计算机网络攻防渗透技术的分析和研究

张佩云 郝鹏宇
硅湖职业技术学院，江苏 苏州 215300

[摘要]信息技术快速发展，计算机网络成现代必备基础设施。但网络规模扩大，应用变复杂，网络攻击多发，安全威胁加剧。网络攻防渗透技术是保障网络安全重要方式，涉及分析网络攻击技术、设计防御措施、实施渗透测试等。文章分析当下主流网络攻击技术如 DOS/DDOS 攻击、Web 渗透攻击，探讨相应防御和渗透防护技术，介绍渗透测试技术基本流程与方法，最后展望人工智能、云计算、物联网等新兴技术给网络安全领域带来的挑战与机遇，给网络安全技术研究与实践提供理论参考与技术指导。

[关键词]计算机网络；网络攻击技术；渗透防护技术
DOI：10.33142/nsr.v2i3.17728 中图分类号：TP39 文献标识码：A

Analysis and Research on Computer Network Attack and Defense Penetration Technology

ZHANG Peiyun, HAO Pengyu
Silicon Lake Vocational & Technical Institute, Suzhou, Jiangsu, 215300, China

Abstract: With the rapid development of information technology, computer networks have become an essential modern infrastructure. However, as the scale of the network expands, applications become more complex, network attacks become more frequent, and security threats intensify. Network attack and defense penetration technology is an important way to ensure network security, involving analyzing network attack technology, designing defense measures, and implementing penetration testing. The article analyzes the current mainstream network attack technologies such as DOS/DDOS attacks and Web penetration attacks, explores corresponding defense and penetration protection technologies, introduces the basic process and methods of penetration testing technology, and finally looks forward to the challenges and opportunities brought by emerging technologies such as artificial intelligence, cloud computing, and the Internet of Things to the field of network security, providing theoretical reference and technical guidance for network security technology research and practice.

Keywords: computer network; network attack technology; penetration protection technology

引言

随着互联网的广泛普及以及计算机网络技术持续向前发展，网络环境变得日益复杂且更为开放，网络安全方面的问题渐渐变成了各个行业都重点关注的对象。网络攻击所采用的手段一天比一天多，而且越来越智能，这对信息系统的平稳运行以及数据安全形成了十分严峻的考验。传统的防御技术虽说在某种程度上缓解了安全方面的威胁，但是面对新型的攻击，其防护的效果还是显得不够充分。所以，全面且细致地去剖析计算机网络攻击技术，进一步提升防御以及渗透防护的能力，系统性地开展渗透测试工作，这已然成为了保障网络安全极为关键的一个环节。紧扣计算机网络攻防渗透技术这一主题，从攻击技术分析、防御措施、渗透测试技术以及未来的发展趋势等四个不同的方面来展开阐述，以此为构建起更为坚实的网络安全防线给予相应的理论支撑以及技术方面的帮助。

1 计算机网络攻击技术分析

1.1 网络攻击概述

网络攻击中是指攻击者主要利用系统漏洞、技术缺陷或人为疏忽，对网络环境中的硬件设备、软件系统、数据或用户造成损害的行为。攻击者一般会仔细侦察目标系统的薄弱环节，运用多种技术手段避开防护措施，以此达成破坏系统、窃取数据或者干扰正常服务的目的。随着攻击技术持续发展，攻击方式变得越来越智能化和隐蔽化，网络安全防御所面临的挑战也日益严峻。

1.2 常见网络攻击类型

网络攻击的类型繁多，包含从简单的端口扫描、网络嗅探，一直到复杂的高级持续性威胁（APT）均有涉及。常见的攻击手段有拒绝服务攻击（DOS/DDOS）、系统漏洞利用、网络钓鱼、恶意代码植入以及针对 Web 应用的注入攻击等。

1.2.1 DOS 及 DDOS 攻击技术

拒绝服务攻击（Denial of Service, DOS）属于一种攻击手段，它是借助向目标系统发出数量众多的无效请求，进而将目标系统的资源耗尽，致使服务无法正常运转。DOS 攻击一般依靠单一的攻击来源，虽说具备一定的破坏作用，然而相对而言是比较容易被识别出来的，防御起来也并非难事。分布式拒绝服务攻击（Distributed Denial of Service, DDOS）与之不同，它会利用多个处于受控状态

的僵尸主机一同发起攻击，如此一来，攻击的规模得以明显扩大，隐蔽性也得到了极大的提升。DDOS 攻击不但能够冲破传统防御设备所构建的防护网，而且还可能引发网络出现拥塞状况，甚至让系统发生崩溃情况，对业务的连续性产生极为严重的影响。攻击者常常会凭借漏洞去感染大量的终端设备，进而把这些终端组织成僵尸网络，以此来发动规模庞大的协同攻击。对于 DOS/DDOS 攻击而言，其技术防护主要涵盖了流量清洗、访问控制以及行为分析等多种不同层次的防御策略。

1.2.2 系统漏洞攻击技术

程序员所编写的计算机程序难以避免地会存在或多或少的不足，而这些漏洞也会在计算机程序的持续使用中逐渐显现出来，但是程序员也会编写更多的补丁来修补程序，原有的系统程序会在补丁的帮助下逐渐完善。从漏洞出现到补丁修复的过程中，会存在一些网络攻击。针对网络协议中存在的缺陷，一些不法分子可能会使用虚假的数据包使程序单纯地认为数据包中的信息是合法的，等到数据包进入系统以后才会影响程序，这属于典型的电子欺骗攻击，其影响程度与技术本身相关。一些不法分子要预先掌握用户计算机系统的情况，才能实现电子欺骗攻击，用户的计算机会在遭受攻击的阶段丧失通信能力，不法分子将特定的信息包传输到用户的计算机系统后，执行错误的身份验证，以此来突破计算机的防护程序，由于电子欺骗的攻击需要在特定的情况下实现，许多不法分子会通过修改 IP 地址来获取防火墙的信任，进行持续不间断的攻击。

1.2.3 Web 渗透攻击技术（SQL 注入、XSS 等）

Web 应用身为现代网络服务极为重要的承载形式，凭借着其开放性以及复杂性这两个特点，已然成为了攻击者眼中主要的攻击对象。SQL 注入攻击是通过往输入数据里植入恶意的 SQL 代码，进而对数据库的操作逻辑予以破坏，最终达成数据出现泄露情况、遭到篡改或者后台服务器被控制的目的。跨站脚本攻击，也就是 Cross-Site Scripting，简称 XSS，它是借助注入恶意的脚本代码这一手段，致使用户的浏览器去执行那些不安全的操作，进而窃取到用户的身份信息，或者是对会话进行劫持。除此之外，Web 渗透攻击还涵盖了跨站请求伪造，即 CSRF，还有利用文件上传漏洞等多种不同的攻击方式。这些攻击技术往往都是依靠着程序设计方面存在的缺陷以及输入校验不够严格的情况来实施的。对于这些攻击的防御，就需要综合运用安全编码规范、输入过滤以及 Web 应用防火墙，也就是 WAF 等一系列的手段来加以应对。

2 网络防御与渗透防护技术

2.1 防火墙与入侵检测系统（IDS/IPS）

防火墙是网络安全领域极为重要的一道防线，其主要职责在于对进出网络的数据流加以监控以及实施相应的控制举措，从而阻断那些未经许可的访问行为，进而切实保障网络边界的安危状况。现代意义上的防火墙除了能够支撑基于包过滤所涉及的基础性功能之外，还拥有诸如状态检测、应用层过滤以及深度包检测等诸多能力，凭借这些能力来应对日趋复杂的各类攻击行为。入侵检测系统（IDS）以及入侵防御系统（IPS）主要用于对网络以及主机活动展开实时的监测操作，以此来精准识别出其中存在的异常行为以及潜在的威胁情况。IDS 主要是负责发出报警提示信息，而 IPS 则具备自动阻断的相关功能。将防火墙和 IDS/IPS 相互结合起来，便能够构建起多层的防御架构体系，以此有效地防范网络入侵以及恶意攻击等事件的发生，从而切实保障网络环境能够保持稳定且安全的良好状态。

2.2 漏洞扫描与补丁管理

漏洞属于系统安全风险的关键来源之一，及时察觉并修复漏洞在防御攻击方面属于重要环节，漏洞扫描技术借助自动化工具针对系统、应用程序以及网络设备展开全面检测，以此来识别出存在的安全缺陷以及风险点，扫描得出的结果可助力安全人员去评估威胁等级，并制定出具有针对性的修补方案。补丁管理其实就是对系统漏洞实施修补以及升级的这一过程，其能够修复软件缺陷，进而提升系统的稳定性以及安全性，科学的补丁管理流程需要做到及时测试以及部署补丁，防止因为更新不及时或者操作不当致使系统出现异常或者存在安全隐患。把漏洞扫描和补丁管理相结合起来，可以有效地封堵攻击者利用漏洞发动攻击的途径。

2.3 Web 应用防护技术

Web 应用因其具备开放性以及复杂性的特点，已然成为网络攻击所着重瞄准的关键目标。Web 应用防护技术涵盖了诸如输入验证、身份认证、权限控制、会话管理以及日志审计等一系列举措，其用意在于从源头处尽力削减攻击所带来的风险。就技术手段来讲，Web 应用防火墙（WAF）可对 HTTP/HTTPS 流量予以实时的监控，进而拦截像 SQL 注入、跨站脚本这类常见的攻击请求，以此来阻止恶意流量进入到后台系统当中。安全编码规范以及漏洞修复构成了减少 Web 漏洞极为重要的基础，而安全测试以及动态防护则能够给予持续不断的保障。除此之外，内容安全策略（CSP）等相关技术同样可以有效地抵御来自客户端的脚本攻击，从而促使 Web 应用的整体安全性得以提升。

3 渗透测试技术与方法

3.1 渗透测试基本流程

渗透测试通常会遵循一系列的阶段，依次是信息收集、漏洞分析、漏洞利用、权限提升、保持访问权限以及编写测试报告等（见图 1）。一开始，测试人员会借助多种多样的手段去收集目标系统的相关信息，像网络拓扑情况、开放的端口状况、服务版本详情以及操作系统的类型等方

面，这些收集到的信息能够给后续的攻击策略给予相应的依据。接着开展漏洞扫描以及风险评估相关工作，从中识别出潜在存在的安全方面的缺陷。之后利用已知的漏洞或者是自行定制的攻击方法来对目标展开攻击尝试，以此来验证这些漏洞实际可利用的可能性，并且尝试着去提升权限，进而达成对系统更为深层次的访问控制目的。要撰写出详尽完备的测试报告，把所发现的安全风险以及对应的修复建议都阐述清楚，从而为企业网络安全防护事宜提供一定的参考依据。渗透测试的整个流程是比较严谨的，始终强调要合法合规行事，务必要确保所有的测试活动都是在获得授权的范围之内开展的。

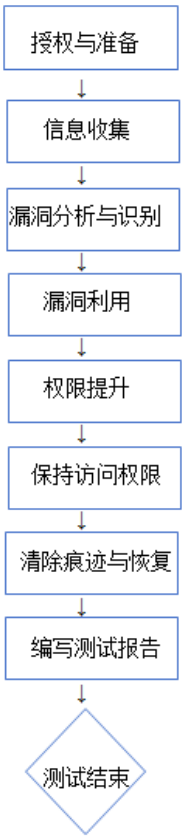

图 1　渗透测试流程图

3.2 信息收集与漏洞扫描技术

信息收集乃是渗透测试当中极为关键的一个基础环节，其主要是借助主动以及被动这两种方式来去获取目标网络还有系统相关的各类信息。就主动方式来讲，这里面包含了像端口扫描、服务探测以及操作系统指纹识别等一系列操作，凭借这些操作便能够较为详尽地将目标环境的具体细节给掌握清楚。而被动方式则是通过公开资源、社交工程或者网络嗅探等这类方式来获取信息，如此一来便能够在很大程度上降低被对方发现的风险。漏洞扫描会运用自动化工具针对系统展开全面细致的检测，从而去识别出配置存在错误、软件漏洞没有打补丁以及安全策略有所缺失等诸多问题。把数据库和漏洞库结合起来之后，扫描工具就能够迅速且精准地定位到已知漏洞，进而为后续的漏洞利用环节筑牢坚实的基础。有效的信息收集工作以及漏洞扫描操作，能够颇为有效地提升渗透测试所具有的针对性以及工作效率。

3.3 漏洞利用与权限提升

漏洞利用在渗透测试里占据着极为关键的地位，它是借助对漏洞的利用来达成对目标系统加以控制或者从中窃取信息的目的。测试人员会依据漏洞扫描所得到的结果，运用各式各样的技术手段去构建攻击载体，像缓冲区溢出、代码注入、逻辑绕过这类情况，进而开展攻击方面的相关行为。当成功地利用了漏洞之后，渗透测试者往往会尝试着去做权限提升这件事，也就是从普通的用户权限去争取获得更高的系统管理权限，以此来对系统的安全态势展开更为全面的评估。权限提升所涉及到的技术包含有本地提权漏洞的利用、提权工具的使用以及对配置错误加以利用等等，其常见的方法涵盖了绕过权限验证、提升进程的权限、获取内核级别的访问等内容。权限提升一方面能够验证漏洞究竟有多么严重的程度，另一方面还能助力于发现后续可能存在的攻击路径，从而进一步提升渗透测试所能达到的深度以及广度。

4 未来发展趋势与技术挑战

4.1 人工智能与机器学习在攻防中的应用

人工智能（AI）以及机器学习（ML）技术于网络安全领域所发挥的应用作用变得日益普遍起来，其一方面给防御事宜增添了全新的工具，另一方面同样被攻击者拿来当作是能够强化自身攻击能力的手段。借助大数据方面的分析操作以及智能模式的识别举措，安全系统便可以更为精确地去检测那些异常的行为以及未知的威胁情况，进而达成实时的响应效果以及实现自适应的防护状态。与此在恶意软件的识别工作、入侵检测相关事务以及异常流量的分析事宜等方面，机器学习算法均展现出了颇为显著的优势特点[1]。不过，攻击者也会凭借 AI 技术来开展自动化攻击行动、实施智能化漏洞挖掘操作并且绕开防御机制，如此一来，便能够让攻击的隐蔽性得以进一步提升，其效率同样也会有所提高。所以说，未来的网络安全攻防局面将会呈现出“以 AI 对抗 AI”这样的态势走向，技术双方展开的博弈较量势必会变得更加激烈且复杂多变。

4.2 云计算及虚拟化环境安全问题

云计算的普及应用在很大程度上提高了计算资源所具有的灵活性以及可扩展性，然而与此也催生出全新的安全方面风险。虚拟化技术虽说达成了资源的高效利用目的，可是像虚拟机逃逸、虚拟网络攻击还有跨租户数据泄露这类问题却日渐凸显出来[2]。云环境具备的多租户共享这一特性致使攻击面变得更为宽广，攻击者存在通过云服务漏洞或者配置错误来获取对多个租户资源控制权的可能性。

除此之外，云平台安全管理的复杂程度有所提高，对于身份认证、访问控制以及数据加密等方面提出了更高的要求。怎样确保云环境的隔离性与数据安全，已然成为网络攻防技术相关研究的关键指向所在。

4.3 物联网（IoT）安全挑战

物联网设备广泛普及，给网络攻击开了新入口。IoT设备一般资源有限，安全防护差，常被攻击者盯上。物联网系统设备身份难验证，固件有漏洞，通讯协议不安全[3]。攻击者能劫持IoT设备发动大规模攻击，还能偷敏感信息。物联网种类多、数量大，管理更难。智能家居、工业控制、智慧城市等领域发展快，建物联网综合防护体系迫在眉睫。

5 结语

随着计算机网络技术发展迅速，网络安全问题日益突出，网络攻防渗透技术在保障信息系统安全方面有重要作用，本文分析了主流网络攻击技术及其机制，探讨了网络防御与渗透防护关键技术，介绍了渗透测试流程和方法，展望了人工智能、云计算、物联网等带来的挑战与机遇，网络攻防技术需不断创新完善，未来安全防护体系要利用先进技术，加强安全防御能力建设，实现动态防御和主动防护，有效应对网络攻击，保障信息系统安全稳定运行，为数字经济发展提供安全保障。

[参考文献]

[1]程志宇.计算机网络攻防渗透技术分析[J].中国信息界,2024(4):7-9.
[2]田永民.计算机网络攻防渗透技术研究[J].无线互联科技,2022,19(20):149-151.
[3]王芸芸.网络安全保障与电力网络攻防技术[J].电子技术,2021,50(11):72-73.

作者简介：张佩云（1989—），女，江苏省淮安市涟水县人，助教，2015年6月毕业于南京信息工程大学，硕士研究生，现在硅湖职业技术学院，计算机科学与技术学院任专业教师。