FourandSix：2 - writeup

转载

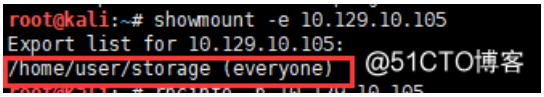
weixin_33701294 于 2018-11-23 17:52:08 发布 43 收藏
文章标签： shell 操作系统
原文链接：http://blog.51cto.com/executer/2321267

nmap扫描

`nmap -sS -Pn -A 10.129.10.105`查询到开放的端口及服务：22-ssh、111-rpcbind、2049-nfs、612-mountd，如图：

mountd服务检查

`showmount -e 10.129.10.105`发现存在可远程挂载的目录：`/home/user/storage(everyone)`尝试挂载目录及其上级目录后发现仅可挂载目录：`/home/user/storage(everyone)`



挂载目录：`mount -t nfs 10.129.10.105:/home/user/storage /tmp/test`，发现存在一个压缩文件：`backup.7z`

解压压缩包时，发现有密码，于是开始破解压缩包密码,破解可使用rarcrack暴力破解或通过7z命令进行字典爆破。其中，rarcrack破解命令为：`rarcrack --threads 4 --type 7z backup.7z`；7z破解脚本：7z-crack

```
./7z-crack.sh /tmp/backup.7z /usr/share/wordlists/rockyou.txt
```

最终，7z破解脚本成功破解到压缩包密码：`chocolate`

压缩包文件检查

压缩包加压后，发现了id_rsa和id_rsa.pub，于是猜测可直接通过id_rsa.pub登陆，在XSHELL中通过id_rsa.pub登陆时，需要输入密码，于是，使用工具破解id_rsa文件的密码，破解工具。

```
./id_rsa-crack.sh /tmp/id_rsa /usr/share/wordlists/rouckyou.txt
```

最后，拿到id_rsa密码：12345678

shell提权

进入shell后，发现当前用户是一个ksh，系统是FreeBSD 6.4的，搜索之后发现内核没有可用来提权的漏洞，于是将重点放在配置、文件和服务上。发现etc目录下有doas配置，发现当前用户可用doas提升到root访问/usr/bin/less来访问/var/log/auth.log文件，于是联想到linux系统中的SUID提权，于是，尝试从less到shell的跳转，最后无法跳转，原因暂不清楚；通过输入h后发现可以使用e来读取一个新的文件，于是读取到flag。

转载于:https://blog.51cto.com/executer/2321267