[6] 岳猛，王怀远，吴志军，刘亮. 云计算中 DDoS 攻防技术研究综述[J]. 计算机学报，2020，43(12)：2315-2336.

思考题

1. 什么是拒绝服务攻击？
2. 拒绝服务攻击的动机有哪些？
3. 拒绝服务攻击按不同的分类依据各有哪些类型？
4. 列出并简要说明典型的拒绝服务攻击。

5. 什么是分布式拒绝服务攻击?
6. 僵尸网络和 DDoS 攻击的关系是什么?
7. 开展 DDoS 攻击的僵尸网络涉及哪四种角色?
8. 简要说明 DDoS 攻击的一般过程。
9. 僵尸网络模型按工作机制可分为哪些类型?各自的特点是什么?
10. 简要说明拒绝服务攻击检测和防御的主要方法。