

# Security Engineering

## Lab 1 (Report)

~Siddharth Sharma (2014104)

Sujeet Kumar (2014108)

### 1. Basic ACLs

Steps followed during the lab assignment :

1)Copy the files to the user directory.

Command : `sudo cp -r /root/httpd_install/* /home/www-user`

2) Move to httpd\_install directory.

Command : `cd /home/www-user/httpd_install`

3)Change DocumentRoot in the httpd.conf

`sudo nano httpd.conf`

```

# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www"
<Directory "/home/www/httpd_install/temp_htdocs">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    [ Replaced 1 occurrence ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    ^Y Prev Page
Use "fg" to return to nano.  ^R Replace     ^U Uncut Text ^T To Spell    ^_ Go To Line   ^V Next Page

[11]+  Stopped                  nano httpd.conf
sec-eng-usr@sec-eng:/home/www-user/httpd_install/conf$ cd ..
sec-eng-usr@sec-eng:/home/www-user/httpd_install$ cd ..
sec-eng-usr@sec-eng:/home/www-user$ cd ..
sec-eng-usr@sec-eng:/home$ cd /var/www
sec-eng-usr@sec-eng:/var/www$ cd ..
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::rwx
user:www-user:rwx
group::r-x
mask::rwx
other::r-x

sec-eng-usr@sec-eng:/var$

```

4) Change the directory to /var/www

```
cd /var/www
```

5) Add user-www permissions in the ACL and remove all others

```
Getfacl www
```

```
Sudo setfacl -m u:www-user:rwx www (add user permission)
```

```
Sudo setfacl -m u:--- ./www (delete permission)
```

```
Sudo setfacl -m g:--- ./www (delete permission)
```

```
Sudo setfacl -m o:--- ./www (delete permission)
```

```
sec-eng-usr@sec-eng:/var$ setfacl -x other www
setfacl: www: Malformed access ACL `user::rwx,user:www-user:rwx,group::r-x,mask::rwx': Missing or wrong entry at entry 5
sec-eng-usr@sec-eng:/var$ sudo setfacl -m u::--- ./www
[sudo] password for sec-eng-usr:
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::---
user:www-user:rwx
group::r-x
mask::rwx
other::r-x

sec-eng-usr@sec-eng:/var$ sudo setfacl -m u*:--- ./www
setfacl: Option -m: Invalid argument near character 3
sec-eng-usr@sec-eng:/var$ setfacl -s u:www-user:rwx www
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try `setfacl --help' for more information.
sec-eng-usr@sec-eng:/var$ sudo setfacl -s u:www-user:rwx www
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try `setfacl --help' for more information.
sec-eng-usr@sec-eng:/var$ sudo setfacl -m o::--- ./www
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::---
user:www-user:rwx
group::r-x
mask::rwx
other::---

sec-eng-usr@sec-eng:/var$ sudo setfacl -m g::--- ./www
sec-eng-usr@sec-eng:/var$
```

```
user::---
user:www-user:rwx
group::r-x
mask::rwx
other::r-x

sec-eng-usr@sec-eng:/var$ sudo setfacl -m u:*:--- ./www
setfacl: Option -m: Invalid argument near character 3
sec-eng-usr@sec-eng:/var$ setfacl -s u:www-user:rwx www
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try `setfacl --help' for more information.
sec-eng-usr@sec-eng:/var$ sudo setfacl -s u:www-user:rwx www
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try `setfacl --help' for more information.
sec-eng-usr@sec-eng:/var$ sudo setfacl -m o::--- ./www
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::---
user:www-user:rwx
group::r-x
mask::rwx
other::---

sec-eng-usr@sec-eng:/var$ sudo setfacl -m g::--- ./www
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::---
user:www-user:rwx
group::---
mask::rwx
other::---

sec-eng-usr@sec-eng:/var$ _
```

6)Run the HTTP server from the bin directory

```
./httpd -f /home/www-user/httpd_install/conf/httpd_conf
```

```
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 8082
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadModule authn_file_module modules/mod_authn_file.so

www-user@sec-eng:~/httpd_install/conf$ cd /home/www-user/httpd_install/b
bin/ build/
www-user@sec-eng:~/httpd_install/conf$ cd /home/www-user/httpd_install/b
bin/ build/
www-user@sec-eng:~/httpd_install/conf$ cd /home/www-user/httpd_install/b
bin/ build/
www-user@sec-eng:~/httpd_install/conf$ cd /home/www-user/httpd_install/bin/
www-user@sec-eng:~/httpd_install/bin$
www-user@sec-eng:~/httpd_install/bin$ ./httpd -f /home/www-user/httpd_install/conf/httpd.conf
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1
.1. Set the 'ServerName' directive globally to suppress this message
www-user@sec-eng:~/httpd_install/bin$ _
```

7)Switch to the www-user and test if permission is obtained by sending a request to the server

```
curl 127.0.0.1:8082
```

Permission given

```

www-user@sec-eng:~/httpd_install/bin$ ps aux | grep http
root      1158  0.0  0.2 52940 4040 tty1    T   17:17   0:00 sudo vim httpd.conf
root      1159  0.0  0.5 54112 8644 tty1    T   17:17   0:00 vim httpd.conf
root      1231  0.0  0.2 73164 3804 ?        Ss   17:26   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
daemon    1232  0.0  0.3 362128 5704 ?        S1   17:26   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
daemon    1233  0.0  0.3 362128 5696 ?        S1   17:26   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
daemon    1234  0.0  0.3 362128 5704 ?        S1   17:26   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
www-user  1602  0.2  0.5 54112 8708 tty1    T   17:55   0:01 vim httpd.conf
www-user  1625  0.0  0.5 54116 8600 tty1    T   17:59   0:00 vim httpd.conf
www-user  1651  0.0  0.2 73164 4012 ?        Ss   18:02   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
www-user  1652  0.0  0.2 362128 4052 ?        S1   18:02   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
www-user  1653  0.0  0.2 362128 4052 ?        S1   18:02   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
www-user  1654  0.0  0.2 362128 4052 ?        S1   18:02   0:00 ./httpd -f /home/www-user/httpd_ins
tall/conf/httpd.conf
www-user  1758  0.0  0.0 11180 516 tty1    R+   18:05   0:00 grep --color=auto http
www-user@sec-eng:~/httpd_install/bin$ curl http://127.0.1.1:8082
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of </title>
</head>
<body>
<h1>Index of </h1>
<ul></ul>
</body></html>
www-user@sec-eng:~/httpd_install/bin$ _

```

ps aux | grep http to verify server running

After that create a new dir name "new" where www-user has no permission to that file

Change documentroot location to var/new

Run http server by foing inside bin

./httpd -f /home/www-user/httpd\_install/conf/httpd\_conf

Curl 127.0.0.1:8082

```

Unable to get valid context for sec-eng-usr
sec-eng-usr@sec-eng:~$ cd /var
sec-eng-usr@sec-eng:/var$ ls
backups cache crash lib local lock log mail opt run spool tmp webapp www
sec-eng-usr@sec-eng:/var$ mkdir new
mkdir: cannot create directory 'new': Permission denied
sec-eng-usr@sec-eng:/var$ sudo mkdir new
[sudo] password for sec-eng-usr:
sec-eng-usr@sec-eng:/var$ getfacl new
# file: new
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

sec-eng-usr@sec-eng:/var$ sudo setfacl -m o::--- new
sec-eng-usr@sec-eng:/var$ getfacl new
# file: new
# owner: root
# group: root
user::rwx
group::r-x
other::---

sec-eng-usr@sec-eng:/var$ sudo setfacl -m g::--- new
sec-eng-usr@sec-eng:/var$ getfacl new
# file: new
# owner: root
# group: root
user::rwx
group::---
other::---

sec-eng-usr@sec-eng:/var$

```

Create new dir in /root and remove other users and group permission.

```

# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/new"
<Directory "/var/new">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:

sec-eng-usr@sec-eng:/home/www-user/httpd_install/conf$ cd /home/www-user/httpd_install/
sec-eng-usr@sec-eng:/home/www-user/httpd_install$ cd bin
sec-eng-usr@sec-eng:/home/www-user/httpd_install/bin$ sudo ./httpd -f /home/www-user/httpd_install/c
nf/httpd.conf
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1
.1. Set the 'ServerName' directive globally to suppress this message
sec-eng-usr@sec-eng:/home/www-user/httpd_install/bin$ su www-user
Password:
www-user@sec-eng:/httpd_install/bin$ curl 127.0.0.1:8082
curl: (6) Could not resolve host: 127.0.0.1:8082
www-user@sec-eng:/httpd_install/bin$ curl 127.0.0.1:8082
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.<br />
</p>
</body></html>
www-user@sec-eng:/httpd_install/bin$ _

```

```

sec-eng-usr@sec-eng:/var/log/apache2$ sudo setfacl -s u:www-user:rwX ./access.log
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try `setfacl --help' for more information.
sec-eng-usr@sec-eng:/var/log/apache2$ ls
access.log  error.log  other_vhosts_access.log
sec-eng-usr@sec-eng:/var/log/apache2$ sudo setfacl -m u:www-user:rwX ./access.log
sec-eng-usr@sec-eng:/var/log/apache2$ getfacl access.log
# file: access.log
# owner: root
# group: adm
user::rw-
user:www-user:rwX
group::r--
mask::rwX
other::---

sec-eng-usr@sec-eng:/var/log/apache2$ _

```



```
:::1 - - [19/Jan/2017:22:12:53 +0530] "GET /index.html HTTP/1.1" 403 219
127.0.0.1 - - [19/Jan/2017:22:13:13 +0530] "GET /index.html HTTP/1.1" 403 219
127.0.0.1 - - [19/Jan/2017:22:13:54 +0530] "GET /index.html HTTP/1.0" 403 219
127.0.0.1 - - [19/Jan/2017:22:15:02 +0530] "GET /index.html HTTP/1.1" 403 219
:::1 - - [19/Jan/2017:22:18:39 +0530] "GET /index.html HTTP/1.0" 403 219
:::1 - - [19/Jan/2017:22:18:51 +0530] "GET /index.html HTTP/1.1" 403 219
:::1 - - [19/Jan/2017:22:20:19 +0530] "GET /index.html HTTP/1.1" 403 219
:::1 - - [19/Jan/2017:22:20:46 +0530] "GET /index.html HTTP/1.1" 200 45
:::1 - - [19/Jan/2017:22:23:41 +0530] "GET /index.html HTTP/1.1" 200 45
:::1 - - [19/Jan/2017:22:25:43 +0530] "GET /index.html HTTP/1.0" 404 208
:::1 - - [19/Jan/2017:22:25:53 +0530] "GET /index.html HTTP/1.1" 404 208
:::1 - - [19/Jan/2017:22:25:57 +0530] "GET /index.txt HTTP/1.1" 200 4
:::1 - - [19/Jan/2017:22:28:55 +0530] "GET /index.txt HTTP/1.1" 200 4
127.0.0.1 - - [24/Jan/2017:18:05:47 +0530] "GET / HTTP/1.1" 200 161
```

"access\_log" 14L, 1014C

1,1

All

access.log

```

[Thu Jan 19 22:12:19.882254 2017] [mpm_event:notice] [pid 3701:tid 140061696747264] AH00489: Apache$
[Thu Jan 19 22:12:19.882400 2017] [core:notice] [pid 3701:tid 140061696747264] AH00094: Command lin$
[Thu Jan 19 22:12:53.473488 2017] [core:error] [pid 3702:tid 140061467195136] (13)Permission denied$
[Thu Jan 19 22:13:13.023879 2017] [core:error] [pid 3702:tid 140061450409728] (13)Permission denied$
[Thu Jan 19 22:13:54.564932 2017] [core:error] [pid 3702:tid 140061341304576] (13)Permission denied$
[Thu Jan 19 22:15:02.330538 2017] [core:error] [pid 3702:tid 140061613057792] (13)Permission denied$
[Thu Jan 19 22:18:39.893828 2017] [core:error] [pid 3702:tid 140061442017024] (13)Permission denied$
[Thu Jan 19 22:18:51.558402 2017] [core:error] [pid 3702:tid 140061433624320] (13)Permission denied$
[Thu Jan 19 22:20:19.901600 2017] [core:error] [pid 3704:tid 140061579486976] (13)Permission denied$
[Thu Jan 19 22:25:35.390696 2017] [mpm_event:notice] [pid 3701:tid 140061696747264] AH00491: caught$
[Thu Jan 19 22:25:39.462600 2017] [mpm_event:notice] [pid 4642:tid 140181840602880] AH00489: Apache$
[Thu Jan 19 22:25:39.462718 2017] [core:notice] [pid 4642:tid 140181840602880] AH00094: Command lin$
[Thu Jan 19 22:35:07.962878 2017] [mpm_event:notice] [pid 4642:tid 140181840602880] AH00491: caught$
[Tue Jan 24 17:26:42.693441 2017] [mpm_event:notice] [pid 1231:tid 139627743160064] AH00489: Apache$
[Tue Jan 24 17:26:42.740956 2017] [core:notice] [pid 1231:tid 139627743160064] AH00094: Command lin$
[Tue Jan 24 18:02:20.871258 2017] [core:warn] [pid 1651:tid 139795073885952] AH00098: pid file /root$
[Tue Jan 24 18:02:20.872110 2017] [mpm_event:notice] [pid 1651:tid 139795073885952] AH00489: Apache$
[Tue Jan 24 18:02:20.872143 2017] [core:notice] [pid 1651:tid 139795073885952] AH00094: Command lin$

```

[ Read 18 lines ]

^G Get Help	^O Write Out	^W Where Is	^K Cut Text	^J Justify	^C Cur Pos	^V Prev Page
^X Exit	^R Read File	^~ Replace	^U Uncut Text	^T To Spell	^_ Go To Line	^U Next Page

error.log

```

[Thu Jan 19 22:12:19.882254 2017] [mpm_event:notice] [pid 3701:tid 140061696747264] AH00489: Apache$
[Thu Jan 19 22:12:19.882400 2017] [core:notice] [pid 3701:tid 140061696747264] AH00094: Command lin$
[Thu Jan 19 22:12:53.473488 2017] [core:error] [pid 3702:tid 140061467195136] (13)Permission denied$
[Thu Jan 19 22:13:13.023879 2017] [core:error] [pid 3702:tid 140061450409728] (13)Permission denied$
[Thu Jan 19 22:13:54.564932 2017] [core:error] [pid 3702:tid 140061341304576] (13)Permission denied$
[Thu Jan 19 22:15:02.330538 2017] [core:error] [pid 3702:tid 140061613057792] (13)Permission denied$
[Thu Jan 19 22:18:39.893828 2017] [core:error] [pid 3702:tid 140061442017024] (13)Permission denied$
[Thu Jan 19 22:18:51.558402 2017] [core:error] [pid 3702:tid 140061433624320] (13)Permission denied$
[Thu Jan 19 22:20:19.901600 2017] [core:error] [pid 3704:tid 140061579486976] (13)Permission denied$
[Thu Jan 19 22:25:35.390696 2017] [mpm_event:notice] [pid 3701:tid 140061696747264] AH00491: caught$
[Thu Jan 19 22:25:39.462600 2017] [mpm_event:notice] [pid 4642:tid 140181840602880] AH00489: Apache$
[Thu Jan 19 22:25:39.462718 2017] [core:notice] [pid 4642:tid 140181840602880] AH00094: Command lin$
[Thu Jan 19 22:35:07.962878 2017] [mpm_event:notice] [pid 4642:tid 140181840602880] AH00491: caught$

```

```

[ Read 13 lines (Warning: No write permission) ]
^G Get Help    ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    ^Y Prev Page
^X Exit        ^R Read File  ^_ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line  ^U Next Page

```

Error log for permission denied

## 2. Default ACLs

1) In this question we create two directories in /var/www,

Give default permissions **rwX** for users, groups and others to /var/www.

```
sec-eng-usr@sec-eng:/var$ rmdir www
rmdir: failed to remove 'www': Permission denied
sec-eng-usr@sec-eng:/var$ sudo rmdir www
[sudo] password for sec-eng-usr:
sec-eng-usr@sec-eng:/var$ sudo rmdir www
rmdir: failed to remove 'www': No such file or directory
sec-eng-usr@sec-eng:/var$ ^C
sec-eng-usr@sec-eng:/var$ ^C
sec-eng-usr@sec-eng:/var$ mkdir www
mkdir: cannot create directory 'www': Permission denied
sec-eng-usr@sec-eng:/var$ sudo mkdir www
[sudo] password for sec-eng-usr:
sec-eng-usr@sec-eng:/var$ ls
backups  cache  crash  lib  local  lock  log  mail  new  opt  run  spool  tmp  webapp  www
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::rwX
group::r-x
other::r-x

sec-eng-usr@sec-eng:/var$ sudo setfacl -d -m u::rwX ./www
sec-eng-usr@sec-eng:/var$ sudo setfacl -d -m g::rwX ./www
sec-eng-usr@sec-eng:/var$ sudo setfacl -d -m o::rwX ./www
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::rwX
group::r-x
other::r-x
default:user::rwX
default:group::rwX
default:other::rwX

sec-eng-usr@sec-eng:/var$
```

2)

**var/www/Test\_dir1** : inherited default permissions as **rwX** from the parent directory (var/www/). Give default permissions as - - - for users, groups and others.

**var/www/Test\_dir2**: inherited default permissions as **rwX** from the parent directory (var/www/)

```
sec-eng-usr@sec-eng:/var$ sudo setfacl -d -m g::rwx ./www
sec-eng-usr@sec-eng:/var$ sudo setfacl -d -m o::rwx ./www
sec-eng-usr@sec-eng:/var$ getfacl www
# file: www
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
default:user::rwx
default:group::rwx
default:other::rwx

sec-eng-usr@sec-eng:/var$ sudo mkdir Test_dir1
sec-eng-usr@sec-eng:/var$ sudo mkdir Test_dir2
sec-eng-usr@sec-eng:/var$ sudo rmdir Test_dir2
sec-eng-usr@sec-eng:/var$ sudo rmdir Test_dir1
sec-eng-usr@sec-eng:/var$ cd www
sec-eng-usr@sec-eng:/var/www$ sudo mkdir Test_dir1
sec-eng-usr@sec-eng:/var/www$ sudo mkdir Test_dir2
sec-eng-usr@sec-eng:/var/www$ ls
Test_dir1 Test_dir2
sec-eng-usr@sec-eng:/var/www$ sudo setfacl -d -m o::--- ./Test_dir1
sec-eng-usr@sec-eng:/var/www$ sudo setfacl -d -m u::--- ./Test_dir1
sec-eng-usr@sec-eng:/var/www$ sudo setfacl -d -m g::--- ./Test_dir1
sec-eng-usr@sec-eng:/var/www$ getfacl Test_dir1
# file: Test_dir1
# owner: root
# group: root
user::rwx
group::rwx
other::rwx
default:user::---
default:group::---
default:other::---

sec-eng-usr@sec-eng:/var/www$ _
```

3) Run getfacl Test\_dir1 and getfacl Test\_dir1 to check the assigned permissions

```
sec-eng-usr@sec-eng:/var/www$  
sec-eng-usr@sec-eng:/var/www$  
sec-eng-usr@sec-eng:/var/www$ getfacl Test_dir1  
# file: Test_dir1  
# owner: root  
# group: root  
user::rwx  
group::rwx  
other::rwx  
default:user::---  
default:group::---  
default:other::---  
  
sec-eng-usr@sec-eng:/var/www$ getfacl Test_dir2  
# file: Test_dir2  
# owner: root  
# group: root  
user::rwx  
group::rwx  
other::rwx  
default:user::rwx  
default:group::rwx  
default:other::rwx  
  
sec-eng-usr@sec-eng:/var/www$ cd Test_dir1  
sec-eng-usr@sec-eng:/var/www/Test_dir1$ getfacl INSIDE_Test_dir1/  
# file: INSIDE_Test_dir1/  
# owner: sec-eng-usr  
# group: sec-eng-usr  
user::---  
group::---  
other::---  
default:user::---  
default:group::---  
default:other::---  
  
sec-eng-usr@sec-eng:/var/www/Test_dir1$ _
```

4) set DocumentRoot : directory /var/www/Test\_dir1

Allowed access and given the following output.

```

</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/Test_dir1"
<Directory "/var/www/Test_dir1">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:

www-user@sec-eng:~/httpd_install/conf$ cd ..
www-user@sec-eng:~/httpd_install$ cd bin/
www-user@sec-eng:~/httpd_install/bin$ ./httpd -f /home/www-user/httpd_install/conf/httpd.conf
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1
.1. Set the 'ServerName' directive globally to suppress this message
www-user@sec-eng:~/httpd_install/bin$ curl 127.0.1.1:8082
<?DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
  <head>
    <title>Index of </title>
  </head>
  <body>
<h1>Index of </h1>
<ul></ul>
</body></html>
www-user@sec-eng:~/httpd_install/bin$ _

```

(Error code 403 : Forbidden (as default access of www is overwritten by default access of Test\_dir1))

Moving to Inside the directory(/var/www/Test\_dir1/INSIDE\_Test\_dir1) where permission is not granted.(first setting DocumentRoot in the httpd.conf file)

```
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/Test_dir1/INSIDE_Test_dir1"
<Directory "/var/www/Test_dir1/INSIDE_Test_dir1">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
```

Get Help	Write Out	Where Is	Cut Text	Justify	Cur Pos	Prev Page
Exit	Read File	Replace	Uncut Text	To Spell	Go To Line	Next Page



Run the server and check for response(Denied 403 Error.)

```
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/Test_dir1/INSIDE_Test_dir1"
<Directory "/var/www/Test_dir1/INSIDE_Test_dir1">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:

www-user@sec-eng:~/httpd_install/conf$ cd ..
www-user@sec-eng:~/httpd_install$ cd bin
www-user@sec-eng:~/httpd_install/bin$ ./httpd -f /home/www-user/httpd_install/conf/httpd.conf
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1
.1. Set the 'ServerName' directive globally to suppress this message
httpd (pid 1543) already running
www-user@sec-eng:~/httpd_install/bin$ kill 1543
www-user@sec-eng:~/httpd_install/bin$ ./httpd -f /home/www-user/httpd_install/conf/httpd.conf
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1
.1. Set the 'ServerName' directive globally to suppress this message
www-user@sec-eng:~/httpd_install/bin$ curl 127.0.1.1:8082
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.<br />
</p>
</body></html>
www-user@sec-eng:~/httpd_install/bin$
```

Logs :

Access Logs (for successful request) :

```
:::1 - - [19/Jan/2017:22:12:53 +0530] "GET /index.html HTTP/1.1" 403 219
127.0.0.1 - - [19/Jan/2017:22:13:13 +0530] "GET /index.html HTTP/1.1" 403 219
127.0.0.1 - - [19/Jan/2017:22:13:54 +0530] "GET /index.html HTTP/1.0" 403 219
127.0.0.1 - - [19/Jan/2017:22:15:02 +0530] "GET /index.html HTTP/1.1" 403 219
:::1 - - [19/Jan/2017:22:18:39 +0530] "GET /index.html HTTP/1.0" 403 219
:::1 - - [19/Jan/2017:22:18:51 +0530] "GET /index.html HTTP/1.1" 403 219
:::1 - - [19/Jan/2017:22:20:19 +0530] "GET /index.html HTTP/1.1" 403 219
:::1 - - [19/Jan/2017:22:20:46 +0530] "GET /index.html HTTP/1.1" 200 45
:::1 - - [19/Jan/2017:22:23:41 +0530] "GET /index.html HTTP/1.1" 200 45
:::1 - - [19/Jan/2017:22:25:43 +0530] "GET /index.html HTTP/1.0" 404 208
:::1 - - [19/Jan/2017:22:25:53 +0530] "GET /index.html HTTP/1.1" 404 208
:::1 - - [19/Jan/2017:22:25:57 +0530] "GET /index.txt HTTP/1.1" 200 4
:::1 - - [19/Jan/2017:22:28:55 +0530] "GET /index.txt HTTP/1.1" 200 4
127.0.0.1 - - [24/Jan/2017:18:05:47 +0530] "GET / HTTP/1.1" 200 161
127.0.0.1 - - [24/Jan/2017:18:39:31 +0530] "GET / HTTP/1.1" 403 209
127.0.0.1 - - [24/Jan/2017:20:50:15 +0530] "GET / HTTP/1.1" 200 161
127.0.0.1 - - [24/Jan/2017:20:56:28 +0530] "GET / HTTP/1.1" 403 209
```

```
[ Read 17 lines ]
^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J Justify       ^C Cur Pos       ^Y Prev Page
^X Exit          ^R Read File     ^_ Replace       ^U Uncut Text    ^T To Spell     ^_ Go To Line    ^U Next Page
```

Error Logs:

```

[Thu Jan 19 22:12:19.882254 2017] [mpm_event:notice] [pid 3701:tid 140061696747264] AH00489: Apache$
[Thu Jan 19 22:12:19.882400 2017] [core:notice] [pid 3701:tid 140061696747264] AH00094: Command lin$
[Thu Jan 19 22:12:53.473488 2017] [core:error] [pid 3702:tid 140061467195136] (13)Permission denied$
[Thu Jan 19 22:13:13.023879 2017] [core:error] [pid 3702:tid 140061450409728] (13)Permission denied$
[Thu Jan 19 22:13:54.564932 2017] [core:error] [pid 3702:tid 140061341304576] (13)Permission denied$
[Thu Jan 19 22:15:02.330538 2017] [core:error] [pid 3702:tid 140061613057792] (13)Permission denied$
[Thu Jan 19 22:18:39.893828 2017] [core:error] [pid 3702:tid 140061442017024] (13)Permission denied$
[Thu Jan 19 22:18:51.558402 2017] [core:error] [pid 3702:tid 140061433624320] (13)Permission denied$
[Thu Jan 19 22:20:19.901600 2017] [core:error] [pid 3704:tid 140061579486976] (13)Permission denied$
[Thu Jan 19 22:25:35.390696 2017] [mpm_event:notice] [pid 3701:tid 140061696747264] AH00491: caught$
[Thu Jan 19 22:25:39.462600 2017] [mpm_event:notice] [pid 4642:tid 140181840602880] AH00489: Apache$
[Thu Jan 19 22:25:39.462718 2017] [core:notice] [pid 4642:tid 140181840602880] AH00094: Command lin$
[Thu Jan 19 22:35:07.962878 2017] [mpm_event:notice] [pid 4642:tid 140181840602880] AH00491: caught$
[Tue Jan 24 17:26:42.693441 2017] [mpm_event:notice] [pid 1231:tid 139627743160064] AH00489: Apache$
[Tue Jan 24 17:26:42.740956 2017] [core:notice] [pid 1231:tid 139627743160064] AH00094: Command lin$
[Tue Jan 24 18:02:20.871258 2017] [core:warn] [pid 1651:tid 139795073885952] AH00098: pid file /roo$
[Tue Jan 24 18:02:20.872110 2017] [mpm_event:notice] [pid 1651:tid 139795073885952] AH00489: Apache$
[Tue Jan 24 18:02:20.872143 2017] [core:notice] [pid 1651:tid 139795073885952] AH00094: Command lin$
[Tue Jan 24 18:38:15.486390 2017] [core:warn] [pid 1226:tid 139790252091136] AH00098: pid file /roo$
[Tue Jan 24 18:38:15.508627 2017] [mpm_event:notice] [pid 1226:tid 139790252091136] AH00489: Apache$
[Tue Jan 24 18:38:15.508662 2017] [core:notice] [pid 1226:tid 139790252091136] AH00094: Command lin$
[Tue Jan 24 18:39:31.748498 2017] [core:error] [pid 1227:tid 139790168401664] (13)Permission denied$
[Tue Jan 24 20:49:57.605572 2017] [core:warn] [pid 1543:tid 140510868186880] AH00098: pid file /roo$
[Tue Jan 24 20:49:57.606721 2017] [mpm_event:notice] [pid 1543:tid 140510868186880] AH00489: Apache$
[Tue Jan 24 20:49:57.606752 2017] [core:notice] [pid 1543:tid 140510868186880] AH00094: Command lin$
[Tue Jan 24 20:50:15.284355 2017] [core:error] [pid 1544:tid 140510559680256] (13)Permission denied$
[Tue Jan 24 20:56:17.658479 2017] [mpm_event:notice] [pid 1543:tid 140510868186880] AH00491: caught$
[Tue Jan 24 20:56:19.388076 2017] [mpm_event:notice] [pid 1692:tid 140612252661504] AH00489: Apache$
[Tue Jan 24 20:56:19.388168 2017] [core:notice] [pid 1692:tid 140612252661504] AH00094: Command lin$
[Tue Jan 24 20:56:28.267281 2017] [core:error] [pid 1693:tid 140612168972032] (13)Permission denied$

```

```

[ Read 30 lines ]
^G Get Help    ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    ^Y Prev Page
^X Exit        ^R Read File  ^M Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line  ^V Next Page

```

-----O-----O-----O-----