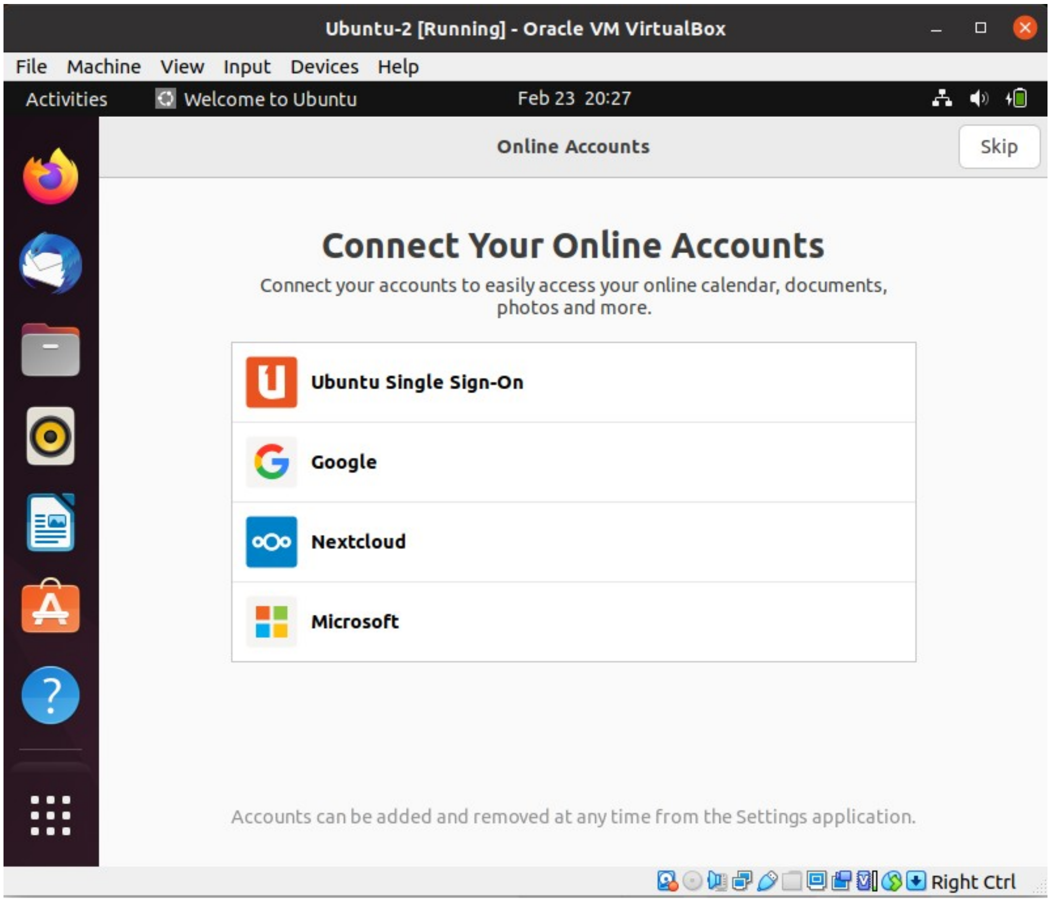
Step 0: Download the php files into a folder. You will need to transfer these into the Ubuntu VM
config.php (Has database connection configuration)
Form.php (The main Form/your index, from here you can create new entries)
create.php (Script that allows you to create an entry)
view.php (View particular entry)
delete.php (Allows you to delete an entry)
update.php (Update an existing entry)
export.php (Allows you to export index as CSV file..which can be opened in excel)
error.php (Just an error page to display if something goes wrong)

Step 1: Create Ubuntu VM with Oracle Virtualbox (or other Hypervisors)

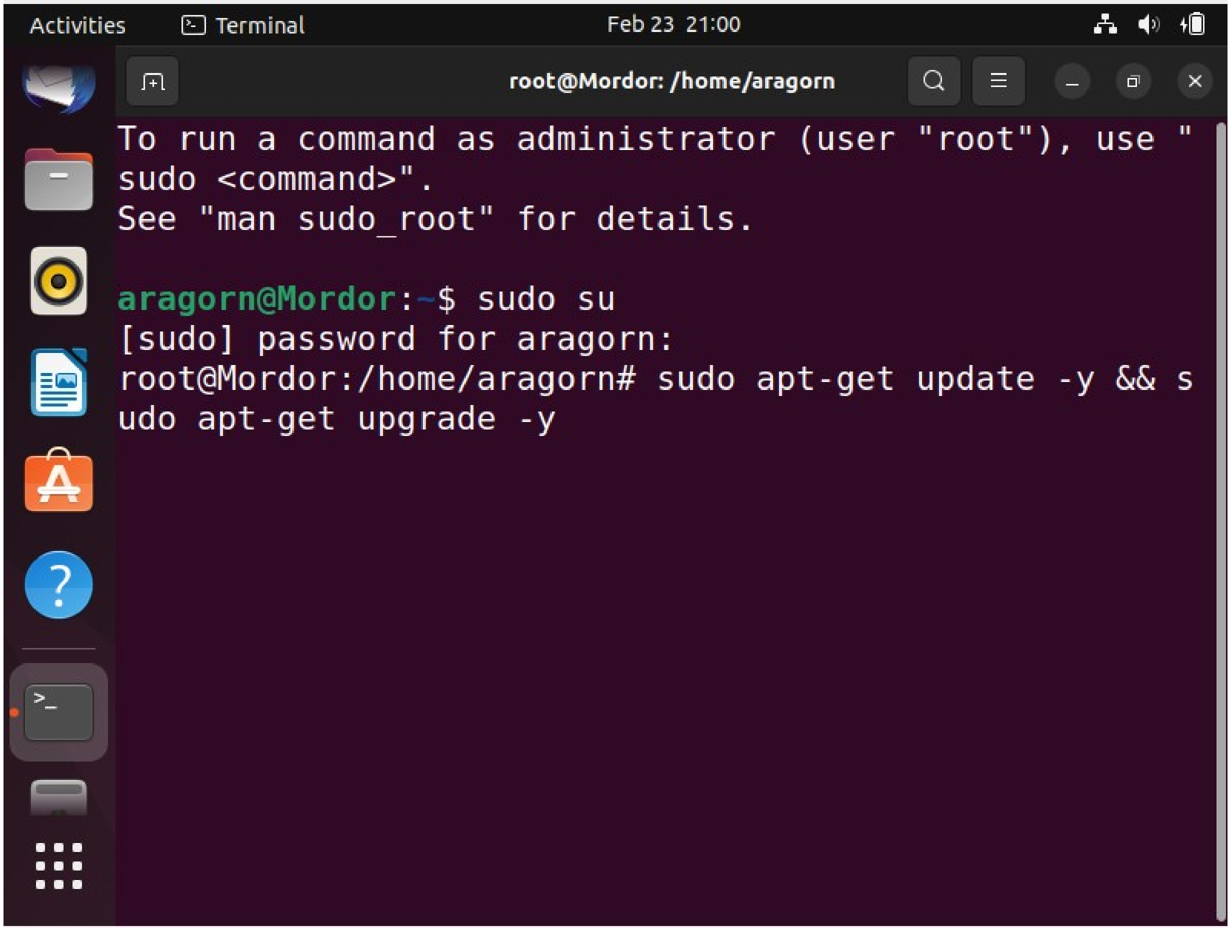


Connect Your Online Accounts

Connect your accounts to easily access your online calendar, documents, photos and more.

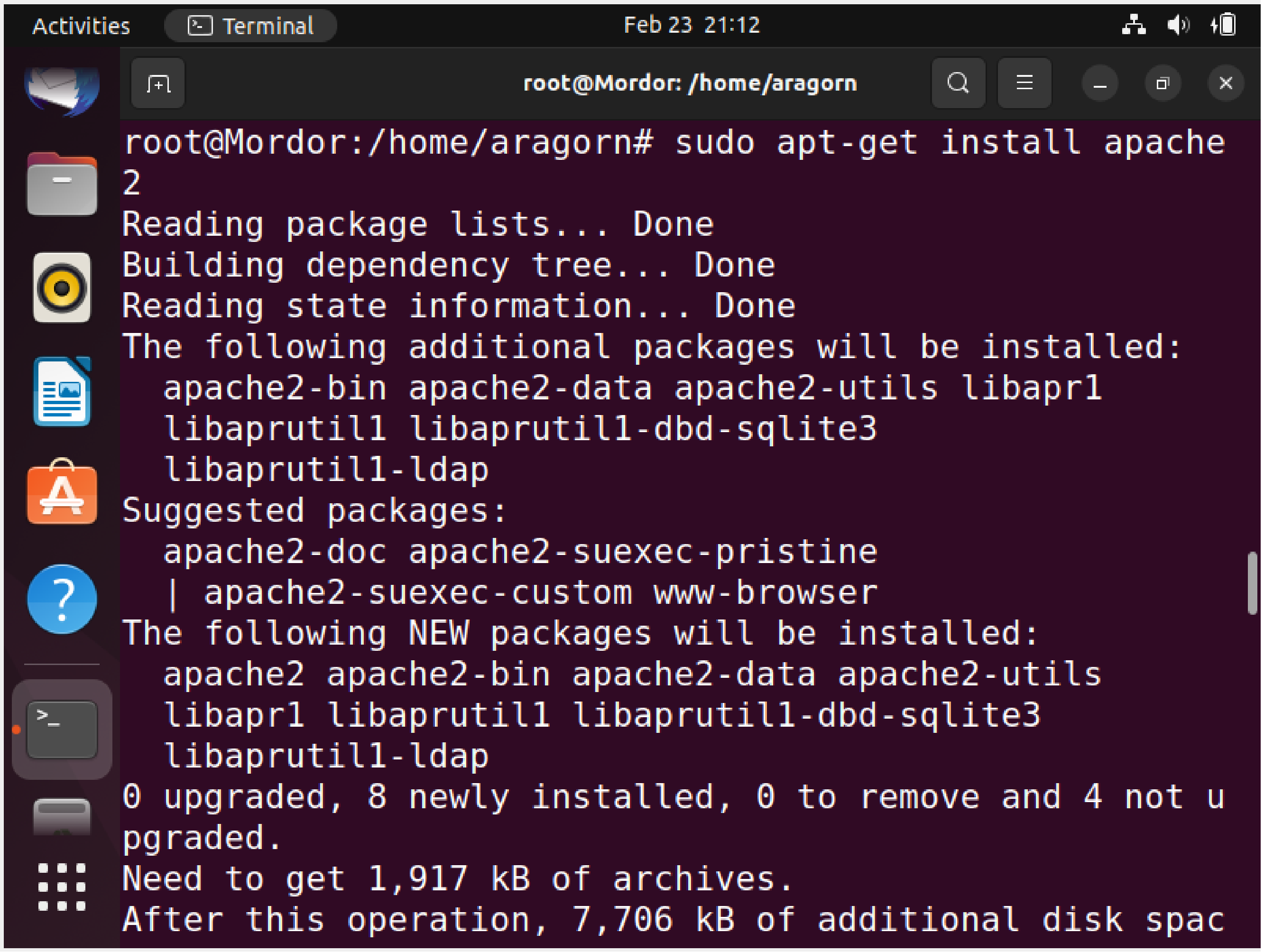
Accounts can be added and removed at any time from the Settings application.

Make sure system is updated



```
To run a command as administrator (user "root"), use "
sudo <command>".
See "man sudo_root" for details.

aragorn@Mordor:~$ sudo su
[sudo] password for aragorn:
root@Mordor:/home/aragorn# sudo apt-get update -y && s
udo apt-get upgrade -y
```

Step 2: Install web server (apache2), drop files in appropriate folders

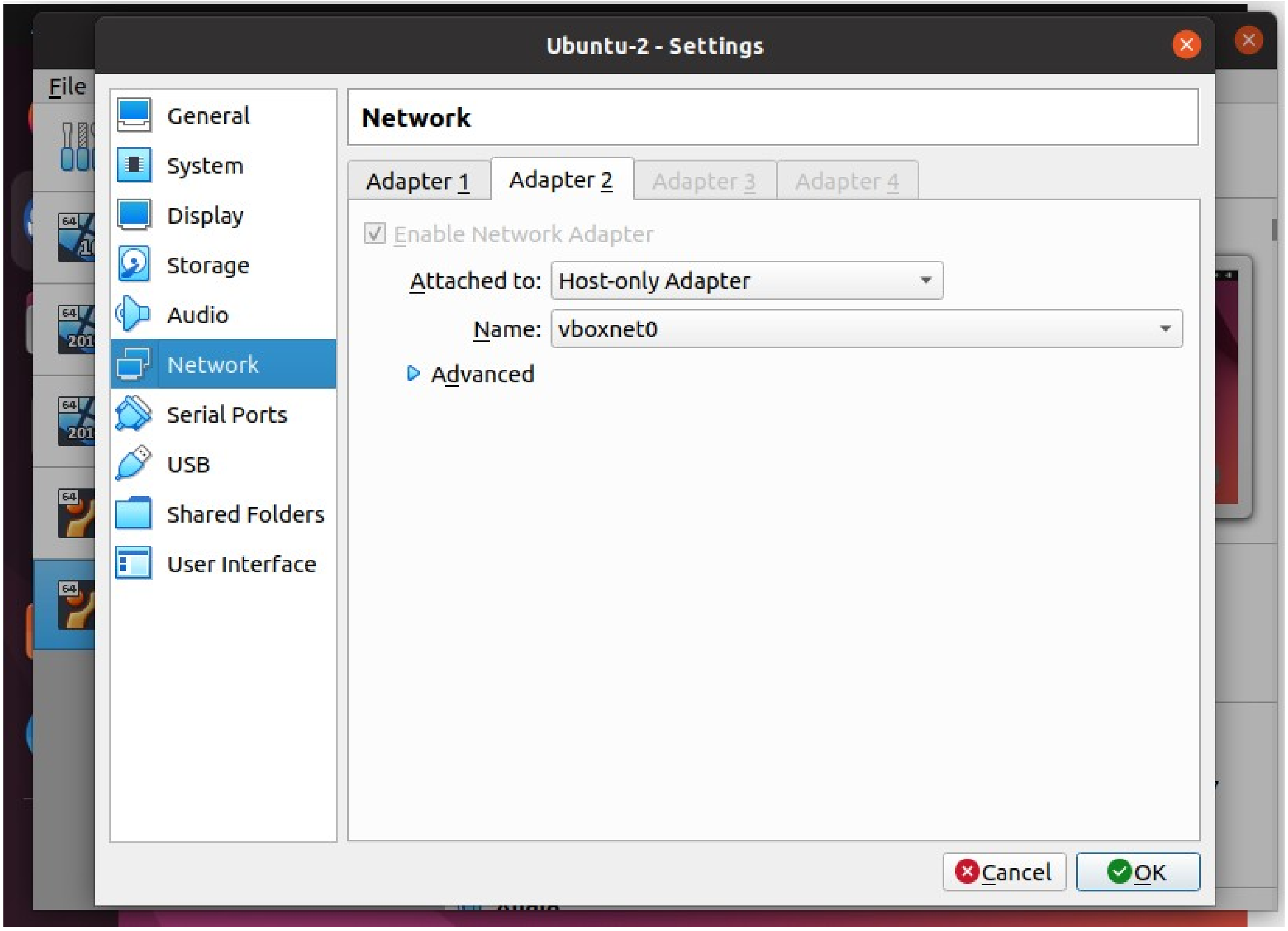


```
root@Mordor:/home/aragorn# sudo apt-get install apache
2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1
  libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine
  | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils
  libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 4 not u
pgraded.
Need to get 1,917 kB of archives.
After this operation, 7,706 kB of additional disk spac
```

Since copy/paste does not work, I can’t drop the four files into the VM (and web folder)

To get around this I just want to ssh into the VM and drop the damned files, but for that we need to do that following;

Add a second ‘host-only’ adapter by right click on VM -> Setting -> Network -> Adapter 2 -> host-only adapter – this gives us access to VM’s network



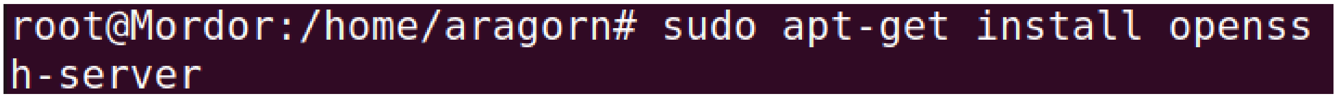
☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vboxnet0

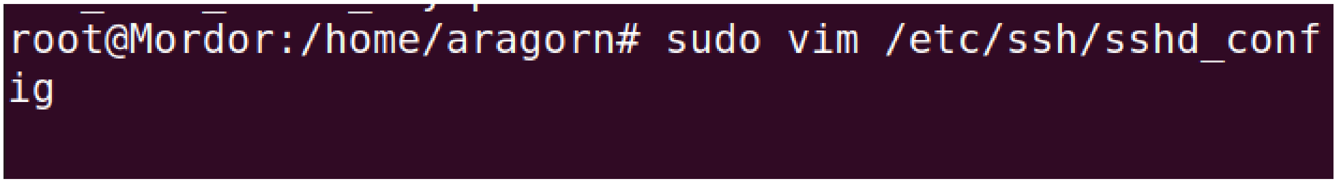
But we need to ssh into it, so need to enable ssh login in the VM

Install openssh-server



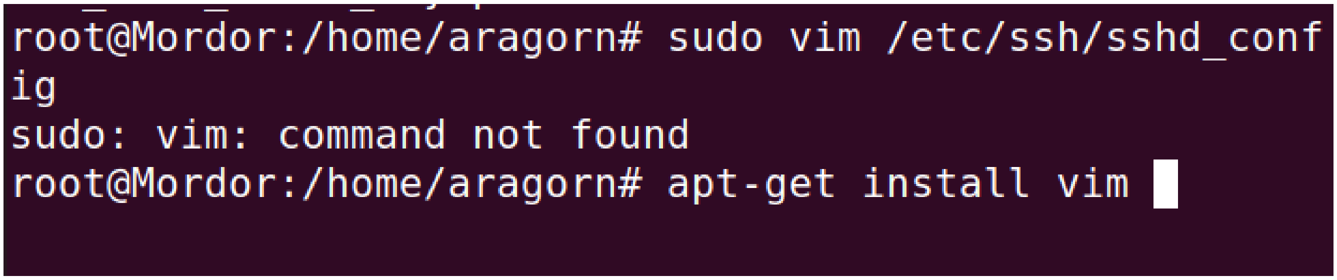
```
root@Mordor:/home/aragorn# sudo apt-get install openss
h-server
```

We need to tell openssh-server – hey, allow access to this vm from outside. So we need to edit a configuration file. This is a good practice of your nano or vim skills!



```
root@Mordor:/home/aragorn# sudo vim /etc/ssh/sshd_conf
ig
```

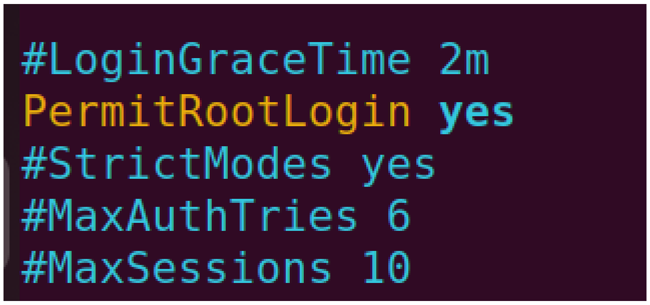
Since I love VIM but it’s not installed by default – I install it



```
root@Mordor:/home/aragorn# sudo vim /etc/ssh/sshd_conf
ig
sudo: vim: command not found
root@Mordor:/home/aragorn# apt-get install vim
```

...

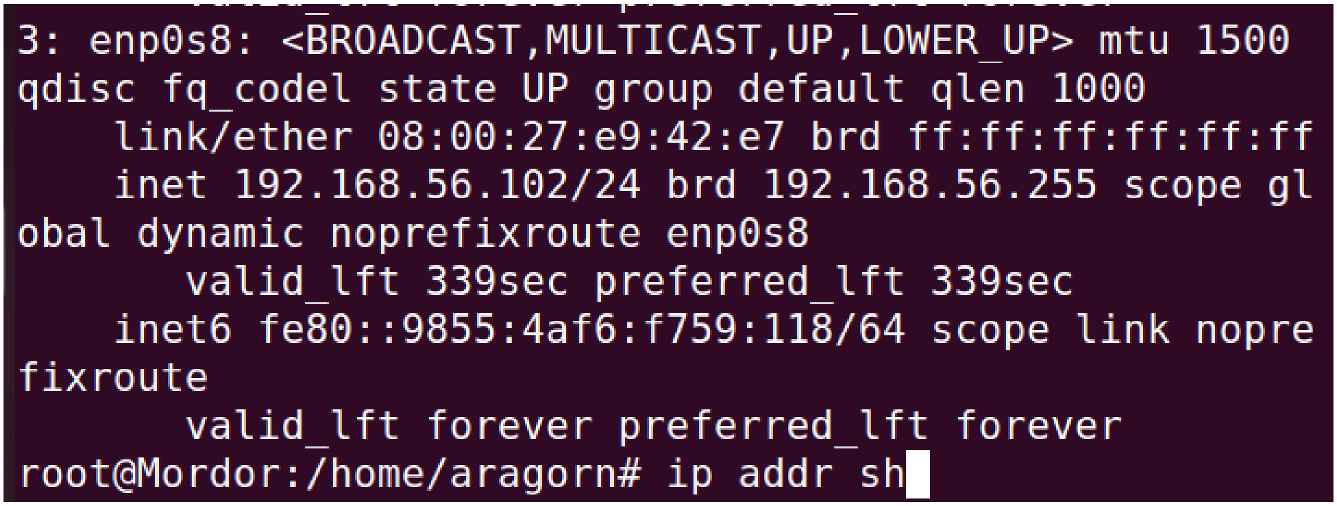
Change #PermitRootLogin prohibit password to **PermitRootLogin** yes and save the sshd_config file



```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

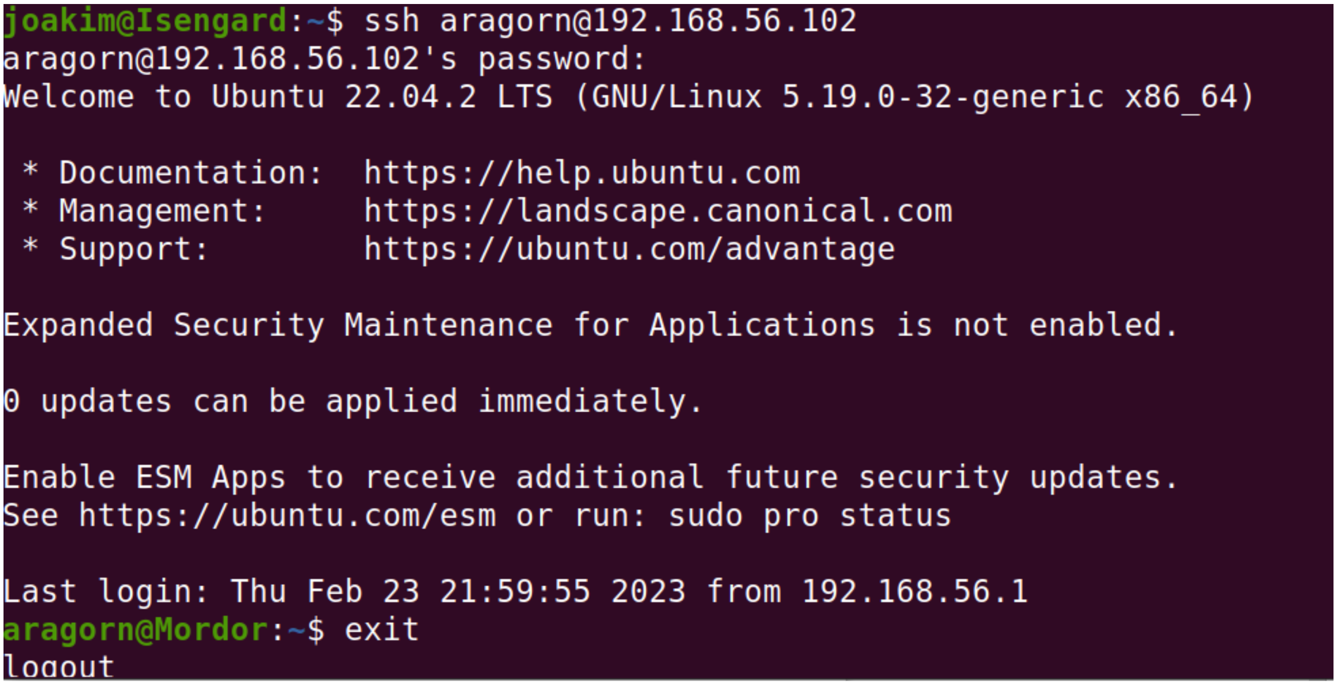
We then check the IP address of the VM..it is our way into the VM via ssh

command is – ip addr sh and we see the IP is 192.168.56.102



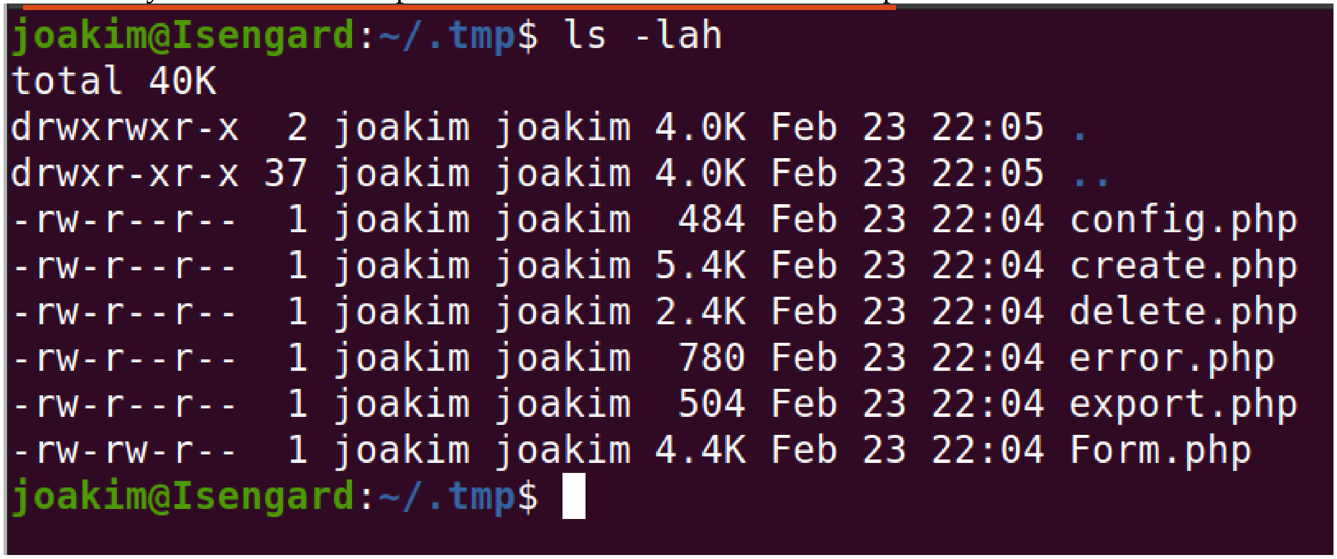
```
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:42:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope gl
obal dynamic noprefixroute enp0s8
       valid_lft 339sec preferred_lft 339sec
    inet6 fe80::9855:4af6:f759:118/64 scope link nopre
fixroute
       valid_lft forever preferred_lft forever
root@Mordor:/home/aragorn# ip addr sh
```

Now we can log into the VM..and can also drop the files



```
joakim@Isengard:~$ ssh aragorn@192.168.56.102
aragorn@192.168.56.102's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Feb 23 21:59:55 2023 from 192.168.56.1
aragorn@Mordor:~$ exit
logout
```

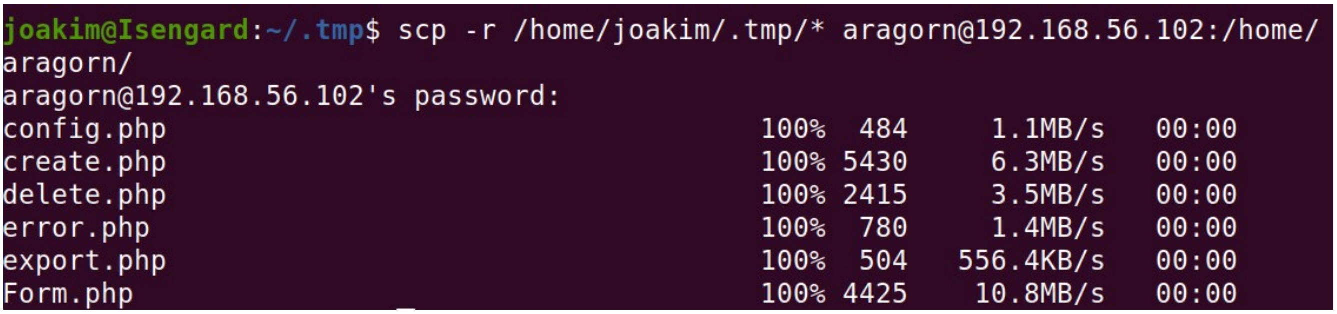
Here are my files I need to drop into the web server's folder on a .tmp folder I created



```
joakim@Isengard:~/.tmp$ ls -lah
total 40K
drwxrwxr-x  2 joakim joakim 4.0K Feb 23 22:05 .
drwxr-xr-x 37 joakim joakim 4.0K Feb 23 22:05 ..
-rw-r--r--  1 joakim joakim  484 Feb 23 22:04 config.php
-rw-r--r--  1 joakim joakim 5.4K Feb 23 22:04 create.php
-rw-r--r--  1 joakim joakim 2.4K Feb 23 22:04 delete.php
-rw-r--r--  1 joakim joakim  780 Feb 23 22:04 error.php
-rw-r--r--  1 joakim joakim  504 Feb 23 22:04 export.php
-rw-rw-r--  1 joakim joakim 4.4K Feb 23 22:04 Form.php
joakim@Isengard:~/.tmp$ 
```

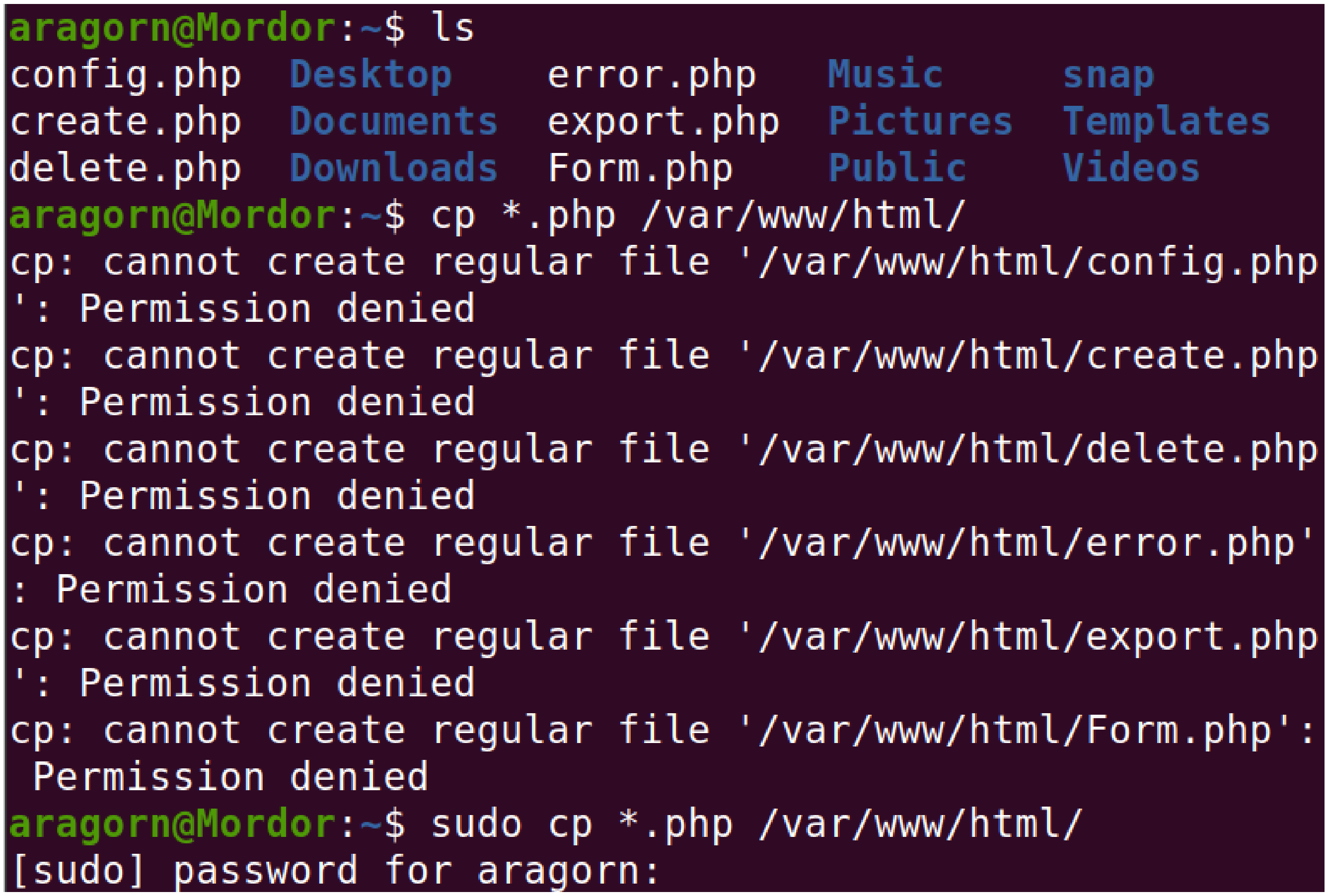
We user scp (secure copy) to transfer the files first 1) into the VM's home folder (or Aragorn's) and then 2) log into the VM via ssh and move the files to web serve as root/super user

1)
scp -r /home/joakim/.tmp/* aragorn@192.168.56.102:/home/aragorn/



```
joakim@Isengard:~/.tmp$ scp -r /home/joakim/.tmp/* aragorn@192.168.56.102:/home/
aragorn/
aragorn@192.168.56.102's password:
config.php                                    100%  484     1.1MB/s   00:00
create.php                                    100% 5430     6.3MB/s   00:00
delete.php                                    100% 2415     3.5MB/s   00:00
error.php                                     100%  780     1.4MB/s   00:00
export.php                                    100%  504   556.4KB/s   00:00
Form.php                                      100% 4425    10.8MB/s   00:00
```

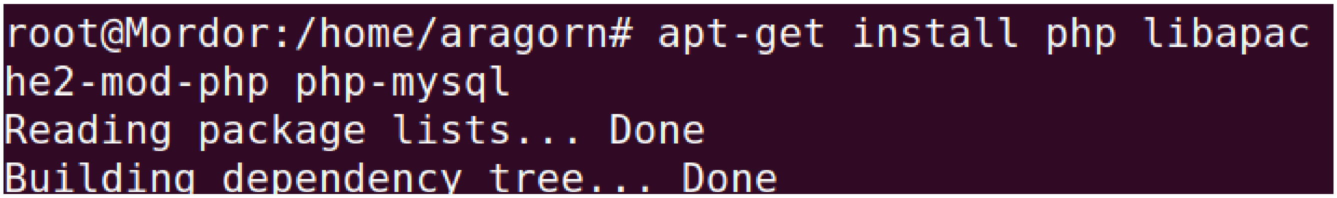
2)



```
aragorn@Mordor:~$ ls
config.php  Desktop    error.php   Music     snap
create.php  Documents  export.php  Pictures  Templates
delete.php  Downloads  Form.php    Public    Videos
aragorn@Mordor:~$ cp *.php /var/www/html/
cp: cannot create regular file '/var/www/html/config.php
': Permission denied
cp: cannot create regular file '/var/www/html/create.php
': Permission denied
cp: cannot create regular file '/var/www/html/delete.php
': Permission denied
cp: cannot create regular file '/var/www/html/error.php'
: Permission denied
cp: cannot create regular file '/var/www/html/export.php
': Permission denied
cp: cannot create regular file '/var/www/html/Form.php':
 Permission denied
aragorn@Mordor:~$ sudo cp *.php /var/www/html/
[sudo] password for aragorn:
```

Now we need to install PHP so our php files actually do something like create forms, add entries to database, etc

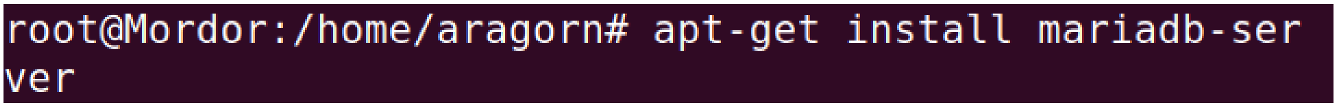
Commands to install all the tools: apt-get install php libapache2-mod-php php-mysql



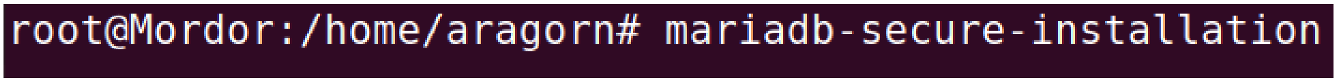
```
root@Mordor:/home/aragorn# apt-get install php libapac
he2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
```

Our Website is now almost ready..but without the database the page won’t load up

Step 3: Install and configure MariaDB



```
root@Mordor:/home/aragorn# apt-get install mariadb-ser
ver
```

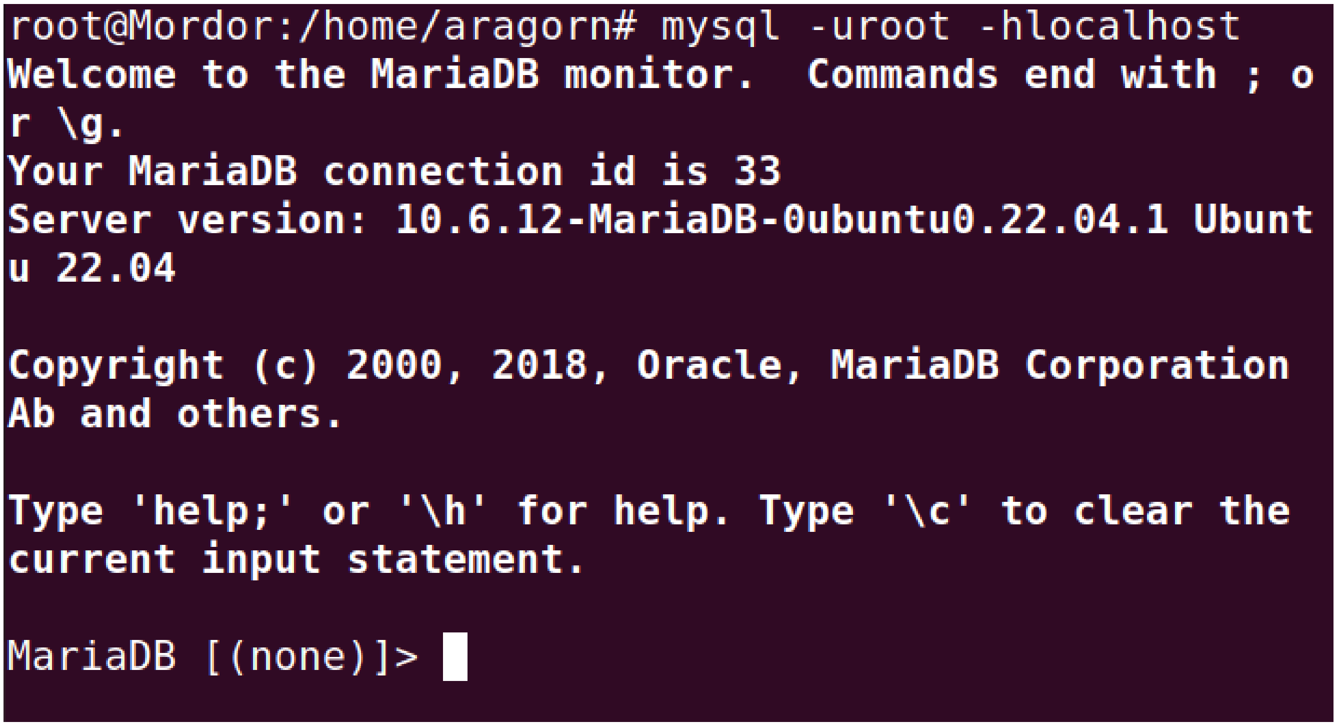


```
root@Mordor:/home/aragorn# mariadb-secure-installation
```

For questions asked, I answered ‘n/no’ for all of them except last one (flust privilege? - yes)

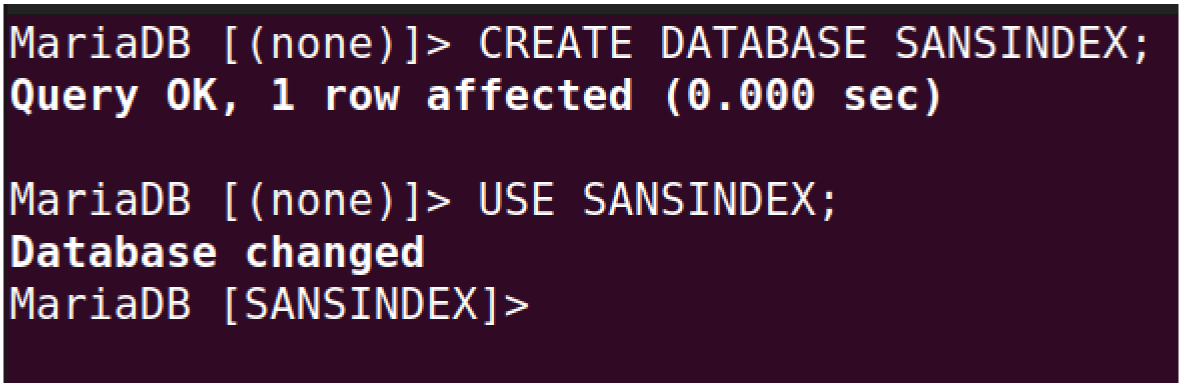
Almost done.

Log into mysql



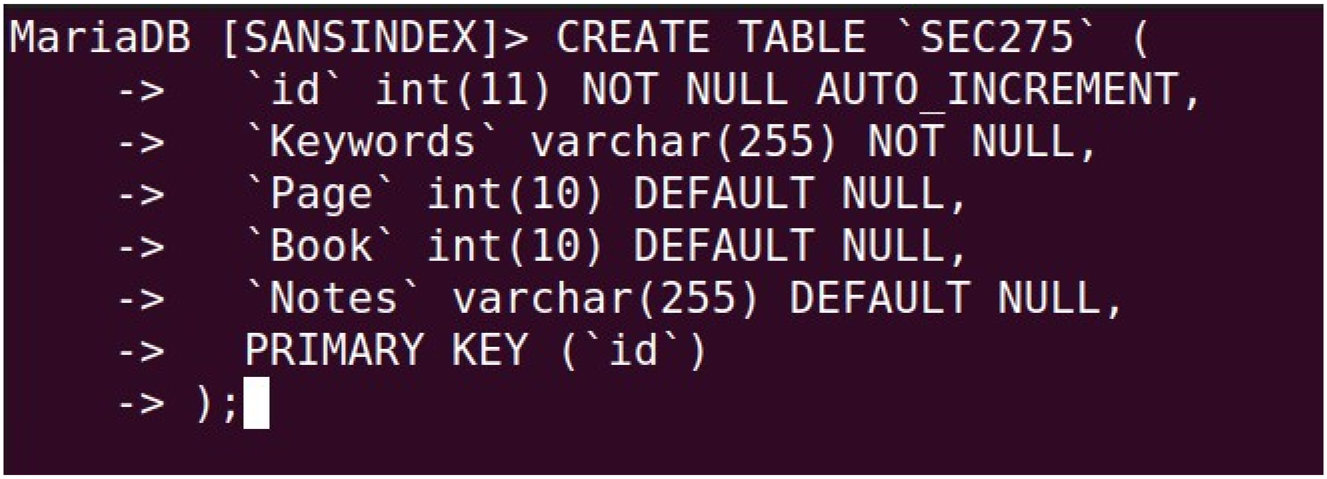
```
root@Mordor:/home/aragorn# mysql -uroot -hlocalhost
Welcome to the MariaDB monitor.  Commands end with ; o
r \g.
Your MariaDB connection id is 33
Server version: 10.6.12-MariaDB-0ubuntu0.22.04.1 Ubunt
u 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation
Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the
current input statement.

MariaDB [(none)]>
```

Create database for SANS course



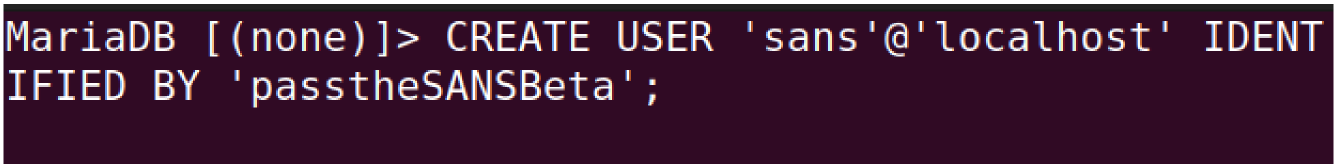
```
MariaDB [(none)]> CREATE DATABASE SANSINDEX;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> USE SANSINDEX;
Database changed
MariaDB [SANSINDEX]>
```

Create table for SEC275

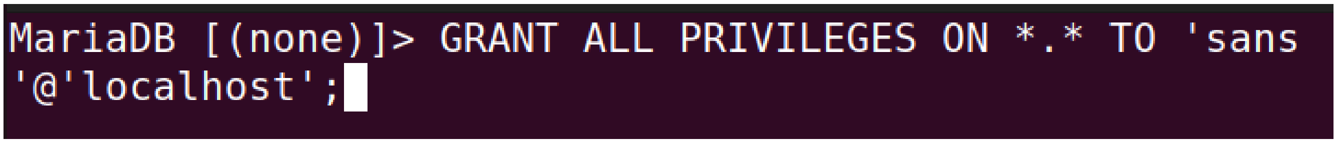


```
MariaDB [SANSINDEX]> CREATE TABLE `SEC275` (
    ->   `id` int(11) NOT NULL AUTO_INCREMENT,
    ->   `Keywords` varchar(255) NOT NULL,
    ->   `Page` int(10) DEFAULT NULL,
    ->   `Book` int(10) DEFAULT NULL,
    ->   `Notes` varchar(255) DEFAULT NULL,
    ->   PRIMARY KEY (`id`)
    -> );
```

Create a user for our index app and give it access to the database and tables



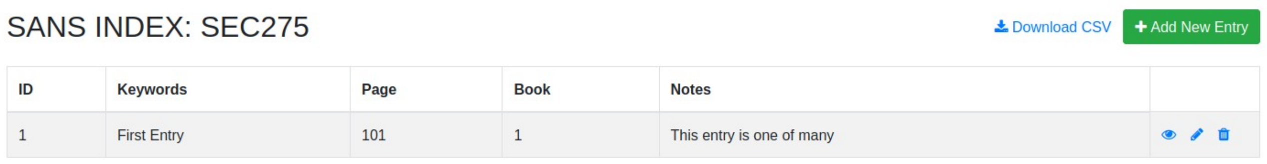
```
MariaDB [(none)]> CREATE USER 'sans'@'localhost' IDENT
IFIED BY 'passtheSANSBeta';
```



```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'sans
'@'localhost';
```

Now you can access the website by simply type in your IP

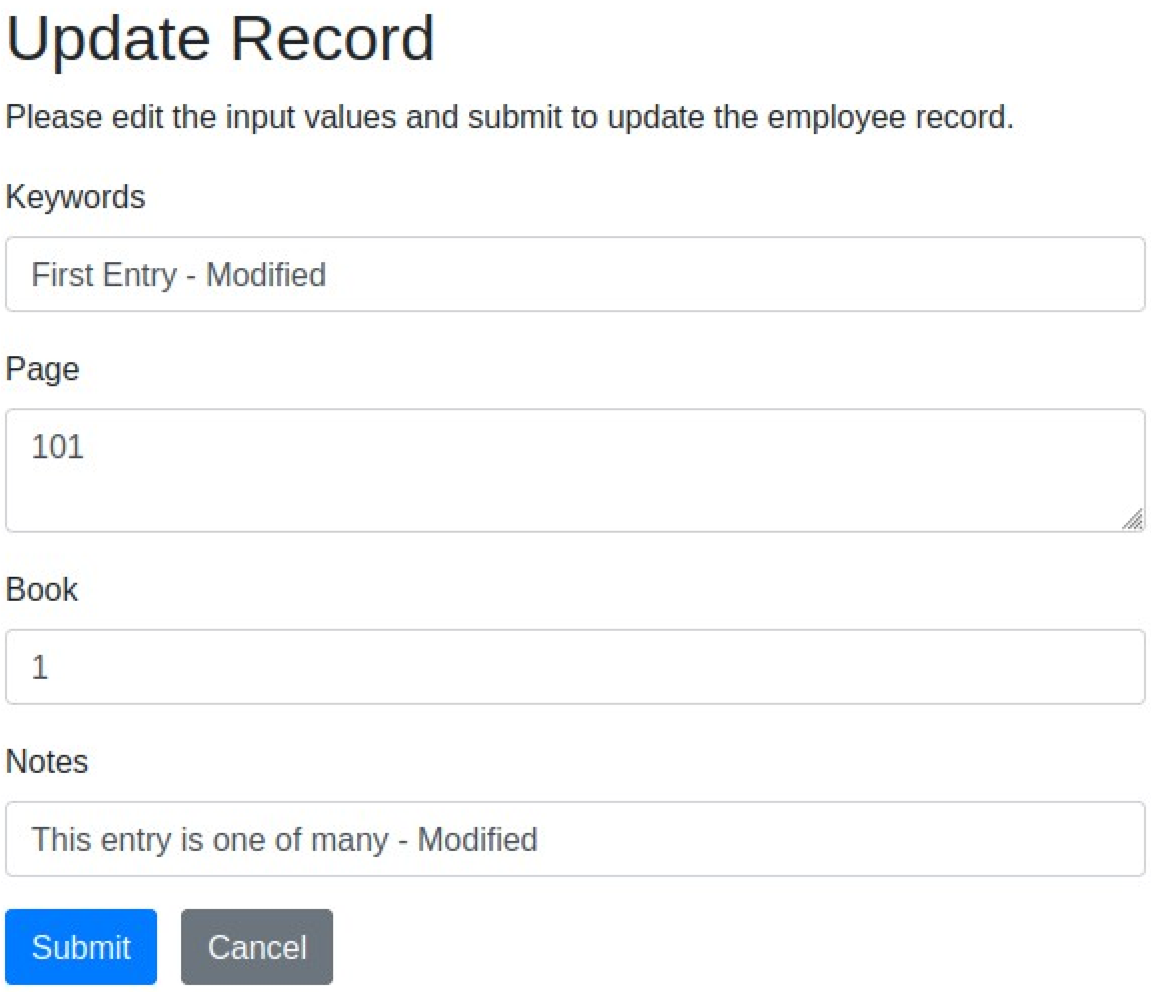
http://192.168.56.102/Form.php



SANS INDEX: SEC275

ID	Keywords	Page	Book	Notes	
1	First Entry	101	1	This entry is one of many	

Edit entry (marker icon)



Update Record

Please edit the input values and submit to update the employee record.

Keywords

First Entry - Modified

Page

101

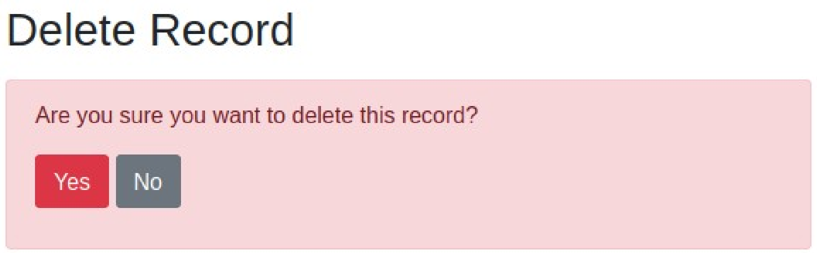
Book

1

Notes

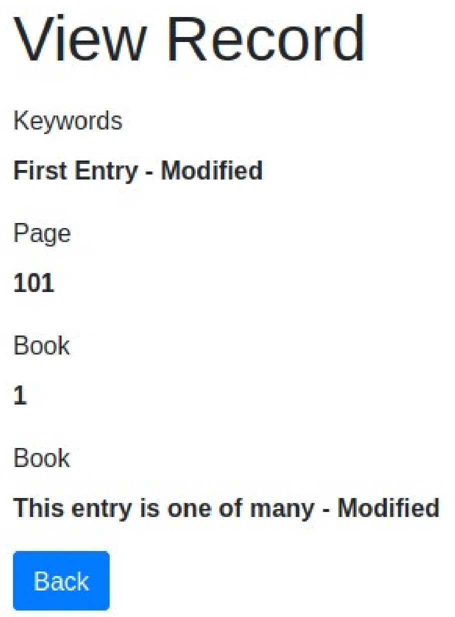
This entry is one of many - Modified

Delete Entry (bin icon)



Delete Record

Are you sure you want to delete this record?



View Record

Keywords

First Entry - Modified

Page

101

Book

1

Book

This entry is one of many - Modified

View Entry (eye icon)