现代计算机技术与应用
2023 年 5 月第 5 卷第 2 期

对常见网络攻击的方法及对策探讨

安　亮

陕西省烟草公司铜川市公司，铜川

摘　要｜随着时代的发展，网络攻击在近几年变得越来越普遍，网络安全也成为当今社会极为重要的话题。网络攻击无处不在，它不仅危害到每一个网络用户，也可能对整个网络系统造成极大的危害，而本文讨论的是几种常见的网络攻击方式及一些常用的防护措施。

关键词｜网络；网络攻击；防护措施

1　网络攻击的特点

（1）从攻击者的攻击方式上来看

网络攻击的方式多种多样，攻击者会通过各种攻击方式达到自己的目的，获取自己所需的数据信息，总体来看，有以下几个特点，如表 1 所示。

表 1　攻击者的方式特点

Table 1　The way characteristics of the attacker

攻击特点	具体描述
规模大	网络攻击的规模非常大，可以波及到上千台计算机
手段杂	网络攻击时会使用各种手段发动攻击

作者简介：安亮，陕西省烟草公司铜川市公司初级工程师，研究方向：计算机技术与应用。
文章引用：安亮．对常见网络攻击的方法及对策探讨［J］．现代计算机技术与应用，2023，5（2）：1–8.
https://doi.org/10.35534/mcta.0502001

续表

攻击特点	具体描述
时间长	有些攻击手段持续时间会非常长，而且无法立即被识破
威胁性	网络攻击通常会损害网络系统，给用户带来了重大的安全威胁
自动化	攻击者使用自动攻击软件，大大提高了攻击效率

（2）从攻击技术的角度去看

攻击者开始攻击时，为了尽快达到攻击目标获取有效信息，会让自己攻击手段多样化，或者加大自己的攻击力度以及隐藏自己的攻击行为，使得防守方无法防守，所以从攻击者的角度去看待网络攻击还有以下几个特点，如表 2 所示。

表 2　攻击者的技术特点

Figure 2　Technical characteristics of the attacker

攻击者	利用特定的技术迅速地以自动化的方式重复发起攻击，达到对系统或网络发动攻击的目的
	通常利用各种不同的方法来获取攻击目标的系统信息，并且会使用软件、木马和其他方式的攻击工具来攻击网络资源
	通常会试图绕过安全系统，或者企图在攻击发生前隐蔽攻击行为
	非常具有侵略性，旨在破坏保护网络的安全系统，如防火墙和密码保护等
	可能会导致数据泄露、网络无法使用和网络服务被破坏

2　网络攻击的方式以及说明

2.1　网络攻击的形式

在这里主要阐述以下四种网络攻击方式，如图 1 所示。

图 1　网络攻击方式

Figure 1　Network attack mode

2.2 攻击方式的说明

（1）拒绝服务攻击

拒绝服务攻击主要分为两种，DoS 攻击和 DDoS 攻击，如图 2 所示。

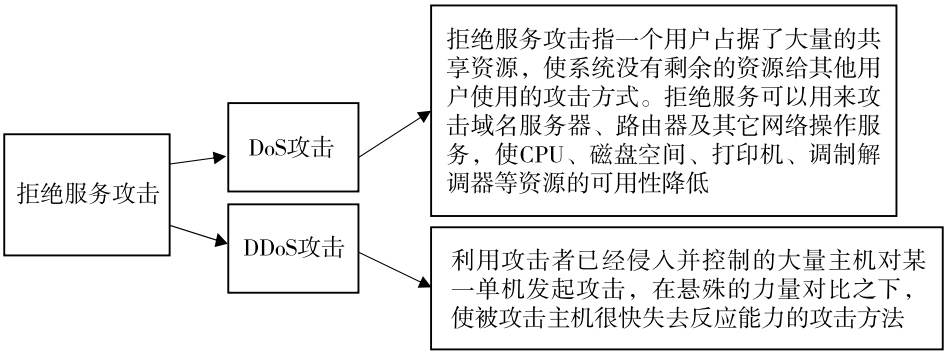

图 2 拒绝服务攻击

Figure 2 Denial of service attack

DoS，全称是 Denial of Service，意思就是拒绝服务。而 DoS 攻击一般都是单一的，使用一对一的方式，根据 TCP 协议，必须要经历三次握手的机制，通过制造并且发送巨大流量的垃圾数据，造成网络拥塞，使得被攻击目标（服务器、网站、计算机等）服务资源大量占用，可使用资源降低，致使被攻击目标无法正常服务于外界的正常用户。

DDos，全称是 Distributed Denial of Service，分布式拒绝服务攻击。DDoS 攻击是从 DoS 攻击发展而来，一个以上的 DoS 攻击源同时一起攻击单个目标就组成了 DDoS 攻击。现在攻击者可以通过伪造 IP 地址的手段，间接地增加攻击流量。通过伪造源 IP 地址，受害者会误认为存在大量主机与其通信。黑客还会利用 IP 协议的缺陷，对一个或多个目标进行攻击，消耗网络宽带及系统资源，使被攻击目标无法正常使用。

（2）特洛伊木马

特洛伊木马也是一种程序，攻击者通常会将这种恶意程序伪装成合法的、正常的程序依附在其他软件上（如游戏、远程操作软件等）。

https://doi.org/10.35534/mcta.0502001

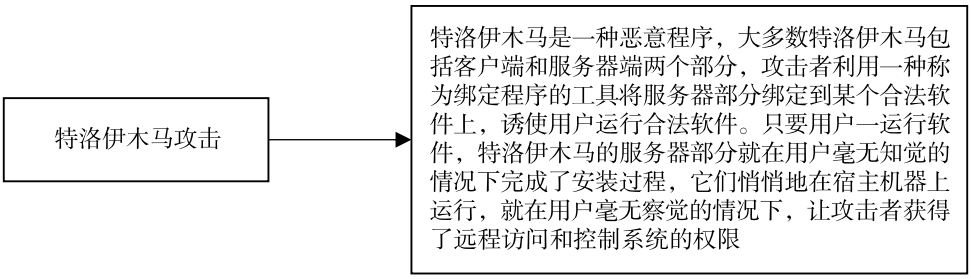

图 3　特洛伊木马挂机

Figure 3　Trojan horse attack

特洛伊木马程序应该包含两个部分程序：控制部分和入侵部分，也就是说攻击者通过控制部分程序，操纵入侵部分程序来实现操纵，对被入侵计算机实施非法操作，比如攻击或将被入侵计算机上的数据发送给攻击者等。

（3）端口扫描攻击

端口就是设备与设备之间进行数据交互的通信通道。

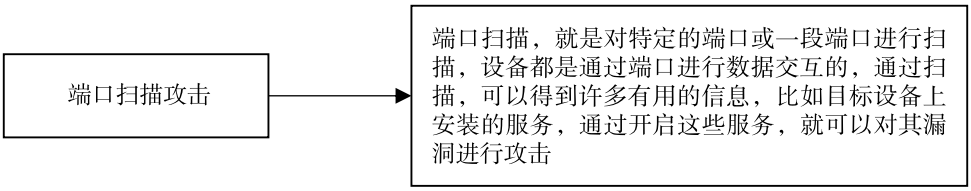

图 4　端口扫描攻击

Figure 4　Port scan attack

（4）安全漏洞攻击

系统漏洞并不是人为制造的，而是受限于当时科技的发展程度和人们的认知程度，并非故意造成的。

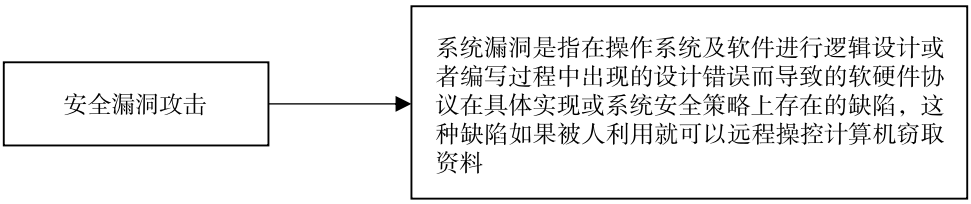

图 5　安全漏洞攻击

Figure 5　Security vulnerability attack

3 防范措施

对出现网络攻击的应对策略主要从以下两个方面考虑。

3.1 提高人员网络防范意识

网络攻击不管是什么形态，最终还是依靠人去完成的，所以在防范网络攻击时，第一要务应该是提高人员的网络安全意识，督促其养成以下几个良好的网络使用习惯。

（1）通过视频、讲座、线上线下等不同方式让员工通过学习了解网络安全的重要性、必要性和一些常用的网络安全防护手段。比如对使用的账号密码进行安全验证，设置密码复杂度规则，密码最少 8 位且必须包含大小写字母、数字和符号，这样可以有效消除原始密码及弱口令问题。避免攻击者通过暴力破解的手段，轻易拿到大门钥匙。

（2）不要浏览非法网站，不要运行和安装不明来路的安装程序，不要点击陌生邮件。因为非法网站缺乏监管，在浏览的同时就很可能会被网站上的病毒、木马攻击，通过网络感染计算机，导致信息或数据泄露。

（3）在离开电脑时将电脑关闭或者用快捷方式 WIN+L 将电脑设置为屏幕锁定状态，虽然现在因为网络的发展，导致每个人使用的账号密码特别多，少则几个、多则十几个，但是千万不要贪图方便将电脑的开机密码以及自己使用的账号密码明文写在电脑桌上或者写在便签纸上贴在电脑旁边，这会导致任何一个人都能够很顺利地利用机主在网络中的权限进行活动，窃取资料、数据等。

（4）在电脑上安装必要的杀毒软件，定期进行杀毒软件的升级，以及进行杀毒、体检漏洞修复等操作，这些可以有效避免木马、病毒等侵入计算机。

（5）如果有外来人员由于工作原因需要进入机房时，相关工作人员首先要确认来人身份是否是外来工作人员，然后对工作过程全程进行陪同和记录，对进入机房的人员还要进行身份登记等，确保不是攻击者采用社工攻击手段。

3.2 加强网络系统的安全防护

对公司的整个网络来说，一旦遭受攻击，网络就无法正常运行，影响公司

https://doi.org/10.35534/mcta.0502001

员工工作效率。那么从网络整体的防护上来说，最常见的就是防火墙和入网准入控制，防火墙是一种硬件设备及软件组合而成的集合体，它可以将内部网络和外部网络分开，按照使用人设定的规则，允许或者不允许数据进入网络。最大限度地阻止攻击者访问公司网络。网络准入控制主要是用来自主判断人员或者设备是否可以进入网络，并且禁止不符合要求的人员进入网络，一般包括人员或者设备的身份识别认证、安全检查及修复、网络权限控制及解除等步骤。有效解决了在内部网络中非法接入的问题。另外还可以通过备份的手段进行防护，就是说将重要的数据在其他设备上进行备份，在遭到攻击后可以通过备份的数据来进行恢复，将损失降低到最低。

3.3 加强网络使用管理工作

首先，在公司内部，对于计算机的管理可以按照部门进行 IP 段的划分，例如财务部门划分为 1 ~ 10，安全部门划分为 11 ~ 20，以此类推，当然也可以按照公司自身的实际情况来自己制定划分规则，将 IP 段与部门绑定，IP 与人员绑定，IP 与设备绑定，做好记录台账，能做到查询一个 IP 就能知道是哪台设备、设备在哪、谁在使用，而网络工作人员一旦发现 IP 有可疑情况，就可以立即锁定设备、人员，及时进行处理。避免病毒、木马或者其他攻击方式通过该 IP 进行感染，导致整个网络被攻破，数据泄露。

其次，从员工使用的角度去看，每个人使用的网络虽然都在同一个局域网内，但是使用时对于网络的关注点是绝对不一样的，例如营销部门可能更关注的是公司的销售数据，那么他们在使用网络时查看的相关数据一定是跟销售有关，而财务部门在网络中看的绝大多数是财务的数据信息，那么就可以以部门为单位对网络访问权限进行不同的设置，甚至对于公司的网络管理人员也可以进行权限的划分，例如 A 可以管理网络安全设备，但是不能管理路由器设备，而 B 工作人员可以管理路由器设备但是不能管理网络安全设备，通过在网络中对重要区域做好访问限制，从而降低网络风险，减少信息数据泄露的可能性。

再次，从网络管理的角度去看，可以按照不同的网络安全等级进行网络区域划分，比如可以分成互联网服务区、服务器区、网络安全区、办公网络区等，

公司的网络管理部门网络权限最大，可以查看公司网络中所有的部分，但是不能查看如财务数据、销售数据等，而财务人员可以查看财务数据，但不能查看网络安全设备等，通过网络区域的划分，将网络访问的权限最小化，确保工作任务能够顺利完成但是又避免了其他操作的可能性，降低了账号的使用风险，让数据泄露的危害降低。

最后，要建立健全计算机及网络使用的规范制度，让网络用户知晓在网络中应该干什么不应该干什么，比如要保护好自己的账号密码，不能随意泄露自己的账号密码，不能将重要文件随意放在共享网络中，确保无关人员不能随意查阅自己的重要文件等。

4　结语

随着科技的不断发展，计算机及网络技术也在向前迈步，而网络攻击也随着技术的发展越来越频繁，攻击手段也越来越高明，网络攻击所付出的代价也令人们越来越重视网络安全。网络安全靠人民，网络安全为人民，网络安全防护技术也将会越来越成熟。

参考文献

［1］裘萍．现阶段网络攻击技术及网络安全探讨［J］．网络安全技术与应用，2022（6）．

［2］彭修杰．计算机网络常见攻击方法及防范对策［J］．电子技术与软件工程，2014（23）：236–237．

［3］周雅立．浅谈计算机网络攻击方法的探讨及其如何防范［J］．才智，2010（27）．

［4］贾硕．网络攻击的方法及对策［J］．电子技术与软件工程，2018（5）．

https://doi.org/10.35534/mcta.0502001

Discussion on the Methods and Countermeasures of Common Network

An Liang

Shaanxi Province Tobacco Company Tongchuan City Company, Tongchuan

Abstract: With the development of The Times, cyber attacks have become more and more common in recent years, and network security has become a very important topic in today's society. Network attacks are everywhere, it not only harms every network user, but also may cause great harm to the whole network system, and this paper discusses several common network attacks and some commonly used protection measures.

Key words: Network; Network attack; Protective measures