



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Cloud Computing

**Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW**

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.

Task 1: Securing ownCloud from Malicious File Uploads using ClamAV

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 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.

Pre- Activity exercise

To carry out the lab, you 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

Overview of Lab

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.

Activity:

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

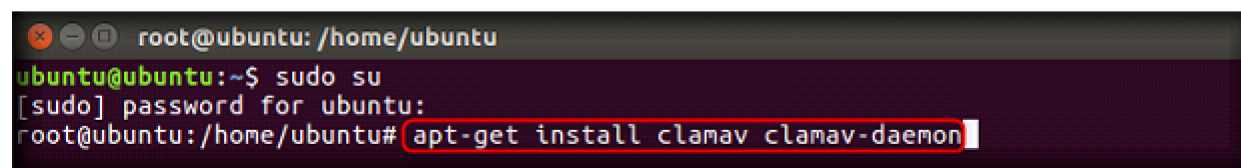
1. Launch a **terminal window**, type **sudo su** and hit **Enter**. You will be asked to enter your password, type your password (here **toor**) and hit **Enter**.

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



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

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
```

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 liblvm3.6v5
Suggested packages:
  clamav-docs daemon libclamunrar7
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav7
  liblvm3.6v5
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
```

4. After ClamAV installation is finished, type **sed -i -e "s/^NotifyClamd/#NotifyClamd/g" /etc/clamav/freshclam.conf** and hit **Enter**.

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

5. 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
root@ubuntu:/home/ubuntu# netstat -a|grep clam
unix 2      [ ACC ]     STREAM     LISTENING   18417      /var/run/clamav/clamd
.ctl
root@ubuntu:/home/ubuntu#
```

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

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

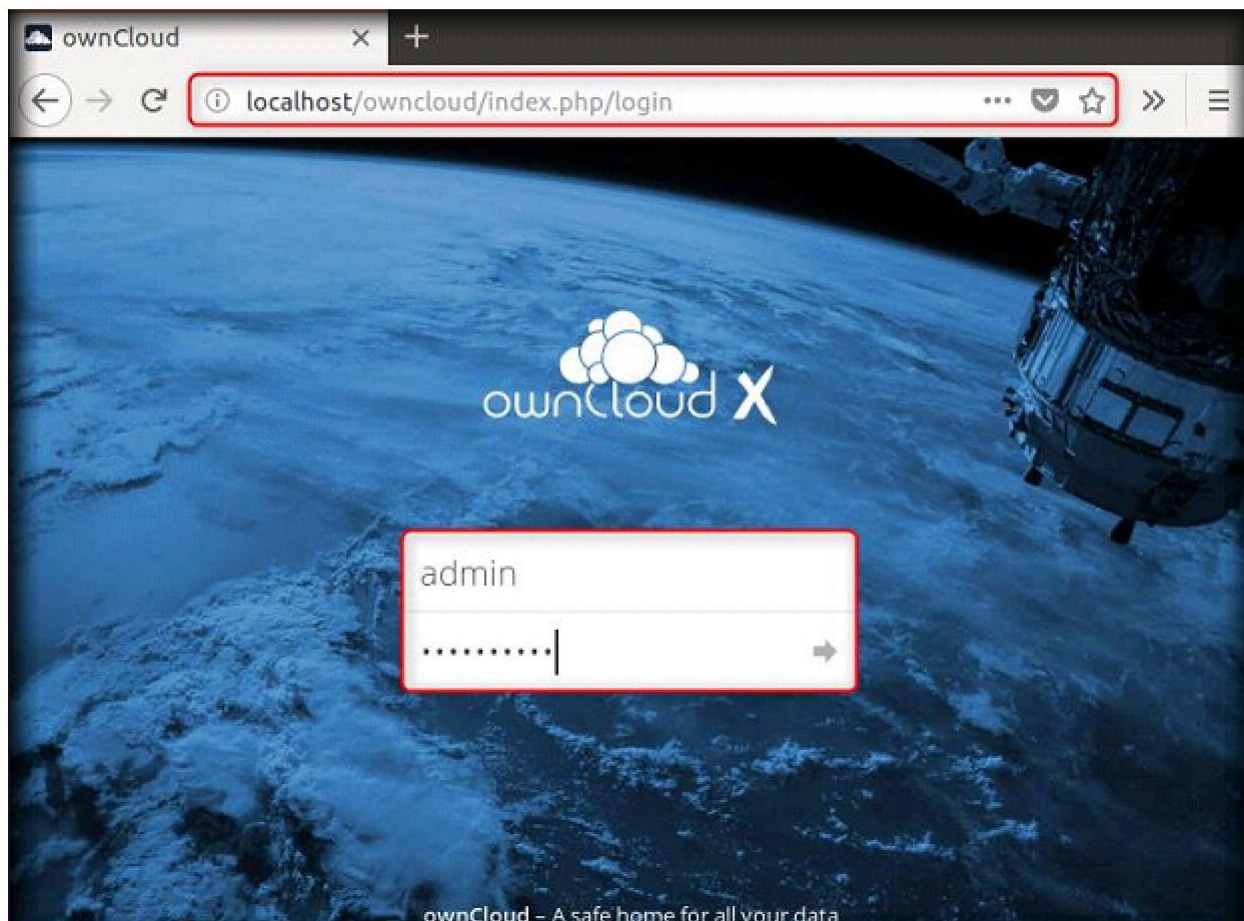
7. To enable clamav service, type **systemctl enable clamav-daemon.service** and hit **Enter**.

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

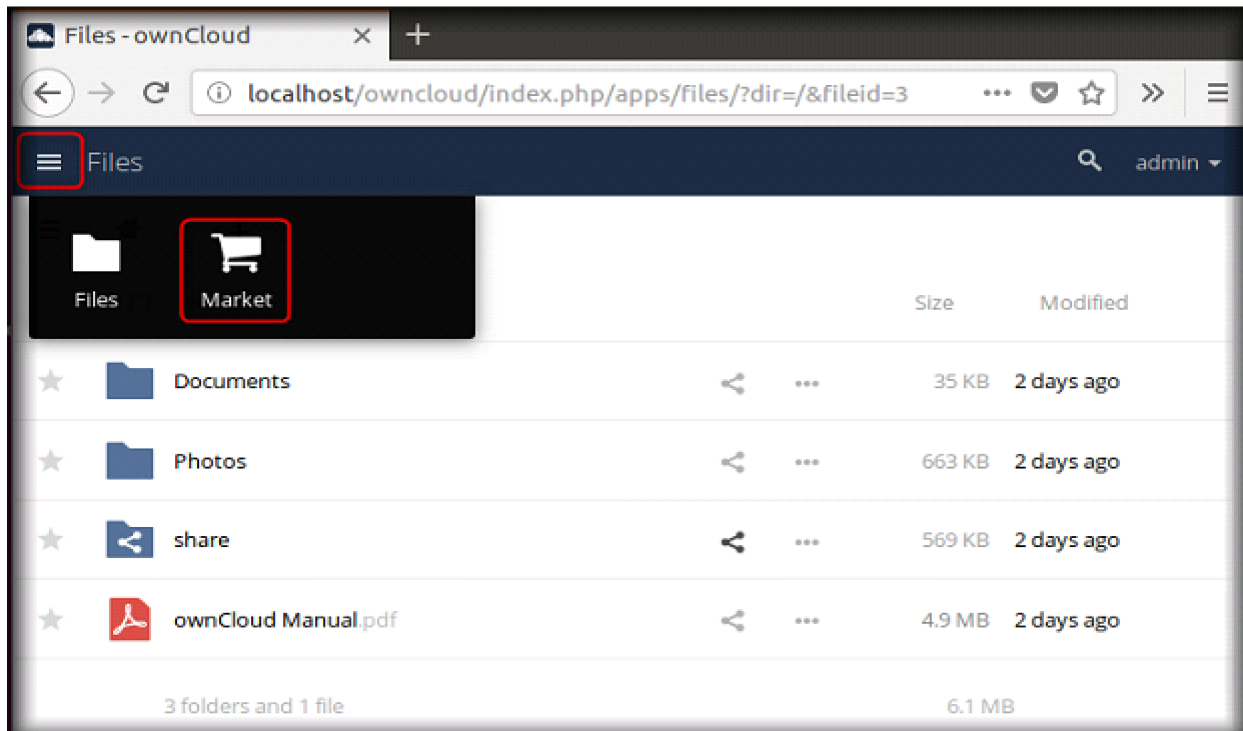
8. To start clamav service, type **systemctl start clamav-daemon.service** and hit **Enter**.

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

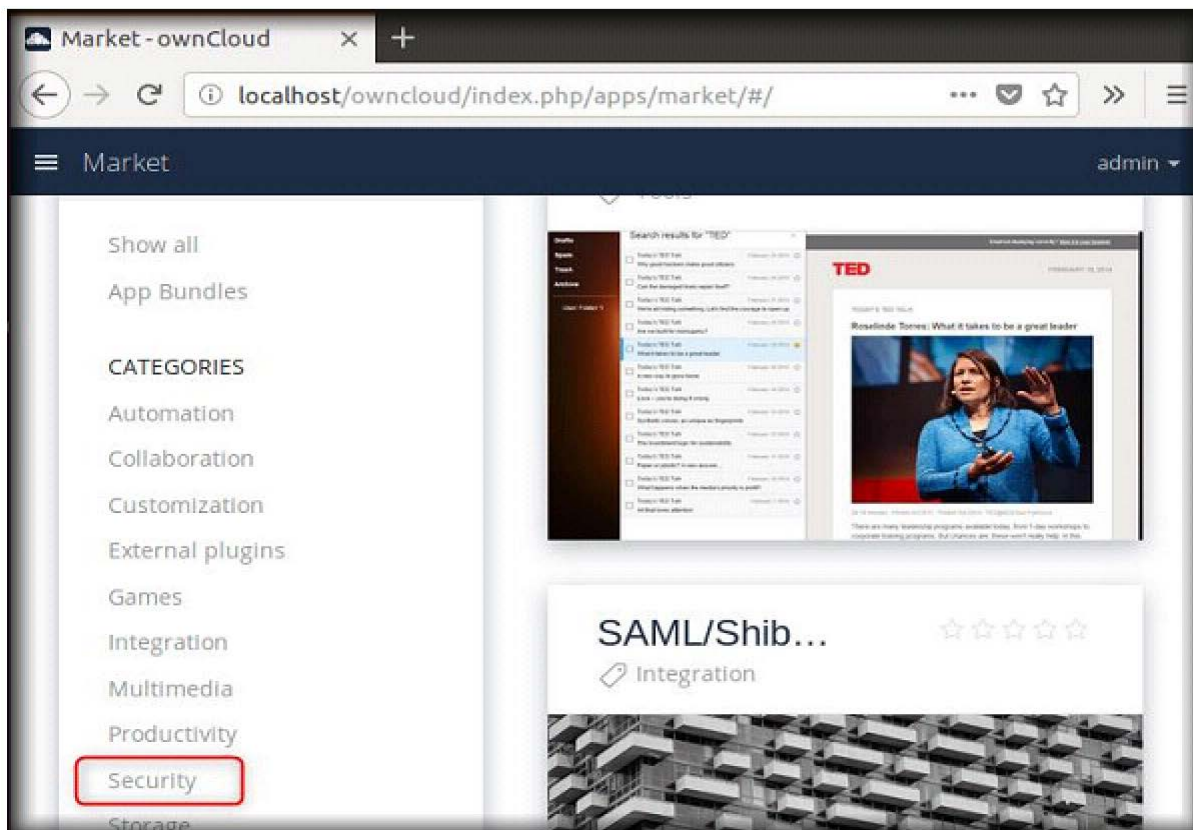
9. Now open a **browser** (here **Firefox**) and type **http://localhost/owncloud/** as the URL and hit **Enter**. ownCloud login page appears, log-in as the admin by providing the user credentials (here **admin/qwerty@123**) and hit **Enter**.



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



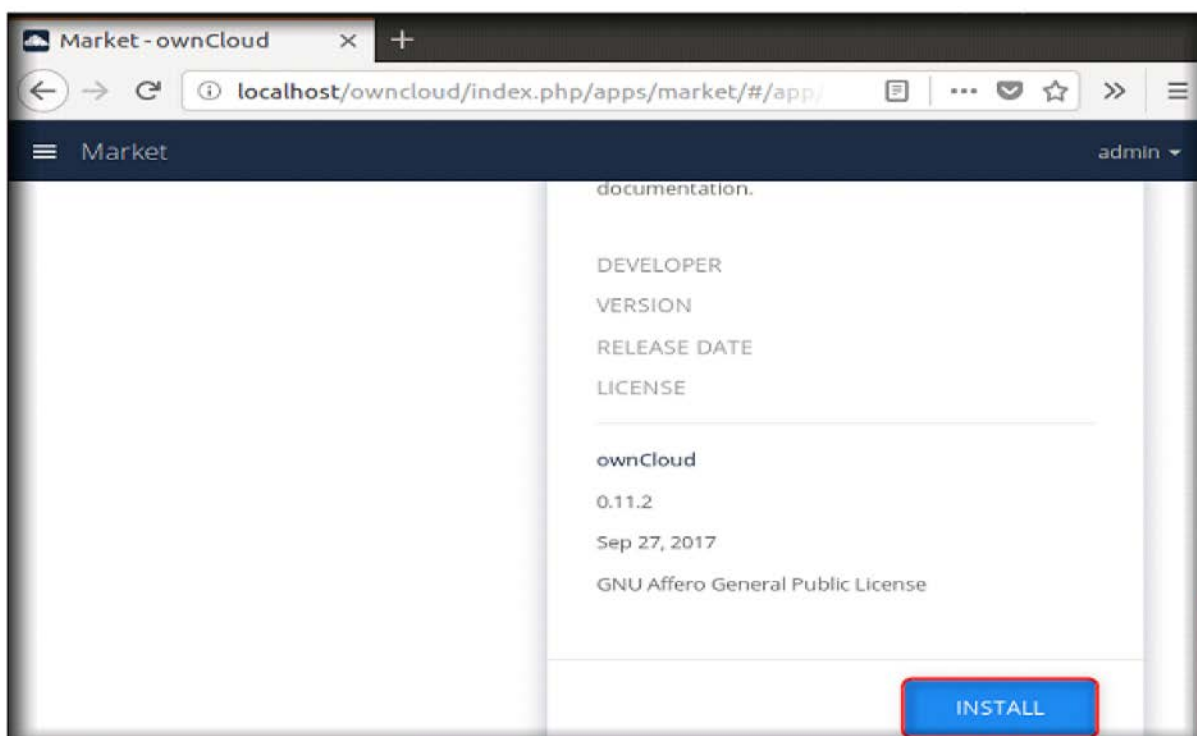
11. Market page loads, click **Security** under **CATEGORIES** in the left pane.



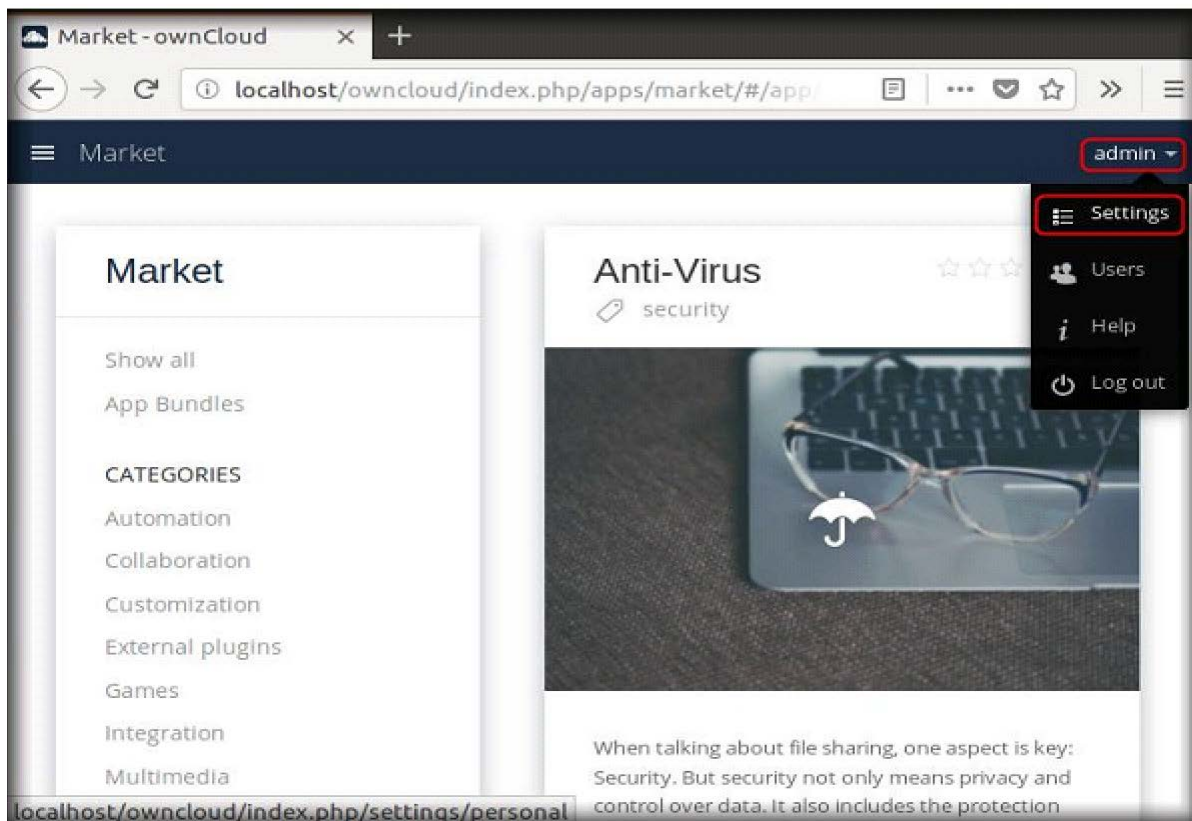
12. You will see the security apps in the market, click **Anti-Virus** as shown in the screenshot.



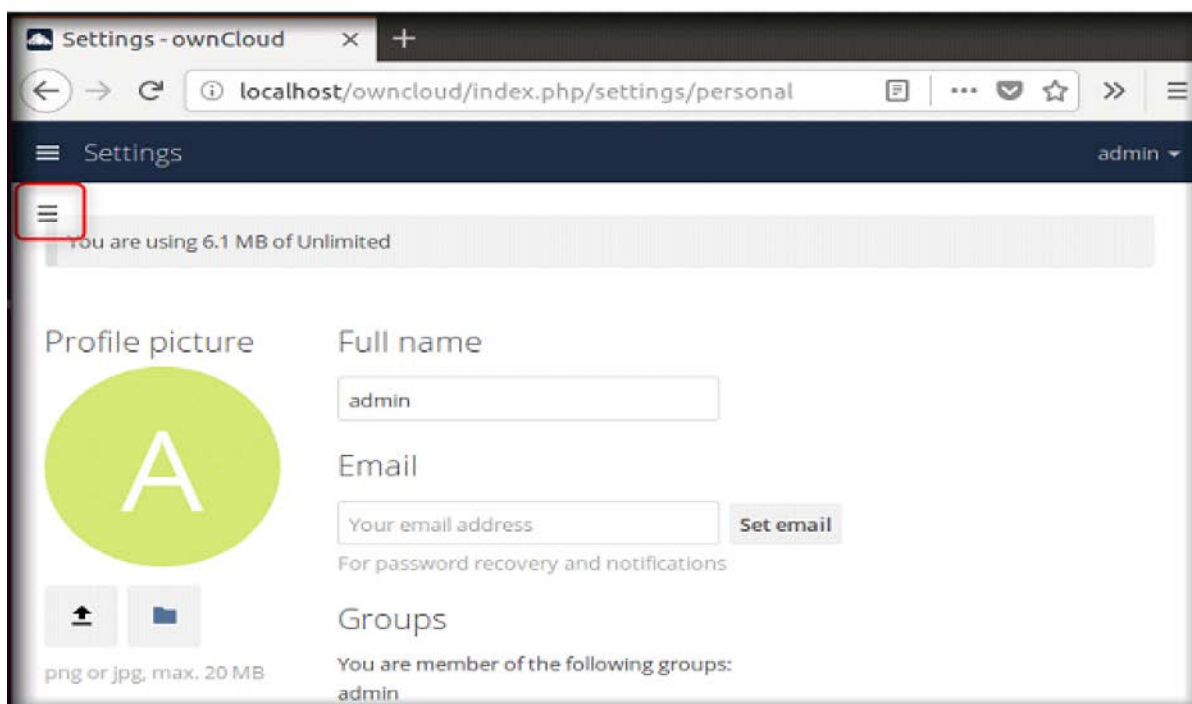
13. Read the details of the anti-virus and click the **INSTALL** button at the bottom.



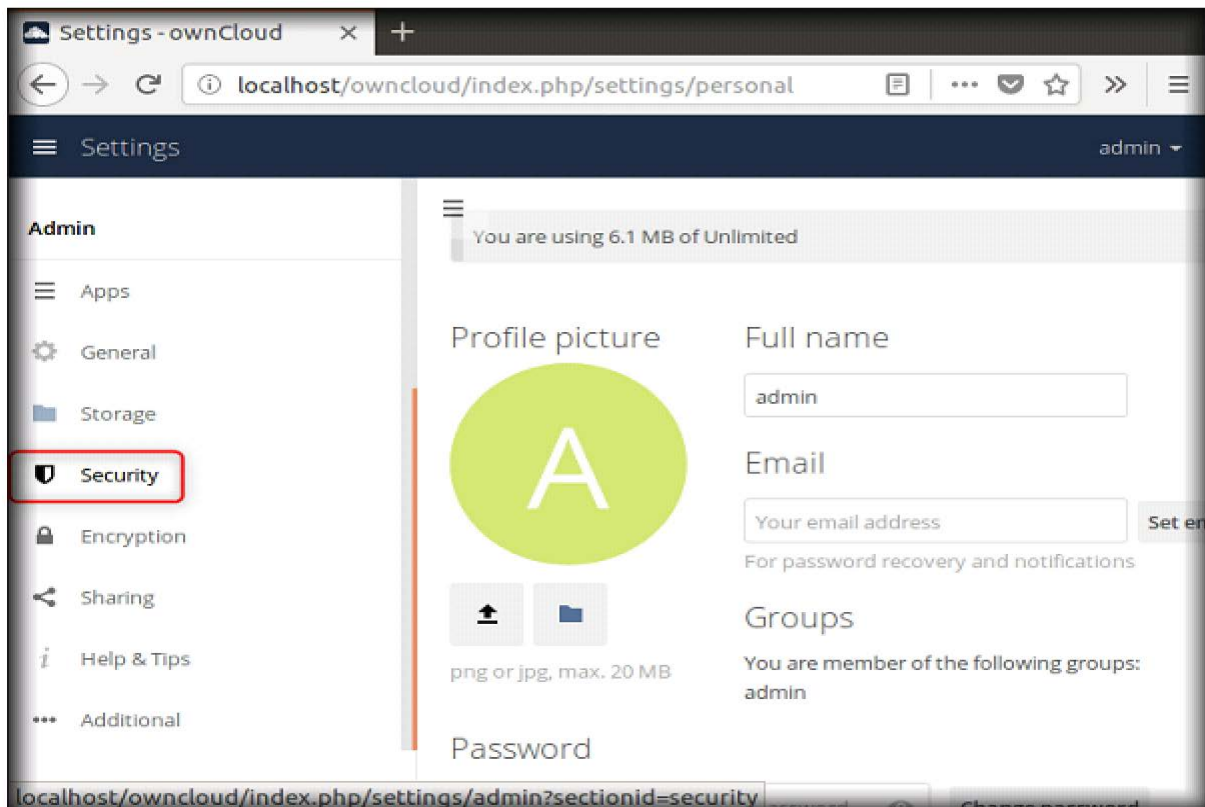
14. After the anti-virus is finished installing, scroll to the top and from the menu bar, select **admin** → **Settings**.



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

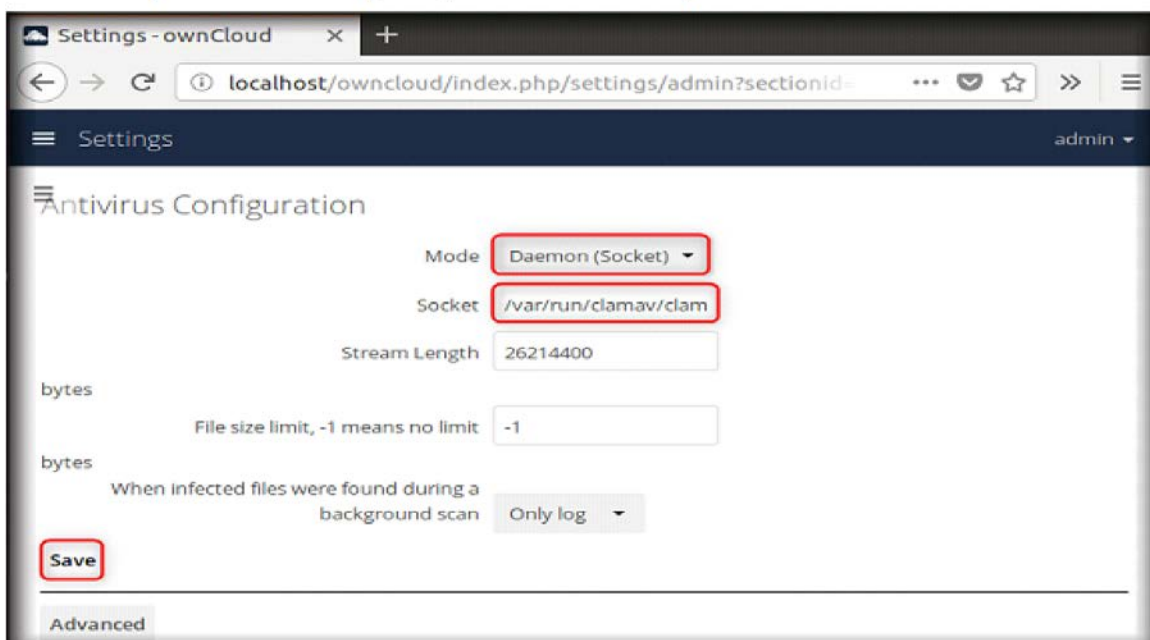


16. Left-pane appears with the setting options, under the **Admin** section select **Security** as shown in the screenshot.

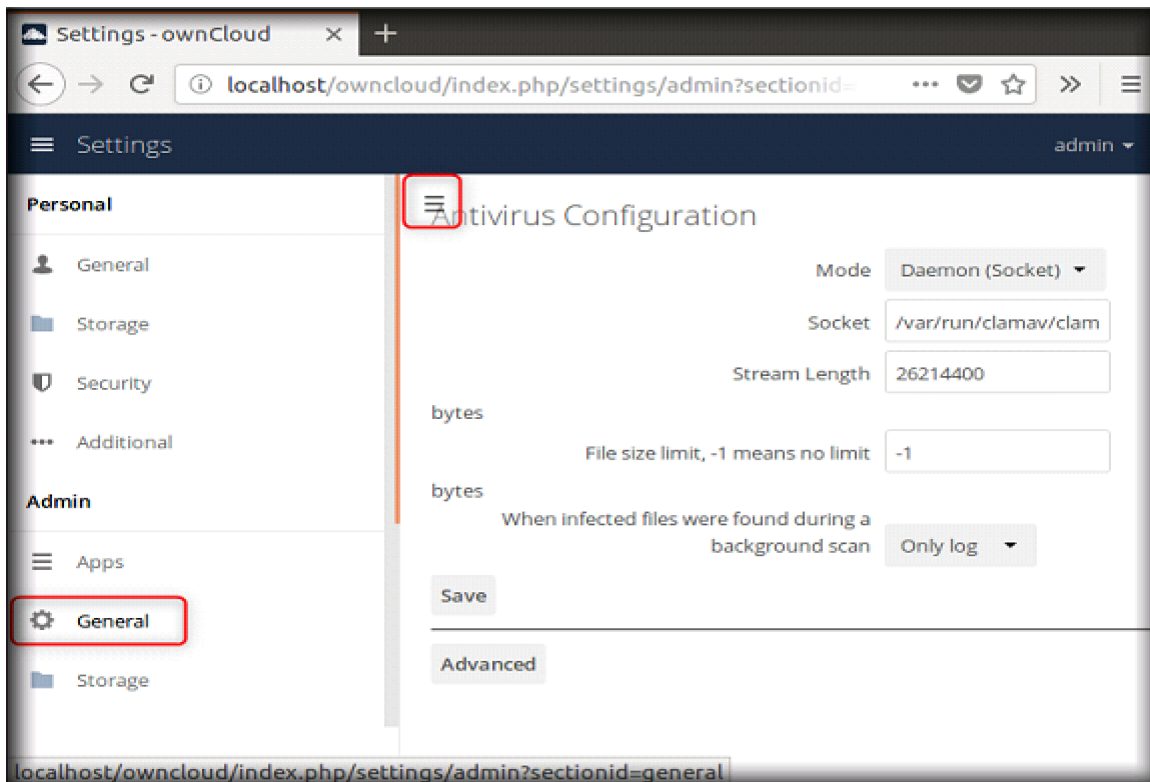


17. **Antivirus Configuration** section appears, select **Daemon(Socket)** in the **Mode** field and type the socket path for clamAV in the **Socket** field. Leave the other settings to default and click **Save**.

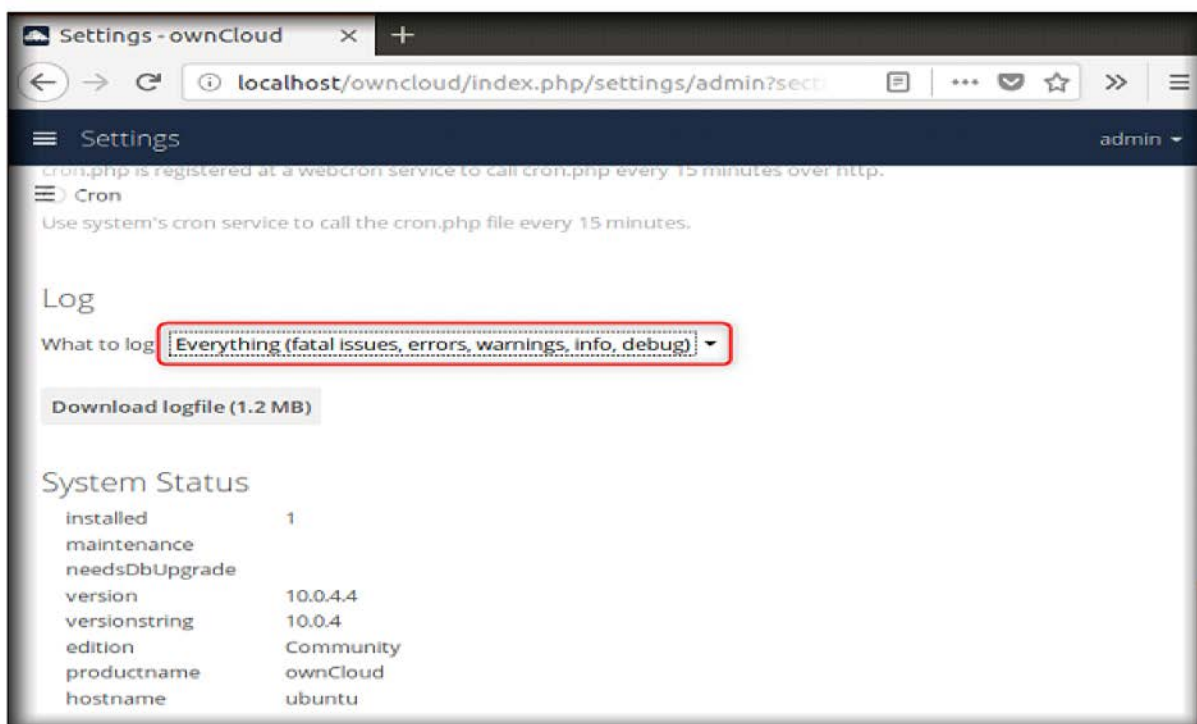
Note: Input the socket path you noted in **step 5**.



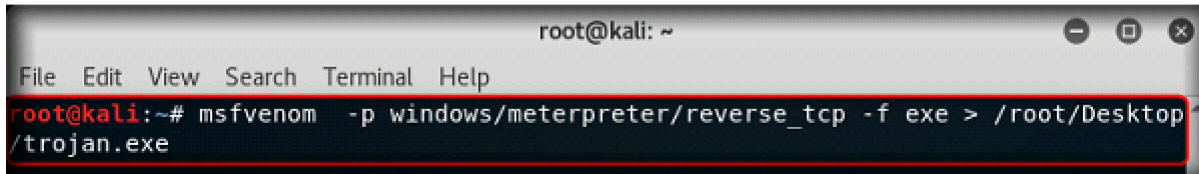
18. Now open up the setting options once more by clicking on the **menu** icon and select **General** in the **Admin** section as shown in the screenshot.



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.

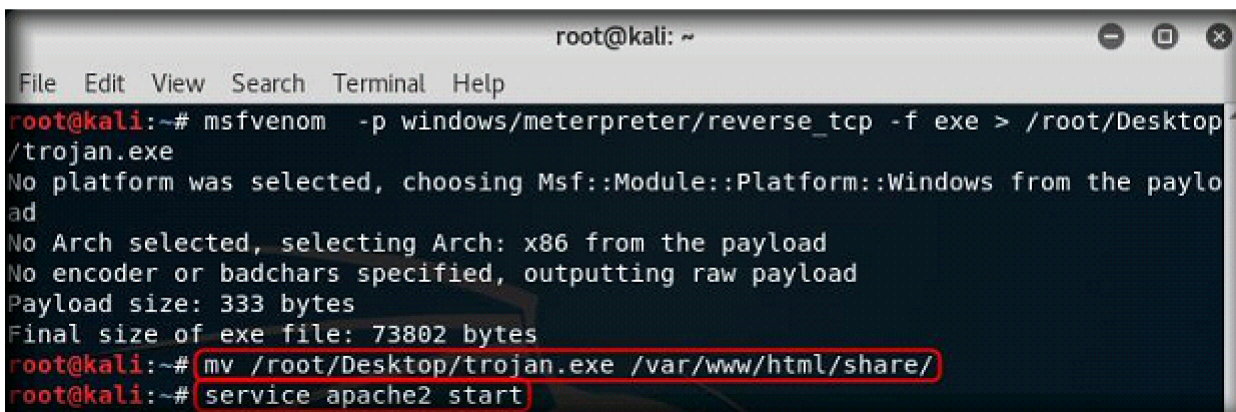


20. Now we shall test out configured anti-virus by uploading a Trojan file.
Switch to **Kali Linux** machine and log-in.
21. Open a terminal window and type **msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe** and hit **Enter** to generate a Trojan file.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe
```

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**.



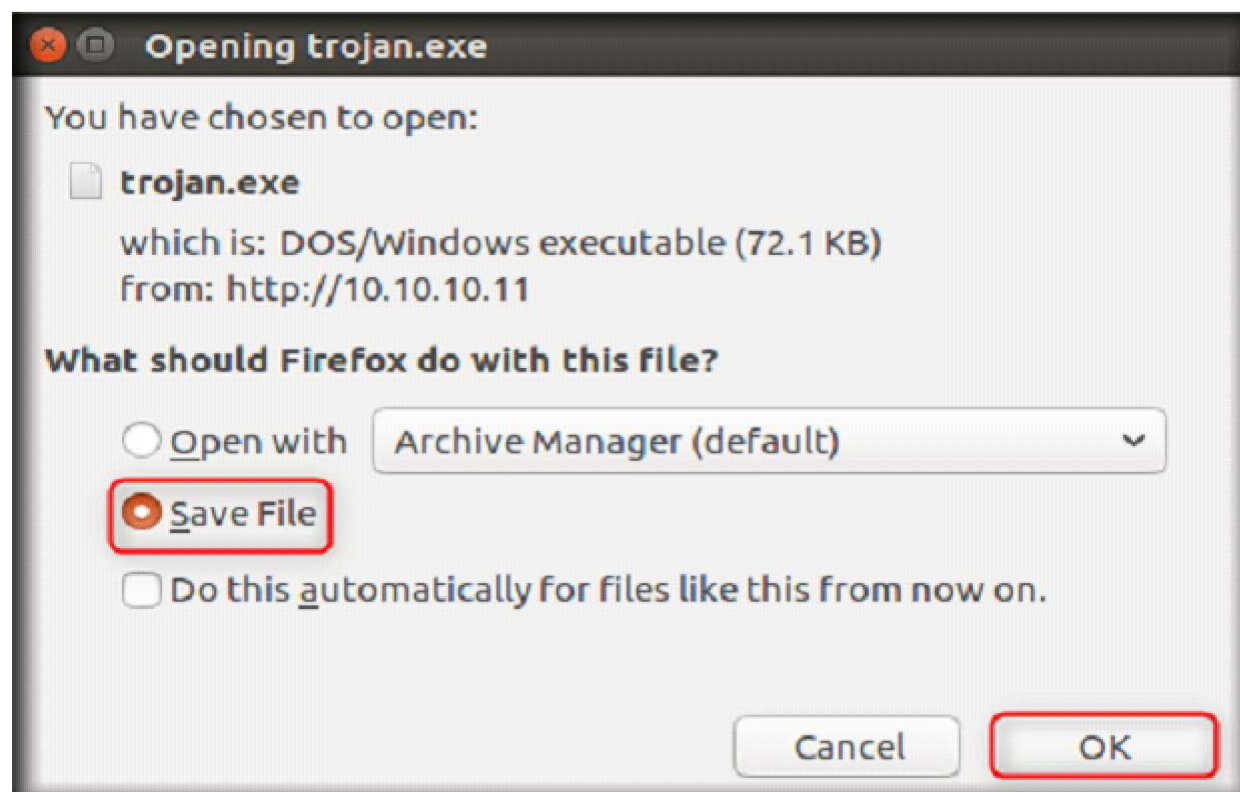
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe  
No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
No Arch selected, selecting Arch: x86 from the payload  
No encoder 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
```

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.

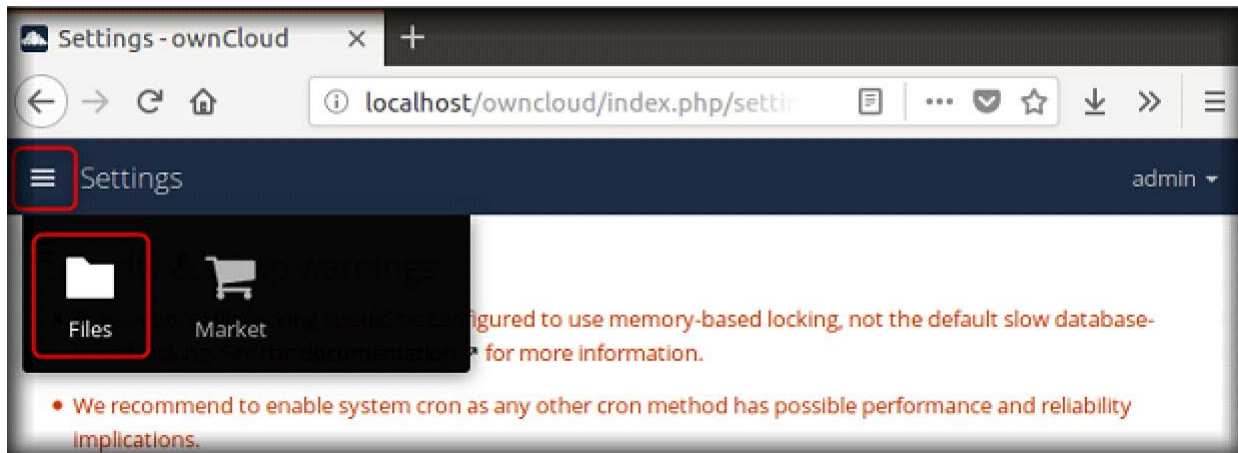
Note: 10.10.10.11 is the IP address of the kali linux machine, this may vary in your lab environment.



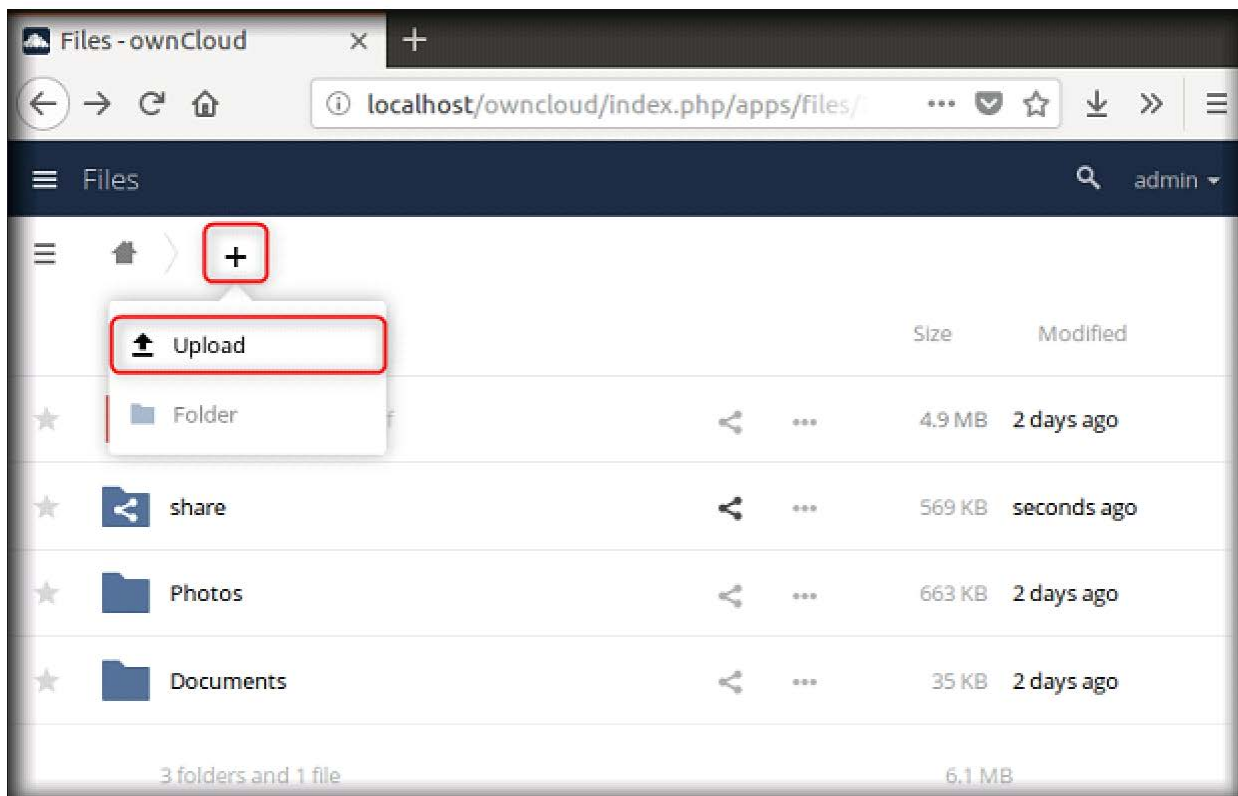
25. **Opening trojan.exe** pop-up window appears, select the **Save File** radio button and click **OK** to download the sample Trojan. **Close** the **Index of /share** tab after the Trojan is finished downloading and go back to the **Settings-ownCloud** tab.



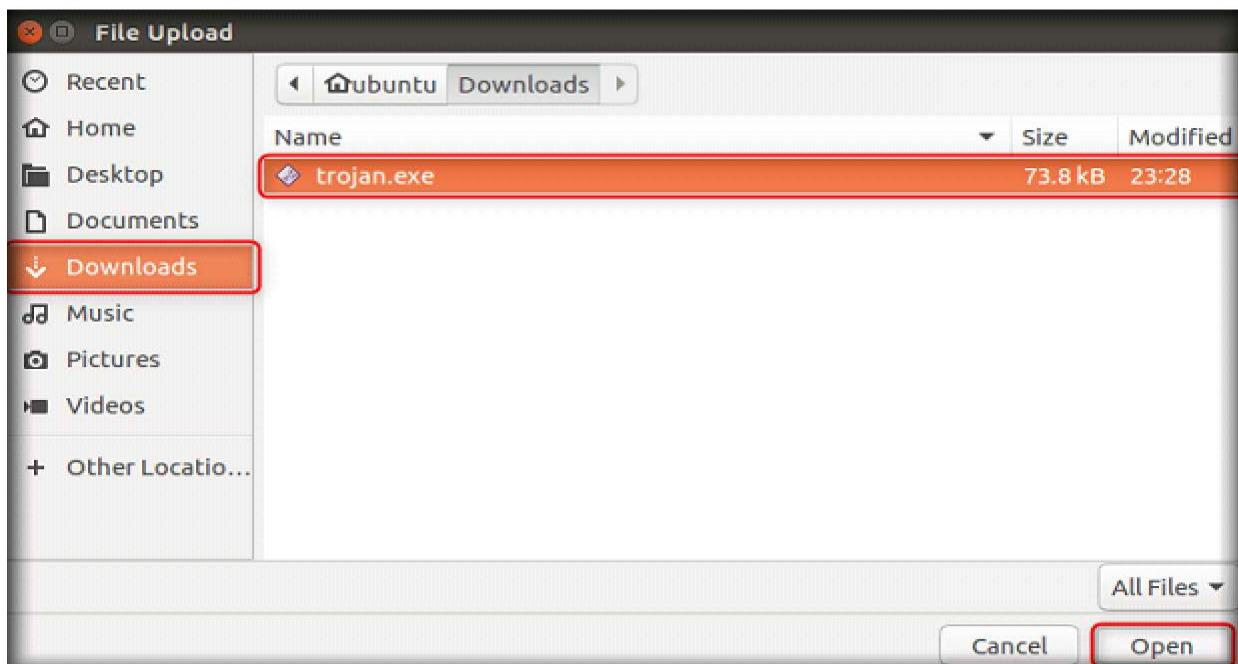
26. Now click the **menu** icon beside **Settings** heading and click **Files**.



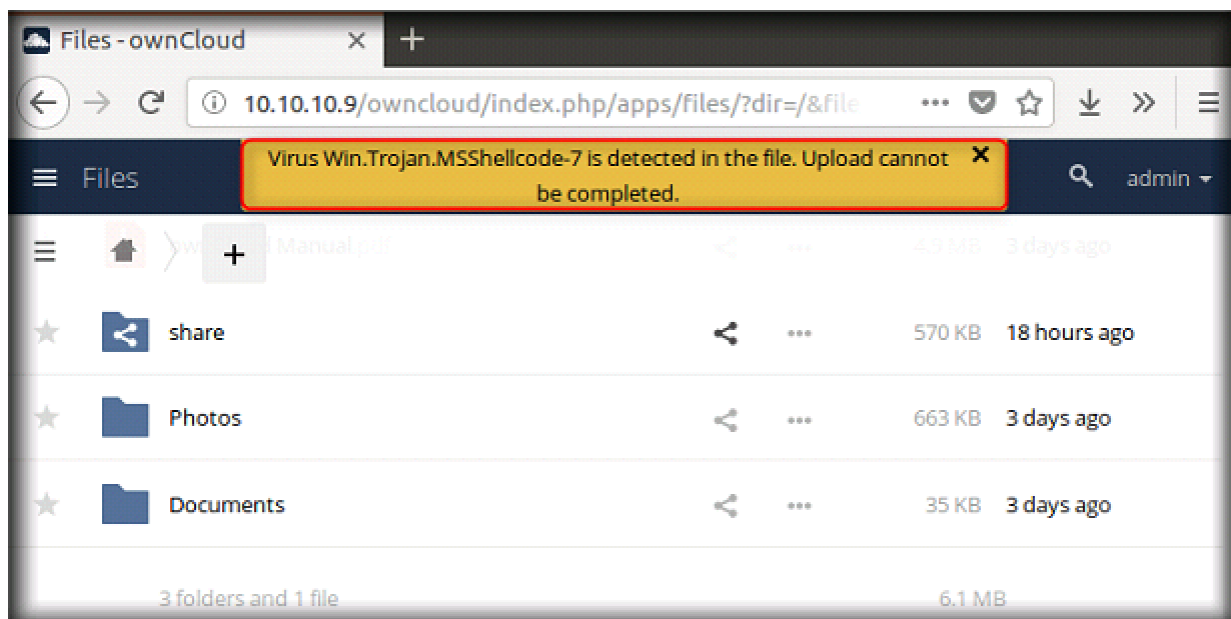
27. Now click the **Add** icon and select **Upload** as shown in the screenshot.



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



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



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.

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.