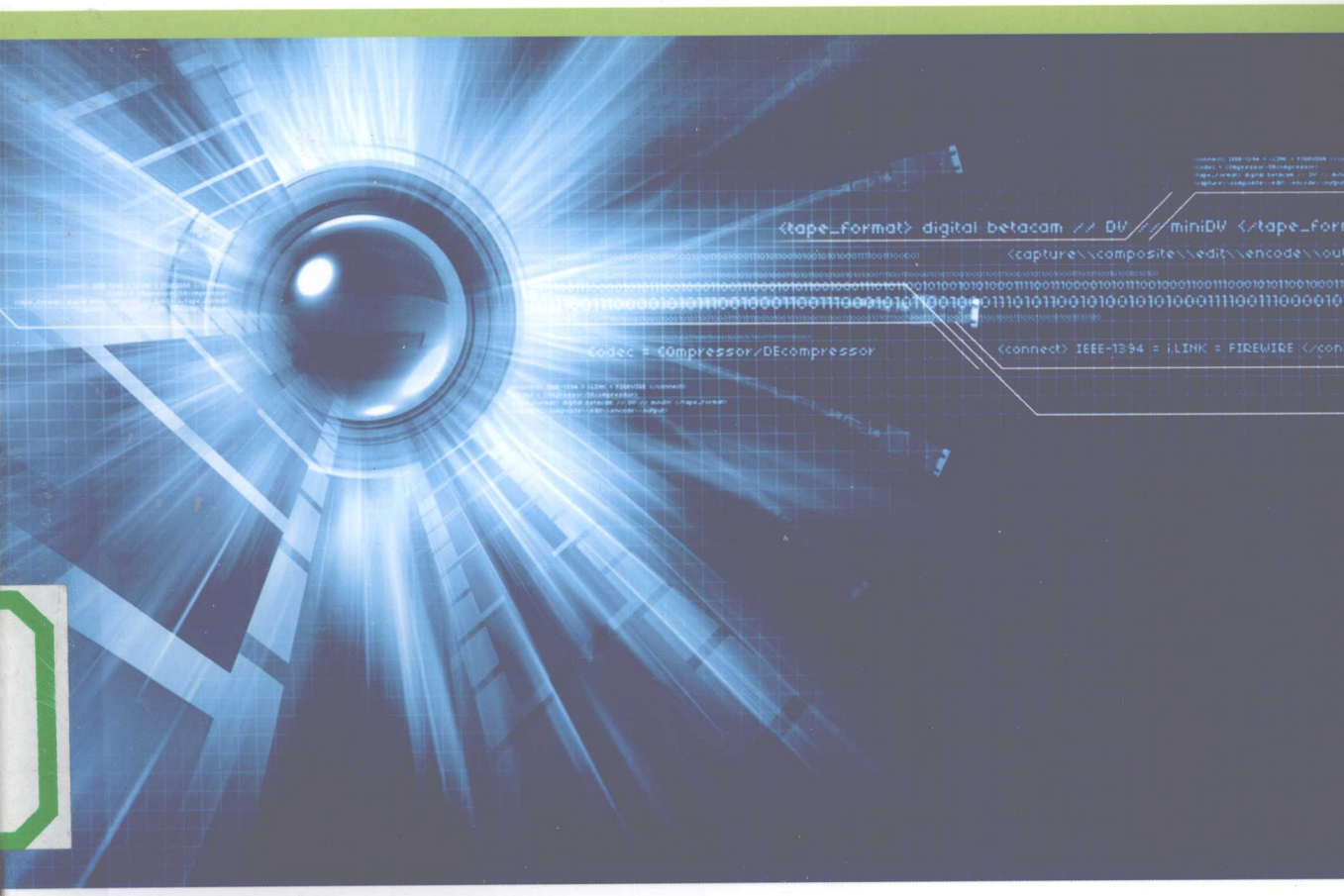
国家信息安全培训丛书

信息安全积极防御技术

中国信息安全测评中心　编著



航空工业出版社

国家信息安全培训丛书

信息安全积极防御技术

中国信息安全测评中心　编著

航空工业出版社

北京

内 容 提 要

本书从信息安全积极防御的视角描述了信息安全积极防御的技术基础，并给出了10个信息安全积极防御的实验。在信息安全积极防御技术基础方面，描述了以主动攻击为核心的积极防御的工作步骤和流程，并重点介绍了网络和系统信息搜集技术、密码破译以及拒绝服务、缓冲区溢出、木马和病毒的积极防御技术；通过10个可操作、练习的信息安全积极防御实验，理论结合实践，帮助读者更深刻地理解和实践信息安全积极防御技术。

本书是中国信息安全测评中心注册信息安全专业人员（CISP）和注册信息安全员（CISM）的正式教材，可作为高等院校信息安全专业的学生教材，并可作为信息安全培训和从业人员的信息安全积极防御的实验参考书。

图书在版编目（CIP）数据

信息安全积极防御技术/中国信息安全测评中心编著.
北京：航空工业出版社，2009.6
（国家信息安全培训丛书）
ISBN 978-7-80243-277-2

Ⅰ.信… Ⅱ.中… Ⅲ.信息系统—安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字（2009）第061520号

信息安全积极防御技术
Xinxi Anquan Jiji Fangyu Jishu

航空工业出版社出版发行
（北京市安定门外小关东里14号 100029）
发行部电话：010-64815615 010-64978486
北京地质印刷厂印刷 内部发行
2009年6月第1版 2009年6月第1次印刷
开本：787×1092 1/16 印张：16.5 字数：406千字
印数：1—3000 定价：49.00元

国家信息安全培训丛书

序

世界正经历一场伟大的信息革命，信息成为一种重要的战略资源。它改变着人们的生活方式和工作方式，形成新的社会形态。

随着我国社会信息化进程的不断发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的工作中发挥着越来越重要的作用。然而，信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。由于信息系统是一个复杂巨系统，它存在着脆弱性，信息安全问题不断暴露。信息安全关系到国家的经济安全、政治安全、军事安全和文化安全。信息安全已经成为维护国家安全和社会稳定的一个重要因素。

当前，社会对信息安全专业人员的需求逐年增加。发展信息安全技术与产业，关键是人才。培养信息安全领域的专业人才，已成为当务之急。高素质的信息安全人才队伍是保障国家重点基础网络和重要系统安全的基石，是制定信息安全发展战略规划与政策并建设国家信息安全保障体系的骨干力量，是发展我国信息安全产业的排头兵。

目前我国的信息安全教育工作仍相对滞后，信息安全人才十分匮乏，社会需求与人才供给间还存在着很大差距。如何培养信息安全的专业人才，是我国目前面临的重要问题。

《国家信息安全培训丛书》力图涵盖信息安全知识体系的方方面面，蕴含了信息安全保障体系的各个组成部分，是一套很好的信息安全专业人员培训丛书。相信这套丛书的出版，将有利于信息安全专业人员的培养。

何德全

2009 年 5 月

《信息安全积极防御技术》编委会

目　录

第一部分　信息安全积极防御技术基础

第 1 章　信息安全积极防御概述 ····· 3

1.1　引言 ····· 3
1.2　攻击的定义和目标 ····· 4
1.3　攻击的一般过程 ····· 4
1.3.1　攻击准备 ····· 4
1.3.2　攻击实施 ····· 5
1.3.3　攻击后处理 ····· 6
1.4　攻击的类型 ····· 6
1.4.1　基于威胁和攻击对象分类 ····· 7
1.4.2　基于攻击方式分类 ····· 7
1.5　攻击的演变与发展 ····· 9
1.6　本章小结 ····· 10

第 2 章　网络信息收集技术 ····· 11

2.1　信息收集概述 ····· 11
2.2　目标初始信息探查 ····· 12
2.2.1　Google Hacking ····· 12
2.2.2　Whois 查询 ····· 14
2.2.3　社会工程学 ····· 16
2.2.4　Nslookup ····· 16
2.3　找到网络地址范围 ····· 18
2.3.1　ARIN ····· 18
2.3.2　Traceroute ····· 19
2.3.3　网内拓扑结构查询 ····· 21
2.3.4　SNMP ····· 22

2.4 本章小结 …… 23

第 3 章 系统信息收集技术 …… 24

3.1 活动机器查找 …… 24

3.1.1 Ping 命令 …… 24

3.1.2 Nmap …… 26

3.1.3 ARP …… 27

3.2 开放端口和入口点 …… 28

3.2.1 端口扫描概述 …… 28

3.2.2 Nmap 扫描 …… 30

3.2.3 命令行下的端口扫描 …… 33

3.2.4 Windows 下的端口扫描工具——WS_Ping ProPack …… 34

3.3 操作系统信息收集 …… 35

3.3.1 利用 Banner …… 35

3.3.2 利用 TCP/IP 协议栈指纹 …… 35

3.3.3 利用端口扫描结果 …… 36

3.4 开放服务的收集 …… 37

3.5 漏洞扫描 …… 39

3.5.1 X-scan …… 40

3.5.2 Nmap 工具 …… 41

3.5.3 Shadow Security Scanner …… 42

3.5.4 MS06040Scanner …… 43

3.5.5 漏洞扫描工具的选择 …… 43

3.6 本章小结 …… 44

第 4 章 密码破解 …… 45

4.1 密码破解的基本方法 …… 45

4.1.1 密码、密钥和口令 …… 45

4.1.2 密码分析原理 …… 46

4.1.3 口令破解原理 …… 47

4.1.4 其他密码破译方法 …… 49

4.2 常见密码破解举例 …… 51

4.2.1 字母频率攻击 …… 51

4.2.2　对 RSA 算法的攻击 …… 52
4.2.3　对单向哈希算法的“生日”攻击 …… 54
4.2.4　口令破解 …… 54
4.2.5　利用社会工程学攻击 …… 56
4.3　本章小结 …… 57

第 5 章　拒绝服务攻击与防御 …… 58

5.1　拒绝服务攻击概述 …… 58
5.1.1　拒绝服务攻击案例 …… 58
5.1.2　什么是拒绝服务攻击 …… 59
5.1.3　拒绝服务攻击的动机 …… 59
5.1.4　拒绝服务攻击分类 …… 61
5.1.5　拒绝服务攻击原理 …… 63
5.2　是否发生了 DoS 攻击 …… 63
5.3　常见的拒绝服务攻击 …… 65
5.3.1　Ping of Death（死亡之 Ping） …… 65
5.3.2　Teardrop（泪滴） …… 65
5.3.3　SYN Flood（SYN 洪水）攻击 …… 66
5.3.4　UDP Flood（UDP 洪水）攻击 …… 72
5.3.5　ICMP Flood（ICMP 洪水）攻击 …… 72
5.3.6　Land 攻击 …… 74
5.3.7　Smurf 攻击 …… 74
5.3.8　电子邮件炸弹 …… 77
5.4　分布式拒绝服务攻击（DDoS） …… 78
5.4.1　TFN2000 …… 80
5.4.2　分布反射式拒绝服务攻击（DRDoS） …… 84
5.5　DoS 攻击防范 …… 85
5.5.1　从管理上防御 …… 85
5.5.2　防御 DoS 攻击 …… 85
5.5.3　监测 DoS 攻击 …… 86
5.6　DDoS 攻击防范 …… 87
5.7　本章小结 …… 88

第 6 章　缓冲区溢出积极防御 ····· 90

6.1　缓冲区溢出基本原理 ····· 90

6.1.1　缓冲区溢出的研究概况 ····· 90

6.1.2　缓冲区溢出漏洞的危害性 ····· 93

6.2　Win32 平台缓冲区溢出 ····· 94

6.2.1　Windows 下缓冲区溢出的实例 ····· 94

6.2.2　返回地址的控制 ····· 97

6.2.3　Shellcode 基础 ····· 98

6.2.4　通过缓冲区溢出获得用户的 Shell ····· 101

6.3　格式化串漏洞攻击 ····· 102

6.3.1　格式化串漏洞攻击原理 ····· 102

6.3.2　实例分析格式化串漏洞攻击 ····· 106

6.4　常用缓冲区溢出防范措施 ····· 108

6.5　基于 Shellcode 检测的缓冲区溢出防范 ····· 111

6.5.1　获取控制权前 Shellcode 的检测和防御 ····· 111

6.5.2　获取控制权后 Shellcode 的检测和防御 ····· 112

6.6　本章小结 ····· 114

第 7 章　Web 及数据库的积极防御 ····· 115

7.1　Web 积极防御 ····· 115

7.1.1　SQL 注入攻击 ····· 116

7.1.2　保护好 SQL Server 数据库 ····· 124

7.1.3　注入过程中的一些常见问题 ····· 125

7.2　跨站脚本攻击技术 ····· 126

7.2.1　跨站是如何产生的 ····· 127

7.2.2　如何利用跨站漏洞 ····· 128

7.3　利用 cookie 的攻击 ····· 130

7.3.1　cookie 欺骗 ····· 130

7.3.2　cookie 注入 ····· 131

7.4　配置安全的服务器 ····· 132

7.5　数据库安全 ····· 137

7.6　数据库保护 ····· 139

7.6.1　网络系统层次安全技术 ····· 139

7.6.2　宿主操作系统层次安全技术 …… 141
7.6.3　数据库管理系统层次安全技术 …… 141
7.7　本章小结 …… 143

第 8 章　计算机木马积极防御 …… 144

8.1　木马技术 …… 144
8.1.1　木马的发展 …… 144
8.1.2　启动技术 …… 145
8.1.3　特征码修改技术 …… 150
8.1.4　木马的检测与清除 …… 153
8.2　Rootkit 技术 …… 155
8.2.1　Rootkit 的一些已公开的隐藏技术 …… 155
8.2.2　一些隐藏技术的应对方法 …… 163
8.2.3　关于 RING0 Rootkit …… 164
8.2.4　Rootkit 的检测 …… 164
8.3　本章小结 …… 166

第 9 章　计算机病毒积极防御 …… 167

9.1　计算机病毒概述 …… 167
9.1.1　计算机病毒的特性 …… 168
9.1.2　计算机病毒分类 …… 169
9.1.3　病毒的逻辑结构 …… 170
9.1.4　恶意代码 …… 171
9.2　病毒的入侵 …… 172
9.3　病毒编写技术 …… 173
9.3.1　Windows 病毒编写技术 …… 173
9.3.2　脚本病毒编写技术 …… 176
9.3.3　病毒隐藏技术 …… 178
9.4　反病毒技术 …… 179
9.4.1　反病毒技术发展 …… 179
9.4.2　计算机病毒的防治技术 …… 180
9.4.3　计算机病毒的预防 …… 180
9.4.4　病毒的检测 …… 181

9.4.5 病毒的清除 …… 183
9.5 本章小结 …… 186

第二部分 信息安全攻防实践

实验 1 账号口令破解实验 …… 189
一、实验目的 …… 189
二、实验要求 …… 189
三、实验内容 …… 189
实验 2 拒绝服务攻防实验 …… 197
一、实验目的 …… 197
二、实验要求 …… 197
三、实验步骤 …… 197
实验 3 系统端口扫描与漏洞检测实验 …… 203
实验 3.1 Windows 下端口扫描——Ping ProPack …… 203
一、实验目的 …… 203
二、实验要求 …… 203
三、实验内容 …… 203
实验 3.2 Linux 下的端口扫描 …… 206
一、实验目的 …… 206
二、实验要求 …… 207
三、实验内容 …… 207
实验 3.3 使用 X-scan 进行漏洞检测 …… 208
一、实验目的 …… 208
二、实验要求 …… 209
三、实验内容 …… 209
实验 4 缓冲区溢出积极防御实验 …… 213
一、实验目的 …… 213
二、实验要求 …… 213

三、实验内容 …… 213
实验 5　木马积极防御实验 …… 220
一、实验目的 …… 220
二、实验要求 …… 220
三、实验步骤 …… 220
实验 6　网络嗅探攻防实验 …… 225
一、实验目的 …… 225
二、实验要求 …… 225
三、实验步骤 …… 225
实验 7　信息安全攻防综合实验 …… 229
一、实验目的 …… 229
二、实验要求 …… 229
三、实验内容 …… 229
实验 8　Windows2000/WindowsXP 中文件加密及证书的管理 …… 233
一、实验目的 …… 233
二、实验要求 …… 233
三、实验内容 …… 233
实验 9　Windows2000/WindowsXP 下的系统审核 …… 239
一、实验目的 …… 239
二、实验要求 …… 239
三、实验内容 …… 239
实验 10　Windows2000/WindowsXP 下的文件权限设置 …… 244
一、实验目的 …… 244
二、实验要求 …… 244
三、实验内容 …… 244

第一部分

信息安全积极防御技术基础

本部分包含以下章节：

第 1 章　信息安全积极防御概述
第 2 章　网络信息收集技术
第 3 章　系统信息收集技术
第 4 章　密码破解
第 5 章　拒绝服务攻击与防御
第 6 章　缓冲区溢出攻击与防御
第 7 章　Web 及数据库的积极防御
第 8 章　计算机木马积极防御
第 9 章　计算机病毒积极防御

第 1 章　信息安全积极防御概述

内容简介：

在本章中将讨论攻击的定义和攻击目标；详细介绍一个攻击行为发生的三个阶段，即攻击准备、攻击实施和攻击后处理；然后介绍基于不同角度对攻击分类；最后阐述攻击技术的演变和发展。

阅读成果：

通过本章阅读，读者应掌握以下内容：

- 攻击的定义；
- 攻击的目标；
- 攻击的一般过程；
- 攻击的分类。

1.1　引言

随着互联网发展，信息技术已经日渐深入到日常生活和工作当中，信息网络化突破了信息在时间和空间上的障碍，使信息的价值不断提高。然而，互联网本身的开放性、跨国界、无主管、不设防和无法律约束等特性带来了一些不容忽视的问题，如信息安全问题。由于安全漏洞导致的信息篡改、数据破坏、信息泄密、恶意信息的发布，以及服务瘫痪等信息安全事件层出不穷，由此造成的经济损失和社会不良影响难以估计。

尽管信息安全的研究得到越来越多的关注，然而，信息安全问题并没有因此而减少。相反，随着网络规模的飞速扩大，结构日益复杂和应用领域不断扩大，信息安全事故呈迅速增长趋势，造成的损失也越来越大。根据公安部 2007 年全国信息网络安全状况调查结果显示，我国信息网络安全事件发生比例连续 3 年呈上升趋势，2007 年达到 65.7%，较 2006 年上升了 11.7%。信息网络安全事件的主要类型有：感染计算机病毒、蠕虫和木马程序，垃圾电子邮件，遭到网络扫描、攻击和网页篡改。计算机病毒通过 U 盘等移动存储介质传播的问题比较突出，从 2006 年的 23%上升到 2007 年的 40%；互联网上以盗取用户账号、密码为目的的“间谍软件”、木马病毒明显增多，“熊猫烧香”、“木马代理”、“网游大盗”和“传奇木马”等一批以侵占他人财产为目的的计算机病毒大量传播，直接危害个人的切身利益，造成的影响较大。

我们的生活已经无法脱离对网络与计算机的依赖，但是网络是开放的、共享的，因此，信息安全就成为科学研究的一个重大课题。而对信息安全的研究不能仅限于防御手段，还

要从非法获取目标主机的系统信息、非法挖掘系统弱点等技术进行研究。正所谓对症下药，只有了解了攻击者的手法，才能更好地采取措施，来保护网络与计算机系统的正常运行。

1.2 攻击的定义和目标

攻击是用户未经授权的访问尝试或者未授权的使用尝试。攻击的方法众多，但其攻击的目标主要是破坏信息的机密性、信息的完整性、信息的可用性、信息的非否认性和信息系统运行的可控性。

1.3 攻击的一般过程

一个攻击行为的发生一般有三个阶段，即攻击准备、攻击实施和攻击后处理。当然并不是每次攻击都能成功。

1.3.1 攻击准备

攻击准备阶段可分为确定攻击目标和信息收集两个子过程。攻击者可能在一开始就确定了攻击目标，然后专门收集该目标的信息；也可能先大量地收集网上主机的信息，然后根据各系统的安全性强弱确定最后的攻击目标。攻击前首先确定攻击目标，而后确定要达到什么样的攻击目的，即给对方造成什么样的后果，常见的攻击目的有破坏型和入侵型两种。破坏型攻击指的是破坏目标，使其不能正常工作，而不是控制目标系统的运行。另一类是入侵型攻击，这种攻击是要获得一定的权限达到控制攻击目标或窃取信息的目的。入侵型攻击较为普遍，威胁性大，因为一旦获得攻击目标的管理员权限就可以对此服务器做任意动作，包括破坏性的攻击。此类攻击一般利用服务器操作系统、应用软件或者网络协议等系统中存在的漏洞进行。在确定攻击目标之后，最重要的是收集尽可能多的关于攻击目标的信息，以便实施攻击。这些信息主要包括：目标的操作系统类型及版本，目标提供的服务类型，各服务器程序的类型、版本及相关的各种信息。对于攻击者来说，信息是最好的工具。它可能就是攻击者发动攻击的最终目的（如绝密文件、经济情报等）；也可能是攻击者获得系统访问权限的通行证，如用户口令、认证、票据等；还可能是攻击者获取系统访问权限的前奏，如目标系统的软硬件平台类型、提供的服务与应用及其安全性的强弱等。攻击者感兴趣的信息主要包括以下几个方面。

（1）系统的一般信息

如系统的软硬件平台类型、系统的用户和系统的服务与应用等。

（2）系统及服务的管理、配置情况

如系统是否禁止 root 远程登录， SMTP 服务器是否支持 decode 别名等。

（3）系统口令的安全性

如系统是否存在弱口令，缺省用户的口令是否没有改动等。

（4）系统提供的服务的安全性及系统整体的安全性能

这一点可以从该系统是否提供安全性较差的服务、系统服务的版本是否是老的版本等因素来做出判断。攻击者获取这些信息的主要方法有以下几种。

①对系统进行端口扫描，弄清每个端口运行的是哪种服务。基于公有的配置和软件，攻击者能够比较准确地判断出每个端口在运行什么服务。例如，如果知道操作系统是 UNIX 和端口 23 是开放的，他能判断出机器正在运行 Telnet 服务，如果操作系统是 Microsoft Windows 和端口 25 是开放的，他能判断出正在运行邮件服务器。

②探测特定服务的弱点。应用漏洞扫描工具，如 ISS、SATAN、NESSUS 等来探测特定服务的弱点。

③使用口令攻击。如口令猜测攻击、口令文件破译攻击、网络窃听与协议分析攻击，以及社交欺诈等手段。

④体系结构探测。有一些探测远程主机操作系统的程序通过向远程主机发送不平常的或者没有意义的数据包来完成。由于每种操作系统都有其独特的响应方式，通过这些响应方式，攻击者通过解析响应信息就能够确定出目标主机所运行的操作系统及其版本等信息。例如，Nmap 目前它能检测出接近 400 种不同的设备。X-scan 也可识别出常见的操作系统及网络设备。

1.3.2　攻击实施

当收集到足够的信息后，攻击者就可以实施攻击了，对于破坏型攻击只需利用必要的工具发动攻击即可。但作为入侵型攻击，往往要利用收集到的信息找到系统漏洞，然后利用该漏洞获得一定的权限，有时获得一般用户的权限就足以达到攻击的目的，但一般攻击者都想尽办法获得系统最高权限，这不仅为了达到入侵的目的，在某种程度上也是为了显示攻击者的实力。系统漏洞一般分为远程漏洞和本地漏洞两种，远程漏洞是指可以在别的机器上直接利用该漏洞进行攻击并获得一定的权限，这种漏洞的威胁性相当大，攻击行为一般是从远程漏洞开始，但是利用远程漏洞不一定获得最高权限，往往获得一般用户的权限，只有获得了较高的权限（如管理员的权限）才可以进行入侵行为（如放置木马程序）。因此在获得一般账户权限之后，攻击者经常会试图获得更高的权限，如系统管理账户的权限。获取系统管理权限通常有以下途径：

- 获得系统管理员的口令，如专门针对 root 用户的口令攻击；
- 利用系统管理上的漏洞，如错误的文件许可权，错误的系统配置，某些 SUID 程序中存在的缓冲区溢出漏洞等；
- 令系统管理员运行特洛伊木马程序，如经篡改之后的 Login 程序等；
- 窃听管理员口令。

攻击者进行攻击时，还要常常注意隐藏自己，以免引起目标系统管理员的注意。进入系统之后，攻击者要做的第一件事就是隐藏行踪，攻击者隐藏自己的行踪通常要用到下面的技术：

- 连接隐藏，如冒充其他用户、修改 LOGNAME 环境变量、修改 utmp 日志文件、使用 IP Spoof 技术等；
- 进程隐藏，如使用重定向技术减少 ps 给出的信息量、用特洛伊木马代替 ps 程序等；