快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- **安全技术 <=**
- 业界动态

本类热门
- 如何利用黑客技术跟踪并分析一名目标人物
- 有关无线安全与黑客的话题
- 让我们回归(by 默难)
- 通用ShellCode深入剖析[转]
- Format String 漏洞介绍/总结(一)
- 结合实例解读ELF文件-阅读笔记(1)

如何利用黑客技术跟踪并分析一名目标人物

提交文章： xhacker
提交日期： 2004-06-22
文章属性： 原创
文档类别： 安全技术
相关图片： **=>查看<=**
浏览次数： 今39次/总15219次

如何利用黑客技术跟踪并分析一名目标人物

创建时间：2004-06-21
文章属性：原创
作者：王亮(小叮当/xhacker)
主页：xhacker.blogger.cn

目前，网络安全问题引起了越来越多人们的重视。但是绝大多数人都会认为，网络安全问题
只是基于网络基于主机的安全问题，只要主机系统网络系统配置合理也就能大大降低风险，所以一般人只注重机器的安全而忽视了个人在网络上随时随地可能出现的敏感信息泄露问题，而个人的信息泄露安全问题往往会带来不可预想的严重后果。

在这篇文章里，我尽量不涉及什么技术细节，只是使大家对黑客的跟踪和分析技术作一个大概的印象。让大家能体会到我们在这个网络世界里是多么缺乏安全保障，轻微会影响到个人隐私，严重甚至能影响到你的工作你的生活,在下面我将会利用所举的一个真实实例让你看到这绝不是骇人听闻,也让大家清晰的看到这种危害以及黑客跟踪技术的基本过程。

在这里我将要分析的主角是kevin,kevin是国内某著名网络安全公司的一位技术骨干。因为他的职业关系，我很快的联想到他在网络上应该会喜欢在一些比较有名的网络安全站点交流，所以如果我利用漏洞获取kevin在这些安全站点上注册账号的密码的话，那么这些密码有可能会与kevin在其他地方注册账号的密码相同从而进一步获取敏感信息。在众多安全站点目标当中我先选择了国内一个人人皆知的安全站点,用了不到十分钟我就成功的获取了这个网站的web管理权限，我利用sql查询语句很快找到了kevin的注册密码：

经过解密后明文密码是：“ k&YPYTr6yep3u444 ”。这里用常理推断一下，因为这个密码非常的复杂，而且做为普通人记忆力的限制，不太可能在网络上这么多需要密码的地方每处都设一个完全不同的复杂密码，所以这个密码有可能是个重要的常用密码。接下来我在后面看到了kevin注册时使用的邮箱zenith46793750@sina.com.cn，我就立刻想到邮箱的密码会不会也是这个复杂密码，随手到sina.com.cn一试，果然与期望的结果一样，我成功的进入了他的sina邮箱：

接下来就不用问了，查看他的邮箱里有没有敏感的邮件：



看到一封来自tencent的《密码保护的注册资料》的邮件，里面有密码回复答案等信息，但是tencent出于安全的考虑并没有给出是哪个QQ号的密码保护答案只是给出了QQ号码的最前两位数字，可是这位kevin大哥又犯了个错误，他在QQ密码提示问题里包含了一串数字，而这串数字的前两位数字与tencent提示信息里的QQ前两位数又相同，所以我们又顺利的利用密码保护的功能得到了这个QQ号码的密码并且成功登录了。另外在接下来的分析行为当中，又成功的得到了kevin的另一个QQ密码以及一些网站的密码。因为这是演示的原因，所以我并没有继续深入跟踪和分析，我想只要有时间还可以进一步扩大资源，比如利用现有密码信息尝试获取他公司的邮箱使用权，假设可以进入他公司的商业邮箱的话，说不定又会因此泄露商业上的敏感信息了。

深入的思考：
假设有个web主机的管理员与你有QQ上的联系，你通过套近与他的爱好从而从他口中得知他最喜欢上的一些站点名，然后通过黑客技术获取这些站点有关他的注册信息（QQ号、邮箱、爱好、口头蝉、密码、密码保护答案以及密码保护提问），那么从中找到的密码或对找出的密码进行一定规则的变形可能就是他web主机的管理密码或者说是web主机上某应用程序的账号密码，而他管理的web主机可能配置的相当安全，所以这种情况就可能会成为黑客案件的无头案，让任何人都找不到如何被黑客得知web主机密码的真正原因。我们暂且不讨论这种技术的成功概率有多少（我想只要肯花时间研究对方的习惯和心理是肯定会有些结果的），我再从一个方向举例：就拿我入侵的这台kevin所注册的网站来说，里面还有数万个账号，而我先前研究的目标人物kevin只是其中之一，如果我通过这几万个账号的密码分别尝试登录相应会员所使用的主机或管理的网站或公司邮箱的话，肯定会有为数不少的主机或邮箱等信息因此被非法占取。而同时也会产生大量的无头案。

结论：
计算机和我们的生活结合地越紧密，人们将会越来越依赖于网络的生活功能，而普通人是很难做到用一个非常精确的行为遵守个人网络安全准则的，不要说是普通人，就连很多一流的网络安全专家也不能做到保证在网络上不会受此类黑客跟踪技术攻击所影响。在此我也暂时没有可操作性的解决方案，我只是在此提出了一个新的安全观点，一个会影响千千万万网民自身隐私安全、个人网络资源安全、甚至是间接影响到自已公司网络安全的新观点。如果大家有什么新的想法可以给我来信root@21cn.com

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net