设计研究与应用

浅谈黑客攻击技术及防御方法

赵小厦[1] 夏嵬[2]
（1.南京技师学院，江苏南京 210023；2.南京信息职业技术学院，江苏南京 210023）

摘 要：随着信息科技的迅速发展，网络安全愈加重要。本文系统全面地介绍了黑客攻击技术和防御，叙述了黑客入侵过程中的行为，分析了不同阶段使用的不同入侵攻击方法和辅助工具及预防或防御方法。

关键词：黑客攻击技术；防御方法；网络安全
中图分类号：TP393.08 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2023.01.040
本文著录格式：赵小厦,夏嵬.浅谈黑客攻击技术及防御方法[J].软件,2023,44(01):147-149

Brief Introduction on Hacker Attack Technology and Defense Methods

ZHAO Xiaosha[1], XIA Wei[2]
(1.Nanjing Technician College, Nanjing Jiangsu 210023;
2.Nanjing Vocational College of Information Technology, Nanjing Jiangsu 210023)

【Abstract】：With the rapid development of information technology, network security is becoming more and more important. This paper systematically and comprehensively introduces hacker attack technology and defense, describes the behavior of hackers in the process of intrusion, and analyzes the different intrusion attack methods, auxiliary tools and prevention or defense methods used in different stages.

【Key words】：hacker attack technology;defense methods;network security

黑客是一群计算机技术高超且乐于钻研程序设计的人，在计算机技术的发展过程中，一部分人用他们高超的技术造诣促成了优秀计算机产品的问世等，推动了计算机技术的发展，一部分人致力于入侵或者破坏其他计算机，受到或多或少的惩罚或反对。随着互联网技术的不断发展，黑客攻击技术也层出不穷花样多变，攻击破坏程度也越来越大。

黑客入侵攻击过程分为 3 个阶段：入侵攻击前阶段、入侵攻击中阶段和入侵攻击后阶段，如图 1 所示[1]。入侵攻击前阶段主要是黑客攻击前所做的准备工作，通过网络踩点、网络扫描和查点确定目标 IP 地址范围，收集目标主机操作系统的类型、开放了哪些网络服务、是否存在漏洞等信息；入侵攻击中阶段，如果能够通过多种方式获取访问权，则提升权限而进行窃取信息或者破坏活动等入侵攻击，否则采用拒绝服务攻击方法进行入侵攻击；入侵攻击后阶段，主要是针对能够获取访问权限的入侵攻击，清除入侵痕迹包括清除目标主机的日志等数据信息并可能会创建后门。黑客在攻击过程中不同的阶段会采用不同的攻击技术方法。

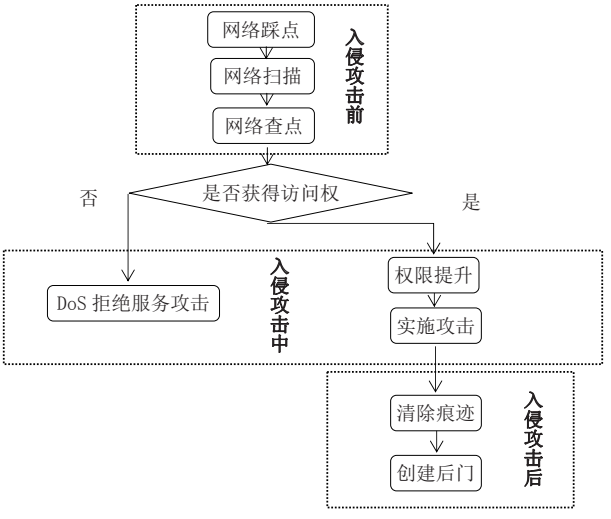

图 1 黑客入侵攻击流程图

Fig.1 Hacker intrusion attack flow chart

作者简介：赵小厦（1982—），女，河南南阳人，硕士研究生，讲师，研究方向：软件技术、网络安全；夏嵬（1979—），男，湖北武汉人，博士研究生，讲师，研究方向：人工智能。

1 黑客攻击前阶段

黑客获取相关信息后，在进行入侵攻击之前，首先要获得系统的基本访问权限才能登录目标主机，这需要通过密码技术实现，目前常用的是密码窃听术和字典攻击术。常用的密码窃听辅助工具有 Sniffer Pro、TCPdump、LC4、Read SMB 等，常用的字典攻击辅助工具有 LC4、John the RIPper、NAT、SMBCrack、SMBGrind 及 fgrind 等。针对暴力破解操作系统口令，可以启动账户锁定策略。

黑客在局域网中采用网络监听技术 [2] 来获得有用数据，比如账户和密码、服务器地址和防火墙防范规则等。网卡工作在数据链路层，传输的数据是以帧为单位，有几部分构成，其中帧头包括数据的目的 MAC 地址和源 MAC 地址。网卡在收到数据时会查看数据头的目的 MAC 地址，符合与本地 MAC 地址或广播地址的数据才接受，否则丢弃。但是如果安装了 Sniffer 等监听工具，就会把网卡置于混杂模式，接收一切所能收到的数据，可以捕获数据包和分析数据包从而获得敏感数据。常用的网络监听工具有 Sniffer Pro、Wireshark、Net monitor、EffTech HTTP Sniffer 等。防范网络监听的方法是尽量在传输口令等敏感数据时对其加密，尽量采用安全的网络拓扑，并通过划分 VLAN 等技术手段来划分网络。

黑客在交换环境采用 ARP 欺骗攻击技术 [3] 来嗅探用户发送的信息。ARP 是地址解析协议，是利用网络层地址来获取数据链路层地址的协议，已知网络层的 IP 地址转化为数据链路层的 MAC 地址。黑客可以分别向目的计算机或被欺骗的计算机发送伪造的 ARP 应答，其包含的源 MAC 地址不是对应的被欺骗的计算机的或目的计算机的，而是自己的 MAC 地址，这样做的效果就使得目的计算机与被欺骗的计算机之间的通信数据都会转发到黑客所在的计算机，从而黑客就可以嗅探被欺骗的计算机和目的计算机之间有用的通讯数据，或使得目的主机进入死循环。防范 ARP 欺骗攻击的主要方法：（1）静态绑定网管等关键主机的 MAC 地址和 IP 地址的对应关系；（2）使用一些第三方的 ARP 防范工具，如 360ARP 防火墙等；（3）通过加密传输数据、使用 VLAN 技术细分网络拓扑等方法。

2 黑客攻击中阶段

黑客如果能够获得目标计算机的访问权，则对目标主机的一些敏感数据进行篡改、添加、删除及复制等破坏活动。获取访问权后为了更有利地进行破坏活动，会进一步采用各种攻击手段提升用户权限，如提升至超级管理员权限可以完全控制系统。提升权限技术通常包括利用现有的软件分析相关密码文件从而破解系统中用户名及口令、利用操作系统和服务程序的漏洞、利用管理员不正确的系统配置等。目前常用口令破解工具包括 Cain、John The RIPper、L0phtCrack、Aoxppr 等，获取 Windows 管理员权限的软件有 Invisible Keystroke Logger、Getadmin、Sechole 和 Lc_message 等。

黑客攻击经常使用一种非常重要的方法就是木马技术，使用木马技术黑客可以轻易地入侵并控制目标计算机，并在用户不知情情况下窃取信息或者进行破坏活动。常见普通木马的结构一般是客户端 / 服务器（即 C/S）模式，C 和 S 之间采用的通信方式是 TCP/UDP，黑客端使用的是客户端程序，被攻击的计算机上安装的是服务器端程序。木马服务器端程序隐藏和伪装在被控计算机中，采用非授权式“里应外合”的方式与客户端进行通讯连接，从而实现黑客对被攻击的计算机的监听和控制。常见的木马分为远程访问型木马、键盘记录木马、密码发送型木马、破坏性木马、代理木马、FTP 木马和下载型木马。常见的木马有冰河木马和灰鸽子木马等。对木马的检测，可以通过查看端口（如用 netstat 命令，用 Fport、TCPView 等工具）、检查注册表、检查 DLL 类（如用 IceSword 工具检测）。对于木马的防御，要提高防范意识，不要打开陌生人的邮件，去正规网站下载软件，尽量不适用在线状态安装软件。对于木马的清除最简单的方法就是使用杀毒软件。

如果黑客不能获得目标计算机的访问权，一般采用拒绝服务攻击技术对目标计算机进行攻击。实施拒绝服务攻击（即 DoS 攻击）的最终目的是迫使目标计算机停止提供服务，或所有访问目标计算机资源的请求都得不到相应的响应 [4]，采用的方法有两种：一种是以消耗目标计算机的资源（如内存、磁盘空间等）为目的，故意制造了大量非法的、无用的连接请求来让目标计算机响应，从而占用了目标计算机所有资源，造成目标计算机死机等，从而导致正常请求的服务中断，常用的攻击方法有 SYN Flood、死亡之 Ping、ICMP Flood、UDP Flood、Teardrop 和 Land 等；另一种就是以消耗目标计算机链路有效带宽为目的，故意发送大量的有用或无用数据包，全部占用目标计算机的整条链路带宽，从而导致正常用户的请求因为通信阻塞而无法到达目标计算机。在此详细介绍其中的 SYN Flood 攻击技术，由于该技术是利用 TCP 连接的缺陷而实施的，故在介绍其之前首先回顾下建立 TCP 连接步骤：（1）客户端发送 SYN 包到服务器端；（2）服务器分配一定的资源同时发回 SYN/ACK 包，接着等待 ACK 包的返回；（3）客户端回复

ACK 报文。SYN Flood 攻击技术是大量发送 SYN 报文，但不返回 ACK 报文。服务器由于没有收到客户端的确认包故会隔段时间重发 SYN/ACK 包，一直到超时才将此条目从未连接队列删除。从而导致多次重发操作和预留大量资源给没有完全建立的连接。SYN Flood 攻击会导致服务器由于资源最终占用过多，而没有能力去完成其他操作或响应正常的网络请求。网上可下载很多 SYN Flood 攻击工具，如 SYN-Killer、Pdos 和 XDoS 等。现在很多黑客为了大大增强破坏力，会采用分布协作的大规模 DoS 攻击来实施。通常黑客会挟持网络上很多计算机，在它们上面部署攻击代理程序而形成肉鸡，黑客控制众多的肉鸡采有 DoS 技术攻击目标服务器。常用的有 Smurf 技术、Autocrat 等工具。针对 DDoS 攻击技术，目前应用最普遍的方法是采用防火墙 [5]。

有时黑客为了安装木马或者传播运行病毒，会采用缓冲区溢出攻击技术。缓冲区是一块连续的计算机内存区域。缓冲区溢出是在程序编译完以后，缓冲区中存放数据的长度事先已被程序或者操作系统定义好，如果写入超出程序的缓冲区长度的内容，会导致缓冲区溢出，覆盖其他空间的数据，从而破坏程序堆栈，使得程序执行其他指令。黑客正是利用缓冲区溢出发生时，使程序执行其事先设置好的一段代码或者程序，最终获得目标计算机的控制权或者转而执行相应木马程序或病毒程序。C 和 C++ 等语言在编译的时候没有进行内存检查，如数组的边界检查和指针的引用或标准 C 库中还存在许多非安全字符串操作，这都容易发生缓冲区溢出异常。为预防缓冲区溢出攻击技术，需要软件编程者提高安全编程意识，如加强边界检查、在程序指针失效前进行完整性检查等，需要计算机的管理使用人员及时给操作系统升级打补丁。

3 黑客攻击后阶段

为了避免被目标计算机的管理员发觉，黑客在完成入侵之后需要清除其中的系统日志文件、应用程序日志文件和防火墙的日志文件等。常用的清除日志工具有 ZAP、WZAP 和 WTED 等，或使用简单的 Shell 命令 Echo 把日志文件内容写入空。

若黑客为了长期入侵目标计算机，会在目标计算机中建立访问后门或者安装木马。常用的工具有 Rootkit、Sub7、Cron、AT、Netcat、VNC 等。

黑客技术不断发展，呈现越来越复杂化，加上与病毒技术相互融合，攻击的破坏程度也越来越大。但网络上可以用的各种攻击工具非常多，使用也越来越简单，对黑客的技术水平也要求越来越低。在防御黑客攻击的道路上也会有越来越多的困难要解决。

本文叙述了黑客入侵过程中不同阶段使用的不同入侵攻击方法和辅助工具，以及预防或防御方法，对于需要系统全面了解黑客攻击技术的读者很有用。

参考文献

[1] 周明全,吕林涛,李军怀.网络信息安全技术[M].西安:西安电子科技大学出版社,2016:120-121.

[2] 王双庆.网络机房中网络监听与防范技术探究[J].电脑与电信,2018(Z1):50-52.

[3] 徐书欣,赵景.ARP欺骗攻击与防御策略探究[J].现代电子技术,2018,41(8):78-82.

[4] 石淑华,池瑞楠.计算机网络安全技术(第4版)[M].北京:人民邮电出版社,2021:67-68.

[5] 杨峰.计算机网络中的黑客攻击技术及其防御技术研究[J].软件导刊,2013,12(8):131-132.