反黑经典

实例手册

聊天室隐患

经典加密解密

黑客实例经典

扫描工具详解

黑客工具详解

目　录

Hacker 文化 1
安全技术 11
网络安全技术指南 11
网络有漏洞 14
操作系统简介 16
GCC 编译器使用简介 17
gdb 基本命令 19
Windows 98 MSDOS.SYS 的设置和编辑 27
MSDOS.SYS 的重要性 30
Windows NT 注册表 31
理解 Hives 34
TCP/IP 协议介绍 36
以太网的基本工作原理 42
扫描工具 46
端口扫描 52
扫描工具 58
Retina 介绍 60
Narrow 安全扫描器 61
Nessus 指南 63
Nmap 网络安全扫描器说明 65
www.netcraft.com 密码破解 75
Word 密码 76
ARJ 密码的破解——PCYAPR16 78
制作词典——万能钥匙 Xkey 78
生成用户名 82
Emailcrack 82
Password Recovery Kit 87
LOpht 89
entry 90
KeyKey 90
什么样的密码是危险的 90

危险口令排行榜 90
破解之道 92
Crack Jack V1.4 中文使用说明 (By CoolFire 12-1-1996) 101
本次主题: 字典档的维护及更新 123
**** 新工具程式 Global KOS Krack (KOS) **** 127
[CGI Hole (phf.cgi) 的延伸] 129
[Crack 工具介绍] John the Ripper V1.4 [Size:743K] 135
Crack 工具 142
**** John the Ripper v1.4 中文说明 **** 148
**** CoolFAQ **** 179
甚麼是 John the Ripper? 180
字典檔的規則 184
設定檔 192
攻击聊天室 197
聊天室的攻击 199
聊天室内如何看人家的IP 201
在聊天室里找别人的IP 205
聊天室里踢人 206
聊天室页面炸弹的攻击 207
OICQ的安全问题 209
OICQ的溢出问题 214
如何利用OICQ得到对方的IP地址 218
ICQ的漏洞 218
OICQ炸弹 219
Back Orifice 2000 221
配置BO2K服务器 224
Back Orifice远程管理系统 232
Becoming: 238
LockDown 2000 243
如何隐藏自己 249
入侵NTserver典型途径V2.0 252
基于Telnet协议的攻击 255
攻击Email 257
手工清除“YAI”法 258
挑战 Nuke 260

KaBomber v3.0 邮件炸弹工具使用说明 261
几种常见的木马程序: 262
利用工具进行简单的入侵 272
NetBus v.1.60的说明 273
NetSpy攻防宝典 274
利用wingate隐藏IP 275
FTPBounce跳跃攻击法 276
《关于如何使用G_OOB软件及可能遇到的困难》..... 284
FTP使用精华 286
NET命令的基本用法 289
yhq 破解实战录 299
yhq 破解实战录 300
yhq 破解实战录 301
yhq 破解实战录 04 --- Master Converter v1.73 破解法 !!! 303
yhq 破解实战录 05 --- Video Clip MPEG 1.7 破解法 !!! 305
yhq 破解实战录 06 --- WinTex95 v2.01 破解法 !!! 307
yhq 破解实战录 07 --- PrimaSoft AutoFTP v1.0 破解法 !!! 309
yhq 破解实战录 08 --- HyperSnap-DX v3.00 破解法 !!! 310
yhq 破解实战录 09 --- 汉X通 v3.0 破解法 !!! 312
yhq 破解实战录 11 --- Internet Utilities 97 v2.0.24 破解法 !!! ... 315
屏保中的“曲线”解密技巧..... 317
基于NetBIOS的简单Windows进攻法..... 319
如何检测你的网络上是否安装了 Sniffer 321
其他工具..... 323
如何破解天网..... 324
网上常见的攻击方法..... 328
攻破www.apache.org 330
蓝屏攻击的防范..... 332
WINDOWS9XDDoS攻击 333
其它脚本程序 334

Hacker文化

黑客的产生与变迁，有一语难以概之的复杂背景，并且与计算机技术的发展紧密相关。一部“黑客史”其实就是一部计算机发展的历史。早自1945年起，计算机科学便不断地吸引世界上的顶尖高手投入其中。从Eckert & Mauchly发明ENIAC （电子数字积分计算机）后，便不断有狂热的程序员(programmer)投入其中，以编写软件和研究各种程序设计技巧为乐，逐渐形成具有自我意识的一套科技文化。这批主要来自工程界与物理界的先驱者用机器语言、汇编语言、FORTRAN等古老的语言写程序。他们默默贡献，却鲜为人知。从二次大战结束后到70年代早期，是由这批先驱者主宰电脑文化的年代,他们即所谓的Real Programmer(真正的程序员)。虽然他们从不自称是Real Programmer、Hacker或任何特殊的称号。Real Programmer 这个名词是在80年代才出现的，所谓Real Programmer指的就是用组合语言或甚至机器码，把程序用打卡机打出一片片纸卡片，由主机读卡机输入电脑的那种石器时代Programmer。取代Real Programmer时代的是逐渐盛行的交互式计算(Interactive computing)。

Hacker时代始于1961年，最先使用Hacker这个字应该是麻省理工学院(MIT，Massachusetts Institute of Technology)。Hacker源于英语动词hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，Hacker则有恶作剧之意，尤指手法巧妙、技术高明的恶作剧。而在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不象绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”当时麻省理工学院出现第一台电脑DEC公司 (Digital Equipment Corporation) PDP-1。它当成最时髦的科技玩具，各种程序工具与电脑术语开始出现，整个环境与文化一直发展下去至今日。80年代早期学术界人工智慧的权威：麻省理工学院的人工智能实验室(Artificial Intelligence Laboratory，简称AI Lab)的核心人物即原至当年。现在黑客使用的侵入计算机系统的基本技巧，例如破解口令（password cracking)，开天窗（trapdoor)，走后门（backdoor)，安放特洛伊木马(Trojan horse）等，都是在这一时期发明的。从1969年正好是ARPANet(Advanced Research Projects Agency Network)美国国防部高级研究计划局建立的计算机网，这个国际网允许其成员使用其设备并对大批不同的计算机存取数据建置的第一年，ARPANET是第一个横跨美国的高速网络，由美国国防部所出资兴建，一个实验性质的数位通讯网络，逐渐成长成联系各大学、国防部承包商及研究机构的大网络。INTERNET即由其发展而来。

ARPANET另一项好处是，资讯高速公路使得全世界的Hacker能聚在一起，

不再像以前孤立在各地形成一股股的短命文化，网络把他们汇流成一股强大力量。开始有人感受到Hacker文化的存在，在网上发表讽刺文学与讨论Hacker所应有的道德规范。Hacker文化在有接上ARPANET的各大学间快速发展，特别是(但不全是)在资讯相关科系。

一开始，整个Hacker文化的发展以麻省理工学院的人工智能实验室为中心，但斯坦福大学（Stanford University）的人工智能实验室(简称SAIL)与稍后的卡内基－梅隆大学（Carnegie-Mellon University，简称CMU）正快速崛起中。三个都是大型的资讯科学研究中心及人工智慧的权威，聚集著世界各地的精英，不论在技术上或精神层次上，对Hacker文化都有极高的贡献。随著科技的进步，主角麻省理工学院人工智能实验室也从红极一时到最后淡出舞台 。

从麻省理工学院那台PDP-1开始，Hacker们主要程序开发平台都是DEC公司的PDP迷你电脑系列。DEC率先发展出商业用途为主的交互式计算及分时（time-sharing）操作系统，当时许多的大学都是买DEC的机器，因为它兼具弹性与速度，还很便宜(相对于较快的大型机)。便宜的分时系统是Hacker文化能快速成长因素之一，在PDP流行的时代，ARPANET上是DEC机器的天下，其中最重要的便属PDP-10，PDP-10受到Hacker们的青睐达十五年；TOPS-10(DEC的操作系统)与MACRO-10(它的组译器)，许多怀旧的术语及Hacker传奇中仍常出现这两个字。麻省理工学院像大家一样用PDP-10，但他们不屑用DEC的操作系统。他们偏要自己写一个：传说中赫赫有名的ITS（Incompatible Timesharing System），ITS始终不稳，设计古怪，bug也不少，但仍有许多独到的创见，似乎还是分时系统中开机时间最久的纪录保持者。ITS本身是用汇编语言写的，其他部分由LISP写成。LISP在当时是一个威力强大与极具弹性的程序语言LISP让ITS的Hacker得以尽情发挥想像力与搞怪能力。LISP是麻省理工学院人工智能实验室成功的最大功臣，现在它仍是Hacker们的最爱之一。斯坦福大学人工智能实验室的中坚份子后来成为PC界或图形使用者介面研发的要角。卡内基-梅隆大学的Hacker则开发出第一个实用的大型专家系统与工业用机器人。

另一个Hacker重镇是施乐（XEROX）公司的帕乐阿尔托研究中心（Palo Alto Research Center，简称PARC)。从70年代初期到80年代中期这十几年间，PARC不断出现惊人的突破与发明，不论质或量，软硬件方面。如现今的视窗滑鼠界面等帕乐阿尔托研究中心这群人对Hacker文化仍有不可抹灭的贡献。

70年代ARPANET与PDP-10文化迅速成长茁壮。邮件发送清单（Mailing list）的出现使世界各地的人得以组成许多SIG(Special-interest group，有共同特殊观点或要求的群体)，不只在电脑方面，也有社会与娱乐方面的。美国国防部高级研究局（DARPA）对这些非正当性活动睁一只眼闭一只眼，因

为会吸引更多的聪明小伙们投入电脑领域呢。

此时在新泽西州的郊外，另一股神秘力量积极入侵 Hacker 社会，终于席卷整个 PDP-10 的传统。它诞生在 1969 年，也就是 ARPANET 成立的那一年，有个在 AT&T 贝尔实验室（Bell Labs）的年轻人肯·汤普逊（Ken Thompson）发明了 Unix。肯·汤普逊很喜欢 Multics（多路存取计算机系统，是源自 ITS 的操作系统，用来实做当时一些较新的 OS 理论）上的作业环境，于是他在实验室里一台报废的 DEC PDP-7 上胡乱写了一个操作系统，该系统在设计上有从 Multics 抄来的，也有他自己的构想。他将这个操作系统命名 Unix。他的同事丹尼斯·莱齐（Dennis Ritchie）发明了一个新的程序：C 语言，汤普逊与他用 C 把原来用汇编语言写的 Unix 重写一遍。C 与 Unix 很快地在 Bell Labs 得到欢迎，开始在 Bell Labs 中流行。肯·汤普逊和丹尼斯·莱齐他俩是唯一两位获得图灵奖（Turing Award，电脑界的诺贝尔奖）的工程师（其他都是学者）。五年后，Unix 已经成功地移植到数种机器上。这当时是一件不可思议的事！它意味著，如果 Unix 可以在各种平台上跑的话，Unix 软件就能移植到各种机器上。再也用不著为特定的机器写软件。除了跨平台的优点外，Unix 与 C 还有许多显著的优势。可以发挥强大的威力。C 与 Unix 的应用范围之广，出乎原设计者之意料，很多领域的研究要用到电脑时，他们是最佳排档。尽管缺乏一个正式支援的机构，它们仍在 AT&T 内部中疯狂的散播。到了 1980 年，已蔓延到大学与研究机构，还有数以千计的 hacker 想把 Unix 装在家里的机器上。

当时跑 Unix 的主力机器是 PDP-11、VAX 系列的机器。不过由于 UNIX 的高移植性，它几乎可安装在所有的电脑机型上。一旦新型机器上的 UNIX 安装好，把软件的 C 原始码抓来重新编译就一切 OK 了，谁还要用汇编语言来开发软件？于是 UNIX 站点连成了专属的一套网络，形成其 Hacker 文化。在 1980 第一个世界性的新闻组网络系统（USENET）站点成立之后，组成了一个特大号的分散式布告栏系统，吸引而来的人数很快地超过了 ARPANET。少数 UNIX 站点有连上 ARPANET。PDP-10 与 UNIX 的 Hacker 文化开始交流，不过一开始不怎么愉快就是了。PDP-10 的 Hacker 们觉得 UNIX 的拥护者都是些什么也不懂的新手，比起他们那复杂华丽，令人爱不释手的 LISP 与 ITS，C 与 UNIX 简直原始的令人好笑。“一群穿兽皮拿石斧的野蛮人”他们咕哝著。在这当时，又有另一股新潮流风行起来。第一部 PC 出现在 1975 年，苹果电脑在 1977 年成立，以飞快的速度成长。微电脑的潜力，立刻吸引了另一批年轻的 Hackers。他们最爱的程序语言是 BASIC，由于它过于简陋，PDP-10 派与 UNIX 迷们根本不屑用它，更看不起使用它的人。1980 年同时有三个 Hacker 文化在发展，尽管彼此偶有接触与交流，但还是各玩各的。

ARPANET/PDP-10 文化，玩的是 LISP、MACRO、TOPS-10 与 ITS。UNIX 与

C的拥护者用电话线把他们的PDP-11与VAX机器串起来玩。还有另一群散乱无秩序的微电脑迷，致力于将电脑科技平民化。三者中ITS文化（也就是以麻省理工学院 人工智能实验室为中心的Hacker文化）可说在此时达到全盛时期，但乌云逐渐笼罩这个实验室。ITS赖以维生的PDP-10逐渐过时，开始有人离开实验室去外面开公司，将人工智慧的科技商业化。麻省理工学院人工智能实验室的高手挡不住新公司的高薪挖角而纷纷出走，斯坦福大学人工智能实验室与卡内基-梅隆大学也遭遇到同样的问题。致命一击终于来临，1983年DEC宣布：为了要集中在PDP-11与VAX生产线，将停止生产PDP-10；当时有远见的人都看得出，在快速成长的微电脑科技下，Unix一统江湖是迟早的事。同样在快速成长的微电脑科技下，当前一统江湖的却是“瘟到死”。

微电脑与区域网络的科技，开始对Hacker文化产生影响。Motorola 68000 CPU加以太网（Ethernet）是个有力的组合，也有几家公司相继成立生产第一代的工作站。1982年，一群伯克利市（Berkeley ）出来的UNIX Hacker成立了SUN微系统公司（Sun Microsystems）。Sun一开始生产的工作站CPU是用Motorola 68000系列，到1989才推出自行研发的以SPARC系列为CPU的SPARCstation。

1984年AT&T解散了，UNIX正式成为一个商品。当时的Hacker文化分成两大类，一类集中在Internet与USENET上（主要是跑UNIX的迷你电脑或工作站连上网络），以及另一类PC迷，他们绝大多数没有连上Internet。Sun与其他厂商制造的工作站为Hacker们开启了另一个美丽新世界。工作站诉求的是高效能的绘图与网络，1980年代Hacker们致力为工作站撰写软件，不断挑战及突破以求将这些功能发挥到百分之一百零一。伯克利发展出一套内建支援ARPANET协议的UNIX，让UNIX能轻松连上网络，Internet也成长的更加迅速。尝试为工作站开发一套图形界面最有名的要算麻省理工学院开发的X window了。X window成功的关键在完全公开原始码，展现出Hacker一贯作风，并散播到Internet上。X window成功的干掉其他商业化的图形界面的例子，对数年后UNIX的发展有著深远的启发与影响。少数ITS死忠派仍在顽抗著，到1990年最后一台ITS也永远关机长眠了，那些死忠派在穷途末路下只有悻悻地投向UNIX的怀抱。

UNIX们此时也分裂为Berkeley UNIX与AT&T两大阵营。就销售量来说，AT&T UNIX始终赶不上BSD（Berkly Software Distribution,加州大学伯克利软件分校）/Sun，但它赢了标准制订的战争。到1990年，AT&T与BSD版本已难明显区分，因为彼此都有采用对方的新发明。随著90年代的来到，工作站的地位逐渐受到新型廉价的高档PC的威胁，他们主要是用Intel 80386系列CPU。第一次Hacker能买一台威力等同于十年前的迷你电脑的机器，上面跑著一个完整

的UNIX，且能轻易的连上网络。

随着Internet越来越普及普及，各种Hacker软件的蔓延，各种网络破坏事件的屡屡发生，现在的Hacker已经和当年的Hacker迥然不同了。虽然真正的Hacker不屑干这些专门窥探他人隐私，任意篡改数据，进行网上诈骗活动的下三滥的事，认为真正干这些事的是Cracker（骇客），但Hacker已成为人们眼中“网上捣乱分子和网上犯罪分子”的代名词。很大程度上是因为这些Cracker总是用Hacker自我命名和自我辩护。加上那些只会用各种Hacker软件，自称Hacker的刚入门或不入门的“高手”们，搅得Internet乱糟糟！

就像大多数没有经济活动的文化一样，Hacker Dom 的运作是建立在名望之上。当你尝试去解决一个有趣的问题时，你所做事是否有趣，你的解决方案是不是真的好用，这些只有你的技术上的同好或前辈准备好为你做评价。因此，当你开始玩起 Hacker 的游戏时，你的主要分数是来自其它 Hacker 们对你的技术的看法(这就是为什么只当其它的 Hacker 都认为你是 Hacker 时，你才算是一位真正的 Hacker)。这个事实被人们认为 hacking 是一种孤独的工作的印象所蒙蔽了；也被Hacker 文化的禁忌(现在已渐渐的朽坏了，但依然存在) 和存在人们内心动机的自大或特权之间的冲突所蒙蔽。

具体的说，Hacker Dom 就是人类学家所说的「天才文化」。你在其中所得到的地位和名望并不来自于支配其它人，或是因为长的漂亮，或因为你有一些别人想要的东西，而是因为你送出东西。特别是，你给送出你的时间，你的创造力和你的技术成果。

下面有五种事，你会因为做了这些事而爱到 Hacker 们尊敬：

1 。写免费的软件。

第一种是写那些其它 Hacker 们觉的有趣或好用的程序，并把源代码（source）公开开放给整个 Hacker 文化中的人使用。Hacker 们最爱尊敬的是写出大而功能强的程序的人，而且这程序是广为大家需要的，所以大家都在做用这些程序 。

2。帮忙 test 和 debug 免费的软件

Hacker 们也尊敬帮忙 debug 免费软件的人。在这个不是很完美的世界，你不可避免的必须花掉大部分的软件发展周期在 debug 阶段上。这就是为什么在任何免费软件发展者的脑子都会告诉你一件事，好的 beta 测试者(能很清楚的描述发生的状况，正确的发现问题出处，可以容忍测试版本的 bug，并且能进行一些简单的诊断程序)和红宝石一样贵重。

如果你是一只菜鸟，试着开始去找一个你有兴趣的正在发展中的程序，并且成为一位好的 beta 测试者。从帮忙测试开始，很自然的你开始帮忙 debug，进而开始帮忙修改程序。你将在这过程中学习到很多东西，并且和以后可以帮

助你的人结下因果。

3 。公布有用的资讯。

另一项好事是收集和过滤有用和有趣的资讯，整理成 Web page 或 FAQ 之类的文件，让大家能很容易的收得。几种主要技术 FAQ 的维护者都能得和免费软件的作者几乎一样多的尊敬。

4 。帮忙维持一些简单的工作。

Hacker 文化是由一群自愿者维持运作著。有一些工作很无趣但却必须维持正常运作的，如： 管理 mailing list，维护 newsgroup，维持大的软件供应站台，推动RFC 和其它技术标准。做这类的事将会得到很多的尊敬，因为大家都知道这些工作是很花时间，但又不像玩弄程序码般有趣。

5。为 Hacker 文化而努力。

最后一项，你可以为这个文化效劳，并推广这个文化。例如，写一份正确的入门手册，教别人如何成为一位 Hacker ：-)。在你因为做了前面四件事之一而出名之前，这不是你该做的事。

正确的说，Hacker 文化并没有任何的领导者，但在这文化有所谓的文化英雄，族群历史学家。当你在其中混的够久之后，你也许会成为这之中的一员。注意：Hacker 们并不相信族群，喧骚自大的长者，所以成为这样的长者是非常的危险。与其去和别人竞争，你宁可为自己定位，给自己一个亲切谱虚的身份 。

黑客文化首先包含了自由不羁的精神。黑客在网络上自由驰骋，他们喜欢不受束缚，喜欢挑战任何技术制约和人为限制。黑客认为所有的信息都应当是免费的和公开的。黑客行为的核心，就是要突破对信息本身所加的限制。黑客就是那些在网络上对信息“劫富济贫”的人。从事黑客活动，意味着对计算机的最大潜力进行智力上的自由探索，意味着尽可能地使计算机的使用和信息的获得成为免费的和公开的，意味着坚信完美的程序将解放人类的头脑和精神。

其次，黑客文化也包含了反传统、反权威、反集权的精神。这是对60 年代反主流文化价值观的继承。黑客蔑视现行电子世界的行为规则。他们认为这些规则并不能起到维持法律秩序和保护公共安全的作用，相反是为了获取利润和镇压异己，是不道德的，而他们自己是既有反抗精神又身怀绝技的天才，是电子时代的“侠盗罗宾汉”，他们有自己的一套行为准则。

无论对黑客的行为如何评说，没有人能够否认黑客对计算机技术发展所作出的巨大贡献。而在这样一个崭新的、前所未有的网络时代，黑客文化何去何从呢？

目前，政府和公司的管理者越来越多地要求黑客传授给他们有关电脑安全的知识。许多公司和政府机构已经邀请黑客为他们检验系统的安全性，甚至还请

他们设计新的保安规程。在两名黑客连续发现网景公司设计的信用卡购物程序的缺陷并向商界发出公告之后，网景修正了缺陷并宣布举办名为“网景缺陷大奖赛”的竞赛，那些发现和找到该公司产品中安全漏洞的黑客可获 1000 美元奖金。无疑黑客正在对电脑防护技术的发展作出贡献。

同时，黑客也正在越来越多地保护网络空间，使其免受非法闯入者和恐怖分子的袭击。正如一位黑客所言：“黑客爱电脑，他们希望电脑化空间平安无事”。

最近，《纽约时报》在一篇文章中称加州大学的研究生黑客为“数字交流新卫士”，并评论说，包括黑客道德准则在内的黑客文化也许会融合进商业化利用 Internet 的主流中。

Hacker 们解决了问题并创造新东西，他们相信自由并自愿的互相帮助。想要被别人接受成为一位 Hacker，你必须发自内心的表现出这种态度。为了要表现出这种态度，你就必须先完全认同这些态度。如果你只是把学习 Hacker 态度这件事当作一种能在这个文化赢得认同的途径，那么你已经乎略了真正的重点。由衷的接受这些态度是很这要的，这能帮助你学习并维持你的动机。就像那些具创造性的艺术一样，成为一位大师的最有效方法是学习大师们的精神，并不只是学习知识和情绪而已。所以，如果你想要成为一位 Hacker，请反复的做下面的事情，直到你完全领会它们：

1。这世上充满著等著被解决的迷人问题

作为一个 Hacker 是充满快乐的，但这是一种因为努力得到成果所带来的快乐。努力的成果则带来动机。成功的运动家的动机则来自于，使他们的身体不断进化，并把自己推向物理上的极限所带来的快乐。类似的情形，要成为 Hacker，你必须要能从解决问题，精进技术，和运用知识的过程中感受到一种悸动。如果你不是天生就能感受到这种悸动的人，那么，为了要成为 Hacker，你必须使自己变成这样的人。否则，你会发现你的 hacking energy 就会像性，金钱，和社交活动一样，因为分心而被消磨掉。你也必须为你的学习能力建立一种信念直到你完成你的工作 -- 即使你只处理一小部份，而你也不知道你到底还要学些什么东西才有辨法解决你的问题，但是你会努力学习，准备充足，以应付下一个问题。

2。没有任何人必须一再的解决同一个问题

富创造力的头脑是贵重而有限的资源。有这么多迷人的新问题在那等著被解决。因此富创造力的头脑不该被浪费的用来重复发明轮子。身为一位 Hacker，你必须了解到其它 Hacker 们的时间也是很宝贵的。所以，分享资讯，解决问题和提供解决方案给其它 Hacker 以解决新的问题，这些几乎算是道义上的责任。即使 Hacker 们所拥有的大多是从其它 Hacker 的身上得来的，

但这并不意谓你必需把你创造的作品全部交出来，你可以卖出足够数量的产品，以求得温饱，给付房租和买电脑设备，这和 Hacker 的价值观并不相违背。使用你的 hacking 技能以供给一个家庭的生活，甚至是致富，只要你仍不忘记你是一位 Hacker，那么这些行为并不会产生矛盾。

3。无聊而单调的工作是有害的

Hacker 们(有创造力的人也是一样)永远不该做一些无聊而单调并且愚蠢的反复性工作。因为，如果这样的事情发生的话，这表示他们正在做一些不是他们该做的事 -- 解决新的问题。这样的浪费对任何人而言都是一种伤害。无聊单调的工作不只是无趣而已，而且是一种有害的物质。要做为一位 Hacker 要能尽可能的自动避免无聊，对此你必须有相当的认知。这不只是为了你自己而已，也是为了所有的人(尤其是其它的 Hacker)。这有一些例外。有时侯 Hacker 们会去做一些被认为无聊或重复性的工作，当做脑力的训练，或是为了要学习得某种技能或某种你所没有的特殊经验。不过这是一种选择，任何人都不该被强迫面对无聊事。

4。自由才好

Hacker 们天性上是反对独裁的。任何一个给你命令的人就能给你一个独裁式的工作，并且可以给你一些笨的可以的理由，停止你解决任何吸引著你的问题。所以任何独裁式的行为都会被挑战，以免会危害到你和其它的 Hacker 们。这和为反对而反对是不同的，小孩子是需要被指导和阻止他们犯错。Hacker 也会同意接受某些权威，照著指示做以较短的时间得到他想要的。不过那是一种有限且理性的协定 ……

专制在监察和保密这些事上是很有效的方法。这些行使专制的人并不相信自愿性质的合作和资讯分享 -- 他们只相信在他们控制之下的合作关系。所以，身为一位 Hacker，你必具有一种敌对的天性，以对抗监察，秘密和使用外力强迫或迷惑可以信任的人等行为。你必须以互信做为你行为的基础。

5。态度并非不等效于能力

要成为一位 Hacker，你必须开始培养这些态度。但，如果你只是单独的模仿某一种态度，这并不能使你成为一位真正的 Hacker，也不会使你成为一位运动冠军或摇滚明星。因此，你必须学会猜疑态度和尊敬各种能力。Hacker 们不会想浪费时间在虚华的人的身上，他们尊敬的是能力 -- 特别是身为 Hacker 的能力，但对于其它方面的能力也是充满敬意。如果有能力追求一些很少人能弄懂的技术，追求精神上的技巧，并能集中精神，那就再好不过了。

如果你尊敬各种的能力，那么你就会乐于自己发展这些能力 -- 这会使的努力工作和奉献成为一种刺激性的消遣而非一份苦差事。这对于想要成为 Hacker 的人而言，是很重要的。

Hacker 的精神态度是很重要的，但技术则更是重要。Hacker 的态度虽然是无可取代，但在梦想别的 Hacker 开始也叫你 Hacker 前，有些基本的工具和技术是必备的。

随著新科技的发明和旧技术的取代，这些工具随时间在慢慢的改变。例如： 以往总是会学会用机器码写程序，现在我们开始使用 HTML。下面所举的工具是很明显的被需要的：

1 学习程序设计。

这是基础的 hacking 技能。理所当然的你必须学会 C。但如果你只是学一种语言，那么你不能算是一位 Hacker，了不起只能算是一个 programmer。除此，你还必须学会学会以独立于任何程序语言之上的概括性观念来思考一件程序设计上的问题。要成为一位真正的 Hacker，你必须要能在几天之内将 manual 内容和你目前已经知道的关连起学会一种新的语言。也就是说，你必会学会数个不同的语言。

学了 C 之外，你至少还要会 LISP 或 Perl、Java 等。除了几重要的 hacking 常用语言之外，这些语言提供你一些不同的程序设计途径，并且让你在好的方法中学习。

程序设计是一种复杂的技术，我没辨法在这提供完整的学习步骤。但是我能告诉你一些在书本上和课堂上所没有的东西（有很多，几乎全部最好的 Hacker 们都是自习而来的）。(a) 读别人的程序码 和 (b) 写程序，这两项是不错的方法 。

学习写程序就像在学习写一种良好的自然语言，最好的方法是去看一些专家们所写的东西，然后写一些你自己的东西，然后读更多，再写更多……然后一直持续，一直到你发展出一种属于自己的风格和特色。

要找到好的程序码来看是很一件很困难的事，因为，对菜鸟 Hacker 们而言，适于供他们阅读和努力的大型程序的 source 数量很少。但这事已有了戏剧性的变化了；现在免费的供应的软件、程序设计工具和操作系统（大都公开提供 source，而且全都是由 Hacker 们写成的）到处可看。进入下一个主题……

2 取得一个免费的 UNIX ，并学习使用和维护。

我先假设你已经有一部个人电脑或者是可以使用任何一部。取得 Hacker 技巧的第一个步骤是取得一份 Linux 或者一份免费的 BSD-Unix，并将它安装在自己的机器，并使之顺利的运作。

没错，在这个世界上除了 Unix 之外，还有其它的操作系统。但是他们只提供做好的程序（binary），你不能看到他们的程序码，你也不能修改他们。想要在 DOS 或 Windows 或 MacOS 开始 hacking，无疑就是要你绑著枷锁跳舞一样。

除此之外，Unix 是 Internet 上的操作系统。当你在不懂 Unix 的情况下学习使用 Internet 时，你没辨法在不懂 Unix 的情况下成为 Internet 的 Hacker。因为这个原故，现在的 Hacker 文化还是很牢固的以 Unix 为中心绕著。(这并不完全是正确的，而且有些活在旧时代的 Hacker 甚至也不喜欢这种情形，但是 Unix 和 Internet 之间的共生共成已经到了牢不可破的地步，即使是 Microsoft 的大块肌肉也没能在上面留下明显的伤痕。)因些，把 Unix 装起来吧！(我自己是喜欢 Linux，但是还有其它的东东可用。) 学习它，让它运作起来，让它陪你努力精进。用他向整个 Internet 喊话。看程序码，改程序。有一天你成为一位高竿的 Hacker，你回头往后看时会发现，你得到比 Microsoft 操作系统所能提供的还要好的程序设计工具(包括 C，Lisp 和 Perl)。而且得到快乐，并学到比你想像中的还要多的知识。

3 学习使用 World Wide Web 并学会写 HTML。

在 Hacker 文化创造出来的东西，大多在他们的活动范围外被使用著，如，在工厂和辨公室或大学被漠漠的使用著。但 Web 是一个很大的例外，这个 Hacker 眼中的大玩具甚至还被政客们接受，并巧巧的在改变这个世界。因此(还有很多好的理由)，你必须学习 Web。

并不只是学习使用浏览器（browser）而已，这太容易了，还要学会写 HTML 这个 Web 的标签语言。如果你不知道如何设计程序，写 HTML 也可以给一些习惯上的帮助。嗯!! 建立 home page 吧!

不过，有一个 home page 并没任何特别之处能让你成为一位 Hacker。Web 上到处都是 home page，而且大部份都没什么重点，没什么内容的烂泥 -- 很好看的烂泥巴，但是看起来都一样，差不多。为了让你的 page 有其价值，它必须是有内容的东西 -- 它必须是有趣并且(或者)对其它 Hacker 有用处的。

安全技术

网络安全技术指南

在网络上，最致命的就是木马缠身，后门大开！所谓木马，用通俗的话来说就是一个可以在机器上悄悄打开某个端口的程序。打开端口后"坏人"就可以通过控制端程序大摇大摆地通过这个端口进入你亲爱的计算机啦！进去了他可以

任意读写查找改删除上传下载你机器上的文件，他可以拿到你机器上存储的一切用户名和密码（包括缓存中的），他可以修改你的注册表（这个最痛苦了），他也可以把你的机器变成自己的玩具，于是你的鼠标被锁死啦，你的桌面隐藏啦，你啪一下蓝屏掉线啦...末了如果运气好（主要是"坏人"比较仁慈），你还能重新进入系统，然后你也许会在桌面上看到一个陌生的文本文件，里面写着：某某某到此一游！呵呵，你简直是衰到头了！要是赶上个心理变态的"坏人"，那你就可以重装系统了。

也许初级朋友们会想：这东西不一定就非得落在我机器上吧？我天儿，实话说了吧，你中这个东东的几率绝对比想象中的要高几百倍！不信你用代理猎手随便搜索一段国内用户IP域的7306端口（NETSPY木马），看看显示出来的长长的用户IP列表吧，那些都是中标的！其中是不是有你呢？

木马程序一般由两部分组成，一个控制端，一个SERVER端。SERVER端就是在你机器上开后门的那个东东了。当它被运行的时候一般来说都没有任何反应，但实际上你的那个特殊端口已经被敲开了，只要一上网，任何一个拥有控制端程序的人都可以登陆到你的机器上，然后他们要干啥也就不用我废话了。

目前国内比较流行的几个木马是Netspy，Netbus，BO，冰河，SUBSeven等，这些仅仅是国内流行的而已，已经在世界范围内被发现及证实的木马数不胜数。有一些甚至还具备了病毒的特征，不用上网就开始破坏系统了。

那么自己的机器是怎么被木马感染上的呢？这你就得问问你自己了。因为残酷的事实表明，这些木马几乎都是初级你自己亲手种上去的：

1.通过电子邮件传播：这种方法和病毒的传播方法有些类似，只不过其大多数是特殊有目的，有专门针对对象的传播。一般都是在邮件中夹带一个附件（就是木马Server），然后附上天花乱坠的说明，比如告诉你这是一个新出来共享工具，欢迎你来试用，又比如告诉你现在出现了一种新病毒，要预防必须装入这个免疫程序。呵呵，最残忍的就是用匿名信冒充你的好友发送，冷丁看到是朋友的伊妹儿，警惕自然就放松啦，然后...你就中招了呗！

2.文件捆绑：这种方法在现阶段来说可算是最流行最有效了。对方把一个木马的server端通过特殊工具捆绑在另一个应用程序软件中。这样你在运行那个应用程序时就不知不觉的连带着运行了木马。所以朋友们在网站下载软件时一定要时刻提高警惕。我所知道的最损的一招就是在某个知名站点上提供一个著名的清除木马工具下载，当你下载后运行时它工作正常，而且清除掉了所有支持的木马，但是就在程序执行完的一霎那，它却悄悄地把捆绑在身上的一个木马植入了机器。正所谓道高一尺，魔高一丈！

3. 你的好奇心：有些初级朋友对这些所谓的黑客工具感兴趣，就去黑站上下载了一个回来。解压后看到有两个文件，因为不会用就顺手运行了一个，结果正好是 server 端，于是自己把自己搞定了！

上面提到的是比较常见的传播木马方法，事实上还有更多意想不到的招式正在挑战你的 IQ。

面对种种不可预知的危险，一个好的病毒防火墙是很重要的，现在许多国产病毒防火墙已经可以监测到大多数木马程序，甚至可以揪出捆绑在应用程序中的木马。但是，木马作者们也不是吃闲饭的，他们也正在以前所未有的热情与速度编写新的木马程序，你能保证你的病毒防火墙更新速度可以追上新木马的诞生速度吗？反正据我知，冰河推出后都升级了一个版本国内的几个著名杀毒软件才刚刚能检测到，至于彻底清除，那更是几百辈子以后的事儿了。那么，目前最好的办法是装一个网络防火墙，比如我在上面提到过的 ConSeal PC FIREWALL，天网以及 LOCKDOWN 2000 等，都可以在连网的状态下提供对端口的监测，一旦发现有某个 IP 试图连接你的特殊端口或者已知可被木马利用端口时就会立刻做出提示，这时你就可以从容的拒绝对方的非法访问，从而保障了自己的系统安全。

几点补充：

1. 怎么在没有防火墙且连网的状态下判断是否被入侵？

根据我的经验，如果你在上网的时候，发现自己的硬盘总是莫名其妙的狂读，同时伴随着网速变慢；或者是软驱光驱灯突然亮了；以及出现了莫名的桌面空白或鼠标停止响应且不久恢复了正常；或者在不进行任何浏览器操作而且也没有带有广告条的网络工具在运行的时候，MODEM 却在不停的发送或接受数据，在以上情况下及有可能是被入侵了。

2. 被入侵了以后，该做些什么？

如果确定自己正在被入侵，应该果断掉线，然后进行彻底查修，如果有必要，可以考虑重装系统。另外，回忆一下是否在硬盘上某文档中保存了自己的一些重要口令数据，如果有则尽快更改！连带着更改自己的拨号上网口令，很多人就是冲着这个用木马的呀！当年刚上网时，有位高手请我用免费的账号，现在考虑他平日的所为想想，那应该是他从某人那里黑来的……别以为你没有在拨号时保存口令就安全了，我就见过一个老实朋友的机器上有一个目录叫"我的隐私"，里面有一个 mybak.txt 的文件，上面记的是该朋友的个人主页 ftp 地

址，用户名，口令以及上网账号，口令和信箱口令……重要口令不应该用自己的传呼号码呀，女朋友的生日呀等特别有意义的数字字母来构成这大伙都知道的。我要提醒的是，尽管很多朋友都知道在拨号上网时候不应该选择保存口令，但这并不意味着安全了。事实上大家往往忽略了一点，如果你是注册用户，那么ISP会送你一个.CN结尾的收费信箱（通常一兆之内免费，超了就要按K收钱哦），用于提供最新服务信息。这个信箱的用户名及口令与你拨号上网时的完全对应，为了图方便，很多朋友在使用OutlookExpress的时候往往顺手保存了口令。如果有人利用工具破解了你的这个信箱口令文件，你就知道后果了！

其次，现在好像邮件炸弹没有那么横行了，估计是目前免费邮箱提供的空间都很大的缘故。呵呵，反正我是想象不出来哪个朋友会用Up Yours轰炸新浪的五十兆信箱；）但是值得注意的是刚才提到的那个ISP提供的一兆信箱，保存邮件容量如果超过了一兆，就按每K收钱（好像都很贵哦），要是这个信箱被炸了，那你的银子可就哗哗淌到电信的虎口里啦（随着你的电话费走）。所以说，不仅保护口令要紧，用户名也不要轻易让别人知道呀！

最后，提醒各位初级要养成多上ISP的页去查询自己近期上网费用的习惯。我最近发现了一个问题：中国电信最近正在进行163，169并网工作，结果在某些城市出现了下一现象，那就是曾经注册163的用户，可以用其账号口令拨打169上网。也许朋友们会说，这个我们也知道呀，但是，对于某些已经窃取了别人用户口令的"坏人"来说，却有了极大的利用价值。当你用注册163的用户名和口令拨169上网时，在163的网上计费查询系统中查不到使用纪录（因为拨的是169呀），而在169的网上计费查询系统中也同样查不到纪录（因为原169用户数据库中没有该账号登记）。所以不少朋友明明每个月上网次数不多，却收到了一笔不菲的账单，而且按传统的在线查询方式也没有结果，只能打落了牙自己吞了。尤其是最近惊悉一些城市的电信竟公然说出卡用户账号被盗用后果一律自负，感觉真TMD不爽！所以更加要求初级朋友们提高网络安全意识，只有我们自己才能保护自己！

网络有漏洞？

网络有漏洞是可以肯定的。随着网络的飞速发展，掌管一些企业网络系统的人可能以前只是PC 机的操作员，他们虽然懂得一些网络的基本的安全规范，但并不是及时的了解关于网络漏洞的最新知识，不能及时的发现新的网络漏洞，就可能被入侵。国内电子商务站点的网络管理人员有90%以上没有受过正规的网络安全培训。这几年中国的互联网处于发展建设阶段，大部分的ISP和其他从事信息产业的公司都没有精力在网络安全上进行必要的人力和物力投入。很多